Towards the Adoption of EU General Data Protection Regulation

An Empirical Study of Businesses' Perception on Privacy and Data Protection

A. R. Faradina

Technische Universiteit Delft

TU Delft Delft University of Technology

Deloitte.

lpdp lembaga pengelola dana pendidikan

TOWARDS THE ADOPTION OF EU GENERAL DATA PROTECTION REGULATION

AN EMPIRICAL STUDY OF BUSINESSES' PERCEPTION ON PRIVACY AND DATA PROTECTION

by

A. R. Faradina

in partial fulfillment of the requirements for the degree of

Master of Science
in Engineering and Policy Analysis

at the Delft University of Technology,
to be defended publicly on Tuesday December 19, 2017 at 15:00.

Chairman:	Prof. Dr. M.J.G. van Eeten,	TU Delft
Thesis committee:	Dr. Hadi Asghari,	TU Delft
	Dr. Ir. B. Enserink,	TU Delft
	Dr. Maarten van Wieren,	Deloitte

ACKNOWLEDGEMENT

And that there is not for man except that (good) for which he strives – Quran 53:39

For this thesis project, I challenged myself to experience a whole new journey, to explore a world that is new to me. The purpose is clear: to create more space for me to learn. EU General Data Protection Regulation (EU GDPR) is a topic that effortlessly comes to mind. It is a hot topic, so relevant to our daily life, it covers a socio-technical perspective, it is entirely new to me, and it is intriguing. Having many things to learn requires a decision on what to focus on and a resilient attitude to reach the finish line. With God's grace and abundant support from supervisor, friends and family, I have finally reached the end of my journey in this chapter of life. To those people: I cannot thank you enough.

Firstly, I would like to express my deep and sincere gratitude for my graduation committee members. I would thank my first supervisor, Dr. Ir. Hadi Asghari, for his relentless support for my ups and downs throughout this learning journey despite his full schedule. He provided me with on-point inputs for methods, analyses, insights and my works in general. To my graduation chairman, Professor Michel van Eeten for his valuable feedbacks, especially in setting the direction of this project and in packaging the deliverable of this project. To Dr. Ir. Bert Enserink, my second supervisor, for his detailed feedbacks and for convincing me to take the opportunity and challenge that was given to me through this thesis project.

Secondly, I would thank the people from Deloitte. To my external supervisor, Dr. Ir. Maarten van Wieren, for his attentive support and open attitude. His creative ideas have contributed a lot to the interview and survey designs and execution. To Liselotte Mulder, for giving me a chance in the first place. To Vivian Jacob, for her weekly if not daily motivations. To Marrit Plat, for her salient help in publishing the survey. To all my colleagues for the jokes, the do's and don't's that was shared during our lunches and coffee breaks. Without their help, gathering data for this project would be more challenging on a different level.

Thirdly, my appreciation goes to everyone who participated in the interview and online survey. To keep the interviewee anonymous, it is not possible to thank them by name. Nonetheless, their insights have helped in formulating the survey and providing general sentiment towards the EU GDPR. I believe your collective aspirations will play a role on the discourses regarding privacy and data protection in the future.

I would also like to thank LPDP (Indonesian Endowment Fund for Education), who has financed my master degree for the first two years. Moreover, I thank all other parties who have helped in sharing the online survey: Indonesian Embassy in The Netherlands, Indonesian Trade Attaches, involved privacy groups and BNI. Without their support, I would not be able to experience this study and finish this project.

Finally, and still importantly, I would like to direct my gratitude to my family and friends. My parents and brothers who have always prayed for me and continuously reaching and giving support in any way possible. To all my fellow EPA students, going through this program with the most ambitious batch has been a privileged to me. To all my friends in the Netherlands (Adibah, Alfian, Aprima, Azzam, Bela, Bryan, Dedi, Dola, Eleni, Fadhila, Gerin, Ghina, Majo, Mumtaz, Reiner, Ryan, Sachira, Sasongko, Shani, Shiddiq, Thio, Wahyu, Yohana, Zamroni, other PPI friends whom I will always treasure), thank you for giving me a home away from home. To those in the other parts of the globe (Adam, Aisha, Alessandra, Diane, Ricky, Tita, Vania), thank you for reminding me that your thoughts are always with me.

I set myself to see the world. With your support, I have found not only that but also myself. Thank you for walking the miles with me.

Delft, 13 December 2017
Andita R Faradina

EXECUTIVE SUMMARY

The EU General Data Protection Regulation (EU GDPR) is about to come in force in May 2018. The European Union, through EU GDPR, aims to improve the attempt of previous EU Data Protection Directive (EU DPD) in resolving asymmetry issue. The privacy and data protection regulation anticipated a more controlled citizens personal data processing. Better control in data processing also means more transparency, which results in the reduction of information asymmetry between businesses and customers/citizens. Stronger control on data processing allows a scheme where certain rights of citizens upon their personal data processing are legally enforceable, generating more power for them in the dynamics of economics of information.

In a nutshell, the context is as follows. Contracts exist between agent and principal that entail personal data processing. Information asymmetry comes as a result of the agency problem between businesses and customers/citizens. Information asymmetry leads to power asymmetry in the market, which may result in market failure. The lack of power by citizens/customers gives rise to a remedy for the asymmetries that includes higher active authorities' involvement.

Up to this point, the aim and expectation of the government from the EU GDPR are known. In the opening remarks of EU GDPR, the aim of distributing power to citizen/customer through the empowerment of their rights is supported with point number 11 and 13 (See the main text of EU GDPR). However, the expectation of the businesses remains as a question, and therefore becomes the object of this study. Expectation of businesses (i.e. data users) is important because it builds perception which in turn shape the way business think and plan to implement EU GDPR. Consequently, the actual changes/behaviors can be predicted as an endeavor to learn the effectiveness of EU GDPR.

Subsequently, the objective of this research project is defined to provide the empirical analyses on how businesses intend to change due to the EU GDPR; by investigating current practices in privacy and data protection under the past directives' influences and by analyzing their privacy views and planned changes related to EU GDPR. Based on this research objective, this study aims to answer the main research question of: **How do businesses plan to change due to the implementation of the EU General Data Protection Regulation (GDPR),given its differences with the directives and the different business interests?**

RESEARCH APPROACH

Mixed methods are used in this research. It starts with the qualitative approach that includes literature review, stakeholder analysis and exploratory interview. Literature review is used mainly in the conceptualization phase, resulting in a framework to set up the following interview and survey questions. Subsequently, interview is done to explore the current implementation of the past EU DPD.

Then, this research enters the quantitative approach that incorporates data gathering via an online survey and data analysis using various statistical tools. Both the framework and the interview results are utilized to set up the survey protocol. Various statistical tools are used to test a number of hypotheses and estimate regression models. Two metrics are developed to measure organizations intention to change for EU GDPR: Considered Internal Changes, and Planned Investment.The independent variables are *regional footprint*, *revenue*, *industrial sector*, *DPO existence*, *perceived gap*, *expected impact*, *value on privacy* and *value on personal data processing*. The formulated hypotheses are listed in the following table.

Table 1: List of Hypotheses to Test

	Hypotheses
	Related to Control Variables
H1	Companies having footprints in EU will plan more changes related to EU GDPR.
H2	Larger companies will plan more changes related to EU GDPR.
H3	The magnitude of planned changes by companies differs across industrial sectors
	Related to Independent Variables
H4	The existence of Data Protection Officer will lessen the changes planned by the companies
H5	Companies that perceive higher compliance gap with EU GDPR will plan more changes related to EU GDPR.
H6	Companies that expect more positive impact from EU GDPR will plan more changes related to EU GDPR.
H7	Companies that place a higher value on data privacy will plan more changes related to EU GDPR
H8	Companies that place a higher dependency on personal data processing consider less changes related to EU GDPR.

FINDINGS

Most companies process personal data, be it internally (employee data) or externally (customer/3rd partypersonal data). The purpose of the processing vary from marketing to measuring their success rate. Some multinational companies have their Binding Corporate Rule formulated and approved. Those following the past directive does not see much differences with the EU GDPR. However, for those who had not been paying much attention to privacy and data protection find EU GDPR quite challenging. Important notes are found on the challenges of existence of DPO and governance, implementing Privacy by Design and establishing a mechanism for Personal Data Breach Notification. It is also understood that some companies are more in a passive position, waiting to see how the enforcement will take place, especially in UK, Ireland, and Sweden. Moreover, organizations perceived different challenges when it comes to the implementation of EU GDPR. Those are the limited resources, IT and data security complexity, being compliance itself and the uncertain impact.

The intention to change regarding to EU GDPR is rather high. Changes of companies are measured from companies' own judgments on planned investment and considered internal changes. A big portion of the respondents (i.e. 74%) falls in 'agree' and 'strongly agree' to the thoughts of having their organizations planning investment for changes related to EU GDPR. Planned Investment is influenced positively by the perceived gap, existence of DPO and perceived overall gap. Factors influencing considered internal changes are value on processing personal data and the organization regional footprint. The regression model for Considered Internal Changes as dependent variable can be seen in Table 2.

When it comes to the organizations' perceptions, both perceived gap and expected impact do play a role in the planning the changes, especially when observed based on the planned investment. However, the power of perceived compliance gap is stronger than the expected impact. Expected impact is only found to be statistically significant when tested alone, while perceived gap is also found to be significant when tested simultaneously with other variables.

Moving to our hypothesis, 3 out of 8 hypotheses are proven. First, companies having footprints in EU would plan more investment on changes related to EU GDPR compared to those not having footprint in EU (H1). Second, the organizations perceiving large compliance gap would be likely to plan more investment, presumably to cover those gap (H5). Third, those having high value would also be likely to plan high investment to the aforementioned changes (H7). Moreover, the other 2 hypotheses are proven to the opposite spectrum. The organizations that have places a DPO would be more likely to plan more investment instead of planning less (H4). The dependency of data processing would still increase the considered internal changes changes (H8). Furthermore, the rest of the hypotheses are simply not proven, which are H2, H3, and H6.

Table 2: Multiple Regression Model (DV = Considered Internal Changes

Variable	Mean (SD)	Unstandardized Coefficients		P > |z|	Collinearity Statistics	
		Coefficient	Std Error		Tolerance	VIF
Dependency on Personal Data processing	2.0654 (1.14520)	0.799	0.195	0.000	0.993	1.007
Dummy EuandOther	0.1830 (0.38794)	0.669	0.207	0.001	0.857	1.166
Dummy EU Only	0.3791 (0.48675)	0.473	0.164	0.005	0.863	1.158
Constant		-0.960	0.193	0.000		

R Square = 0.179; Adjusted R Square = 0/163
Excluded Variables: Revenue, DPO Existence, PrivacyImportance, PerceivedGap, ExpectedImpact, DummyMedia, DummyIT_Sector, DummyGovernment, DummyFinance, DummyExecutives, DummyITInfoSec, DummyLegal, DummyMarket

RECOMMENDATIONS

Based on the findings of this research, several recommendations can be drawn for both policymakers and data processors and users. First, from a general point of view, policymakers may want to consider extending training and expanding the number of legal and technical experts. Furthermore, based on the statistically significant variables found, several recommendations can be found on a more specific areas. Policymakers may want to focus on encouraging organizations to designate a DPO, socializing the importance of protecting privacy, socializing the differences between the EU GDPR and the past privacy acts, providing different approach on organizations with different personal data processing dependency, and to also periodically supervise and examine the transfer and certification of data transfer outside the EU.

Recommendations are also drawn for organizations based on their perceived challenges to implement the EU GDPR. Organizations may want to consider having a DPO in place, to talk to peers and join forces when plausible, to be open to the policymaker, to outsource when the resources are found to be limited and impossible to utilize, and to come up with menu of contracts in order to keep balance of being compliant, preserving customers' trust and not cutting of their source from utilizing personal data.

ABBREVIATION

ACM	: Authority for Consumers and Markets
AP	: *Autoriteit Persoonsgegevens*
APEC	: Asia Pacific Economic Cooperation
AU	: African Union
CBP	: *College Bescherming Persoonsgegevens* (Dutch Supervisory Auhtority)
CEDPO	: Confederation of European Data Protection Organizations
CJEU	: Court of Justice of the European Union
CoE	: Council of Europe
DPA	: Data Protection Authority
DPO	: Data Protection Officer
DV	: Dependent Variables
ECSEL	: Electronic Components and Systems for European Leadership
EDPB	: European Data Protection Board
EDPS	: European Data Protection Supervisor
ENISA	: European Union Agency for Network and Information Security
EPA	: European Privacy Association
EU	: European Union
EU DPD	: European Union Data Protection Directive
EU GDPR	: European Union General Data Protection Regulation
FIP	: Fair Information Practices
FRA	: Fundamentals Right Agency
FTC	: Federal Trade Commission
IAPP	: International Association of Privacy Professionals
ICT	: Information and Communication Technology
IDPC	: International Data Protection Commissioners
IGZ	: *Inspectie voor de Gezondheid* (Health Care Inspectorate)
INEA	: Innovation and Networks Executive Agency
IV	: Independent Variables
NGFG	: *Nederlands Genootschap van Functionarissen voor de Gegevensbescherming*
OECD	: Organisation for Economic Co-operation Development
OPTA	: *Onafhankelijke Post en Telecommunicatie Autoriteit* (Independent Post and Telecommunications Authority)
POV	: Point of View
SA	: Supervisory Authority
SNS	: Social Network Sites
TPB	: Theory of Planned Behavior
TPP	: Trans Pacific Partnership
UN	: United Nations
US	: United States
WP29	: Article 29 Working Party

CONTENTS

1

INTRODUCTION

1.1. RESEARCH BACKGROUND

With the ever-evolving ICT, we have never been more connected than before. More exposure to our daily life has prevailed, and consecutively more personal data are imposed on the Internet (WEF, 2012). For quite some time, the abundant amount of these data is automatically processed and has started to become an integral part of the economy throughout the world. IDC asserts that the overall data market is estimated at more than 130.1 Billion Euros in 2016 and will get to 203 Billion in 2020 under high-growth conditions (Shirer, 2016). At the same time, malicious measures in the dynamics of cyber world are increasing (Jang-Jaccard & Nepal, 2014; Srinidhi, Yan, & Tayi, 2015; Allianz, 2015). Consequently, concerns towards information privacy emerge (Banisar & Davies, 1999; Luftman & McLean, 2004; TRUSTe, 2015).

The importance and issues of data processing for the global economy have brought up the need for legal protections over personal data. A number of influential entities in both public and private sectors have called for an international legal framework for privacy and data protection (Kuner, 2009). On the European level, European Commission (EC) has stipulated the Data Protection Directive 95/46/EC (EU DPD), which set the milestone in the history of data protection. EU DPD aims to protect the rights and freedoms of persons with respect to the processing of personal data by laying down the key criteria for making processing lawful and the principles of data quality. As a following effort to the EU DPD, Directive 2002/58/EC (e-Privacy Directive) –now amended to Directive 2009/136/EC, is stipulated. E-Privacy Directive mainly concerns to the processing of personal data and the protection of privacy in the electronic communications sector. It deals with a number of important issues like confidentiality of the communication, treatment of data, unsolicited communications (spam), which also boils down to the use of cookies.

The high degree of the directives' abstraction leaves room for individual members to interpret the aligned legislation differently (Walczuch & Steeghs, 2001; Ashford, 2012). This results in an uneven level of protection for personal data throughout the European Union (EU) (EC, 2012). Moreover, the globalization and evolution of technology that generates new privacy threats, which strengthen the need for an EU Data Protection reformation (Poullet, 2009; EC, 2012).

EC proposed the EU General Data Protection Regulation (EU GDPR) to reform the EU DPD. After four years of negotiating, both the European Parliament and Council announced that they had reached an agreement on the consolidated text in December 2015 (Carson, 2015). As the resolution of the decaying Directive, the EU GDPR aims to provide a single robust set of rules on data protection, valid across the EU (EC, 2012). The policymakers perceive it to be a vital agreement for Digital Single Market effort that ensures Europe has data protection rules that are fit for purpose in the Digital Age (Pfeifle, 2015). The reformation will also affect e-Privacy Directive as a complement towards EU DPD in specific rules concerning the processing of personal data in the electronic communication sector. Adjustment of e-Privacy Directives towards the change in EU GDPR will be a subject of review in the near future (EC, 2015).

The difference between EU DPD as a directive and EU GDPR as a regulation lies in the binding force. A regulation is a binding legislative act, which must be applied in its entirety across the EU. A directive is a legislative act that sets out a goal that all EU countries must achieve where it is up to the individual countries to devise their own laws on how to reach these goals (EU, 2017).

The implementation of EU GDPR will make controls on data processing stricter and more extensive in

Europe. Along with its stronger force, EU GDPR might simplify the previously layered regulations from different EU members. Further, although there is new regulation to increase fines in case of a data breach, such increase might reduce the uncertainty of risks by making it more quantifiable. Nevertheless, compliance with the GDPR will require effort from controllers and cannot be completed overnight (Mikkonen, 2014).

The EU GDPR sets forth new challenges for both policymakers and businesses. This leads to the research problem and its relevance, which is further elaborated in Section 1.2 below. Section 1.3 delineates the objective and the questions of this research that will be answered. Section 1.4 explicates the relevance of this research project both scientifically and practically. Finally, Section 1.5 depicts how this research is carried out and how the deliverables are outlined in this thesis report.

1.2. RESEARCH PROBLEM

The European Union portrays this privacy issue in terms of consumers versus businesses (Berkgamp, 2002) which is reflected in the past EU DPD and the new EU GDPR. Up to this point, the myriad of actors involved can be classified into three poles: the regulator as the policymakers, the businesses or other entities as the data controller and processor, as well as the consumer or citizen as the data subject. Naturally, one can say the objective of the regulation can only be achieved when the needs of the two ends –the businesses and the consumers, are met.

The emergence of EU GDPR poses new queries for both policymakers and businesses. Policymakers want to know how effective the new EU GDPR will be while the businesses would like to know how EU GDPR should be implemented. However, in order to be able to answer these questions, the current implementation of the former EU DPD and the complementing e-Privacy Directive shall be comprehended and made clear. More importantly, since EU GDPR is yet to be enforced, the effective implementation can only be estimated. It is true that the regulation has to be fulfilled by any organizations concerning personal data of EU citizen. However, the level of organizations willingness and intentions to comply will play affect on the effort given by the organizations to keep in line with the aim of the EU GDPR itself.

Only by having the current situation and the organizations intention regarding EU GDPR, a prediction on how well the EU GDPR will be implemented can be predicted. Thus, assessment of necessary additional compliance can be determined for businesses. Moreover, the effectiveness of EU GDPR implementation can be predicted by the policy makers and the areas to focus on (if any) can be highlighted. *Nevertheless, there is no apparent empirical study on how EU DPD and ePrivacy Directive are interpreted and implemented by businesses, let alone the organizations' intention to change regarding EU GDPR. This serves as the problem of this research.*

There are some studies that attempted to provide the empirical study on how EU DPD and the complementing e-Privacy Directive are implemented. A number of these studies are bounded in a specified business sector. In the health sector, Batty, Glozier, and Holland-Elliott (2009) investigated the understanding and practice of occupational physicians in the UK to see if a consensus view towards Data Protection Act 1998 –as the national level interpretation of EU DPD in the United Kingdom (UK)– existed. Nevertheless, this study barely touched the empirical facts of the implementation itself. In the public sector, Beldad, Jong, and Steehouder (2009) analyzed the contents of privacy statements on Dutch municipal websites. Their study, however, falls short in evaluating other important provisions of EU DPD outside privacy statements. Another study in gaming (Leichtenstern, Bee, André, Berkmüller, & Wagner, 2011) analyzed the compliance of game-network providers with data protection law. Similarly, the approach is limited to only a few qualifications of the law, namely the provided privacy policy in their network and the fulfillment to provide one's information on demand. In the social media sector, where many empirical studies often focused on, analogous limitation is found: mainly focused on narrow EU DPD provisions and only seen from the external perspective, which is based on the privacy policy on their websites (e.g., Kuzma (2011)).

Further, a number of empirical studies towards the implementation of DPD and e-Privacy Directive at the national level also prevail. Peguera (2015) examined how the 'right to be forgotten' (RTB) is applied in Spain. However, the study was limited in that one point of RTB based on the case laws. In the UK, Borghi, Ferretti, and Karapapa (2013) surveyed the methods used to seek and obtain consent to process personal data for direct marketing and advertisement, and a test on the frequency of unsolicited commercial emails received by customers as a consequence of their registration and submission of personal information to a website. Their study indicates the inappropriate standard of implementation, information, and supervision by the UK authorities. Similar studies are conducted to examine the practice of the Dutch cookie regulation in increasing consumer control (Leenes & Kosta, 2015) and to investigate the lack of enforcement of Data

Protection Acts in Germany (Burghardt, Böhm, Buchmann, Kühling, & Sivridis, 2010). Burghardt et al. (2010) gathered empirical facts on few juridical assessment criteria and validated the lacking enforcement. Another study in Finland, with a little shift of focus towards the businesses' awareness and willingness to comply with the new EU GDPR, was executed (Mikkonen, 2014).

Nevertheless, from these past studies, *none has examined the empirical facts of data protection implementation using a thorough DPD provisions.* Only a small number of the requirements of EU DPD are used as the assessment criteria in each study. More importantly, the perspective used in the studies is the external point of view; that is by observing through what is put down on the websites (e.g. existence and content of privacy policy; existence and methods of consent request). *Company-internal perspective, which can give more insights on the process of data related to data protection and their intentions regarding EU GDPR, is still lacking.*

The key questions here are how businesses and other entities interpret the binding regulations and carry out the previous directives; and how these organizations plan to change in accordance with EU GDPR. Answering such question comes of importance for two reasons. First, as previously mentioned, it serves as the preliminary evaluation to answer the challenge of the new EU GDPR for both policymakers and businesses. Second, it will provide insights to enable further improvement of the industry guidelines. A Dutch Data Protection Agency stated that the current most available assistance for data protection is not particularly helpful regarding system adaptation to the Directive (Kenny & Borking, 2002).

1.3. RESEARCH OBJECTIVE AND QUESTION

In the light of research problem explained above, the objective of this research project is defined *to provide the empirical analyses on how businesses intend to change due to the EU GDPR; by investigating current practices in privacy and data protection under the past directives' influences and by analyzing their privacy views and planned changes related to EU GDPR.*

There are two focal points in this research. The first one is stretched out in the current implementation of EU DPD, the past directive. This includes the theoretical notion of how data and privacy protection should be done as well as practical view and opinions on the implementation itself. The second focal point lies in the pragmatic perspective within the realm of data protection, related to the adaptation of EU GDPR in particular. This is not only limited to the point where businesses interpret what the challenges are, but also to their perceptions on their own current position and where they are heading.

Based on the research problem and objective, the main research question that shall be answered is

> ***"How do businesses plan to change due to the implementation of the EU General Data Protection Regulation (GDPR), given its differences with the directives and the different business interests?"***

To answer the main research question, the following sub research questions (SRQ) are derived. Each sub research question aims at different aspect that will construct the answer to the main research question.

1. What are the concepts of privacy and data protection and how do they relate to the data protection acts?
   (a) What are the principal notions in data protection and privacy?
   (b) Who are the important stakeholders involved and what are their responsibilities and objectives at stake in data and privacy protection?
   (c) What are the primary requirements in the EU DPD, e-Privacy Directive, EU GDPR and the related industry guidelines?
2. How do organizations interpret and implement the existing EU DPD and e-Privacy Directive?
   (a) What businesses or technical practices do they have in place?
   (b) Do they follow any guidelines or code of conducts in dealing with data protection? Why?
   (c) How do different sectors measure the accompanying privacy and information risks and their performance in complying with the EU DPD and e-Privacy Directive?
3. How do organizations plan to change in terms of processes and investments with the implementation of the EU General Data Protection Regulation?
4. How do businesses properties and privacy views influence the plan to change, and what are the policy implications of the findings?

1.4. SCIENTIFIC AND PRACTICAL RELEVANCE

This research will have scientific relevance in the following manner: Firstly, it would contribute to closing the important knowledge gap within data protection by addressing insights on how EU DPD and e-Privacy Directive are interpreted and implemented by businesses, particularly with company-internal perspective. Secondly, it will provide a conceptual framework on measuring the organizations intention to comply with an EU Regulation, particularly EU GDPR. Thirdly, it will shed some light on how diverging business interests drive different incentives in protecting the involved data. Additionally, such insights will have societal relevance from the perspective of practitioners and policymakers. While perspectives from the distinct business sector will help professional alliances in improving the guidelines, the regulatory insights will be useful for policymakers to make necessary enhancement in privacy protection through regulatory approach.

1.5. RESEARCH FLOW AND THESIS OUTLINE

This research is divided into three phases. The first phase involves literature study on privacy and data protection concept. It includes theories regarding privacy, data protection. Additionally, the literature review also seek the pivotal stipulation from the EU GDPR and its differences with the past privacy and data protection act. Moreover, a stakeholder analysis is done to grasp the dynamics among the important stakeholders in the privacy and data protection realm. Ultimately, a conceptual framework is also formulated in this phase. The framework is further used to develop interview and survey questions in the empirical investigation.

The second phase is the execution of exploratory interview and survey to investigate the empirical evidence on organizations current situation and their intentions to change regarding the EU GDPR. The results from the previous phase are used to generate the questions and protocols needed in the interviews. Both experts and practitioners in data protection from different business sectors are plausible candidates for the interview. The interview is focused on investigating how businesses interpret and implement the directives as the main concern, and how prepared are businesses in dealing with the new EU GDPR as the secondary issue. Meanwhile, the survey focuses more to examine the later issue, which is on the organizations plan to change.

Finally, the third phase draws the conclusion of the analyzed findings. Findings on main and secondary issues are drawn as the first two deliverables of this research. The empirical findings are then juxtaposed with the objectives the EU GDPR to reflect on the policy implications. Based on these deliverables, conclusions to answer the main research question can be drawn. Figure 1.1 shows the research flow diagram and the important steps needed to be carried out in the research.

To have a systematic flow, the results of this research are divided into 6 parts. This research proposal is used as the introduction in the first chapter. The second chapter presents the literature review. The literature review will consist two part: privacy and data protection context, as well as generated conceptual framework as a assisting tool for the rest of this research. In the third chapter, the research methods is presented. This chapter will explain the techniques used in gathering and analyzing the data. Sources for each data gathering, measurements for the previous conceptual model including the hypothesis are represented here. The fourth and fifth chapter presents the obtained results respectively from interview and survey. The interview results will be qualitatively analyzed and summed up in chapter three. The main findings from this step are used to formulate the survey question. The survey results will be quantitatively analyzed using various statistical tests. The sixth chapter concludes this thesis by providing summary on the findings, discussing obtained findings, and presenting recommendations related to policy implications and future research.

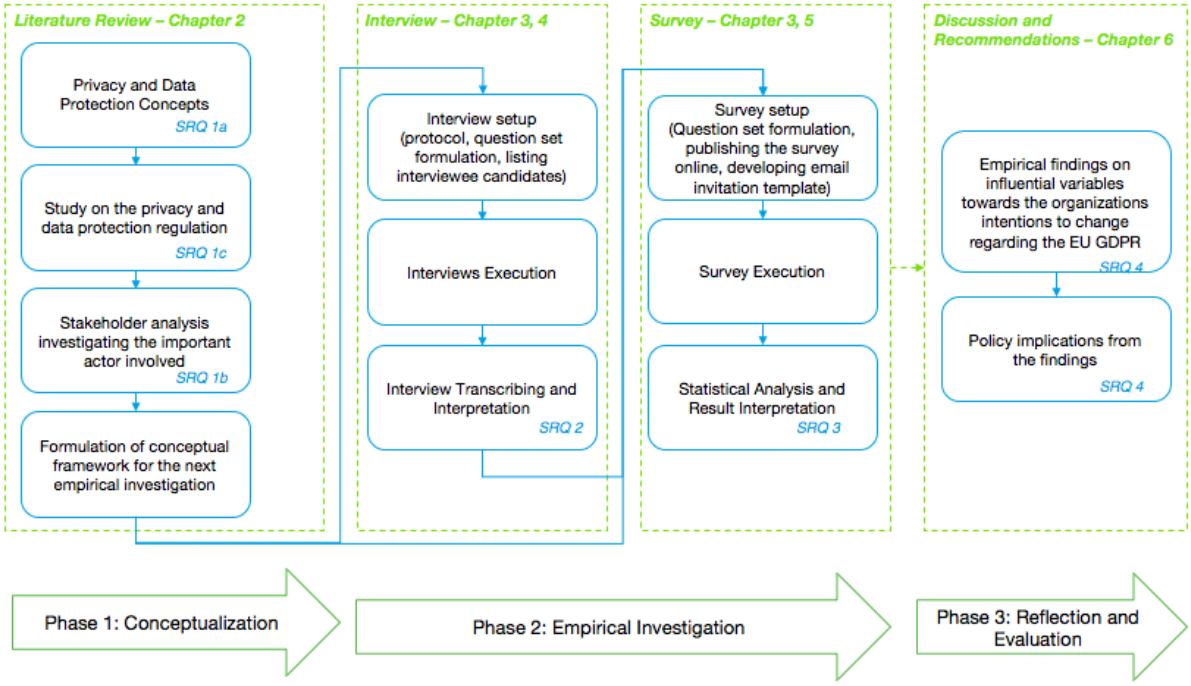


Figure 1.1: Research Flow Diagram

2

LITERATURE REVIEW

This chapter provides a conceptual framework of privacy and its view in the regulation for a guide throughout this research. Section 2.1 describes the conceptual definition of (information) privacy, the data protection that entails and the important stakeholders involved in the privacy and data protection.

2.1. INFORMATION PRIVACY AND DATA PROTECTION

2.1.1. INFORMATION PRIVACY

The term privacy has been researched for quite some time in the past century (Miltgen & Peyrat-Guillard, 2013). However, there is no consensus on what privacy means (Solove, 2006). Many legal and social scholars believe that general privacy is so dependent on the specific context that it is impossible to develop a-one-size-fits-all conceptualization of general privacy (Smith, Dinev, & Xu, 2011).

According to Smith et al. (2011), general privacy can be classified into physical privacy and information privacy. Physical privacy concerns *physical* access to an individual or his/her surroundings and private space, while information privacy concerns access to individually identifiable person *information*. Historically, recent evolution of information privacy concept emerged after physical privacy concept was explicated (Westin, 2003). Moreover, the definition of general privacy can be broadly classified as *value-based* or *cognate-based* (Smith et al., 2011). Privacy conceptualization using both time (and technology advancement) classification as well as value-cognate classification, can be seen in Figure 2.1.

The value based initially views *general privacy as a human right* integral to society's moral value system. For instance, (Warren & Brandeis, 1890) defined general privacy as 'the right to be left alone'. However, with the advancement of technology, this general definition started to show its shortcoming, which is the lack of boundaries. Therefore, a new notion of *privacy as commodity* was conceptualized (Bennett, 2001). In this view, privacy is subject to the economic principles of cost-benefit analysis and trade-off (Smith et al., 2011).

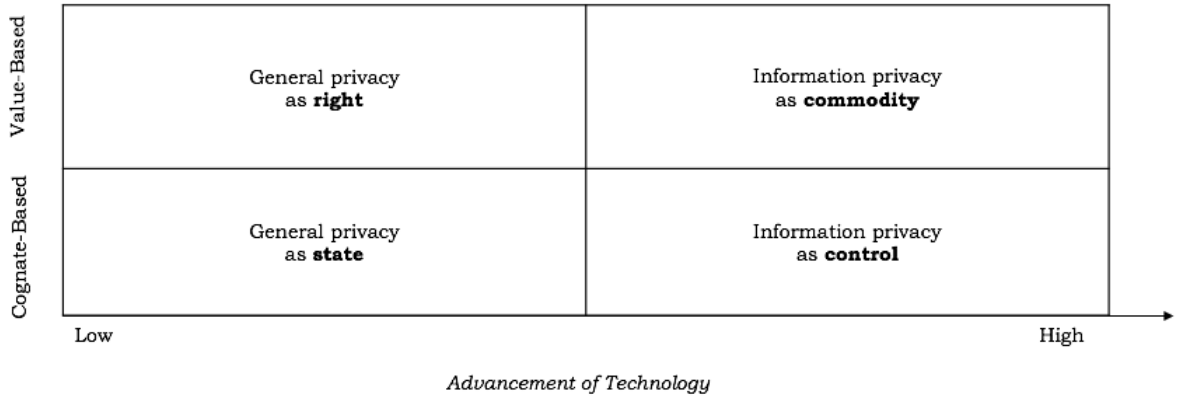


Figure 2.1: Privacy Conceptualization based on Smith, Dinev, and Xu (2011)

The cognate-based, on the other hand, initially views *general privacy as a state*. For instance, Schoeman (1984) defined general privacy as a state of limited access to a person. Taking information context into account, the state of limited access was translated to state of limited access to information (Smith et al., 2011). From this point, privacy as a state coherence with a discrete condition whether privacy is obtained or not. However, to better explains the reality, continuous states of privacy from maximum to minimum must exist. Thus, a concept of *general privacy as control* was generated. Originated by Westin (1968) and Altman (1976) as cited in Smith et al. (2011), general privacy as control views privacy as a whole or in part, represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability.

It is noteworthy to be aware that this research focuses with information privacy as opposed to physical privacy. Although information privacy also can be defined in multiple ways, this research accedes to most scholars, and define **information privacy as an individual desire to control or have influence over the acquisition and potential secondary uses of personal data** (Belanger, Hiller, & Smith, 2002; Bélanger & Crossler, 2011; Miltgen & Peyrat-Guillard, 2013). Following Smith et al. (2011), the rest of this research use 'privacy' to refer to information privacy. Occasional reference to physical privacy or general privacy are made where necessary.

2.1.2. DATA PROTECTION

Privacy has become our issue in this age of information (H. J. Smith, Milberg, & Burke, 1996). This is due to Information and Communication Technology (ICT) that has inevitably affected our experiences in privacy. In turn, these privacy experiences affect our privacy concerns to a generally higher level (Harris, 1990; Katz & Tassone, 1990; as cited in H. J. Smith et al., 1996). Consequently, increasing privacy concerns led to the need of privacy protection. Protecting (information) privacy, often means protecting the data containing such information. Thus, privacy protection is at times included in the so called data protection. Based on the performing subject, data protection can be classified to at least four levels: individual, organizational, and governmental level.

INDIVIDUAL LEVEL

On the individual level, despite the existence of privacy paradox (Kokolakis, 2015), evidences of individuals taking control to protect their privacy do exist. Such controlling acts include disclosing less private information, particularly when the website is not found to be trustworthy (Wakefield, 2013; Tsai, Egelman, Cranor, & Acquisti, 2011), using pseudonyms and giving false information (Miltgen & Peyrat-Guillard, 2013), adjusting privacy settings or restricting access to their profile in SNS (Boyd & Hargittai, 2010). And finally, Son and Kim (2008) summarize those acts in their taxonomy of Information Privacy-Protective Responses (IPPRs), such as refusing to provide information, providing false information, removal information from online companies databases, negative word-of-mouth, complaining directly to inline companies, and complaining indirectly to third-party organizations. They also found a strong correlation between privacy concern and at least five of the IPPRs. As customers, individuals may depend on the companies, such as by paying a premium for privacy (Egelman, Felt, & Wagner, 2013). Their reliance on the company can also be as thin as trust based on the companies' privacy agreement. As citizens, individuals may also depend on the regulatory bodies of their country. (Milberg, Smith, & Burke, 2000) suggested that if consumers do not perceive firms as adequately protecting their privacy they will distrust self-regulation and prefer state intervention. Kokolakis (2015) also argues that government policy makers justify privacy regulation on people's raised privacy concern.

ORGANIZATIONAL LEVEL

On the organizational level, data protection is translated into companies' strategies to secure their enterprise data. Companies owning such data, where privacy information maybe inherited, are entitled to protect the data for at least two reasons. First is related to its own interest, where information as the new currency (Duri et al., 2004) has to be protected. Second is related to its customers or business partners' interests, where their customers or partners' trust has to be ensured (Kokolakis, 2015; Ajigini, 2015). According to Ajigini (2015) security strategy model, data protection strategies on the companies level encompass at least the following nine arrangements

1. Identification, location and classification of sensitive data, including privacy-related data
2. Development of security policies
3. Identification of organizational risks

4. Selection of appropriate controls
5. Implementation of mode of data privacy
6. Implementation of data privacy solution
7. Management of central security and ensure cyber-security awareness
8. Implementation of security audit
9. Enforcement of existing technology standards

On a more practical level, there is a strong correlation between some of the data protection strategies with data protection induced from the upper national or governmental level. For instance, the identification of organizational risk and sensitive data with Privacy Impact Assessment, as well as implementation of data privacy solution and the enforcement of existing technology standards with Privacy by Design. More about these regulation can be seen in section 2.2.

GOVERNMENTAL LEVEL

On the governmental level, data protection is often translated to policy or regulation oriented form. The nomenclature of "data protection", derived from the German term "Datenschutz", describes the field of law and policy which crystallized from the early European discussions on privacy-related threats posed by ICT. Its use, though, is being increasingly supplemented by "data privacy" which better communicates the central interests at stake (Bygrave, 2014). The principal aim of data protection policy is to safeguard the privacy of individuals (Raab, 1998). The realm of data protection law evolves over time around the globe. As Westin (2003) summarizes, the early recognition of potential dark sides of new technologies brings about the rise of information privacy as an explicit political and legal issue. Government started to establish regulatory mechanism marked by Privacy Act of 1974.

Let's review some milestones of data protection law evolution based on four privacy development period defined by Westin (2003): privacy baseline (1945-1960), first era of contemporary privacy development (1961-1979), second era of privacy development (1980-1989), and third era of privacy development (1990-current). During the privacy baseline, the rights to a private life and associate freedoms were first stated in the Universal Declaration of Human Rights in 1948 (UN, 2016). There was a high trust on government, but the second world war prompts governments, particularly in US, to surveillance without their citizens' knowledge. Due to this phenomenon, along with rapid increase of personal data repositories in federal agencies, Fair Information Practices (FIP) were issued by the US Department of Health Education and Welfare (HEW) in 1973 (Solove, 2016), marking the first era of of contemporary privacy development . Shortly after, Privacy Act of 1974 was coded. The act regulates the collection and use of records by federal agencies, and affords individuals right to access and correct their personal information (Solove, 2016).

In the second era of privacy development, updates on FIP were made and Privacy Protection Act were issued in 1980 by the US. The core privacy principles addressed by FIP are notice/awareness, choice/consent, access/participation, integrity/security, enforcement/redress (Gellman, 2014). While the Privacy Protection Act 1980 restricts the search or seizure of "any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." (Solove, 2016). Within the same year, Organization for Economic Co-operation and Development (OECD) defined 8 privacy principles in OECD Guidelines, which consist collection limitation, data quality, individual participation, purpose specification, use limitation, security safeguards, openness and accountability. The OECD guidelines quickly influence the content of privacy laws around the world beyond the OECD member base (UN, 2016). European nations move to national data protection laws for both the private and public sector. Council of Europe established Council of Europe Data Protection Convention 1981 (also known as Convention 1981 or CoE Convention). Although it was established by the Council of Europe, its membership is open to any other country, making CeO Convention the most prominent binding International agreement on data protection (UN, 2016).

In the third era of, the privacy development from legal point of view is escalating quickly. Starting to review it from outside Europe, the United Nations (UN) joined the effort by defining guidelines concerning computerized personal data files in 1990. The UN Guidelines consist lawfulness and fairness, accuracy, purpose-specification, interested-person access, non-discrimination, power to make exceptions, security, supervision and sanctions, trans-border data flows, and field of application. Then, the Federal Trade Commission Act

was proposed in 1998, which prohibits unfair or deceptive acts or practices in or affecting commerce (Solove, 2016). Moreover, International Data Protection Commissioners (IDPC) made a statement on global privacy principles in 2005, which is later called as the Montreux Declaration (UN, 2016). The Declaration stated, as quoted in UN (2016):

> The Data Protection and Privacy Commissioners express their will to strengthen the international recognition of the universal character of these principles. They agree to collaborate in particular with the governments and international and supra-national organizations for the development of a universal convention for the protection of individuals with regard to the processing of personal data.

Movements in Asia were also detected and marked with Asian Pacific Economic Cooperation (APEC) Privacy Framework in 2005 (UN, 2016).Moving to Africa, the African Union (AU) Convention on Cyber-security and Personal Data Protection in June 2014. The act aims to establish regional and national legal frameworks for cyber-security, electronic transactions and personal data protection (Rudgard, n.d.). Aside from the aforementioned laws, numerous trade agreements have emerged as a new source of both data protection law and guidelines on managing the potential conflict between data protection law and cross-border data flows. One example of a relevant agreement that has been made public is the Trans-Pacific Partnership agreement (TPP). (Rudgard, n.d.). While does not impose any significant requirements for data protection, it does address the issue of balancing data protection laws against trade considerations.

Simultaneously, developments in Europe were as accelerated as it was in the other part of the globe. Initiated by European Convention on Human Rights (ECHR) in 1950, many European countries took the lead in implementing legislation aimed to control the use of personal information by government agencies and large companies from 1960s to 1980s. With the increased need for a harmonized European approach, European Commission set out European Data Protection Directive in 1995. It has a significant influence on global privacy development, particularly in cross-border transfer rules and the 'adequacy decision of foreign data protection regimes (Rudgard, n.d.). Since then, the privacy laws on European level went to an even more a rapid development. A number of related directives were issued, for instance e-Commerce Directive in 2000, e-Privacy Directive in 2002, and Data Retention Directive in 2006. Treaty of Lisbon was designed in 2007 to strengthen and improve core structure of EU. The treaty also established the European Data Protection Supervisor. Moreover, the e-Privacy Directive were amended in 2009 with particular changes concerning cookies. Finally, the most recent development which is the subject of this research is the EU General Data Protection Regulation coming into force in 25 May 2018.

Table 2.1: Historical Context of Data Protection Laws . Adapted from (UN, 2016; Solove, 2016; Rudgard, n.d.)

Historical Context of Data Protection Laws			
Year	**Main Affected Region**	**Policy Maker**	**Milestone**
1948	Global	UN	The **Universal Declaration of Human Rights**. It recognizes universal values and traditions—'the inherent dignity and the equal and inalienable rights of all members of the human race' to freedom,justice, and peace in the world
1950	Europe	CoE	The **European Convention on Human Rights (ECHR)**. It recognizes human rights and fundamental freedoms
1970	Germany	Germany	**First modern privacy law** in European states was formulated in **Germany**
1973	Global	FTC	**Fair Information Practices Principles**. It consists 8 principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability
1974	US	US	**Privacy Act** in US is first postulated. It regulates the use and collection of records by federal agencies, and affords individuals right to access and correct their personal information

Continuation of Table 2.1

Year	Main Affected Region	Policy Maker	Milestone
1979	Europe	7 EU Members	**Data protection laws** had been enacted **in 7 EU member states** (Austria, Denmark, France, Federal Republic of Germany, Luxembourg, Norway andSweden) with legislation planned in several others. In three European countries,Spain, Portugal, and Austria, data protection was also incorporated as a fundamental right in the Constitution.
1980	Global	OECD	**OECD Guidelines** on the Protection of Privacy and Transborder Flows of Personal Data
1981	Global	CoE	**Council of Europe Convention** for the Protection of Individualswith regard to Automatic Processing of Personal Data (Convention 108)consolidates and re-affirms the 1973 and 1974 resolutions and is the first legally binding international instrument in the area of data protection. It differs from the OECD Guidelines in that it requires signatories to Convention 108 to take the necessary steps in their domestic legislation to apply the principles it lays down.
1990	Global	UN	**UN Guidelines** concerning computerized personal data files. The guidelines consist 10 principles, lawfulness and fairness, accuracy, purpose-specification, interested-person access, non-discrimination, power to make exceptions, security, supervision and sanctions, trans-border data flows, and field of application.
1995	Europe	EU	**Directive 95/46/EC** on the protection of Individuals with regard tothe processing of personal data and on the free movement of such data(the Data Protection Directive or the Directive) further reconciled the protection of the fundamental rights of individuals with the free flow of data from one member state to another
1998	US	FTC	**The FTC Act**, which prohibits 'unfair or deceptive acts or practices in or affecting commerce
2000	Europe	EU	**Directive 2000/31/EC** on certain legal aspects of information societyservices, in particular electronic commerce, in the Internal Market ('Directiveon electronic commerce') or the **e-Commerce Directive**
2000	Europe	EU	**Charter of Fundamental Rights of the European Union** further consolidated fundamental rights applicable within the EU, and included the general principles set out in the ECHR but specifically refers to the protection of personal data
2001	Europe	EU	Additional Protocol to the Convention for the Protection of Individualswith regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows was designed to address the fact that Convention 108 did not provide for transfers of personal information to countries which are not signatories to Convention 108. It introduced the concept of an 'adequate' (rather than an equivalent) level of protection for personal informationtransferred to non-EU states

Continuation of Table 2.1

Year	Main Affected Region	Policy Maker	Milestone
2002	Europe	EU	**Directive 2002/58/EC** concerning the processing of personal dataand the protection of privacy in the electronic communications sector(Directive on privacy and electronic communications) (The e-PrivacyDirective) deals with the regulation of a number of important issues such as confidentialityof information, treatment of traffic data, spam, and cookies.
2005	Global	IDPC	International Data Protection Commissioners (IDPC) made a statement on global privacy principles, which later called as the **Montreux Declaration**. The IDPC commits to strengthen the international recognition of the universal character of these principles. They agree to collaborate with governments and supra-national organizations for the development of a universal convention for the protection of individuals with regard to the processing of personal data.
2005	Asia	APEC	**Asian Pacific Economic Cooperation (APEC) formulates a privacy framework** that endorses the importance of the development of effective privacy protections. It consists of eight principles: Preventing Harm, Notice, Collection Limitations, Uses of Personal Information, Choice, Integrity of Personal Information Security Safeguards, Access and Correction, Accountability.
2006	Europe	EU	**Directive 2006/24/EC** on the retention of data generated or processed in connection with the provision of publicly available electroniccommunications services or of public communications networks and amending Directive 2002/58/EC
2007	Europe	EU	**Treaty of Lisbon** was designed to strengthen and improve the core structuresof the European Union to enable it to function more efficiently. It made the 2000Charter binding law. The Treaty established the **European Data Protection Supervisor**
2009	Europe	EU	**Directive 2009/136/EC** amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networksand services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws
2014	Africa	African Union	**African Union (AU) Convention on Cyber-security and Personal Data Protection in June 2014**. The act aims to establish regional and national legal frameworks for cyber-security, electronic transactions and personal data protection
2016	Europe	EU	**EU General Data Protection Regulation (EU GDPR)** is approved by the EU Parliament in January 2016. Designed to replace the EU DPD, it aims 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.

End of Table

2.1.3. PIVOTAL ACTORS IN PRIVACY AND DATA PROTECTION

Examining the dynamics in privacy and data protection, means to also understand who the significant actors are in this field. We will use the preliminary step in the basic procedure for actor analysis (Enserink et al., 2010, Chapter 4) as a guide to generate a thorough overview. These steps incorporate inventory of of the actors involved and exhibiting the formal chart.

ACTORS INVENTORY

Various actor identification techniques are discussed by Mitroff (1983). From the *imperative approach*, on an aggregated level, players in this realm can be classified into three categories: regulator, users of personal data, and individual "data subjects". First, regulators are bodies and entities that create laws and regulations to protect data subjects' privacy and also make sure the regulations are abide by the personal data user. Second, users of personal data are bodies and entities, both public and private, that collect, process, use, and communicate personal data of individuals. In many legal text, this second player is often called as data collector and/or data processor. Third, individual "data subject", in the conventional data protection paradigm (Raab, 1998), is defined as those whose personal data are used, whose rights to control their own data becomes a subject in recent development of data protection laws.

Further, with *positional approach*, actors are further explicated based on their formal position in policy making (e.g. legislation, procedures, policy pieces). Following the scope of this study, we will focus the stakeholder analysis within Europe and particularly the Netherlands. Starting from the European level, it includes legislative bodies in EU: **European Council**, **European Parliament**, **Council of the European (CoE)**, and **European Commission (EC)**. European bodies are not exempted from the obligations to respect privacy and data protection. To ensure this, **European Data Protection Supervisor (EDPS)** is held responsible. Securing the judicial body on the European level, there is **Court of Justice of the European Union**.

Moreover, as laid out in the EU GDPR and its antecedent, EU DPD, Article 29 Working Party (WP29), Member State Supervisory Authority and Data Protection Officers are established. WP29 is an independent body that supervises privacy and data protection on the European level. Among it functions, it provides comment and recommendation to the Commission, and gives opinion on codes of conduct on the community level. Based on EU GDPR, WP29 will be replaced with **European Data Protection Board (EDPB)** to provide more consistent mechanism and more indpendence from the EC. Next, Supervisory Authority (SA) is an independent public authority which is supposed to be established by a Member State pursuant to Article 51 of EU GDPR. In the Netherlands, the Duch SA was called *College Bescherming Persoonsgegevens* (CBP) until January 2016 when it is changed to ***Autoriteit Persoonsgegevens*** **(AP)**. The AP supervises the compliance and application of the relevant privacy acts, which include EU DPD, EU GDPR, as well as the national Personal Data Protection Act (*Wet bescherming persoonsgegevens*: Wbp), the Police Data Act (*Wet politiegegevens*: Wpg), and the Municipal Personal Records Database Act (*Wet gemeentelijke basisadministratie persoonsgegevens*: Wgba). **Data Protection Officer (DPO)**, has to be appointed by Data Controller and Data Processor (both public and private bodies) as an internal advisor and supervisor, as well as contact point with the SA. In the Netherlands, DPOs are called *functionaris voor de gegevensbescherming*, reaching 240 registered DPO by 2007 (Koops, Cuijpers, Nouwt, Roosendaal, & Cehajic, 2009).

On the member state level, a related ministry can be considered as the highest position having significant interest with privacy and data protection. In the Netherlands, it is **Ministry of Economic Affairs, Agriculture and Innovation** that falls into that definition. From its economic perspective, it highlights the side of digital single market behind EU GDPR. While the innovation part sees technological issues and opportunities as the point of interest. In addition, a specialized body is established under the Ministry of Economic Affairs, called ***Radiocommunications Agency*** **(RCA)**. RCA supervises the obligations of internet access and telecom providers (Zeldin, 2012). Then, there is ***Onafhankelijke Post en Telecomunicatie Autoriteit*** **(OPTA)**, independent governmental agency, oriented toward promoting investment in the communications sector while protecting consumer interests.

Using *reputational approach*, FRA mentions some relevant actors on the state level from the sectorial point of view. In the Netherlands, there are **Health Care Inspectorate (Inspectie voor de Gezondheid (IGZ))** for health sector as well as the aforementioned OPTA for the telecommunication sector. Moreover, there are also established committees resulting from specific code of conducts.

1. ***Nationale Ombudsman***. Provides opportunity for individuals to place complaints about the practices of government.

2. Appeal Committee of the Association of Private Security Organisations (***Beroepscommissie van de Vereniging van Particuliere Beveiligingsorganisaties***). Established in connection with the Code of Conduct for

Private Detective Offices

3. Supervision Council (***Raad van Toezicht***). Established in connection with the Code of Conduct on the Employment of Personal Data by the Dutch business Information Offices

4. Chamber of Court Bailiffs (***Kamer van Gerechtsdeurwaarders***). Established in connection with the Code of Conduct for Court Bailiffs

5. Complaints Committee (***Klachtencommissie***). Established in connection with the Code of Conduct for Medical Scientific Research.

6. Committee of Supervision (*Commissie van Toezicht*). Established in connection with the Code of Conduct for the Recruitement and Selection Industry

More about national data protection authorities and instruments from other countries can be found in thematic legal studies by FRA.

Finally, *opinion leadership approach*, brings about influential groups that has yet to be mentioned. These are, but not limited to, **data protection and privacy interest groups** (e.g. Bits of Freedom and Vijshrift), groups of DPOs in the state (e.g. ***Nederlands Genootschap van Functionarissen voor de Gegevensbescherming* (NGFG)**), a European umbrella group of DPO Associations alike (i.e. **Confederation of European Data Protection Organisations (CEDPO)**, and associations of professionals with interests in privacy and data protection **International Association of Privacy Professionals (IAPP)**. On the European level, there are European Agencies which opinions are focused on research and innovation. These agencies are **Electronic Components and Systems for European Leadership Joint Undertaking (ECSEL JU)**, **European Union Agency for Network and Information Security (ENISA)**, **Innovation and Networks Executive Agency (INEA)**, and also **Fundamental Rights Agency (FRA)** which provides opinion from the rights point of view. All of the aforementioned actors are summarized based on their roles in governance and issues of interest as seen in Table 2.2.

Table 2.2: Actors Involved in EU GDPR

Actors Involved with EU GDPR in EU and the Netherlands	
Based on roles in governance	**Based on issue of interest**
European Union Institutions	*EU Harmonization (Digital single market)*
European Council	European Council
European Parliament	European Parliament
Council of the European Union	Council of the European Union
European Commission	European Commission
Court of Justice of the European Union (CJEU)	Article 29 Data Protection Working Party (WP29) / European Data Protection Board (EDPB)
EU Agencies and Decentralized Bodies	*Law Enforcement*
European Data Protection Supervisor (EDPS)	Court of Justice of the European Union (CJEU)
European Union Agency for Fundamental Rights (FRA)	Judicial Bodies Responsible in the Netherlands
European Union Agency for Network and Information Security (ENISA)	*Supervisory*
Article 29 Data Protection Working Party (WP29) / European Data Protection Board (EDPB	European Data Protection Supervisor (EDPS)
Innovation and Networks Executive Agency (INEA)	Autoriteit Persoonsgegevens (AP) / College Bescherming Persoonsgegevens(CBP)
ECSEL Joint Undertaking (ECSEL JU)	Independent Post and Telecommunications Authority(Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA))
National/State Government (Within the Netherlands)	Radiocommunications Agency (RCA)
Ministry of Economic Affairs, Agriculture and Innovation	Health Care Inspectorate (Inspectie voor de Gezondheid (IGZ))
Judicial Bodies Responsible in the Netherlands	National Ombudsman (Nationale Ombudsman)

Continuation of Table 2.2

Based on roles in governance	**Based on issue of interest**
Autoriteit Persoonsgegevens (AP) / College Bescherming Persoonsgegevens(CBP)	Appeal Committee of the Association of Private SecurityOrganisations (Beroepscommissie van de Vereniging vanParticuliere Beveiligingsorganisaties)
Independent Post and Telecommunications Authority(Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA))	Supervision Council (Raad van Toezicht)
Radiocommunications Agency (RCA)	Chamber of Court Bailiffs (Kamer van Gerechtsdeurwaarders)
Sectorial Supervisor	Complaints Committee (Klachtencommissie)
Health Care Inspectorate (Inspectie voor de Gezondheid (IGZ))	Committee of Supervision (Commissie van Toezicht)
National Ombudsman (Nationale Ombudsman)	Data Protection Officers
Appeal Committee of the Association of Private SecurityOrganisations (Beroepscommissie van de Vereniging vanParticuliere Beveiligingsorganisaties)	*Privacy and Data Protection Best Practices*
Supervision Council (Raad van Toezicht)	International Association of Privacy Professionals (IAPP)
Chamber of Court Bailiffs (Kamer van Gerechtsdeurwaarders)	Confederation of European Data Protection Organisations (CEDPO)
Complaints Committee (Klachtencommissie)	Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (NGFG)
Committee of Supervision (Commissie van Toezicht)	*Research and Innovation*
Non-governmental Organizations (International)	European Union Agency for Network and Information Security (ENISA)
International Association of Privacy Professionals (IAPP)	Innovation and Networks Executive Agency (INEA)
Confederation of European Data Protection Organisations (CEDPO)	ECSEL Joint Undertaking (ECSEL JU)
Non-governmental Organizations (Netherlands)	Bits of Freedom
Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (NGFG)	*Digital Market (Business and Economy)*
Data Protection and privacy interest groups in the Netherlands	Ministry of Economic Affairs, Agriculture and Innovation
Bits of Freedom	Small and Medium sized Enterprises
Vrijshrift	Large Enterprises
Companies and Non-organized Interests	*Individuals Privacy and Data Protection*
Dutch Citizens	Dutch Citizens
Small and Medium sized Enterprises	Vrijshrif
Data Protection Officers	*Fundamental Rights*
Large Enterprises	European Union Agency for Fundamental Rights (FRA)

End of Table 2.2

FORMAL CHART

The dynamics of aforementioned actors in this field are depicted in Figure 2.2. European Union has the highest formal position as the regulator on the European level. It governs member states with privacy data protection instruments, namely EU DPD, EU GDPR and e-Privacy Directive, with Court of Justice of The European Union coordinating enforce law on European level. ECSEL-JU, INEA and ENISA are EU agencies and decentralized bodies that focus on research and innovations. ECSEL-JU and INEA are both mainly involved in pooling experts and in managing projects, particularly in routing EU financial resource. While INEA's re-

search budget is bigger, its focus is rather wide considering its aim on infrastructure of transportation and energy. On the other hand, ECSEL-JU is more specific to the EU's electronic components and systems industry, which relates better with the issue of EU GDPR (e.g. telecommunication and the Internet). ENISA is a centre of expertise for cyber-security in Europe. It helps the EU and EU countries to be better equipped and prepared to prevent, detect and respond to information security problems. These agencies provide practical solutions not only for EU institutions to enrich law disputes and improvements, but also for users of personal data in general to be aware of the current issue and solutions. WP29 is an independent body. Among its functions, it initially worked on generating guidelines and advises for EU institutions and practitioners in general. However, with the upcoming EU GDPR, WP29 will be replaced by EDPB. Besides getting more independence from EC, EDPB will have more legal and supervisory power, and with stronger coordination with EDPS. FRA and EDPS support the EC in providing opinions and comments respectively from the human rights point of view as well as pros and cons from supervisor point of view.

Member states' governors play a significant role in controlling the execution of the European data protection instruments. Initially, Ministry of Economic Affairs in the Netherlands has RCA to regulate frequency matter and on the specific retention obligations of Internet access and telecom providers. The Ministry also works closely with OPTA (which has now merged into Authority for Consumers and Markets; ACM), to monitor market competition and a number of specific sectors and consumer law including EU GDPR. Nevertheless, with a strong recommendation of EU DPD and mandatory requirement of upcoming EU GDPR, AP also takes part in this arena by supervising the processing of personal data. RCA and AP have closed a cooperation covenant, signed on 15 September 2009, detailing their collaboration in the supervision on this specific issue of the sector. Along with these three main supervisors on the nation level (i.e. RCA, AP, OPTA), sectorial supervisors also help specifically on some industrial sector according to the established code of conducts.

Going closer to the level of personal data users, there are assigned DPOs. Public and private organizations and institutions as data controllers/processors are required to appoint a DPO as their advisor and supervisor. The DPO is also a contact point between data controllers/processors with respective Supervisory Authority, in this case with Autoriteit Persoonsgegevens. Up to this point, three main supervisors, each on personal data users, member state, and European level, can be highlted (i.e. DPO, AP, EDPS). The three work closely to maintain the obligations fulfillment pursuant to EU GDPR and to other Union or Member State data protection provisions. Every citizens in Europe, whose personal data are processed within the scope of EU GDPR, may exercise their rights as data subjects. They can file a complaint or request remedy according to the infringement done by data processor. The complaint route are as shown in the blue arrows Figure 2.2. Data subject may complaint directly to the private or public institutions processing their data (arrow 1). If they are not satisfied, they may contact the respective DPO of the data processor (arrow 2). If this is not sufficient, data subject may go to a higher level, depending on the context of the problem. If the respective data processors is a part of European institutions, citizens may go to EDPS (arrow 3b). Otherwise, they can go to supervisor authority (arrow 3a). Finally if this still fails, citizens may seek judicial remedy to Court of Justice of the European Union (arrow 4b) or the ones on the national level (arrow 4a).

Tension in this dynamics arise from an alternative point of view of business and economics. A number of organizations might see this issue to be of restriction to expand their products or services, particularly those in the world of social media or online media. That is why non-governmental bodies exist on national and international level. Each with distinct aims and goals, but with the same pursuit of sharing expertise and representing their members to policy-makers or practitioners alike in order to balance this two oposing views and finding the middle point. Privacy and data protection interest groups in the Netherlands like Bits of Freedom and Vrijshrift are a pool of experts who share, research and make innovation to help individuals protect their own privacy, be it by providing tools or raising awareness through publications. Groups of personal data users like IAPP share their best practices to better manage privacy and data protection in its members' respective organizations. Finally, groups of DPOs also exist. In the Netherlands, there is NGFG that with DPO groups from 4 other countries initiated a European umbrella group for DPOs, i.e. CEDPO. In this light, CEDPO position papers on legislative proposals to representatives of the EU Commission, the Parliament and the Council.

This thesis focus on the marked actors in the blue box. The object of this study to study their perspectives regarding privacy and data protection. Figure 2.2 is helpful to give the idea where their positions are in the middle privacy and data protection world. Particularly in the relation with data subjects and policy-makers as data subjects' representatives.

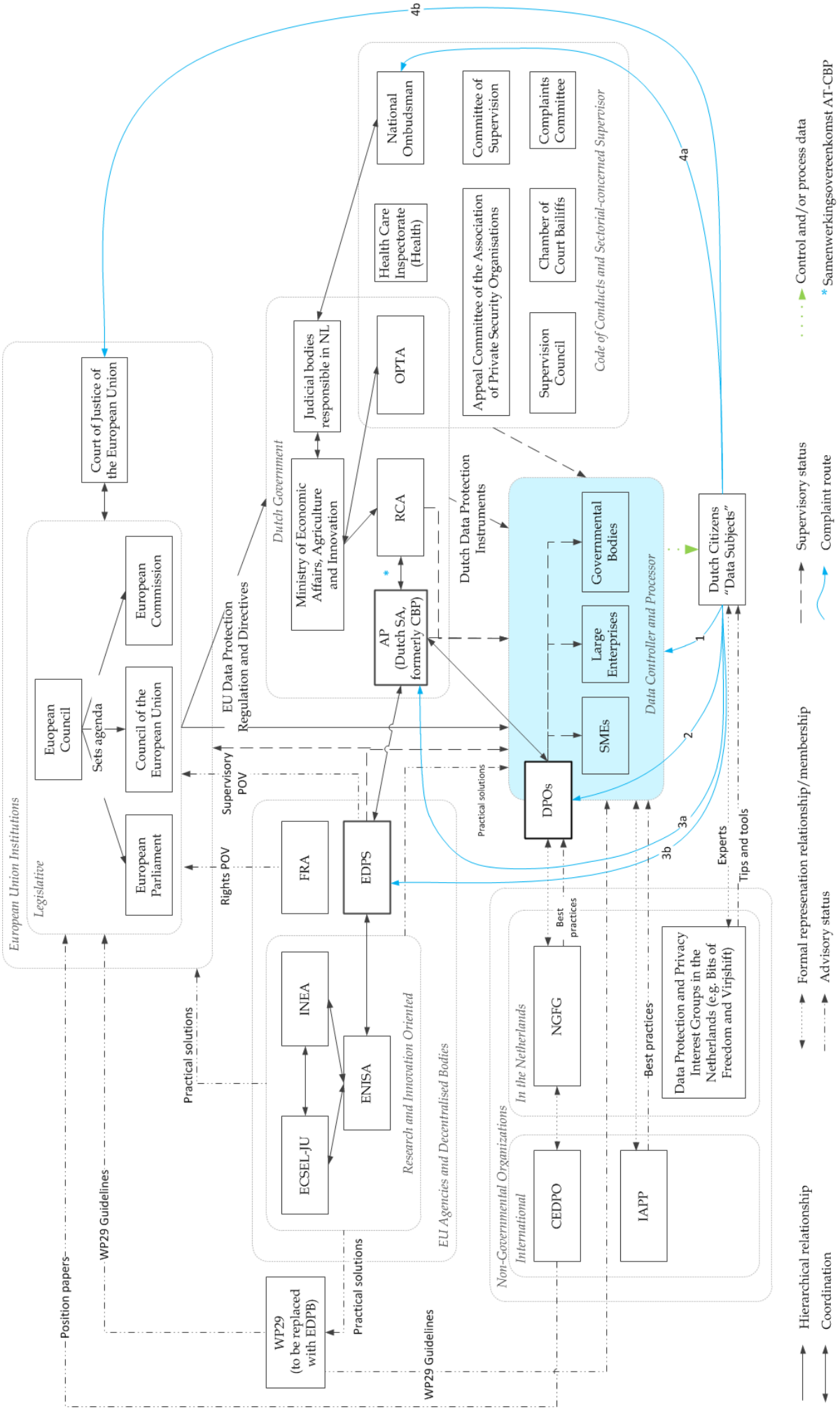


Figure 2.2: Formal Chart for Privacy and Data Protection on EU and Member State Level (the Netherlands)

2.2. REGULATIONS OF PRIVACY

Global data protection scene is exceedingly complex (Bygrave, 2010). Regulatory bodies on the state and international level (e.g. APEC, Council of Europe, and OECD) have formed many regulatory approaches for privacy. In this section, however, we are going to focus our review on several three relevant privacy laws on the European level (i.e. EU DPD, EU GDPR, and e-Privacy Directive) as well as some privacy provisions in the Netherlands.

2.2.1. EU DPD AND EU GDPR

As known, EU GDPR supersedes EU DPD as an active regulation on EU member regarding privacy and data protection. Hence, a number EU GDPR principles and elements are found to be built on top of the previous EU DPD. EU GDPR is a long and extensive text. To highlight and compare both main stipulations, a work by Tikkinen-Piri, Rohunen, and Markkula (2017) is used as a main reference among other literature. The comparison is summed up in the following Table 2.3.

Comparison Between EU DPD and EU GDPR

Principles & Elements	**EU DPD**	**EU GDPR**
General provisions and principles	Article 2, 4, 6,7, 8	Article 1-11 - Extended territorial scope - New definitions: pseudonymisation, genetic data, biometric data, data concerning health, BCD, personal data breach - New provisions and principles: transparency of data processing, accountability, and processing which does not require identification - Clarified/specified provisions: data minimisation principle, conditions for consent and lawful data processing - Added conditions conserning a child's consent in relation to information society services
Transparency and modalities	Article 12	Article 12 - New obligations of controllers
Information and access to personal data	Article 10, 11, 12a	Artcile 13-15 - Specified obligation of the controller to provide information about the controller, data subject's rights and data transfer to third countries
Rectification and erasure	Article 12b-c	Article 16-20 - Data subject's specified rights to rectification erasure and restriction of processing of personal data - Data subject's new right: data portability from one system to another
Right to object and automated individual decision making	Article 14-15	Article 21-22 - Specified right to object to personal data processing, including profiling - Specification relative to the data subject's right not to be subject to a decision based on automated processing

Continuation of Table 2.3

Principles & Elements	**EU DPD**	**EU GDPR**
General obligations	Article 16, 17, 18, 19	Artcile 24-31 - New grounds: principles of data protection by design and by default - Clarifications concerning responsibilities and obligations - New obligations of controllers and processors
Security of personal data	Article 17, 4	Article 32-34 - Extend obligation to cover processors - New obligation of the controller: notifications of personal data breach to the supervisory authority and to the data subject - New obligation of the processor: notification of a personal data breach to the controller
Data protection impact assessment and prior consultation	Article 20	Article 35-36 - New obligation of the controllers: a data protection impact assessment prior to likely risky processing operations - Simplification relative to controllers' obligation to obtain authorisation to process personal data
Data Protection Officer (DPO)	Article 18	Article 37-39 - New obligation of the controller and processor to assign a DPO if data processing operations require regular and systematic monitoring
Codes of Conduct and Certification	Article 27	Article 40-43 - Simplifications relative to approval of codes of conduct: National-level codes of conduct can be directly approved by the supervisory authority - New means to demonstrate the processing operations' compliance with the GDPR: data protection certification mechanisms, seals and marks
Transfer of personal data to third countries or internationational organisations	Article 25-26	Article 44-49 - New conditions for personal data transfers: BCRs, approved code of conduct and approved certification mechanism are new means of appropriate safeguards for personal data transfers to third countries or international organisations.

Continuation of Table 2.3

Principles & Elements	EU DPD	EU GDPR
Remedies, liability and penalties	Article 22,23,24	Article 77-84 - Specifications concerning the data subject's right to a judicial remedy - Extended liability to cover processors - Clarified liability of joint controllers and processors - Administrative fines imposed on the controller and the processor

End of Table 2.3

2.3. THEORETICAL FRAMEWORK

This section discusses the relevant theories for the intended studies. The theories are used as a perspective in seeing the dynamics of privacy and data protection in the real world. The theories are information asymmetry, power asymmetry, stakeholder analysis and planned behavior.

PRINCIPAL-AGENT PERSPECTIVE

The problem of information privacy can be explained using the principal-agent perspective. It is originated from the agency theory that is rooted in the economics of information (Eisenhardt, 1989). The principal–agent perspective virtually applies to all transactional exchanges that occur in a socio-economic system of opportunism, asymmetric information, and bounded rationality (Milgrom & Roberts, 1992). This perspective aims to explain *transactional arrangements* (e.g. contracts) between *self-interested parties* with *incongruent goals* in the presence of *uncertainty* (Pavlou, Liang, & Xue, 2007). Note that it consist of four elements: self interested parties (the principal and the agent), transactional arrangements as usually agreed in contracts, goals or self interest which usually is affected by rationality, and uncertainty which arises with the existence of information asymmetry (Husted, 2006).

The parties are defined as one entity (the principal) who delegates work to another (the agent) who performs the work according to a mutually agreed contract (Eisenhardt, 1989). In the privacy and data protection world, data subjects can be considered as the principal, while data controller and processors (data users) as the agent. This resonates with data subjects delegating the responsibility of processing of their personal data to the data users. The personal data used here can be the main exchanged commodity (e.g. in SNS) or a secondary commodity (e.g. in online transactions), and it should be processed accordingly to the intention of personal data usage laid in agreed contracts in both scenarios.

2.3.1. INFORMATION ASYMMETRY

Using the principal-agent perspective, information privacy issues can be perceived as the agency problem in the agency relationship between data subjects and data users. Eisenhardt (1989) defines difficult or costly effort for the principal to verify what the agent is actually doing (i.e. information asymmetry) as one of the agency problems. In many cases, the principal is the uninformed party and the agent is the informed party. Pavlou et al. (2007) take agency theory into online transaction and define agency problem in a similar nuance, that is: the adverse selection (hidden information) and moral hazard (hidden action), which is the results of the information asymmetry (Akerlof, 1970; Arrow, 2001; Jensen & Meckling, 1976). Or as *Husted2006* argue: Time plays a crucial role in the nature of the information problem that the parties confront. Before a contract is created, the parties face a situation referred to as adverse selection. After the contract, whether implicit or explicit, is created, the principal and agent face another form of information asymmetry known as moral hazard.

This approach can be applied to describe the dynamics of information asymmetry in privacy and data protection world. The advanced ICT, including the Internet, allows the personal information of the data subject to be easily collected by the data user. While on the other end, different space and time makes it hard for the data subjects to know how their personal information is processed after the transaction has taken place. This information asymmetry could create agency problem that can be easily described with the later type of information problem, i.e. moral hazard. Data subjects, acting as the principals, wants their privacy to be

protected through the protection of their personal information containing their privacy. However, cases have shown personal data process that goes beyond the agreed upon contract both intentionally and unintentionally. Intentional privacy invasion includes practices connected with data brokers for targeted advertisements (DNews, 2013; Morris & Lavandera, 2012) and public surveillance (Weaver, 2017; Best, Krueger, & Ladewig, 2006). Other cases of unintentional privacy breaches are due -but not limited to information security breach (Armerding, 2017; Grande, 2016).

Privacy issues through the misuse of personal data is a moral hazard. It is a risk where uncertainty lies within. Personal data misuse does not happen at any time at any place to any personal data. Not all data users do such practices and not all practices is considered privacy invasion when the data subjects agree upon it. The risk or possibilities of this agency problem remains to exist in a form of information privacy concern.

EU GDPR AS A REMEDY TO INFORMATION ASYMMETRY

Agency problem from asymmetric information can be mitigated through the logic of signals and incentives (Pavlou et al., 2007). *Signals* are formulated information by agents about themselves to reveal their true quality and to distinguish themselves from other agents. Sequentially, principals take these signals to carefully select which agents are credible. Signaling is suitable for mitigating the problem of adverse selection. Even though privacy issues are largely the case of moral hazard, some part of the problem can also be caused before the transactions of personal data are done (case of adverse selection). For instance, information of personal data processing is not transparently informed by data users to data subjects (e.g. inadequate privacy policies). Hence, decisions made by data subjects are not based on the best information regarding the credibility of data users candidates. Therefore, some of privacy issue can also be partly be mitigated before the contract begin using the logic of signaling.

Table 2.4: Remedies to Problem of Asymmetric Information (Husted, 2006)

Information Asymmetry	Remedies
Adverse Selection	• Menu of contracts • Vertical integration • Signaling • Transparency policies
Moral hazard with hidden action	• Incentive alignment • Proxies for incentive alignment - Rewards based on past effort or truthfulness - Punishment for unethical behavior - Corporate culture and normative control

EU GDPR depicts the trait of signaling utilization to reduce information asymmetric. For example, Article 13 and Article 14 require information to be provided when the personal data is collected. It advises that the data processing to be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or *will be processed* (European Union, 2016). Moreover, the new requirement of explicit 'opt in' to validate data processing is 'information-forcing' which can reduce information asymmetry. This is due to the fact that it places 'pressure on the better-informed party to disclose material information about how personal data will be used' (Lynskey, 2014). Relevant disposition of the EU GDPR can be found in Article 5, 6 and 7.

Incentives are formulated to prevent the tendency of moral hazard by making opportunism irrational or costly (Pavlou et al., 2007). This makes the logic of using incentive plausible to help solving privacy issue. However, in practice, incentive may not be immediately possible because of difficulties in measuring performance. Nevertheless, proxies may be available in a form of rewards, punishments or control mechanism (Husted, 2006). The information problem like privacy breach can be solved if the third trusted party provides incentives in order the agents to act appropriately and in accordance with the principals (Anastasopoulou, Kokolakis, & Andriotis, 2017).

EU GDPR shows the idea of using the incentives' proxy of punishment. Intentional personal data exploitation is addressed in the early part of EU GDPR in section 1 of the first chapter. It principally requires the process of personal data to be in accordance of the purpose of data collection and that it has to be approved by the data subjects. Unintentional personal data exploitation is addressed in the Chapter 4 in Section 1 in

general and in Section 2 in particular regarding the security of personal data. Negligence of this requirements may result in the imposition of penalties as written in Article 83. The fines can be at the value of minimum ten million Euros or maximum 4% of the data users' world annual turnover. The huge nominal of the fines consequently makes the opportunism costly. For that reason, data users' opportunism is expected to be mitigated. The work of Anastasopoulou2017 supports this statement that regulation enforcing the implementation of fair information practices can be efficient from the social welfare perspective, mainly by limiting the incentives of the firms to exploit the competition-mitigation effect.

2.3.2. POWER ASYMMETRY

In the economics, information holds a significant value. It affects many decision-making processes in businesses, starting from planning, executing, evaluating and even predicting. The one who has more information and make use of it, may gain a lot of benefits or profits. Or in other words, the one with more information wins while the other loses. In a way, information gives power in the market. However, the problem of information asymmetry as above-mentioned can result in power asymmetry, creating an uneven level of playing field. In privacy and data protection field, the result of such power asymmetries makes individual a weaker party who is unable to protect his interests without state intervention. Power and information asymmetries are market failures which data protection legislation seeks to correct (Lynskey, 2014).

EU GDPR AS A REMEDY TO POWER ASYMMETRY

While aiming reduce information asymmetry, EU GDPR also makes a straightforward effort in distributing the power. It does so by giving more rights for the data subjects to decide whether they would like their personal data to be processed. Rights of transparency and modalities, access to personal data, to be forgotten, to data portability and others are set down in Article 12 to Article 22 in Chapter 3. For instance, it imposes an obligation on controllers to adopt procedures and mechanisms to respond to data subject access requests within set deadlines and to give reasons in the event that they refuse to take action. These more effective rights strengthen the hand of the individual data subject vis-à-vis those who process personal data (Lynskey, 2014).

2.3.3. STAKEHOLDER ANALYSIS

The perceiving of data users towards EU GDPR can now be estimated using stakeholder analysis, which is done by analyzing interdependencies of power and resources (Enserink et al., 2010). A hint of game theory is also provided useful in understanding privacy-related behavior (Anastasopoulou et al., 2017).

EU GDPR is a move made by the EU government in favor of data subjects. As a rational entity, data users would like to make the next move to create maximum utility. Generating profit with personal data through the violation of EU GDPR (e.g. processing data without consent) seems to be not possible, considering the expected penalties for privacy breach. A related work by Lee, Ahn, and Bang (2011) that tries to analyze privacy protection strategically, finds that 'as consumers become more concerned about their privacy, it is more likely that all firms adopt privacy protection'. In other words, compliance is the immediate expected result as the first stage of the privacy protection game. Nevertheless, it should also be noted that this move may hinder their initial freedom and power in the market. Despite the fact that comply is a must, the expected impact by data users might be negative and it might affect the way they follow the rule (in the later stage of privacy protecion game.

Complying with rules may not be the same as having the same sentiments with the goal of the rules. It is then crucial to differentiate two major elements building *overall perception of EU GDPR*: 1. *Willingness* and 2. *Expected impact*. The term willingness used here does not describe the psychological condition of wish or desire. Rather, it describes the actual condition and plan to change in accordance with the EU GDPR. Therefore, the term willingness is also deconstructed to 'perceived gap' and 'planned investment to be compliance'. Deconstruction of this variable is due to the term willingness that cannot be solely defined by the planned investment. For example, data user that is not having anything planned cannot be considered to not be willing to adapt. It may be caused by the small gap between its current condition and the required condition by EU GDPR. Willingness is not flexibly valued due to the obligation effect from the regulation. On the other hand, the term 'expected impact', relates more to the sentiments of data users. Determination of its value is more relaxed as data users may still have negative or positive sentiments regardless of its direction towards compliance.

The regulator and business form an authority relationship (arrow 1). It is where a more powerful regulation of personal data processing by businesses is made by the higher active authorities (i.e. EU Institutions).

The European Union, through EU GDPR, aims to improve the attempt of pervious EU DPD in resolving the asymmetry issue. EU GDPR strengthens the control of personal data processing by a) providing legal certainty and transparency, as well as obligations and responsibilities for controllers and processors, b) consistent monitoring of the processing of personal data, and c) equivalent sanctions in all Member States.

The companies/businesses form agency relationship with the customers/citizens. The privacy and data protection regulation anticipated a more controlled citizens personal data processing. Better control in data processing also means more transparency, which results in the reduction of information asymmetry between businesses and customers/citizens. Stronger control on data processing allows a scheme where certain rights of citizens upon their personal data processing are legally enforceable, generating more power for them in the dynamics of economics of information.

Based on the findings in 2.1 as well as theoretical lenses discussed in 2.2 and 2.3, the expected mechanisms of privacy and data protection involving the stakeholders are summed up in Figure 2.3 below.

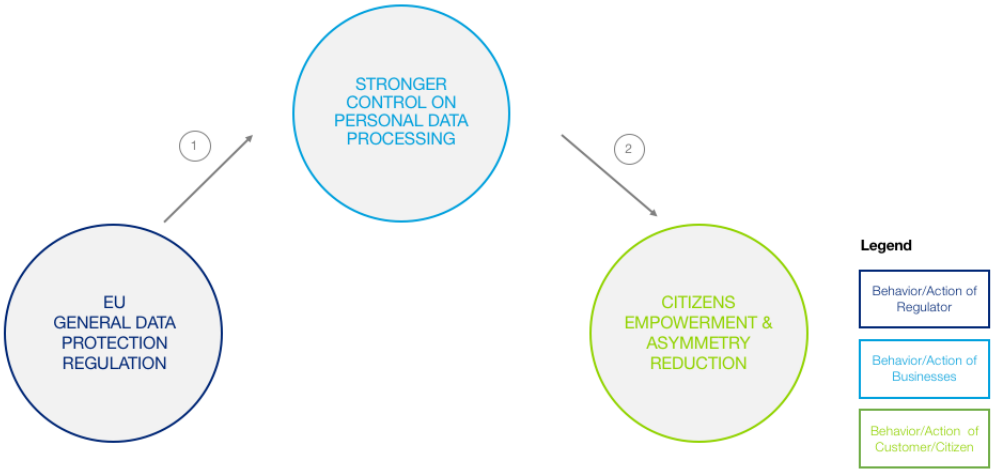


Figure 2.3: Mechanism of privacy and data protection in a nutshell

In a nutshell, the context is as follows. Contracts exist between agent and principal that entail personal data processing. Information asymmetry comes as a result of the agency problem between businesses and customers/citizens. Information asymmetry leads to power asymmetry in the market, which may result in market failure. The lack of power by citizens/customers gives rise to a remedy for the asymmetries that includes higher active authorities.

Up to this point, the aim and expectation of the government from the EU GDPR are known. In the opening remarks of EU GDPR, the aim of distributing power to citizen/customer through the empowerment of their rights is supported with point number 11 and 13 (See the main text of EU GDPR). However, the expectation of the businesses remains as a question, and therefore becomes the object of this study. Expectation of businesses (i.e. data users) is important because it builds perception which in turn shape the way business think and plan to implement EU GDPR. Consequently, the actual changes/behaviors can be predicted as an endeavor to learn the effectiveness of EU GDPR.

2.3.4. THEORY OF PLANNED BEHAVIOR

According to the Theory of Planned Behavior (hereinafter is reffered as TPB, proposed by Ajzen (1991)) , the behavior of an individual/entity can be estimated by its intention to adapt to the behavior itself. The intention is constructed by three main aspects, namely the attitudes, subjective norms, and perceived behavioural control. The definitions of these aspects are borrowed from the theory:

- **Attitudes** refer to the overall positive or negative evaluation of performing the behaviour,
- **Subjective norms** are perception of the entity that assesses if other important people in their life would want them to perform the behaviour, and
- **perceived behavioural control** reflects the extent to which individuals perceive the behaviour to be under their volitional control

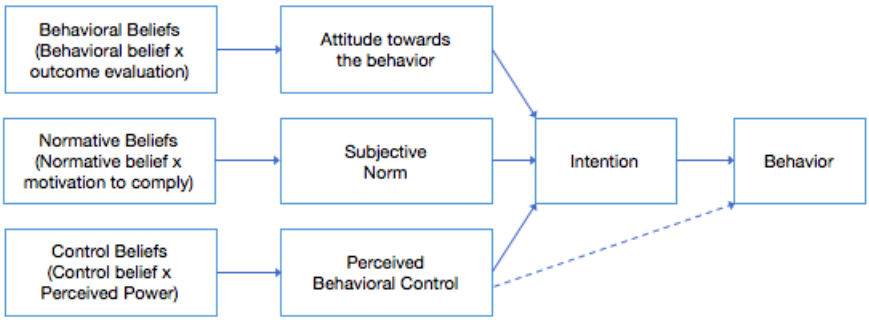


Figure 2.4: Theory of Planned Behavior by Ajzen (1991))

In our case, the behaviour intended is being EU GPDR-compliant, which we refer as 'Actual Changes'. Hence, the entailing intention is meant for the intention to change regarding the EU GDPR. Later, the proxy of the intention to change is defined as the 'Planned changes'. The first two aspects (i.e. attitude and subjective norms) are still relevant for our case. However, the later one is left out. EU GDPR is going to be enforced, and the organizations' control to nullify this is too small at this moment. Hence, to simplify the measurement in the later phase is considered to be irrelevant.

2.4. CONCEPTUAL FRAMEWORK

There is no general understanding on how the perceptions of data users affect the implementation of the proposed EU GDPR (i.e. compliance). A study by (Hartlapp & Falkner, 2009) supported this claim with their findings where substantive theory, conceptual and empirical findings on the implementation of EU policies are ambivalent. The empirical studies are so limited, let alone the theories explaining what factors forming causal relationship in this particular topic.

However, it is possible to build a conceptual model to explain the relations between factors. Based on the above findings, a conceptual framework explaining the factors that influence data user's perception can be seen in Figure 2.5. This framework is not by any means exhaustive, and thus it is wise to note that this framework is formulated to support our venture in generating hypothesis for this study.

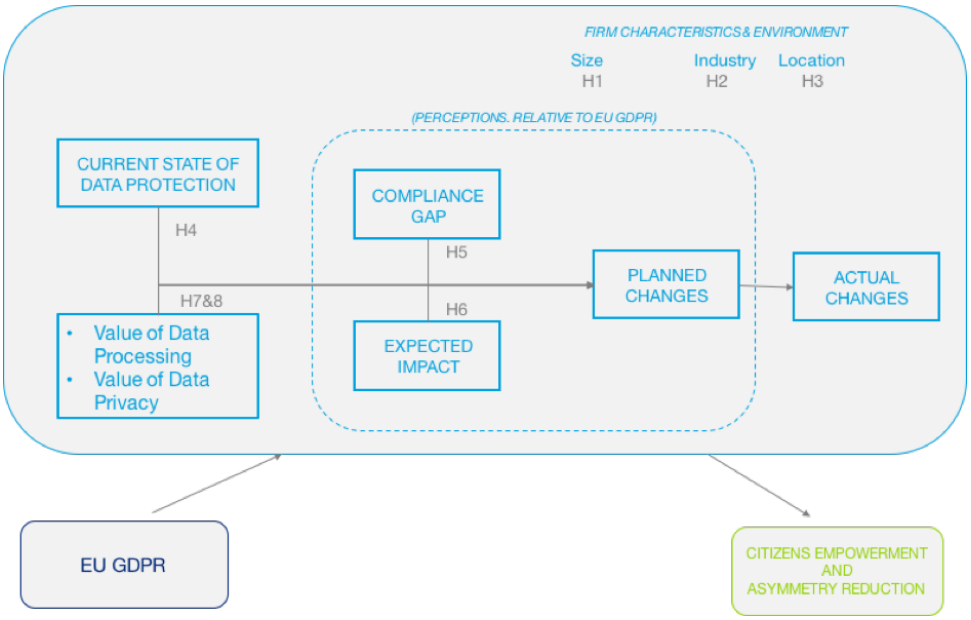


Figure 2.5: Conceptual Model

The aim of this study is to learn their intention to change regarding the EU GDPR **figure 2.4** are presented. As previously discussed, the 'Actual changes' is estimated with 'Planned changes'. Planned changes are the

result from a combination between the organizations characteristics, the organizations' as-is situation and the organizations' perception. Relevant factors explaining the as-is condition are the current state of data protection, value of data processing and data privacy. Relevant aspects explaining the perceptions are as discussed in the TPB, which are the compliance gap, and expected impact.

This high level framework is used as a lens to see the dynamics of privacy and data protection related to EU GDPR, and as a starting point to formulate hypotheses to be test in the following chapters.

2.5. SUMMARY

The literature review covers two main part. The first part is related to the context of privacy and data protection. This part is specifically intended to answer the first sub research question. There are two types of privacy: physical and information. Focusing on the later one, (information) privacy is defined as an individual desire to control or have influence over the acquisition and potential secondary uses of personal data. Protecting (information) privacy, often means protecting the data containing such information. Thus, privacy protection is at times included in the so called larger domain of data protection. Data protection comes in different forms on different level. On individual level, it varies from data disclosure management up to using pseudonyms and giving false information. On the organizational level, data protection is translated into companies' strategies to secure their enterprise data. On the governmental level, data protection is often translated to policy or regulation oriented form.

Important stakeholders in privacy and data protection can be classified into three categories: regulator, users of personal data, and individual "data subjects". Focusing on European level and the Netherlands as a member state example, the regulators can be classified into EU Institutions, related EU Agencies and Decentralized Bodies (e.g. ENISA), related state government (e.g. Autoriteit Persoonsgegevens (AP)), sectorial supervisor (e.g. Committee of Supervision). A list and formal interaction of these stakeholders can be seen in Table 2.2 and Figure 2.2.

Originated from the past principles by OECD and CoE, EU DPD has a similar nuanse in the principles (e.g. transparency, legitimate purpose, proportionality). Following EU DPD, e-Privacy Directive was stipulated to complete the directive focusing on electronic communication. It direct member states on the way they operate their websites related to cookies, their emails for marketing purposes, and their data retention. EU GDPR focuses on a more harmonized system and stronger power distributed on the data subjects. Hence, significant changes can be seen in relevant aspects. First is the obligation of having a supervisory authority for each member state, a Data Protection Officer for each organization, and a clearer information flow in between. Second is the increased rights for data subjects including the right of erasure or right to be forgotten. Imposed fines can also be seen as a significant changes, especially from the practitioners point of view.

The second part of this literature review deals with theory and concepts that will provide a lens for the following part of this studies. A conceptual framework has been made. The focus is to examine what factors that would play roles in affecting organizations intention to behave according to the EU GDPR. The estimated factors are the three control variables (industrial sector, regional footprint, and size). Others are the organizations perception on their gap with being compliant, expected impact from being compliant, value on privacy and data protection and their dependency on processing personal data.

3

RESEARCH METHODS

This chapter delineates the approach and methods used throughout this study. Section 3.1. discusses the approach and design of this research. Section 3.2. describes what research methods are chosen and how they are performed.

3.1. RESEARCH APPROACH AND DESIGN

Mixed method is chosen for this research approach. Mixed method is an approach of study that involves collecting both quantitative and qualitative data, integrating the two forms of data, and using distinct designs that may call for theoretical frameworks (Creswell, 2013). There are numerous different terms used for this approach, such as *integrating, synthesis, quantitative and qualitative methods, multimethod,* and *mixed methodology* but recent studies tend to use the term *mixed methods* (Bryman, 2006; Tashakkori & Teddlie, 2010; Creswell, 2013).

According to Greene, Caracelli, and Graham (1989) and Niglas (2004) rationales to choose mixed methods as a research approach can be classified into at least sixteen scheme (Bryman, 2006). The decision in choosing mixed method for this research follows seven of those rationales. It begins with the *offset* of the methods that each qualitative and quantitative approach entails (Creswell, 2013). This understanding opposed with *different research questions* calls for both approach to be utilized. Qualitative approach is required to provide *contextual* concept for the the the first two sub research questions. The generated knowledge is then employed to *develop instrument* of quantitative approach, which is to have a better wording and concept for a survey can be generated. In this case, an *expansion,* where the breadth and range of enquiry are extended is achieved. Hence, a *complete* better answer to research question can be derived.

Further, this research can be identified with the **exploratory mixed methods** type of design. There are several classifications of mixed methods designs (W. & Clark, 2010; Creswell, 2013). However, the exploratory one is chosen as it fits the flow of sub research questions by character, in which a qualitative phase is performed first followed by a quantitative phase. The qualitative phase generates a conceptual framework to answer the first and partly second sub research questions with a constructive perspective. See Creswell, Hanson, Plano, and Morales (2007) to learn more about constructive perspective. Subsequently, the quantitative phase is preferred to better generate a more generalizable enquiry. Thus, phenomena of EU GDPR implementation across business sectors may be deciphered to answer the later part of the sub research questions.

Following the nature of the research questions, a number of qualitative methods will be carried out. The first method is the literature review. The review is salient in the initial phase to build a conceptual model and to investigate the benchmark in data protection. The addressed issues of the questions have been broadly discussed in the literature. The results from this phase will be employed as the foundation to investigate data protection in practice, which will be carried out using the next method of interview. Further, the results are going through instruments development as a preparation for the quantitative phase, generating a set of survey questions. The proposed methods, motivation, and the intended sub-questions are summarized in Table 3.1.

Table 3.1: Research Methods

SRQ	Research Method	Motivation
1	Literature review; Stakeholder Analysis	The addressed issues of the question have been broadly discussed in the literature. Stakeholder analysis will provide a thorough analysis on the role actors involved to answer SRQ 1b. The results are salient to point out the importance of businesses and their business interests as well as other pivotal players' perspective.
2 – 3	Semi-structured interviews; Qualitative data analysis (General Inductive Approach)	As stated in the text. Subtle organizational dynamics that drive privacy policies and practices are more complex to data collection techniques such as written surveys. With interview, more insights on these dynamics can be better explored.
3 - 4	Survey; Quantitative data analysis;	The empirical findings gathered from survey are analysed further through the lens of policy analysis of multi-stakeholder. As stated, the Directives and Regulations as the subject of the intended RSQ makes it falls into a political discourse. Policy analysis is a broad field that includes the activity of research and analyse policy-relevant issue.

3.2. RESEARCH METHODS

3.2.1. INTERVIEW

SCOPE DEFINITION

The interview is carried out within the Netherlands as the translation of the directives varies for each country (Bygrave, 2010; EU 2016). The time available for the research did not allow for a thorough investigation for multiple countries. However, the result of this study is still noteworthy as the Netherlands has always made relatively extensive use of industry-based codes of practice, which is encouraged by EU DPD (Poullet, 2006; Bygrave, 2010). Hence, more varieties between sectors are expected.

INTERVIEW PROTOCOL FORMULATION

Prior to the interview execution, two major steps are to be carried out. The first step is formulating the interview protocol or interview schedule. Interview schedule contains lists of questions to be asked to the interviewees. The questions are formulated to shed some light on data protection interpretation and implementation in practice. The questions are composed with knowledge acquired from the literature review. Further, the list of questions are sent to experts in field to check the relevancy or if additional questions are necessary. Appendix A depicts the list of the formulated questions.

INTERVIEWEE SELECTION

For this empirical study, two types of interviewees are identified: semi-structured business representative and expert interviews. The semi-structured business representative interviews have several representatives of business sector from chosen companies as the respondents. The expert interviews have individuals equipped with expertise in the field of privacy and data protection as the interviewee. Having both business representatives and experts, the external validity of this research is enhanced, since experts generally are less bound by the course of events in one company or specific business sector.

The interview structure for both types are similar. However, the interviews with business representatives might indicate specific phenomena in a particular business sector or company. The interview with experts shed some light to a more general phenomena of data protection and implementation by businesses or other entities.

The 'purposive sampling' or 'criteria-based' was chosen as the most appropriate. Since the quality of the study strongly depends on the knowledge of the interviewee related to the realm of data protection, the following list of criteria is applied in the interviewee selection process in general.

1. The interviewee must have extensive experience in data, privacy protection and/or cyber security (5 year+ or recently educated) with proficient knowledge regarding the company he represents (3 year+ or recently educated).

2. The interviewee must hold a key data, privacy protection, cyber security, and/or Internet law related position.

Business Sectors Representatives A contextual analysis within multiple companies or organizations (entities) is likely to give a comprehensive understanding of the implementation and interpretation of Data Protection Acts by businesses. Each company or organization has specific way in interpreting and implementing Data Protection Acts. Hence, it would be appealing to have interviews with all entities within each business sector, both from public and private sector. However, that option is not feasible due to the time limitation for this research. A critical selection shall be made to choose companies and organizations that are assumed to be representative for each business sector. This process will be done with the aim to make the results of the study generalizable to for each business sector. The following selection criteria are to be used in choosing the presumed representative companies and organizations (entities).

1. Year of establishment of the representative entity
2. Number of employees and/or customers
3. Entity's exercise of personal data
4. Multinational characteristics
5. Annual turnover/revenue

The decision to use the above criteria is based on the needs to classify the size of the entity, the employment of personal data and the availability of information in the literature.

There were 6 interviewee available from a range of interview. A complete list of approached interviewee candidates can be seen in Table 3.2

Table 3.2: Interviewee Candidates

Candidate Code	**Organization**	**Industry**	**Footprint**	**Size**	**Approaching Method**	**Result (Interview Duration)**
CITV1	n.a. (ITV01)	Energy	Global	Large	Referenced Email	Approved (47 mins)
CITV2	No13	Fashion	Local (Delft)	Small	Email	No response
CITV3	Cult Beauty	Beauty	National (UK)	Large	Email	No respones
CITV4	n.a. (ITV 06)	Supervisory Authority	International (EU)	Large	Direct encounter & Email	Approved (20 mins)
CITV5	TU Delft	Education	Local (Delft)	Large	Email	No response
CITV6	n.a. (ITV02)	Education	Local (Delft)	Large	Referenced Email	Approved. (43 mins)
CITV7	NS NL	Transportation	National (NL)	Large	Referenced Email	Candidate Unavailable
CITV8	Ziggo	ICT	National (NL)	Large	Email	No response
CITV9	n.a. (ITV03)	Consumer goods (drinks)	National (NL)	Large	Referenced Email	Approved (40 mins)
CITV10	Hogeschool	Education	Local (Utrecht)	Medium	Referenced Email	Candidate Unavailable
CITV11	n.a. (ITV04)	Consultancy (privacy and legal)	National (NL)	Large	Direct encounter & Email	Approved (49 mins)
CITV12	n.a. (ITV05)	Chemical	Global	Large	Referenced Email	Approved (62 mins)

3.2.2. SURVEY

To answer the third and fourth questions, the research needs to be descriptive where assumptions has to be initially made. A survey is a good way to test formulated assumptions to better describe the current situation of companies perceptions on the EU GDPR. Therefore, insights from previous phase in literature and interview are used to develop the survey.

A survey is also beneficial for this study particularly due to its power in gathering a widespread data in a short time. Like many researches, this study is bound to a limited time period. On top of that, the object of this study is rather broad: companies in general, and companies within EU in particular. Survey method makes it possible to have enough widespread data in order to make a generalizable findings.

There are at least two disadvantages that need to be aware of: unanswered/unfinished questions, and finished yet biased responses. Not understanding the question or feeling that the survey too long are the two plausible reasons for the first issue. A pretest on practitioners was done to mitigate this. Then, feedbacks were implemented before the survey was published. Moreover, to limit the length of the survey, it is decided to leave only the important aspect as mandatory questions. Noting the target of this survey target, which are mainly executives, the mandatory questions are limited to a small number so that it is possible to finish the survey in less than 6 minutes which is a total of 10 mandatory question. Moving on to the second issue, survey targets tend to give a socially accepted kind of answers, hence the biased responses. Especially when it comes to a legal aspect where their companies' reputation may be hampered. To limit this happenstance, the survey is designed to be anonymous. Neither respondents identity nor the companies name are asked in the survey. However, necessary demographics information is still included to make room for an intact overview from the results.

There are numerous ways on how a survey is implemented. However, studies on one's perceptions, more often than note, use likert-scales. A likert scale is symmetric scale, usually comes in 3 or 5 points-scale. Middle point is where the neutral option lies and the smallest number represents the opposing value with the largest one (e.g. Strongly disagree, disagree, neutral, agree, strongly agree). It is decided to take the 5 point-scale in order to know better the respondents valuation on a statement compared to the 3 point-scale which does not give much added information than the yes/no type of question.

The survey is designed to focus on respondents' perception. This is aligned with the aim of the study encapsulated in the conceptual framework: to get understand the intention of companies by understanding their perceptions related to EU GDPR. Besides respondents perceptions, it is also important to take notes on the demographics information. Demographic information is salient to check whether the sample represents a good variation of the population and to check if there are other influencing factors contributing to the companies intention.

SAMPLING APPROACH

The sample of this research is a subset of targeted population, which are companies and organizations (data controllers) in general. To limit biased answers as much as possible, targeted survey respondents are companies' or organizations' representations who understand privacy and data protection within the company. Instead of limiting the scope at the first phase, it is decided to take a pragmatic approach where the survey is spread to as many plausible respondents as possible. Hence, a more general point of view can be comprehended.

To get through the targeted respondents in a short time, it is most convenient to do the survey with an online questionnaire. Noting the drawbacks of having questionnaire considered as spam, two approaches are used: direct email invitation and webpage survey invitation. Direct email invitation is an approach where the invitation link to the survey is shared via an email from Person A to other people that mutually known him. Other approach is through a webpage survey which was hosted by Deloitte. Having relevant visitors through the webpage helps a lot in capturing people attentions to be a respondents. However, the conventional way of sending links to a group of experts were not left out despite the fact that this approach did not give significant number of respondents. Moreover, having a low number in response is one thing, having a high number of responses as spam is another thing. To limit this from happening, device limitation was utilized. Only one response can be collected from one device. In the gathered result, there possibility of having spam answers is unlikely. Several utilized survey sources are summed up in the following table.

BUILDING EMPIRICAL MODEL

There are many ways to measure the building blocks depicted in the previous conceptual model (See Figure 2.5). Different variables that could add attributes to the concept are listed as seen in the following Figure 3.1. All of these variables were included in the survey questionnaire.

Table 3.3: Survey Channels

Survey Collector	Distribution Method	Responded Invitation
Deloitte Website	Webpage site	143
Weblink TUD	Direct Invitation	7
Weblink Personal Network	Direct Invitation / Thread in a group	27
Weblink Trade Attache	Direct Invitation	13
Weblink LPDP Endowment	Direct Invitation	3

Looking at the collected data, some variables are too limited for further measurement and data analyses (marked with grey fonts). Fortunately, both variables to measure organizations' plan (*Planned Investment* and *Considered Internal Changes*) are quite robust, which are decided to be our dependent variable. Removing all the limited variables leads us to the empirical model as seen in Figure 3.2.

From the empirical model, a set of hypotheses are then formulated to answer the research questions. Sub-research question 3 can be answered by looking at the static description between dependent variables and the independent variables. Meanwhile, to answer sub-research question 4, the dynamic relation between the dependent variables and the independent ones are necessary. The following hypotheses are to meant to predict the relations between the dependent and independent variables shown in the empirical model. There are 8 hypotheses formulated, of which 3 are related to the control variables. The following hypotheses are tested and presented in Chapter 5 of this report.

- **Hypothesis 1: Companies having footprints in EU will plan more changes related to EU GDPR** - The EU GDPR is originated in the EU. Despite the fact that the regulation applies to any organizations processing personal data of EU citizen, the locations of the organizations might play a role in a the willingness to comply. The level of awareness for organizations far from EU are likely to be lower than the ones in EU. Hence, different amount of planned changes are drawn for different organizations at different parts of the globe.

- **Hypothesis 2: Larger companies will plan more changes related to EU GPDR** - The size of the companies/organizations is defined based on its annual revenue. As stipulated in the regulation, a non compliant will get fined between 2-4% of their annual turnover. The larger the size, the more money is at stake. For big organizations, the impact received from a disaster can be bigger due to several reasons. The larger attention is put on them, the larger the system got affected. Therefore, amending an accident, if not well prepared, might be more of a hassle for big companies compared to the small ones. As a result, more changes my be considered by the larger companies when it come to EU GDPR.

- **Hypothesis 3: The magnitude of planned changes by companies differs across industrial sector** - Different industrial sector, focus on different resources to gain profit. For instance, organizations in media sector utilized personal data to have a more effective advertising impact. Others, such as mining, might not consider personal data as a big of importance. Hence, significant difference of planned changes among measured industrial sector can be expected.

- **Hypothesis 4: The existence of Data Protection Officer will lessen the changes planned by the companies** - From our interview, it is found that designating a DPO is considered to be a challenge. Hence, the existence of a DPO would mean one thing crossed the from their to-do list. Hence, having a DPO might lead to less planned changes.

- **Hypothesis 5: Companies that perceive higher compliance gap with EU GDPR will plan more changes related to EU GDPR** - This hypothesis is built upon the Theory of Planned Behavior (TPB). The perceived social pressure to perform the behaviour affects their intention to adapt such behaviour. In this case, the larger gap perceived by the organizations, the further they are to the condition of where they are supposed to be. Hence, the higher the compliance gap with EU GDPR will give incentive to lessen the gap, and thus more changes related to EU GDPR are planned.

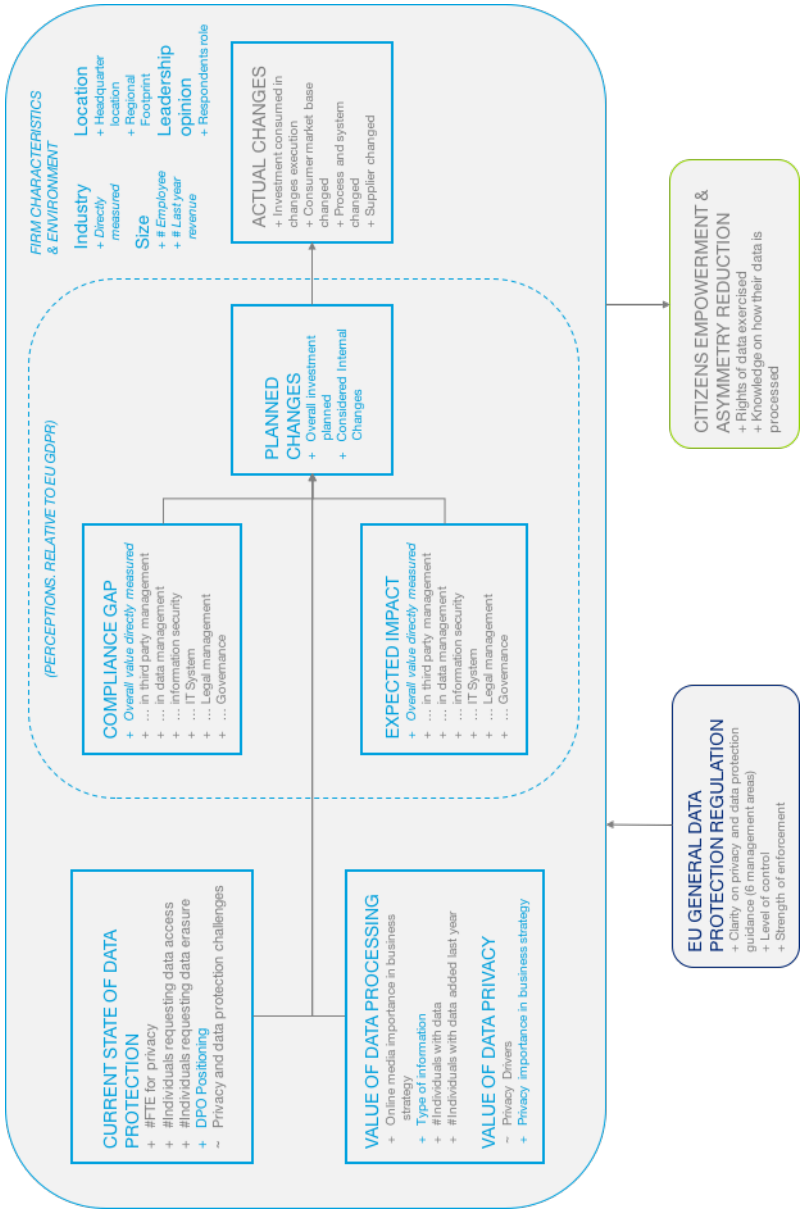


Figure 3.1: Conceptual Model with Measuring Variables

- **Hypothesis 6: Companies that expect more positive impact from EU GDPR will plan more changes related to EU GDPR** - This hypothesis is also built upon TPB. In this case, organizations' favorable or unfavorable evaluation or appraisal of being EU GDPR compliant affects the intention of becoming compliant itself. If the companies expect more positive impact from posing a certain behavior, then the intention to plays such role becomes more favorable.

- **Hypothesis 7: Companies that place a higher value on data privacy will plan more changes related to EU GDPR** - Companies that place a higher value on data privacy would have a similar perspective with the aim of GDPR. Protecting the privacy and personal data of their customer may have become their core of attention. In that case, their considered plan in the future may already be in accordance with the EU GDPR.

- **Hypothesis 8: Companies that place a higher dependency on personal data processing consider less changes related to EU GDPR** - The more benefits received from personal data processing, creates a higher dependency on personal data processing. However, companies might consider the implementation of EU GDPR to be a stumbling block in maintaining the profits/the supporting system. Not

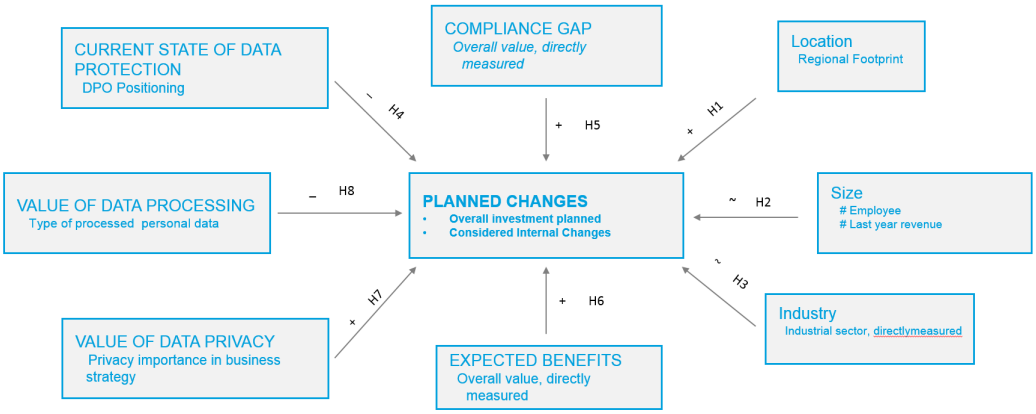


Figure 3.2: Empirical Model

wanting to limit their profits might lessen their willingness to change. Hence, less plan are considered.

4

Interview Results

This chapter presents and compare the findings from conducted interviews. The structure of this chapter follows the interview protocol: the importance of personal data, the existing operations of privacy and data protection, and the future plans considered by the organizations.

4.1. The Importance of Personal Data

4.1.1. Personal Data Processing in Creating Value

Mainly there are two types of data collected by all institutions, their employee data in the upstream level and customer data in the downstream level. ITV01, ITV02, and ITV05 mentioned that they collect the personal data of their employees for company internal values. ITV01 also mentioned to store the data of 3rd parties' employee that have contract with them. ITV05 elaborated more in that they would only collect data that has a clear relationship to the company, and will not use the data to a granular level detail unless there is a justified cause. Additionally, ITV01 mentioned that they collect a limited data of their IT contracts.

In the downstream level, the customer's data from the business-to-business (B2B) chain and business-to-customer (B2C) chain are both collected. ITV05, a company which usually deals with B2B data, collects its B2C data through a CRM system that they use when working with business clients, while ITV01 and ITV03 did mention that they store their B2C data but did not mention the data gathering process.

It is also understood that most companies that work in the retail sector will use the B2C data for marketing purpose. The B2C data gathered would be analyzed to generate an added value to the company. ITV01 mentioned that they use the B2C data for marketing purposes, e.g. loyalty program, mobile applications. ITV03 gathers their B2C data through recording e-commerce transactions and operations which includes the use of the company's website, other data is gathered through customer care where customers could give feedback and questions on products. In contrast to ITV01 and ITV03, a different use of personal data of customers is shown by the ITV02. They prefer using demographics to show their rate of success. They do not do advertising or marketing, so the use of personal data would not affect their value-streams.

4.1.2. Perceptions on EU GDPR

ITV01, ITV04 and ITV06 agrees that there are not many new requirements imposed by the EU GDPR. ITV02 and ITV03 also mentioned that the requirement of having a DPO required by the EU GDPR is already a demand of the Dutch law. However, there are at least three new things that are considered to be unaccustomed and need extra attention:

1. The first one is the significant amount of fines imposed. It forces personal data protection to be carried out into the discussions on the managerial level (ITV01 & ITV04). This change is also seen as EU GDPR giving the National DPAs more power to give sanctions or other type of enforcement in order to ensure the fulfillment of privacy and data protection by data controllers (ITV06).

2. The second is the breach notification process. Incorporating a standardized process to notify supervisory authority is considered to be a novelty within the management. (ITV01)

3. The third one is data portability. Although considered as something new, it is not considered to be very critical. This is due to the high relevance to its technical aspect per se, which is already well taken care by the responsible third party. (ITV01)

Aside from the perceived major changes in EU GDPR, other additional requirements can be seen as small modifications built on top of the previous laws.

1. Risk-based approach enfolded by EU GDPR. It requires the data controller to ensure a level of security appropriate to the risk. The requirement to do a risk assessment is put in a more explicit way (ITV04)

2. The obligation to determine dedicated Data Protection Officer (DPO). DPO will hold a crucial position in the application of EU GDPR with many responsibilities entailed, especially with respect to reporting and accountability related tasks. (ITV04)

3. The involvement of privacy in business processes. Ensuring every process has taken privacy into consideration would fulfill the principle in both Privacy Impact Assessment (PIA) and Privacy by Design embodied in EU GDPR. (ITV04 & ITV06)

4. The data subjects' rights towards their personal data. Most of those rights have been promoted in the past Directive. The change made is that, when requested, those rights shall be made available to be exercised electronically (ITV04).

4.2. EXISTING OPERATIONS OF PRIVACY AND DATA PROTECTION

4.2.1. DAILY OPERATIONS AND COMPANY STRUCTURE

Day-to-day operations differ for each company/organization. Each company has a unique procedure, with different person-in-charge, time and policy throughout the data life cycle (gathering, using, retaining, processing, transferring, and deleting). ITV01, ITV02 and ITV03 explained about their operations clearly while others did not.

ITV01 admitted that PbD-wise, their privacy is not mature in operational. The stakeholder of the operation is the business process owner, legal department and IT department. If there is a breach the IT, legal and risk management are involved. IT team is responsible to ensure the technical measures protecting the personal data are up and running. Moreover, IT team is where the occurrence data breach is noticed at the first place. Then, Legal team is obliged to notify the acknowledged data breach to supervisory authorities. Risk management team would then articulate the risk management from the data breach.

ITV02 explained that all data containing person identifiable information is protected, and an authorization table which assigns the data to each role is linked to that information. Personal data is protected in the whole process, so only the people who need the data in to perform their job-related activities has access to the data. In some crucial processes, a number of check and balances activities are performed to assure that nothing goes wrong.

ITV03 uses a third party to process personal data, where the privacy policy shown in the company website states clearly the involvement of a third-party processing gathered data. There are at least 4 people taking care of privacy and data protection in the company. These people are spread in different departments as an IT risk manager, an IT risk officer, a security officer and a legal counselor. Further, there is a dedicated DPO for the company at the global level. However, there is no formal position for DPO in national level, though the legal counselor is informally assigned as the national-level DPO. The company has been audited to ensure its privacy and data protection meets a good measure

ITV05 mentioned that they have a corporate privacy officer within the company, though they do not know whether the role is the same with the DPO mentioned in the GDPR. Their director of compliance is referred as CPO.

4.2.2. THE EXERCISES OF DATA SUBJECTS RIGHTS AND DATA BREACH NOTIFICATION

ITV01 explained that there are two streams where request of data access/update/deletion are flowing: requests flowing from the employees and requests flowing from the customers. Requests from the employees can be directly done via an internal portal where the employees can edit their personal data themselves. On the other end, requests coming from the customers will have other two different points depending on the level of its significance. The most common ones are handled by the service center, while a more significant case can go through lawyer and legal approach. The most common ones are handled by the service center,

while a more significant case can go through lawyer and legal approach. In a case of data breach incident, there are 3 things required to be done. The first one is scoping. In scoping, the severity of the data breach incident is diagnosed. The second one is containing. In containing, measures to ensure that the data breach will not spread wider takes place. The last thing is reporting, which is usually done by the legal team.

The right of data access/deletion/update for ITV02 could be done through using the e-service or from the service-point desk. This goes for employees and customers (students). They could chose to hide all their information except name and email. ITV02 explained if a data leakage happens, the person involved will be informed in maximum 72 hours. There is an IT responsible for the process and there is a security privacy manager who is also in-charge. There is a team of people who monitor the firewall and also the databases. If a problem occurs they will need to report to the functional privacy legal personal who is a part of the legal department. These incidents are also reported to the board of directors.

ITV03 has defined a formal process to report Personal Data Breach Notification (PDBN). This process has been done two times. The result was a decision to not report the related PDBN as it was considered as a security breach, not data breach. Moreover, the company is in the middle of implementation to define a procedure to handle data subjects' requests, e.g. request to access or modify data. However, it might not be considered as top priority as there has been no major requests so far. Further, has an internal privacy policy defined to guide and control privacy protection within the company. However, there is no Binding Corporate Rules closed to handle privacy and data protection with other Heineken members outside The Netherlands.

ITV05 has a Binding Corporate Rules (BCR) that anticipates on the GDPR as much as possible including a data breach procedure.

4.2.3. CONTROL ON COMPANIES OUTSIDE THE NETHERLANDS AND EXTERNAL LEGAL COUNSEL

ITV01, ITV03 and ITV05 coordinates their privacy and data protection with member firms outside the Netherlands. ITV02 does not have any firms in other countries. There are some companies such as ITV01 and ITV03 that works with third parties (external legal counsel) for data protection. There are also companies such as ITV01 that does not have external legal counsel due to the size of its own company.

ITV01 has obtained authorizations for Binding Corporate Rules (BCR) with the Dutch DPA as the lead DPA to handle privacy and data protection with your member firms outside The Netherlands. This company does not do lots of external legal counsel since the company is a sizeable company. ITV05 stated they also have a Binding Corporate Rules (BCR). They have a global system with limited access. The nine largest country within this company uses this system, while others use local systems with a standardizes interface of the same system. The company also has a separate payroll system with similar behavior.

ITV05 mentioned that the privacy statement of this company is done with a third party, where you could see it on their website. ITV03 also uses the service of a third party regarding privacy and data protection, which is an external legal counsel.

4.3. FUTURE PLANS

ITV04 predicts the expansion of the territorial jurisdiction of EU GDPR will be problematic. On the one hand, it solves one major problem of the past EU Data Protection Directive, which is the lack of jurisdiction over controllers outside the EU processing a multitude EU data subjects' personal data. On the other hand, deciding the proper applicability of EU GDPR to particular cases becomes more uncertain. EU GDPR manages to clarify its territorial jurisdiction for two scenarios. The first scenario is where the processing is done in the establishment of Data Controller/Data Processor. In a company point-of-view, ITV05 mentioned that the GDPR is limiting though it is not a showstopper since it can be resolved in the backstream with digital measures. Then there is overall retention, portability of data that's related to the cloud but also independently.

ITV04 also pointed out that companies by large are now in the early phase of preparation. Where ITV01, ITV02 and ITV03 has shown progress in implementing the EU GDPR. Assessments determining the gap between current condition and the ideal shape that is laid out in the new EU GDPR are their current focus. At the same time, the discussion to appoint DPO is reaching the peak. Organization structure alone does not necessarily represent the readiness of EU GDPR. Of course, bigger organizations would have more leveraged functions, giving higher chances for them to be more equipped. However, small organizations may also do well without having a distinct function in privacy. Nevertheless, the existence of a DPO could hint on their awareness with regards to EU GDPR. Public authorities, in particular, should move fast in resolving this. Many public authorities have not defined one yet while the process to add new functions in typical bureaucratic or-

ganizations would take a long time. With the end of 2016 approaching and the time limit in 2018 when EU GPDR takes place, the decision should be made soon.

ITV01 finds the privacy by Design as it involves a fundamental processing activity. Meanwhile, there are many activities that have been established before the privacy and personal data protection draw a lot of attention. Currently the company has no change plans regarding to the new regulation, though there is a project going on with an aim to assess the gap between the current condition with the new requirements imposed by the EU GDPR. The gap assessment includes aspects around Privacy by Design, actions and necessary stakeholders to be involved. There is no specific budget for this project, with 8 people working per around 12 topics.

ITV02 has already implemented the change of policy in the EU GDPR by using a two-factor authentication system so we could make sure if that people access from outside the organization were in fact authorized employees who have authorized to access that data. They are also planning to make the same procedure for data that is not necessarily privacy related but are sensitive in next couple of months. But they don't know about the e-privacy directive.

ITV03 make 8 actions have been done as a result from the privacy and data protection gap analysis. The 8 actions are as follows:

1. Standardization privacy statement Privacy statements in the websites of Heineken members is made more aligned to the applicable laws.

2. Adjustments for 'cookies' Approval to get cookies is ensured and made more explicit in the website.

3. Modification for privacy policy Privacy policy is not being reformulated to not only talking about employees, but also to the customers (B2B and B2C) as well as related third parties.

4. Reassessment to agreements with third parties Agreements with third parties are being reassessed to ensure that privacy and personal data is still well taken care.

5. PDBN process As previously mentioned, a formal process for PDBN has just been defined.

6. Maintain registered privacy processing The focus has shifted from only maintaining personal data protection the registered data to also maintaining the data moving within the system to third party.

7. Stricter access of passport and identification Unless you are an authorized person with a clear goal to access them, no one can access passport and other identification.

8. Storing protection enhancement Protections for storing and related systems are more enhanced.

ITV05 has started this process on 25th of August 2014. They have already passed the implementation phase, which is for two years, so they has a lot of pieces of a puzzle already in place. They are now working on the implementation of the privacy rules. They will need to make a steering committee that have a vision where we want to go to provide us with the roadmap to put all the pieces in place in a right way, making sure that it's complete, effective, and making sure that the process and awareness are all at the right level towards March 2018.

4.3.1. THOUGHTS ON E-PRIVACY DIRECTIVE

If questioned about the revision of the e-Privacy directive, ITV01 as a company, would want to abolish the rules about cookies. ITV04 analyzed in spite of trending movement in preparation to face EU GDPR, opposing reaction from the companies is also expected. Some companies are more in a passive position, waiting to see how the enforcement will take place, especially in UK, Ireland, and Sweden. Making the policy is at times rather easier than acting on it. Stronger enforcement leads to more effort needed to carrying them out. With regulators' current struggle in increasing the power to control the execution of privacy and data protection, a pattern of actions is expected. Regulators might give much attention towards big companies like the ones in Silicon Valley (e.g. Google, Facebook) or pick one case where incompliance is already visible. By doing this, regulator's chance to win the case will be higher while creating precedents of cases which will be useful if there is a case with smaller companies. Hence, significance benefit could be yield with the lowest effort given.

4.4. SUMMARY

Personal data processing is important to create value. All three of employee, customer and third party personal data may be processed to generate insights for the company. Such insights may be used for marketing purposes or a performance analysis (e.g. success rate). EU GDPR is seen to impose both major and minor changes to their business operations. Changes considered as major focus on the fines imposed, strict data breach notification process, and data portability. Minor changes revolves around the use risk-based approach in treating privacy and data protection, designation of a DPO, involvement of privacy n business processes and fulfilling the data.

Main takeaways we take from this interview results are threefold. The first one is that most companies use personal data to some extent in their business value. Second is most companies are in a condition of not knowing where to start. They tend to wait on others and more directions. This is due to many requirements imposed and that governance is considered as a significant gap. Third is companies that have put a good attention of the past EU DPD think that there are not much left to do to meet the requirement of EU GDPR.

5

Survey Results

This chapter presents the results of various analysis performed on the gathered data. The first section explains the distribution of the data sample using descriptive statistics to provide a general understanding on the data and respondents characteristics. The second section provides a summary of the hypotheses testing that was performed using various statistical tools. Finally, the third section depicts the multivariate analyses and the entailing regression model as an answer to the research question. The online questionnaire used to obtain the data can be seen in Appendix B.

5.1. Analysis Of The Sample

5.1.1. Data File

The data file was analyzed and cleaned with help of the SPSS. As a first step, variable treatment was done. Irrelevant variables were removed, complicated variable names were simplified and labels for values of each variables were added when necessary. Afterwards, data treatment was executed. Empty, incomplete, or trial cases were deleted. Extreme values were identified, and those who were likely to be mistakes were either corrected or removed. Appendix C presents the details of this data treatment process.

5.1.2. Descriptive Statistics

This survey collected information from a wide range of respondents spread around the world. After data clean up, there are 153 cases in total that are used for further analysis. In this subsection, demographic variables are described statistically to draw a better picture of who the respondents are. Those variables are *Headquarter location*, *Regional footprint*, *Industrial sector*, *Last year Revenue*, *Total number of employee* and *Respondents' role*.

Moreover, this subsection also presents descriptive statistics of their collective point of views with regard to EU GDPR. Their point of views are inherited in the variables of *Privacy importance*, *Online media importance*, *Privacy drivers*, *DPO preferences*, *Considered changes*, *Total number of FTE on privacy*, *Perceived compliance gap*, *Planned privacy-related changes*, and *Expected outcome from privacy-related changes*.

Variables with asterisk (*) next to them are generated from a mandatory questions. The ones without asterisk, consequently, are originated from a non-mandatory questions.

Headquarter*

Firstly, from 153 total respondents, 51.63% (79) are representatives of organizations headquartered in Europe. Most are headquartered in the United Kingdom (20), the Netherlands (16) and France (8). Second continent with the largest number of respondents is Asia with 37.25% (37) of total respondents. Most are headquartered in Indonesia (42). America is the third continent with 9.15% (14) of total respondents with United States as the most headquartered country (11). Australia and Africa are covered with 2 and 1 respondents respectively. See Figure 5.1 and Table 5.1.

Regional Footprint*

The data sample covers a good amount of respondents with footprints in both EU and non-EU. Those with EU in their footprints can further be defined as EU-only or Global (EU and other). The distribution is depicted

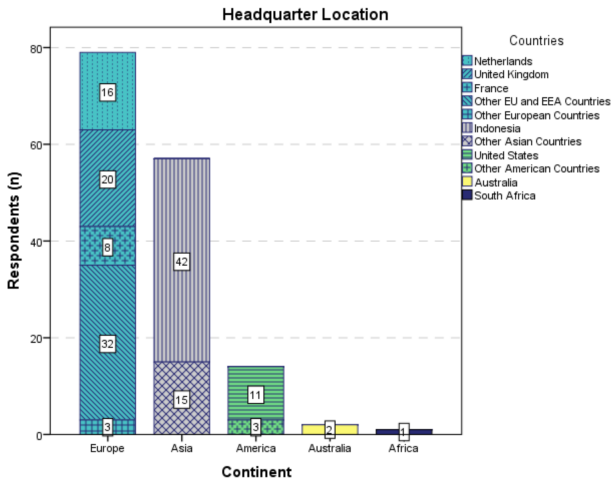


Figure 5.1: Sample Distribution In Terms of **Headquarter Location** Across Continents

in Figure 5.2. More than 50% of total respondents have footprints in EU (58 respondents with footprint in EU only and 28 respondents in EU and other regions (global)). The rest, 67 respondents, have footprints in a non EU region.

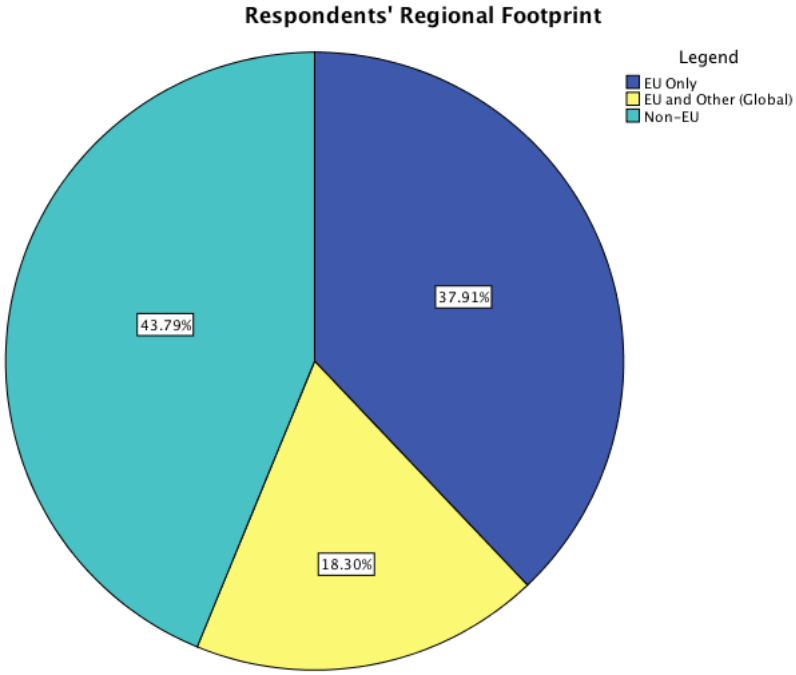


Figure 5.2: Sample Distribution In Terms of **Regional Footprint**

INDUSTRIAL SECTOR*

There are 10 defined *Industrial Sectors* in the data sample. Those sectors are as follows:

- Healthcare stays as **Healthcare** (with 6 respondents);
- Government stays as **Government** (24);
- Banking, Insurance and Pension, Others of e-commerce, Finance, and Finance Intelligence into **Financial** (30);

Table 5.1: Sample Distribution In Terms of **Headquarter Location**

Headqarter Location	Count	Percentage
Europe	*79*	*51.63%*
United Kingdom	20	13.07%
Netherlands	16	10.46%
France	8	5.23%
Sweden	4	2.61%
Belgium	4	2.61%
Italy	4	2.61%
Portugal	3	1.96%
Finland	2	1.31%
Germany	2	1.31%
Greece	2	1.31%
Switzerland	2	1.31%
Norway	2	1.31%
Poland	2	1.31%
Bulgaria	1	0.65%
Cyprus	1	0.65%
Spain	1	0.65%
Albania	1	0.65%
Iceland	1	0.65%
Russia	1	0.65%
Ireland	1	0.65%
Serbia and Montenegro	1	0.65%
Asia	*57*	*37.25%*
Indonesia	42	27.45%
Afghanistan	3	1.96%
Japan	2	1.31%
Singapore	2	1.31%
India	2	1.31%
Korea, South	1	0.65%
Thailand	1	0.65%
Hong Kong	1	0.65%
Bahrain	1	0.65%
Algeria	1	0.65%
China	1	0.65%
America	*14*	*9.15%*
United States	11	7.19%
Canada	1	0.65%
The Bahamas	1	0.65%
Brazil	1	0.65%
Australia	*2*	*1.31%*
Australia	2	1.31%
Africa	*1*	*0.65%*
South Africa	1	0.65%
Grand Total	**153**	**100.00%**

- IT and Security Services, Technology and Electronics, and Telecom into **Information Technology** (43);
- Utilities, Others of Housing, Property, Real Estate, Infrastructure, Construction into **Housing and Infrastructure** (8);
- Automotive, and Personal Transport into **Automotive and Transport** (7);

- Media, Sport, and Entertainment and Leisure into **Media, Entertainment and Leisure** (9);
- Retail and Others of Supply chain into **Retail and Supply Chain** (8);
- Education, Research Office and Academia into **Education** (7);
- Non Profit, Professional Services, Risk Management, Mining, Oil and Gas, Chemicals, Manufacturing, Army Equipment into **Other** (11).

Most surveyed companies are active in Information and Technology sector (43 companies, 28%), with majority of them are headquartered in other EU and EAA countries (24 companies). The second industrial sector with largest respondents number is Financial (20%), and followed by Government (16%). The details of these number can be seen in Table 5.2. Up to this point, the sample is balanced in terms of *Headquarter Countries* and *Industrial Sector*.

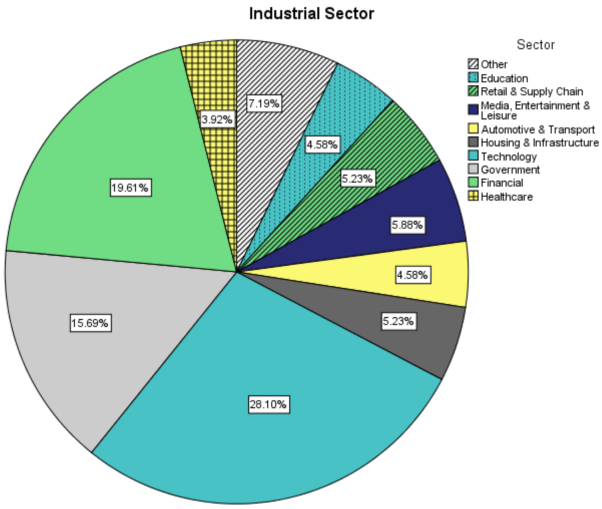


Figure 5.3: Sample Distribution In Terms of **Industrial Sector**

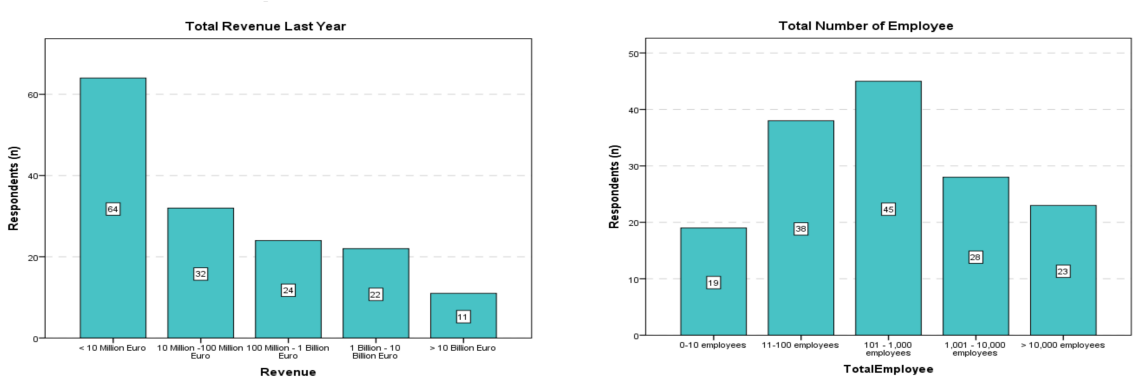
Table 5.2: Sample Distribution In Terms of **Industrial Sector** and Headquarter Location. Color coding is done per row, where darker color shows higher value. A = Information Technology; B = Financial; C = Government; D = Media, Entertainment and Leisure; E = Retail & Supply Chain; F = Housing and Infrastructure; G = Education; H = Automotive & Transportation; I = Healthcare; J = Other.

Headquarter Countries	**Industrial Sector**										**Total (n)**
	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	
Netherlands	4	2			1	1	4	2		2	16
United Kingdom	6	4	1	2	2	3			1	1	20
France	1	3		2		1			1		8
Other EU and EEA	17	3	1	2	2	1		3		3	32
Other European Countries		2								1	3
Indonesia	8	5	21	1	1	1	2		1	2	42
Other Asian Countries	4	4			1		1	2	3		15
United States	3	5		1						2	11
Other American Countries				1	1	1					3
Australia		1	1								2
South Africa		1									1
Total Respondents	**43**	**30**	**24**	**9**	**8**	**8**	**7**	**7**	**6**	**11**	**153**

SIZE OF COMPANY*

Next, it is found that the size of surveyed companies varies in terms of total revenue gained last year (*Revenue*) as well as total number of employee (*Total Employee*) (see Figure 5.4). Looking at the Revenue as a parameter, almost half of surveyed companies (42%) lie in the Small-Medium Enterprise category (less than 10 Million Euros). Another 21% of the surveyed companies lie in the next higher category (10 Million - 100 Million Euros). Last three categories are 100 Million - 1 Billion with 16% of total respondents, 14%, and 7% of the total surveyed companies. This finding is similar to the expectation, where many respondents will come from small companies. This assumption is based on the fact that most economy is made of small and medium companies.

Looking at Employee as a parameter, surveyed companies distributed normally accross defined categories. The distributions is centered on the medium-large size (101-1000) with a slight skew towards the medium-micro sized (11-100 and 0-10) on the left side. Combining both variables results in Table 5.3. The combination of 10-11 Employee with Revenue less than 10 Million Euros has the highest number of surveyed respondents of 28.



(a) Gained Revenue Last Year

(b) Total Number of Employee

Figure 5.4: Size of Respondents' Compaies Based on **Revenue** and **Number of Employee**

Table 5.3: Size of Respondents' Company Based on **Revenue** and **Number of Employees**. Color coding is done per row, where darker color shows higher value.

Revenue		**Total Employee**					**Total**	
(Million Euros)		**0 - 10**	**11 - 100**	**101 - 1,001**	**1,001 - 10,000**	**>10,000**	**n**	**Percent**
< 10		16	28	13	6	1	64	**42%**
10 - 100		1	8	18	1	4	32	**21%**
100 - 1,000		1	2	12	7	2	24	**16%**
1,000 - 10,000		1		1	12	8	22	**14%**
> 10,000				1	2	8	11	**7%**
Total	**n**	19	38	45	28	23	153	**100%**
	Percent	**12%**	**25%**	**29%**	**18%**	**15%**	**100%**	

ROLE OF RESPONDENTS*

Lastly, we will see the respondents demographic from their role in their corresponding organzation. Most of the respondents are found to have positions as executives or directors with 35.29% (54) of the total respondents. Following that number, IT and Information security comes in second place with 22.88% (35) percent of the total respondents. Position in Legal/Compliance and Marketing/Corporation Communications come in the third and fourth place with 19.61% (30) and 14.38% (22). Human resources count up to 2.6% (4) while the rest like consultants and researchers fall in the Other category that amount up to 5.23% (8).

PRIVACY* AND ONLINE MEDIA IMPORTANCE

Hereafter, this report is moving further to presents respondents' collective point of view regarding EU GDPR -started with *Privacy and Online Media Importance*

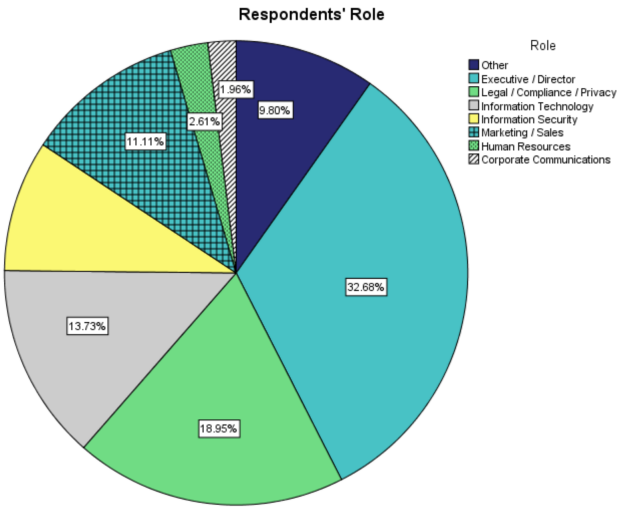


Figure 5.5: Sample Distribution In Terms of **Respondents' Role**

Table 5.4: Sample Distribution In Terms of **Respondents' Role** and Industrial Sector. Color coding is done per row where darker colors show higher total respondents.

Industrial Sector	Executive / Director	IT / Information Security	Legal	Marketing / External	HR	Other	Sum
Healthcare	3	1	1	1			6
Financial	5	10	8	5	1	1	30
Government	15	3	3	1		2	24
Information Technology	12	11	9	9	1	1	43
Housing & Infrastructure	4		2	2			8
Automotive & Transportation	2	4	1				7
Media, Entertainment & Leisure	3	3		2	1		9
Retail & Supply Chain	5	1	1	1			8
Education	2		1	1		3	7
Other	3	2	4		1	1	11
Total	**54**	**35**	**30**	**22**	**4**	**8**	**153**

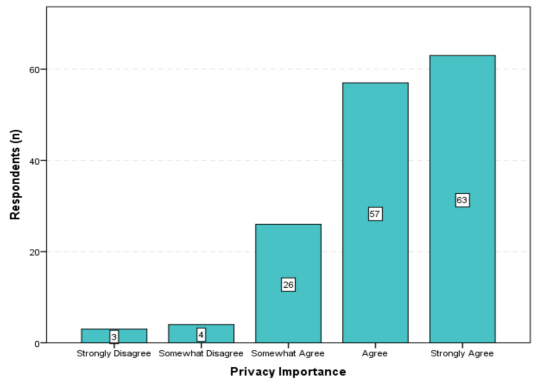
Most surveyed companies perceive privacy and online media to play an important role in their company, as can be seen in Figure 5.6. Additionally, these two variables correlates positively as predicted. This positive correlation is also supported with a Spearman test which resulted in a postitive Spearman correlation coefficient of +0.36 (Table 5.5). It is noteworthy that *Privacy Importance* is the result from a mandatory question, which resulted in 153 filled-in cases. *Online Media Importance*, however, is not mandatory, which resulted in 3 missing values.

As can be seen in Table 5.6, privacy is regarded of high importance in most industrial sector. Minor tendency to the opposite direction, however, exist in several sector such as Government, Information and Technology, Automotive and Transportation, Media Entertainment and Leisure, as well as other category.

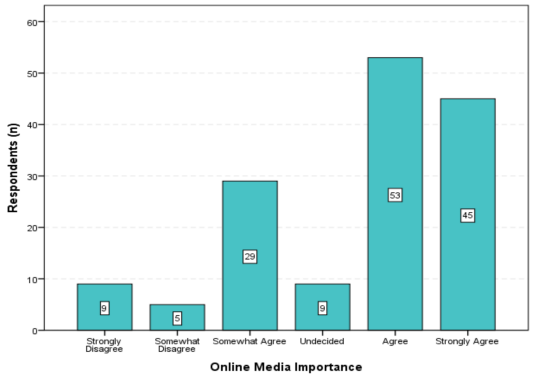
TYPES OF PERSONAL DATA

There are at least four types of data that are perceived as the source of privacy-related information by the surveyed companies: employee data, customer personal data, third party privacy-related data and confidential privacy-related data.

The first thing observed from this result is one peculiarity regarding the employee personal data. Any organization is supposed to process their employee data. However, the gathered result does not represents the expectation. Figure 5.7. This phenomenon can be explained by the non-mandatory nature of the question



(a) Privacy Importance for Surveyed Companies



(b) Online Media Importance for Surveyed Companies

Figure 5.6: Sample Distribution In Terms of **Privacy and Online Importance**. Privacy Importance is a mandatory question, while Online Media Importance is Non-Mandatory

Table 5.5: Correlation Between Privacy and Online Media Importance

			Privacy Importance	Online Media Importance
Spearman's rho	Privacy Importance	Correlation Coefficient	1.000	0.357**
		Sig. (1-tailed)		0.000
		N	153	150
	Online Media Importance	Correlation Coefficient	0.357**	1.000
		Sig. (1-tailed)	0.000	
		N	150	

Table 5.6: Sample Distribution In Terms of **Privacy Importance** and Industrial Sector. Color coding is done per row, where darker colors show higher total respondents.

Industrial Sector	Privacy Importance					Total (n)
	Strongly Disagree	Somewhat Disagree	Agree	Somewhat Agree	Strongly Agree	
Healthcare			2	1	3	6
Financial			13	5	12	30
Government		1	8	3	12	24
InformationTechnology	2	1	20	4	16	43
Housing & Infrastructure			2	1	5	8
Automotive & Transportation	1		1	3	2	7
Media, Entertainment & Leisure		1		5	3	9
Retail & Supply Chain			4		4	8
Education			3	2	2	7
Other		1	4	2	4	11
Total (n)	**3**	**4**	**57**	**26**	**63**	**153**

which may lead the respondents to not answer the question thoroughly. The second plausible explanation is respondents' bias due to lack of information. The corresponding question of "What type of privacy-related information is processed by your organization" might be perceived to know what type of personal data is mostly processed that is closely related to the business model of the surveyed companies. Hence, employee data is out of their consideration.

Furthermore, it is found that customer data is the most processed privacy-related information. Almost three-quarter of respondents (109) process customer data. Moreover, third-party data comes next with 80

respondents. The last category of 'Other' only amounts up to 7 respondents. The type data in this category is further defined as respondents' confidential data (e.g. Research and Development-related data, or Government Confidential Report). The combinations of processed data and the number of companies processing it based on the industrial sector can be seen in Table 5.7.

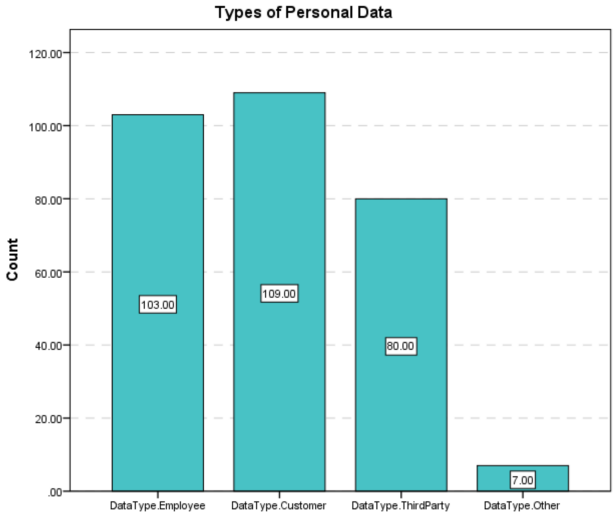


Figure 5.7: Sample Distribution In Terms of Prossed Personal Data Type. Multiple answer was plausible; N is larger than 153.

Table 5.7: Sample Distribution In Terms of **Types of Processed Personal Data** and Industrial Sector. Color coding is done per row, where darker color shows higher value. A = All types of personal data; B = Employee, Customer, Third Party; C = Customer, Third Party, Other; D = Employee, Third Party, Other; E = Employee, Customer, Other; F = Employee & Customer; G = Employee & Third Party; H = Employee & Other; I = Customer & Third Party; J = Customer & Other; K = Third Party & Other; L = Customer Only; M = Employee Only; N = Third Party Only; O = Other Only.

Industrial Sector	**Types of Personal Data**															**Total (n)**
	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	
Healthcare		1				2						2				5
Financial	1	9				5			1		1	6	5			28
Government		9	1				1					3	5	4		23
Information Technology	1	16				7			2			8	2	6		42
Housing & Infrastructure		6				1						1				8
Automotive & Transportation		4					1						1	1		7
Media, Ent. & Leisure		3				3						2				8
Retail & Supply Chain		3				2			1				2			8
Education		1				2						1	2	1		7
Other	1	2				2	1		1				2	1		10
Total (n)	**3**	**54**	**1**	**0**	**0**	**24**	**3**	**0**	**5**	**0**	**1**	**23**	**19**	**13**	**0**	**146**

PRIVACY DRIVERS

Now that we know that most respondents place a high value on privacy, it is interesting to know what the privacy drivers are important for them. Five privacy drivers are ranked by the respondents. It is wise to note that this variable is obtained from a non-mandatory questions, as an attempt to avoid overloading respondents. However, the result is still interesting to see, which also helps in explaining the generated model in the next chapter. The ranking of *Customer Satisfaction* is determined from 131 respondents, 128 for *Talent*, 130 for *Company's Reputation*, 132 for *Compliance* and 131 for *Risk Management*.

Table 5.8 depicts the rank of different types of drivers for company towards privacy. This rank is determined by calculating the means of rank for each drivers and sector. In general, these drivers are ranked from

highest to lowest as customer satisfaction, compliance, company reputation, risk management and talent. Financial, IT, Automotive & Transportation as well as Retail & Supply Chain sectors find customer satisfaction as the most driving factor. Healthcare and government sectors find it in compliance. Media & Entertainment, Education and aforementioned Other sectors in company reputation. Finally, Housing & Infrastructure sector finds risk management as the most important driver when it comes to privacy.

Table 5.8: Ranking of Drivers for Privacy By Surveyed Companies. Color coding is done per row, where lower value shows higher rank. Higher rank (the ones in blue) shows the most important privacy driver for each sector.

Industrial Sector	Customer Satisfaction	Compliance	Company Reputation	Risk Management	Talent
Healthcare	3	1	2	3	4
Financial	1	2	3	4	5
Government	3	1	2	4	5
Information Technology	1	2	3	4	5
Housing & Infrastructure	4	2	3	1	5
Automotive & Transportation	1	3	2	4	5
Media, Entertainment	2	4	1	3	5
Retail & Supply Chain	1	3	2	2	4
Education	3	4	1	2	2
Other	3	2	1	3	4
Overall Ranking	**1**	**2**	**3**	**4**	**5**

CONSIDERED CHANGES TO BE COMPLIANT WITH EU GDPR

As might be expected, there must be changes considered due to EU GDPR companies in general and for the these privacy-conscious respondents in particular. There are at least 8 types of considered changes defined by the surveyed companies, namely changes in information security, access rights, data portability, notification system, product development, data transfer to Non-EU, IT supplier and shrinking market.

These variables depicts the considered changes in processes. Considered changes by most respondents is information security (45% of total respondents), followed by access rights (37% of total respondents), data portability (33% of total respondents) and notification system (31% of total respondents). The combination with the companies sector can be seen in Table 5.9.

In *Healthcare*, considered changes in IT supplier is relatively higher than in other sector. the highest proporsion considering shrinking market base. In *Financial*, considered changes process related to data transfer to Non-EU is higher. In *Government*, Information Security. In *Information Technology*, data transfer and it supplier. In *Automotive*, product development and data transfer. In *Media*, notification is quite high. In *Retail & Supply chain* , almost equally the same (makes sense, due to comprehensive business model (supply chain) except for F and G (expensive, again for large business model). In *Education* has the least changes considered. and it focus on data portability. In *other* focus on IT suppliers.

An anticipated findings are also found in the amount of companies considering changes based on their regional footprints. As a whole, the percentage of companies considering changes are found to be the largest with those having a global footprints, followed with those having footprints in EU only and outside EU. On a side note, the order of considered changes stays the same based on the percentage of considering companies. The detailed numbers presenting the considered changes based on the regional footprint can be seen in Table 5.10.

DPO EXISTENCE AND FTE ON PRIVACY

Several privacy related elements were asked in the survey. The purpose of this question is to get hints on the respondents' understanding as well as current situation in their privacy and personal data protection. The related elements asked were the existence of DPO, the number of total Full Time Employee (FTE) working on privacy, number of individuals with data, number of individuals with data added last year, number of individuals requesting access to data and number of individuals requesting removal of data. Flash forward to question 7.4 and 7.6 in Appendix B if a reminder of the survey question is necessary.

The data for the last four elements is too scattered that it is almost meaningless to draw any conclusion for each specific element (see Table 5.11). However, one might have a tendency to conclude that, in general,

Table 5.9: Sample Distribution Based On **Considered Changes** And **Industrial Sector**. A = Information Security; B = Access Rights; C = Data Portability; D = Notification System; E = Product Development; F = Data Transfer to Non-EU; G = IT Supplier; H = Shrinking Market Base. Color coding is done per row, where darker color shows higher percentage of respondents considering to change.

Industrial Sector		**Considered Changes**							
		A	**B**	**C**	**D**	**E**	**F**	**G**	**H**
Label	**n**	**%**	**%**	**%**	**%**	**%**	**%**	**%**	**%**
Healthcare	6	50%	50%	50%	50%	33%	17%	33%	17%
Financials	30	43%	40%	33%	27%	33%	33%	23%	3%
Government	24	50%	21%	21%	17%	13%	13%	0%	0%
Information Technology	43	47%	42%	40%	37%	26%	30%	30%	12%
Housing & Infrastructure	8	38%	38%	38%	50%	13%	25%	25%	0%
Automotive	7	71%	43%	29%	14%	43%	43%	29%	14%
Media, Entertainment & Leisure	9	44%	44%	33%	56%	11%	11%	22%	11%
Retail & Supply Chain	8	50%	50%	50%	50%	50%	25%	25%	13%
Education	7	14%	29%	14%	0%	0%	0%	14%	0%
Other	11	36%	27%	18%	18%	9%	0%	18%	0%
Total / Average Percentage	153	45%	37%	33%	31%	24%	23%	22%	7%

Table 5.10: Sample Distribution Based On **Considered Changes** And **Regional Footprint**. A = Information Security; B = Access Rights; C = Data Portability; D = Notification System; E = Product Development; F = Data Transfer to Non-EU; G = IT Supplier; H = Shrinking Market Base. Color coding is done per row, where darker color shows higher percentage of respondents considering to change.

Regional Footprint		**Considered Changes (n, % of n in N)**							
Label	***N***	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**
EU Only	58	27, 46.55 %	27, 46.55%	22, 37.93 %	23, 39.66	15, 25.86%	15, 25.86%	11, 18.97%	5, 8.62%
EU and Others (Global)	28	15, 53.57%	12, 42.86%	13, 46.43%	12, 42.86%	11, 39.29%	14, 50%	9, 32.14%	2, 7.14%
Non-EU	67	27, 40.29%	28, 41.79%	15, 22.39%	12, 17.91%	10, 14.93%	6, 8.96%	13, 19.4%	3, 4.48%
Total	153	69, 45.09%	67, 43.79%	50, 32.68%	47, 30.72%	36, 23.53%	35, 22.88%	33, 21.57%	10, 6.54%

Table 5.11: Descriptive Statistics of Privacy Related Element

Elements	**Descriptives**					
	N	**Mean**	**Median**	**Std Dev**	**Min**	**Max**
DPO Existence	153	0.6471	1	0.48	0	1
FTE on Privacy	59	18.05	2	85.10	0	650
# Individuals with personal data	59	897,328.64	20	4747058.19	0	3.5E+7
# Individuals with personal data added last year	59	25,941.42	5	101,329.65	0	500000
# Individuals requesting access to data	59	647.49	8	3290.09	0	25000
# Individuals requesting removal of their data	59	70.13	2	274.97	0	2000

respondents' understanding is not so high. A low number of respondents answering this questions (59) hints just that. Aside from that, there are two expected significant correlations between the number of individual data with the number of individual data added last year (spearman = 0.826), as well as the number of access request with the number of removal request (spearman coefficient = 0.388).

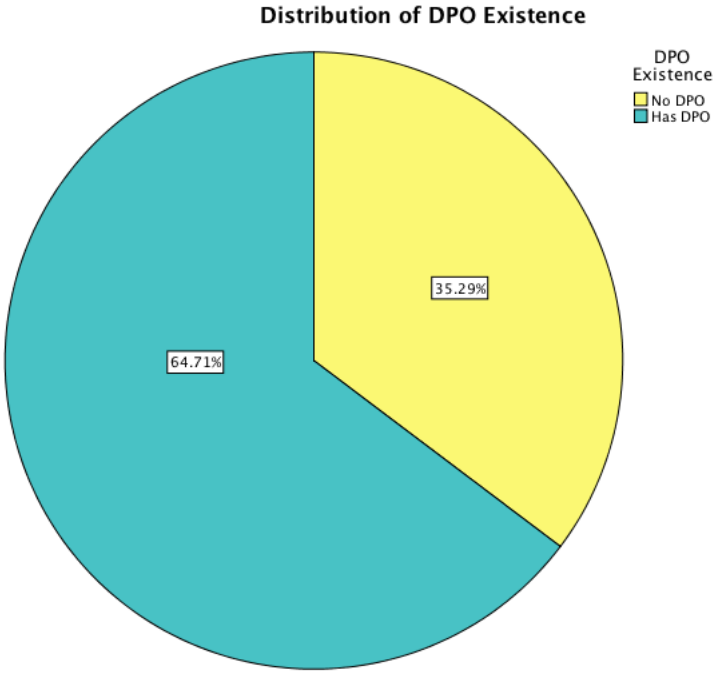


Figure 5.8: Respondents Distribution In Terms of Perceived Overall Gap

Further, a noteworthy significant correlation exist between the number of FTE working on privacy and the existence of DPO (spearman = 0.364). The higher the number of FTE, the higher the chance of a company to have chosen DPO. This hints having an assigned DPO is a no longer a new requirement among the professionals in privacy. In other words, it hints that they know what needs to be covered (DPO) with the extra FTE working on privacy. The distribution of companies based on the existence of DPO in their organization can can be seen in Fig 5.8.

BIGGEST EU GDPR CHALLENGE

Out of 73 respondents, their biggest challenge on EU GDPR can be classified into five major categories.

Firstly, the biggest challenge found is **resources**. Companies might find the biggest challenges stem in their resources as an initial indication of their capability in adopting to a new regulation like EU GDPR. There are three kinds of resources mentioned by respondents, namely human resources, time and money. Human resources can be seen as a challenge from a quantity perspective when it comes to a day-to-day business within large companies that requires more managerial support. However, it can also be seen as a qualitative (or skill) perspective, or as a respondent explicitly express as "a challenge to get an expert implement it". Money is one of the biggest challenge as most companies have a pre-determined budget in a year. EU GDPR was approved on April 2016. A relatively short time left until it comes to force in May 2018 might lead to a higher budget or cost to implement changes on time. This circumstance is what naturally leaves the respondents to feel that "limited budget", "cost", "getting implementation ready on time" and "time scales" as the biggest EU GDPR challenge.

Secondly, it is **IT and data security** that are found to be another big challenge. IT challenges are involved in adjustment needed to be done due to the EU GDPR. For instance, the considered challenges are "Amending data the software product we offer" or "Localization of storage". Furthermore, protecting privacy and data protection means having a robust security system to ensure no data breaching occurs. Hence, "cyber security", "data storage security", "data loss" and "leakage" are As we know, data security at times does not only revolve around IT management, but also the people behind it. A respondent express the challenge to be "Leakage (of) data and information to unauthorized person".

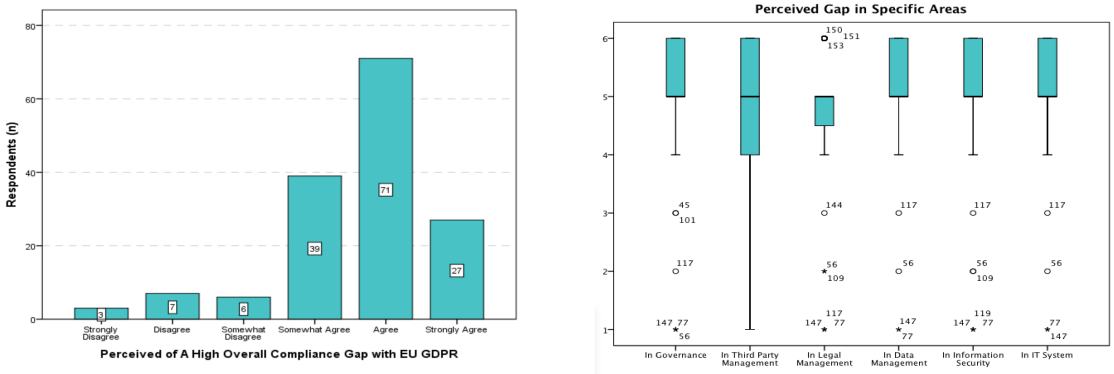
Thirdly, tackling EU GDPR is challenging for its own **complexity**. It is so complex that some companies admit not knowing where to start or even what they are expected to do. The struggles are translated as a challenge in "finding the right balance in implementing relevant controls". Complexity is one side of a coin with the new processes and systems entailing the EU GDPR on the other. Understanding and creating a proper structure, changing process, procedures, and the new processes and systems are all contributing to the complexity of EU GDPR. More so, some companies think that having a measurement to assess the effectiveness of these processes is another big challenge. Among these new processes, three specific new requirements are highlighted: data portability, right to be forgotten and consent management.

Furthermore, **compliance** naturally considered as a big challenge. Like any other cases related to regulation, any object under the regulation is forced to comply. In this case, it is more challenging because EU GDPR comes to force for all data controllers and processors without any exception. This means that companies that are not utilizing personal data for their revenue stream are expected to fulfill the same requirements with the ones who do. Therefore, compliance with EU GDPR is tricky for both type of companies (even in different way). On top of that, being incompliant means opening a window for a high penalty (i.e. 20 Million Euros or 4% of the total worldwide annual turnover), which is of course a risk that every companies need to take into careful consideration.

Last but not least, **uncertain impact** is also heavily mentioned as a big challenge. From the way respondents formulate their statements, one might see uncertain impact as a result from the previous challenge, complexity. Companies can be classified into two types based on the form of challenge induced by impact. The first group contains companies that are concerned with understanding the impact. Understanding the impact could be a challenge for companies as it is a first step to decide of how big the risk are expected and how much effort is necessary as a remedy. The second group contains companies that are concerned with a more specified impact, which is the altered market competitiveness. They argue that they might have a more "limited information access" or "loss of usable data" that are assumed as a challenge in "developing market".

PERCEIVED GAP*

Most surveyed respondents perceived a significant overall compliance gap with EU GDPR. As can be seen in Figure 5.9a, the distribution of respondents' perceivings is skewed to the right with only about 10% (16 out of 153 total respondents) perceive a non significant compliance gap. Looking at the variance in some specific areas (Figure 5.9b), gaps in 'governance', 'data management', 'information security' and 'IT system' seem to be perceived more significantly compared to the gap in 'third party management', as well as 'legal management' where the respondents are more unified in giving the value between 'somewhat agree' (4) and agree (5).



(a) Respondents Distribution In Terms of Perceived Overall Gap. N = 153 respondents.

(b) Perceived Gap in Several Specific Areas. N = 84 respondents.

Figure 5.9: Sample Distribution In Terms of **Perceived Gap** in general (left), and in some specific areas (right)

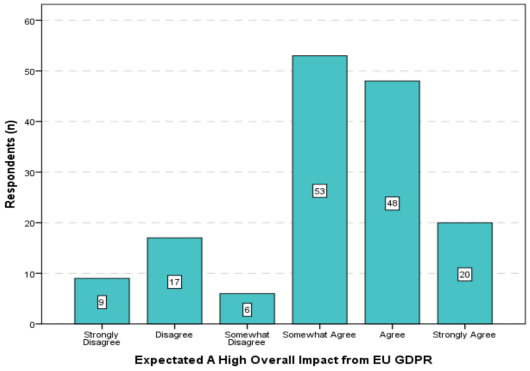
The perceiving of overall compliance gap vary across industrial sectors (Table 5.12). The gap is perceived the most significant in Media, Entertainment & Leisure sector. Followed sequentially by Government, Healthcare, Retail and Supply Chain, Financials, Education, IT, defined Other, Housing & Infrastructure and lastly by Automotive & Transportation.

Table 5.12: Distribution of Perceived Overall Gap Accross Industrial Sector. Color coding is done per column, where darker color shows higher mean. 0 = Undecided, 1 = Strongly Disagree, 2 = Disagree, 3 = Somewhat Disagree, 4 = Somewhat Agree, 5 = Agree, 6 = Strongly Agree

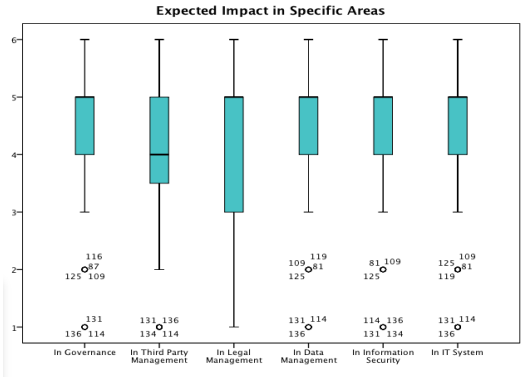
Industrial Sector	Perceived Overall Gap			
	Mean	Median	Std Dev	N
Healthcare	4.833	5	0.687	6
Financial	4.600	5	0.879	30
Government	5.208	5	0.576	24
InformationTechnology	4.465	5	1.168	43
Housing & Infrastructure	4.250	5	1.639	8
Automotive & Transportation	3.857	4	1.641	7
Media, Entertainment & Leisure	5.222	5	0.786	9
Retail & Supply Chain	4.625	4.5	0.992	8
Education	4.571	5	0.904	7
Other	4.273	4	0.862	11

EXPECTED IMPACT*

Most surveyed respondents expect a positive impact from with EU GDPR. As can be seen in Figure 5.10a, the distribution of respondents' expectations is skewed to the right with only about 20% total respondents (32 out of 153) expect a more negative impact from EU GDPR. Compared to perceived overall gap, however, the expected overall impact lies more towards the center. Looking at the variance in some specific areas (Figure 5.10b), the distribution of expected impact is quite similar with perceived gap where expected impact in third party management and especially 'legal management' are lower compared to other areas.



(a) Respondents Distribution In Terms of Expected Overall Impact N = 153 respondents.



(b) Expected Impact in Several Specific Areas. N = 83 respondents.

Figure 5.10: Sample Distribution In Terms of **Expected Impact** in general (left), and in some specific areas (right)

The perceiving of overall expected impact vary across industrial sectors (Table 5.13). The impact is expected to be highly positive in the Housing & Infrastructure. Media sector, which is the sector with highest perceiving on compliance gap, expect a relatively low positive impact (second lowest). Automotive & transportation stays consistent as the sector with the lowest value on expected impact as well.

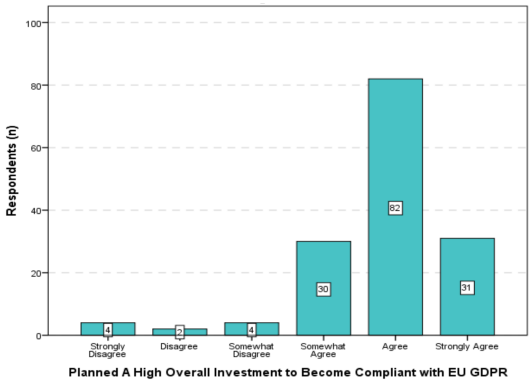
PLANNED INVESTMENT*

Finally, it is found that most respondents are investing in privacy-related changes over the coming years (Figure 5.11b). Respondents on disagreeing side are even lower with only 6.5% (10 out of 153 respondents). Similarly, there are 6 complementary variables to specify in which concerned areas is the investment focused on. The planned investment is also found to be relatively low for the two areas, i.e. 'third party management' and 'legal management'.

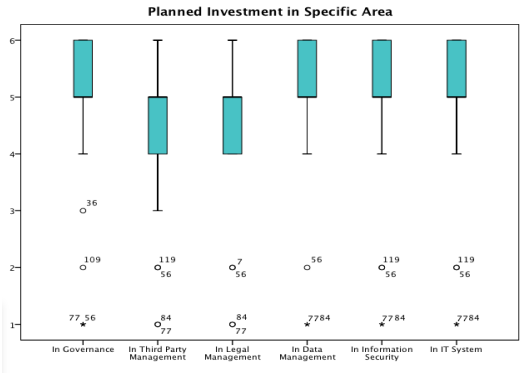
Oddly enough, education is found as the sector with the highest investment planned. Moreover, even though Media sector is expecting impacts on the negative side, it is planning a rather high overall investment.

Table 5.13: Distribution of Expected Overall Impact Accross Industrial Sector. Color coding is done per column, where darker color shows higher mean. 0 = Undecided, 1 = Strongly Disagree, 2 = Disagree, 3 = Somewhat Disagree, 4 = Somewhat Agree, 5 = Agree, 6 = Strongly Agree

Industrial Sector	Expected Overall Impact			
	Mean	Median	Std Dev	N
Healthcare	4.500	4.5	0.957	6
Financial	5.000	5	0.730	30
Government	4.833	5	0.986	24
InformationTechnology	4.837	5	0.861	43
Housing & Infrastructure	5.375	5	0.484	8
Automotive & Transportation	3.714	4	1.979	7
Media, Entertainment & Leisure	4.333	4	1.563	9
Retail & Supply Chain	4.875	5	0.599	8
Education	4.714	5	0.700	7
Other	5.000	5	0.603	11



(a) Respondents Distribution In Terms of Overall Planned Investment. N = 153 respondents.



(b) Planned Investment in Several Specific Areas. N = 82 respondents.

Figure 5.11: Sample Distribution In Terms of **Planned Investment** in general (left), and in some specific areas (right)

Government, followed by IT, Automotive, and Health sectors are on about the same level. Financial, Housing & Infrastructure and Retail & Supply Chain are on the lowest level.

Table 5.14: Distribution of Overall Planned Investment Across Industrial Sector. Color coding is done per column, where darker color shows higher mean. 0 = Undecided, 1 = Strongly Disagree, 2 = Disagree, 3 = Somewhat Disagree, 4 = Somewhat Agree, 5 = Agree, 6 = Strongly Agree

Industrial Sector	Planned Investment			
	Mean	Median	Std Dev	N
Healthcare	4.170	4	1.213	6
Financial	3.800	4	1.447	30
Government	4.333	5	1.344	24
InformationTechnology	4.256	4	1.203	43
Housing & Infrastructure	3.875	4.5	1.452	8
Automotive & Transportation	4.286	5	1.829	7
Media, Entertainment & Leisure	4.222	4	1.474	9
Retail & Supply Chain	3.750	4	1.392	8
Education	4.571	5	0.904	7
Other	4.182	4	1.113	11

5.2. BIVARIATE ANALYSIS - TEST OF HYPOTHESIS

This section presents the hypotheses testing. Various statistical tests are performed to test the relation between two variables (bivariate analyses) of each dependent variable and each independent variable. A list of the hypotheses can be seen in Table 5.15.

This section is started with flashing back on the dependent and dependent variables. Subsequently, the summary of bivariate tests is presented.

Table 5.15: List of Hypotheses to Test

	Hypotheses
	Related to Control Variables
H1	Companies having footprints in EU will plan more changes related to EU GDPR.
H2	Larger companies will plan more changes related to EU GDPR.
H3	The magnitude of planned changes by companies differs across industrial sectors
	Related to Independent Variables
H4	The existence of Data Protection Officer will lessen the changes planned by the companies
H5	Companies that perceive higher compliance gap with EU GDPR will plan more changes related to EU GDPR.
H6	Companies that expect more positive impact from EU GDPR will plan more changes related to EU GDPR.
H7	Companies that place a higher value on data privacy will plan more changes related to EU GDPR
H8	Companies that place a higher dependency on personal data processing consider less changes related to EU GDPR.

5.2.1. DEPENDENT VARIABLES

As previously mentioned, there are two dependent variables (DV) chosen for this study, namely *Planned Investment* and the latent variable of *Considered Internal Changes*. These two dependent variables are used as the metrics to measure the changes planned by companies regarding to EU GDPR. Each variable will be used separately for each hypothesis testing and multivariate regression model.

PLANNED INVESTMENT

Planned Investment is a dependent variable used as a metric to measure how likely it is for companies to plan investment for the considered changes. The distribution of this sample can be seen in previous section in Figure 5.12. Hereinafter, the value of *planned investment* is recoded from (0-5) scale to (-3 to 3) scale).

To enhance the reliability of respondents' answers on this metrics, a check on its consistency with the other 6 complementary variables is done. The test is done using a non parametric correlation test (spearmann). There are statistically significant relation between this 'overall planned investment' with each of the planned investment in 'governance' (spearman coeff. = 0.665), 'third party management' (spearman coeff. = 0.664), 'legal management' (spearman coeff. = 0.651), 'data management' (spearman coeff. = 633), 'information security' (spearmann coeff. = 0.669) and 'IT system' (spearmann coeff. = 0.639). Therefore, it can be assumed that the answers for the chosen metric (i.e., overall planned investment) comes from a consistent thinking process. With that in mind, it is assured to keep this variable as a dependent variable.

Considered Internal Changes

This dependent variable is a result from Principal Component Analysis (PCA) on all considered changes mentioned in the previous section. As high multicollinearity are found among these individuals *considered changes* it is desirable to combine these variables into a variable or a factor.

PCA is used to define how well these variables group and to determine what indexes to be use. The dimension reduction using PCA resulted in two components which represent two underlying variables for the *Considered Changes* variables. The two components explained 52.44% of the variance. Moreover, the PCA resulted with 0.826 for the KMO variables, a desirable high value.

The generated components from PCA can be seen in Table 5.16. Values in grey are considered to be low and less significant than the rest of the other variables in each respective component. It could be concluded that the PCA divides the *considered changes* into: 1) Considered Internal Changes, and 2) External Changes. The variables combined in the first component are variables related to considered changes related to process

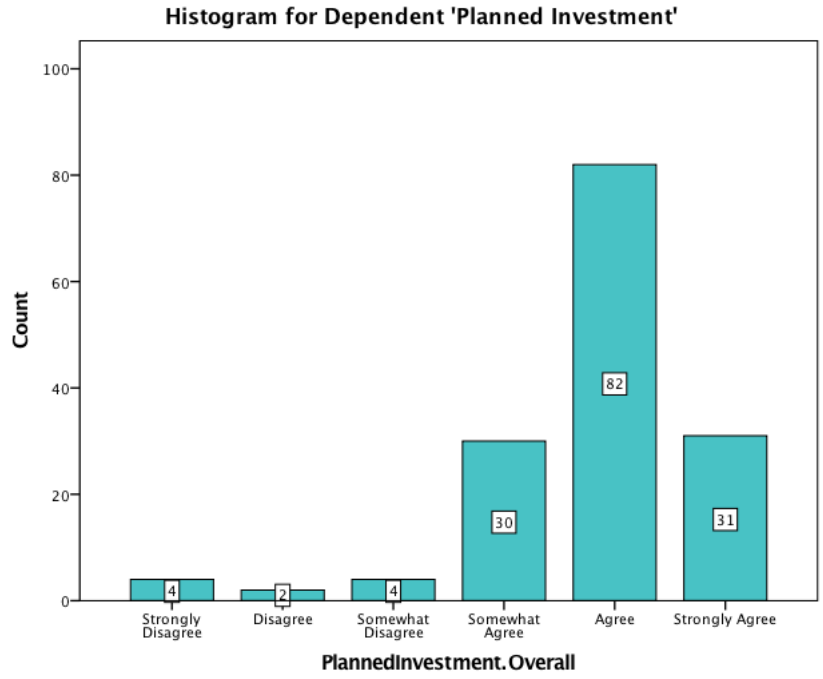


Figure 5.12: Histogram of the dependent *Planned Investment* variable. Mean 1.74 Standard deviation = 1.2

and systems. Meanwhile, the second component consists of two considered changes related to external factor, namely changes of IT Suppliers and Shrinking Market Base. For this study, the first component (Internal changes) is chosen as a dependent variable. The distribution of this variable can be seen in the following Figure 5.13

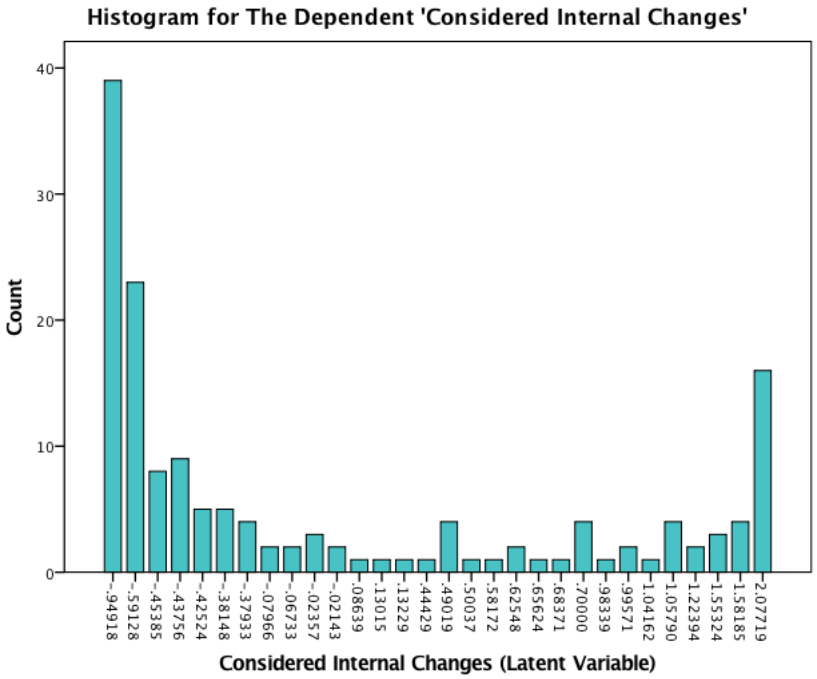


Figure 5.13: Histogram of the dependent *Consider Internal Changes* variable. Mean 0, Standard deviation = 1

Table 5.16: Rotated Component Matrix of *Considered Changes*

Rotated Component Matrix*		
	Component	
	1	2
ConsideredChange. DataPortability	0.806	
ConsideredChange. Notification	0.798	0.162
ConsideredChange. AccessRight	0.722	0.224
ConsideredChange. ProductDevelopment	0.622	0.310
ConsideredChange. DataTransferNonEU	0.618	0.149
ConsideredChange. InfoSecurity	0.603	-0.218
ConsideredChange. ITSuppliers		0.853
ConsideredChange. ShrinkMarketBase	0.261	0.458

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
*Rotation converged in 3 iterations.

THE MAIN DEPENDENT VARIABLE

Among these two dependent variables, a primary one is to be decided based on their distribution. The histograms of the two are presented above. Moreover, the standard deviation for both variables are checked. *Planned Investment* has mean value of 1.74 with standard deviation equal to 1.2. *Considered Internal Changes* has mean value of 0 with standard deviation equal to 1.

There is no good or bad value of standard deviation (SD). It depends on what we want our data set to be. It is desired to choose the main variable with a high variation since it hints a better cover on the different views of the intention to change from the respondents. For this purpose, a coefficient of variation (CV = SD / Mean) is calculated. A CV >= 1 indicates a relatively high variation, while a CV < 1 can be considered low. *Considered internal changes* is found to have higher variation compared to *Planned Investment*. Moreover, a higher value of SD will require larger data set to be able to find small statistically significance differences. These reasons make *Considered Internal Changes* more interesting, and hence chosen as the main variable.

5.2.2. INDEPENDENT VARIABLES

Footprint

Footprint is used as a metric defining companies regional footprint. Hereinafter, the variable is recoded into one categorical variable with three values: EU Only, EU and Other (Global), and Non-EU. For curious reader, the detail of original value of this variable can be seen in Appendix D.1.1.

Revenue

Revenue is used to represent the company size. For the next phase, it is utilized in its original form as ordinal variables. Values of this variable are defined from -2, -1, 0, 1, 2 to represents each category respectively from the smallest to the largest value.

IndustrialSector

Similar to its name, *IndustrialSector* resembles a metric to measure its demographic atribute of industrial sector. Hereinafter, the dimension of this variable is reduced into five categories: Information Technology, Financial, Government, Media and Leisure, and the rest as Others. The grouping is decided based on the median of respondents number per sector, which is 8.5.

DPOExistence

DPOExistence is the variable used as one of the metrics measuring companies maturity in doing privacy and data protection. The variable is a nominal value where 1 represents the existence and 0 represents the absence of DPO.

PerceivedGap

PerceivedGap is used as a metric for measuring companies perception on the gap between their current situation and the ideal situation stipulated in EU GDPR. Values of *Perceived Gap* are recoded to (-3, -2, -1, 0, 1, 2, 3) scale to respectively presents the gap from the smallest to the largest.

ExpectedImpact

ExpectedImpact is used as a metric for measuring companies expectations on the impact they will have after becoming compliant with EU GDPR. Values of *Perceived Gap* are recoded to (-3, -2, -1, 0, 1, 2, 3) scale to respectively presents the gap from the negative to positive impact.

PrivacyImportance

Privacy Importance is chosen as a dependent variable measuring companies value on privacy. The reason of choosing this instead of *Online Media Importance* is obvious: they are correlated (multicolinearity is not desirable in regression model), and that there is no missing values for *Privacy Importance* compared to values for *Online Media Importance* from a non mandatory question. Values of *Privacy Importance* are defined from -2, -1, 0, 1, 2 to represents each category respectively from the smallest to the largest value.

ProcessExtData

ProcessExtData is a a variable to as a metric measuring personal data dependency. This variable is generated from a slight modification on its original values in the previously mentioned *Type of Personal Data*. Under the assumption that all organization and companies process employee data, this variable is recoded into a nominal variable. It has value of '1' where the surveyed company processes either Customer Data or Third Party Data, and '0' where the surveyed company does not process Customer Data nor Third Party Data.

5.2.3. STATISTICAL TESTS RESULT

The results of hypotheses testing (bivariate analyses) are summed up in Table 5.17 below. For curious reader, the details of the performed statistical tests can be found in (Appendix D.2).

The hypotheses proven vary along the chosen dependent variable. With *Considered Internal Changes* as the dependent variable, there are two hypotheses proven. The two hypotheses are the significant influences from the *size* of the companies and their *dependency on personal data processing*. Moreover, influences of *DPO Existence* and *RegionalFootprint* on *Considered Internal Changes* are close to be accepted.

Meanwhile, five other hypotheses are proven for when *Planned Investment* acts as the dependent variable. DPO Existence, Perceived Gap, Expected Impact, Value on Privacy and Dependency on Personal Data Processing are all found to be individually significant in influencing how the companies will invest. On a side note, the 8th hypothesis (dependency on personal data processing) is proven for both dependent variables.

Table 5.17: Results of Hypotheses Testing. **Main Dependent Variable is *Considered Internal Changes***

Hypothesis #. Short Description	Median (sd)	Statistical Test	Test Result			
			DV: Planned Investment		DV: Considered Internal Changes	
			Score	Decision	Score	Decision
1. Regional Footprint	2 (0.905)	Kruskal Wallis	Rank : 1. EU and Other 2. Non-EU 3. EU Only p = .189	Reject	Rank: 1. EU and Other 2. EU Only 3. Non EU p = 0.069	Reject (barely)
2. Size	1 (1.323)	Spearman	coeff = -0.044 p = 0.587	Reject	coeff = -0.182 p = 0.025	Accept
3. Industrial Sector	4 (1.335)	Kruskal Wallis	Rank: 1. Finance 2. IT 3. Govt. 4. Other Sectors 5. Media p = 0.853	Reject	Rank: 1. IT 2. Media 3. Finance 4. Other Sectors 5. Govt. p = 0.501	Reject
4. DPO Existence	1 (0.479)	Mann Whitney	Rank: Has DPO > No DPO p (2 tailed) = 0.000	Accept	Rank: Has DPO > No DPO p (2-tailed) = 0.116	Reject (barely)
5. Perceived Gap	2 (1.338)	Spearman	coeff = 0.350 p = 0.000	Accept	coeff = 0.073 p = 0.184	Reject
6. Expected Impact	1 (1.717)	Spearman	coeff = 0.306 p = 0.000	Accept	coeff = 0.053 p = 0.258	Reject
7. Value on Privacy	2 (1.145)	Spearman	coef = 0.356 p = 0.000	Accept	coeff = 0.097 p = 0.117	Reject
8. Dependency on Personal Data Processing	1 (0.382)	Mann Whitney	Rank: Processing > Not Processing p = 0.043	Accept	Rank: Processing > Not Processing p = 0.000	Accept

5.3. MULTIVARIATE ANALYSIS: MULTIPLE REGRESSION MODEL

In this section, multivariate analysis is done by a linear regression (multiple regression). While performing hypotheses testing in the previous section, the influence of independent variables are tested individually on each dependent variables. However, with multiple regression, all independent variables' influences on the dependent variable are evaluated simultaneously. Hence, the resulted model can be used to make a more powerful and useful predictions about the behavior of the dependent variable; closer to how reality works.

It is wise to be aware that the upcoming estimated models are going to be highly limited in explaining the overall tendency to comply with EU GDPR. This is due to the small number of available variables as well as limited samples compared to the number of companies in the current vast industry. However, considering the absence of empirical study with statistical model explaining general interpretation of and tendency to comply with EU GDPR, this study can be seen as a first effort towards more refined models.

As previously mentioned, there are two dependent variables (DV) chosen for this study, *Planned Investment* and the latent variable of *Considered Internal Changes*. Each variable will be used to create one regression model. However, only the estimated model using the main dependent variable (*Considered Internal Changes* is presented in the following main report. The estimated model with *Planned Investment* as the dependent variable can be found in (Appendix D.3.1).

All Independent Variables (IV) mentioned in the previous section are taken in the model estimation. We are also curious to take the *RespondentsRole* in the calculation. The fact that only the previously proven significant variables are likely to stay in the regression model is known. However, since a stepwise method is chosen for regression model, this inclusion of non significant variables will not affect the final result. Thus, any anomaly (i.e., a previously insignificant variable individually becomes a significant variables when tested simultaneously together with others) can also be detected.

5.3.1. *ConsideredInternalChanges* AS DEPENDENT VARIABLE

MODEL ESTIMATION

An iterative process was performed using SPSS to estimate a linear regression model for internal changes considered related to EU GDPR. The method selected was the Stepwise estimation: it eliminates or adds one variable in each step until the best model is found. The variables are added according to their contribution to the explanation of the variance of the dependent variable and are eliminated if their contribution lacks statistical significance. The iterative process ends when all independent variables with significant contribution in explaining the variance are included in the model. Additionally, backward and forward method from SPSS were also executed but both of them gave similar results with stepwise method.

The model obtained had a practical significance (R^2) equal to 25.9.5%, which means that 25.9% of the total variance of the dependent variable that can be explained by the model. This value is lower than the previous model. The statistically significant variables that influence the model are listed in Table 5.18

Table 5.18: Multiple Regression Model (DV = Considered Internal Changes

Variable	Mean (SD)	Unstandardized Coefficients		P > |z|	Collinearity Statistics	
		Coefficient	Std Error		Tolerance	VIF
Dependency on Personal Data processing	2.0654 (1.14520)	0.799	0.195	0.000	0.993	1.007
Dummy EuandOther	0.1830 (0.38794)	0.669	0.207	0.001	0.857	1.166
Dummy EU Only	0.3791 (0.48675)	0.473	0.164	0.005	0.863	1.158
Constant		-0.960	0.193	0.000		

R Square = 0.179; Adjusted R Square = 0/163
Excluded Variables: Revenue, DPO Existence, PrivacyImportance, PerceivedGap, ExpectedImpact, DummyMedia, DummyIT_Sector, DummyGovernment, DummyFinance, DummyExecutives, DummyITInfoSec, DummyLegal, DummyMarket

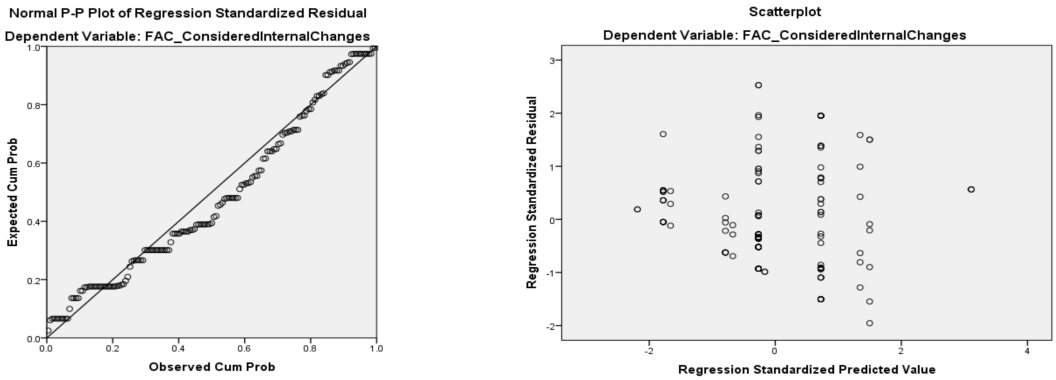
EXCLUDED VARIABLES

More independent variables are excluded from the regression model. These variables are *Revenue*, *DPOExistence*, *PrivacyImportance*, *PerceivedGap*, *ExpectedImpact*, *DummyMedia*, *DummyIT_Sector*, *DummyGovernment*, *DummyFinance*, *DummyExecutives*, *DummyITInfoSec* and *DummyLegal*.

The ones that are significant in bivariate tests were *Size ProcessExtData*. However, *Size* is no longer found statistically significant. It got bounced off the model by *RegionalFootprint*, represented in their dummies, which were barely rejected in the bivariate test. The rest of the variables are all kept excluded as expected.

REGRESSION ASSUMPTION

Before moving further to analyze the result of the model, regression assumptions of the models are checked. First, the homoscedastic residual error is not proven. The heteroscedasticity is found in the model as found in Figure 5.14b. This figure hints that the prediction for lower value is not consistently accurate. Second, the normality can be seen in Figure 5.14a. The regression standardized residual on the P-P Plot still scatered along the normal line. Lastly, the multicollinearity can be checked from the VIF or the critical value. All of the VIF are lower than 10. Hence, there is no multicollinearity in the model.



(a) Residual Plot for the Regression Model with Considered Internal Changes as Dependent Variable

(b) QQ Plot for the Regression Model with Considered Internal Changes as Dependent Variable

Figure 5.14: Residual Plots for the Regression Model with Considered Internal Changes as Dependent Variable

INTERPRETATION

The significant independent variables in these model are found to be *ProcessExtData*, *EUandOther*, *EUOnly*. On top of their statistically significant contribution to the dependent variable, the effect of these variables vary in both the scale and direction (positive/negative). For the sample under study, the following statements can be derived from the analysis of the variables' correlation coefficient:

- Companies that have higher dependency on personal data processing, have higher tendency to *consider internal changes* to move toward EU GDPR compliant.
- Companies having EU in their regional footprint, have higher tendency to *consider internal changes*. The tendency is higher for companies having footprint globally (EU and other region) compared to those having footprint in EU only.

The first finding above fit with our hypothesis in the opposite direction. Companies processing customer and/or third party' personal data are considered to have a high dependency on personal data processing. Hence, it was assumed that these companies would have less incentive to become EU GDPR compliant, which eventually would result in less internal changes considered. Nevertheless, the findings show an opposite phenomenon. Those that have high dependency with personal data processing have higher tendency to consider internal changes related to EU GDPR. One plausible reason is the fact that high dependency means high business interest lies, in which the related companies want to avoiding any risk of having this interest getting disturbed.

The findings regarding *Regional footprint* fit well with our hypothesis. Companies that have global footprint will have higher concern towards the EU GDPR. Naturally, companies with footprint in EU are also

concern since EU GDPR are originated in the EU itself. Thus, the tendency to consider internal changes can be concluded to be significantly affected with companies' regional footprint.

The many exclusion of independent variables is also found in the regression model with *Considered Internal Changes* as dependent variable due to their insignificant contribution in explaining the variance. Again, looking at the unstandardized coefficient of these insignificant variables could still give us a number of interesting findings. Across the *Industrial Sector*, the media is found to be having smallest influence towards the dependent variable, followed by Finance, and IT sector. Across the *Respondents role*, Legal is also found to have the highest positive influence towards the dependent variable, followed by IT, Executives and lastly by marketing. A more elaborated discussion on the plausible explanation behind these findings can be found in the next discussion chapter.

6

CONCLUSIONS

6.1. SUMMARY OF THE FINDINGS

6.1.1. PRIVACY AND DATA PROTECTION CONCEPTS AND THE RELATION TO DATA PROTECTION ACTS

SRQ1: What are the concepts of privacy and data protection and how do they relate to the data protection acts?

There are two types of privacy: physical and information. Focusing on the later one, (information) privacy is defined as an individual desire to control or have influence over the acquisition and potential secondary uses of personal data. Protecting (information) privacy, often means protecting the data containing such information. Thus, privacy protection is at times included in the so called larger domain of data protection. Data protection comes in different forms on different level. On individual level, it varies from data disclosure management up to using pseudonyms and giving false information. On the organizational level, data protection is translated into companies' strategies to secure their enterprise data. On the governmental level, data protection is often translated to policy or regulation oriented form.

Important stakeholders in privacy and data protection can be classified into three categories: regulator, users of personal data, and individual "data subjects". Focusing on European level and the Netherlands as a member state example, the regulators can be classified into EU Institutions, related EU Agencies and Decentralized Bodies (e.g. ENISA), related state government (e.g. Autoriteit Persoonsgegevens (AP)), sectorial supervisor (e.g. Committee of Supervision).

Originated from the past principles by OECD and CoE, EU DPD has a similar nuanse in the principles (e.g. transparency, legitimate purpose, proportionality). Following EU DPD, e-Privacy Directive was stipulated to complete the directive focusing on electronic communication. It directs member states on the way they operate their websites related to cookies, their emails for marketing purposes, and their data retention. EU GDPR focuses on a more harmonized system and stronger power distributed on the data subjects. Hence, significant changes from the past directives can be seen in relevant aspects. First is the obligation of having a supervisory authority for each member state, a Data Protection Officer for each organization, and a clearer information flow in between. Second is the increased rights for data subjects including the right of erasure or right to be forgotten. Imposed fines can also be seen as a significant changes, especially from the practitioners point of view.

6.1.2. CURRENT IMPLEMENTATION OF THE EXISTING EU DPD AND E-PRIVACY DIRECTIVE

SRQ2: How do organizations interpret and implement the existing EU DPD and e-Privacy Directive?

Most companies process personal data, be it internally (employee data) or externally (customer/3rd party personal data). The purpose of the processing vary from marketing to measuring their success rate. Some multinational companies have their Binding Corporate Rule formulated and approved. Those following the past directive does not see much differences with the EU GDPR. However, for those who had not been paying much attention to privacy and data protection find EU GDPR quite challenging. Important notes are found on the challenges of existence of DPO and governance, implementing Privacy by Design and estabilshing a mechanism for Personal Data Breach Notification. It is also learnt that some companies are more in a passive position, waiting to see how the enforcement will take place, especially in UK, Ireland, and Sweden.

6.1.3. ON THE PLAN TO CHANGE

How do organizations plan to change in terms of processes and investments with the implementation of the EU General Data Protection Regulation?

Plans to change by are measured from companies' own judgments on planned investment and considered internal changes. For the surveyed companies, considering the gathered data represent the actual condition of planned changes, investment is influenced positively by the perceived gap, existence of DPO and perceived overall gap. Factors influencing considered internal changes are value on processing personal data, and having regional footprint in EU.

The intention to change regarding to EU GDPR is rather high. A big portion of the respondents (i.e. 74%) falls in 'agree' and 'strongly agree' to the thoughts of having their organizations planning investment for changes related to EU GDPR.

6.1.4. THE INFLUENCE OF BUSINESSES' PROPERTIES AND PRIVACY ISSUES, AND THE POLICY IMPLICATIONS

SRQ4: How do businesses properties and privacy views influence the plan to change, and what are the policy implications of the findings?

In general, industrial sector does not statistically significant in influencing the planned changes. However, sectors of Media, Entertainment and Leisure is the sector where changes are least planned and invested. This is might be the case due to the high relevancy of personal data processing in their business model. Further it is logical to see larger investment for larger companies. The results, however do not represent this expected situation. This might be explained by the relative measurement of the survey. Most companies might think they invest high on changes related to EU GDPR, which cannot be a good objective measure. Moreover, the regional footprint is proved to be significant when it comes to the organizations' plan to change. Naturally, those having footprints in EU are more concerned to EU GDPR compared to the rest.

When it comes to the organizations' perceptions, both perceived gap and expected impact do play a role in the planning the changes, especially when observed based on the planned investment. However, the power of perceived compliance gap is stronger than the expected impact. Expected impact is only found to be statistically significant when tested alone, while perceived gap is also found to be significant when tested simultaneously with other variables. Further, the policy implications of these findings are discussed further in the following Section 6.3.

6.2. DISCUSSION

There are a lot of interesting findings to discuss. Following the research question, it is logical to start the discussion from the general point of view (i.e. discussing the regression models and the relation between the two). Subsequently, we will continue on the individual hypotheses (particularly on the excluded ones), and highlights how it differs according to the industrial sectors.

Businesses intentions are measured from their considered changes and planned investment related to EU GDPR. As shown in the result the two measures are not correlated with each other. This might mean that they measure two different spectrum of the planned changes by the businesses (e.g. whether to change or not (considered internal changes), and to what extent should they invest for that changes (planned investment)).

From the survey results, it can be said that the dependency on personal data processing and companies regional footprint are two things that initiate whether a some changes are necessary. It is logical for several reasons. Businesses that do not have high dependency on personal data processing may not have their primary focus on the privacy topic at the first place. Having their business interest hampered by EU GDPR would also be less likely. Moreover, companies with footprint within EU will be more likely to consider changes related to EU GDPR. On the other hand, those with footprints outside EU are the least to have consider any changes. However, combining EU and non EU means even higher tendency compared to the two previous category. This, indeed, does not a case where the average are taken, which result in the middle level for this global category. Rather, wider larger area covered in their footprints entail a more complex system, including their IT and internal management. Hence, the higher tendency to consider changes for the global companies. Take businesses in mining industry in the 'other' category for example. Their primary focus are probably in maintaining value, property, legal permit, etc. Having to put internal changes related to privacy and personal data protection would probably be add an extra burden without notable gain in return. However, still in the case of mining industry, but let's take a case from our interviewee. A company active in energy and mining sector would still give a room to consider internal changes when their company is big enough that the com-

plexity of their systems need to be assessed to fit the EU GDPR. Because then again, global companies are the large ones. Where not being compliant would means bigger penalty imposed.

Moving further, the existence of DPO, businesses' value on privacy and their perception on gap influence how their investments are planned. Instead of closing the perceived gap by companies that might lead to less planned investment, the existence of DPO is in fact elevates the planned investment. As previously mentioned, the existing DPO might have been succeeded in promoting awareness on the impact of EU GDPR or importance of having privacy and data protection in their respective companies. Therefore, higher planned investment are likely to increase when a DPO exist. Moving further, privacy importance is influential just as expected. The more important privacy means for a, the more serious the effort would be to protect this. Hence, the planned investment are tend to be magnified. Similar idea applies when it comes to the perceived gap. When there is a large gap perceived, it hints that more effort is needed to cover the gap; hence, higher investment is planned. The different thing between the last two element is that the first one is based solely on the companies intrinsic value, while perceived gap is the combining result of both companies internal understanding and the expectations of the so called ideal condition stipulated in the EU GDPR. Understanding the differences between this last two variable would then lead us to this: based on the data analysis, internal awareness is more influential than external intervention in generating larger intentions to change that is represented by the planned investment.

All but three of the predicted businesses properties and perceptions on privacy elements play a significant role in influencing towards either considering changes or planning investment. These three elements are the companies size, industrial sector and expected impact. Size is actually influential in considering changes when tested individually It is somehow related to the relation of footprint and considered changes. The wider the footprint, might hint the larger the size, and hence changes are likely to be considered. However, when it is compared with other variables, 'size' loose its power and thus appear to be not significant in the resulting regression model. Furthermore, industrial sector is found to be not influential for both measures of planned changes. A probable explanation for this is a rather small number of sample compared to the number of defined industrial sector groups. Lastly, expected impact is only found to be influential when tested individually on the extent of planned investment. This is logical for a couple of reasons. Using the same thinking algorithm, expected impact is the result of companies perceptions that are already comparing external expectations (from the EU GDPR). It does not come from within. Hence, when considered together with the rest of variables, this variable may not appear to be significantly influential. Moreover, the number of on individual capability, the planned expected impact is influencing how much companies are planning to invest. In a way, the planned investment could also be seen as how much effort are the companies willing to give as a shield to protect greater resources from falling apart (e.g. from negative impact).

INDUSTRIAL SECTOR

Despite the fact that insignificant influence of industrial sectors on the changing intentions, differences among sector prevails. Two most interesting sectors are financial sector and media & entertainment. Financial sector seem to be the most mature sector when it comes to protecting privacy and data protection. Financial sector has the high positive relation with planned investment. It also has customer satisfaction as it main drivers for privacy. On the other end, media is found to be having the smallest influence toward the considered changes. Consistently, media is related negatively strong with the planned investment, as well as the most significant gap perceived. For media, it is found that the privacy and data protection view are still based on the companies' reputation (not as mature as financial sector). Further, automotive & transportation seem to be indifferent with regard to EU GDPR. It perceives small gap and it does not expect much impact from being EU GDPR compliant as well.

6.3. RECOMMENDATIONS

Based on the findings and discussions of this research, a number of recommendations can be drawn. These recommendations are drawn for both the subject of the data protection (i.e., businesses and organizations) and the policy maker themselves.

6.3.1. FOR POLICYMAKER

THE EXISTENCE OF DPO: ENCOURAGE ORGANIZATIONS TO DECIDE ON A DPO

Firstly, it is recommended to monitor and encourage organizations to determine at least one DPO in their business activity. On top of the high influence from DPO on organizations willingness to change, encour-

aging the determination of DPO is beneficial for several reasons. DPO will come as an *internal force for the organizations* to implement EU GDPR. DPO will relax the policymaker obligation as *a reminder/source of information* regarding the EU GDPR implementation. Moreover, DPO will *facilitate an easier access* and approach from the policymaker to the organizations.

VALUE ON PRIVACY: SOCIALIZE THE IMPORTANCE OF PROTECTING PRIVACY

Secondly, according to the high influence of value on privacy towards the intention to change regarding EU GDPR, it is recommended to socialize the importance of protecting privacy. Instead of considering privacy and data protection only from the organizations perspective, it might give more positive impact if the focus is also shared to their customers' perspective. Benefits can come in a form of customers trust/loyalty or even a new product or selling advantage compared to other companies. If value on privacy manages to become an intrinsic value for the organizations, motivation to protect privacy will come from within. Hence, a hard enforcement (the type of enforcement using punishment) can be likely to be avoided.

PERCEIVED GAP: SOCIALIZE THE DIFFERENCES BETWEEN EU GDPR AND THE PAST PRIVACY ACTS

Thirdly, it is recommended to socialize the differences between EU GDPR and the past privacy acts. It could also include some kind of training explaining how the EU GDPR shall be implemented. This will enhance organizations awareness on EU GDPR, and thus boost the intrinsic motivation discussed in the previous point. Moreover, it will answer the biggest perceived challenges by the organizations simultaneously, which is the unclear directions and not knowing where to start.

DEPENDENCY ON PERSONAL DATA PROCESSING: DIFFERENT APPROACH ON SECTORS WITH DIFFERENT PERSONAL DATA PROCESSING DEPENDENCY

Furthermore, it is recommended to have different approach on different organizations/sectors according to their dependency on personal data processing. Keep an eye to those organizations with high dependency on personal data processing. Despite the positive influence found from the dependency on personal data processing towards the consideration to change regarding the EU GDPR, monitoring on organizations in this sector shall not be cut loose. The high risk triggering the organizations to protect the personal data can both be the initiator or resistor for them to implement privacy and data protection. It becomes an initiator when they don't want to risk anything (getting fined, loosing customers trust). It can become a stumbling block when they think the risk of loosing profit is bigger when EU GDPR is not implemented.

To the organizations with low dependency on personal data processing, policymakers can create different scheme for this particular sector. For example, they might want to consider reducing the requirement accordingly to the weight of personal data processed. The regulation is imposed on all data processors and controllers. However, it with the idea that the risk getting fined or loosing customers trust is low, organizations might think that the cost to comply with EU GDPR will be too high. In that sense, a different approach, such as minimum requirement readjustment, can be done accordingly.

EU AND GLOBAL FOOTPRINT: SUPERVISE AND EXAMINE PERIODICALLY THE TRANSFER OF DATA OUTSIDE EU

Lastly, it is recommended to maintain supervision on the data transfer to country outside the EU. Organizations outside EU are found to have less intention to change according to the EU GDPR. This is one of the reasons why privacy shield between EU-US is made. When the implementation of EU GDPR is mature enough, periodical test or check whether the agreed certification for the data transfer still holds for the actual implementation. Meanwhile, for those in EU, take cautions on the possibility of having inflexible implementation of EU GDPR. When a pragmatic approach is taken by organizations, being compliant would be the only focus. The transfer of power to the customers to create a more balance distribution of power and information may not be reached. For instance, the services or products are made not available to the customers when the customers deny the process of their personal data. As a result, data subjects are indirectly forced to agree with their personal data being processed.

GENERAL POINT OF VIEW: EXTEND TRAINING AND EXPAND THE NUMBER OF EXPERTS

On a more general point of view, some recommendations can also be drawn. Looking at the challenges perceived by the organizations, policy makers may want to consider extending education, training and certification aimed at this audience. Moreover, it is assumed that there will be a lot of supervision needed. Therefore, it is wise to start on expanding the number of legal and technical experts for this work to roll on if not done already.

6.3.2. FOR DATA CONTROLLERS AND PROCESSORS

Recommendations for data users can be drawn upon the findings of the challenges perceived by the organizations. The challenges are found to be resources, IT and data security, complexity, compliance and uncertain impact. The recommendations for each challenges might be mixed with one another. Hence, the recommendations will be described all at once as follow.

- Assign a DPO and talk to peers.

  Assigning a DPO may be the first thing to consider for those organizations that have not determined any. Having a DPO is salient for the initial part in assessing their current situation. Then, organizations may consider talking to peers, which can create rooms for ideas on how to implement challenging requirements from EU GDPR. If ideas are hard to be shared, joining forces might be an option. Collected aspirations must be more powerful compared to individual opinions.

- Be open to policymakers

  Organizations may want to consider an open communication with the policymaker. Instead of seeing the regulator as an opposing party, it might provide a more fruitful result if organization can treat regulator as a guiding or discussing partner. For instance, open communication to supervisory authority when difficulties emerge. Instead of covering and sealing problems, having an open attitude can benefit both sides. Being open would give a more positive impression, creating a more trustworthy impression. On the policymaker side, an open communication would give insights on what to facilitate or provide better for the organizations experiencing the same problem.

- Outsourcing

  When budget is found to be limited, rearranging and allocating the budget for privacy and data protection in the next period would be useful to do. Otherwise, when technical system or human resources are still hard to be fulfilled, outsourcing could be an option. The EU GDPR states that the assignment of DPO can be done via a third party. On the more technical aspect, outsourcing IT system is a widely known practice when an organization is short in human resources, knowledge or capability.

- Menu of contracts

  Organizations are forced to comply, and yet, the impact of being compliant are seem to be uncertain. To bridge the goal of being compliant with the regulation without loosing its flexibility, organizations can provide several menu of contracts for their customers. Instead of having a binary option for the customers, organizations can give different options for the customers to choose. For example, instead of not providing any services on a website when customers are not willing to provide their privacy and personal data; the organization can give option to still provide the services while giving advertisement on the website. In this context, the organization would still comply to the regulation without losing their source of revenue as well as cutting the customers access off of their services.

6.4. LIMITATION AND FUTURE RESEARCH

Closing this research, limitation and future research are made explicit. This section is started on the limitations and followed up with suggestion on how the future research can be progressed.

In the first place, limitations are found in the formulation of the conceptual model. As an initial effort to create a measurement model assessing intentions to change for EU GDPR, relations between variables are a result of combining several static relations found in the vast literature. Due to time limitation to execute the research, such approach is chosen to at least provide the stepping stone to further develop a more robust model and measurement tool. Still related with time, the scope of the research is rather limited on the intentions of organizations to change instead of the actual behaviour (executed changes). In the future, more empirical research on this topic would be really useful. Bear in mind that the scope of this research is stop until the 'intention' part. Further research can use the result of this study to compare it with the actual behaviour/implementation after the enforcement of EU GDPR takes time for a while.

Secondly, each sector is not represented by one interviewee as originally intended. Finding a contact that is willing to share his company's views on an arguably sensitive topic like privacy and data protection is challenging. Bounden by time, it is decided that the interview shall at least cover the policymaker point of view, the organization and the experts (consultants), which was covered. For further studies, the identified

values from policy-maker point of view can also be very useful. By doing so, it would help to stream the information from the policymaker to the organizations (on the reverse flow with this research).

Thirdly, the collected data set for the survey is found to be biased. Originally, it is decided to have a worldwide overview on this topic. Even though many countries and footprint region are represented in the data set, it is found that some country has more representation compared to others. The two countries are The Netherlands and Indonesia. This limitation is due to the many networks of the researcher and the origin of this study that are highly related to those countries.

Lastly, limitations are found to be related with the decision on choosing a wide range of sector. A general brush is one benefit. However, it resulted in a small number of sample when seen on each industry sector. Interesting findings on specific sector would then be lack of reliability. In the future, scope of the study can be more specified on one or two industrial sector.

A

Interview Protocol

General Information

Good morning. Thank you for your time and availability for this interview. Currently, I am conducting a MSc thesis at Deloitte on a topic of the implication of EU GDPR. The perspective I am using in this research is using a policy analysis framework. I would like to examine how effective the EU GDPR would be, indirectly by answering how organizations would be affected in the day-to-day operations. This can be done by investigating both the current practices as well as further changes that might be considered or planned in line with the new regulation. As stated in the research plan summary, this empirical results can also be used as the foundation to draw a landscape within privacy and data protection by firms and organizations. Therefore, the purpose of this interview is to learn the day-to-day operations and the changes that might be planned by organizations with regard to privacy and data protection.

Instructions for Recording Permission

Before I start the interview, I would like to ask your permission for recoding this interview. The purpose for recording out conversation is to ensure that I can get all of the details of your responses while having an attentive conversation with you at the same time. I assure you that the recording will remain confidential. I will be compiling a report which will contain gathered information without any reference to individuals.

==========

Questions

Questions: The Importance of Personal Data

- Q1. Please tell me how the process of personal data would be of use in creating value to your business products/services?
- Q2. What do you think about the new EU GDPR? What are considered to be new to the company?

Questions: Existing Operations of Privacy and Data Protection

- Q3. Would you please share me how privacy and data protection is handled in the day-to-day operations? Probe: Procedure, person in charge, time needed, policy. Throughout the data life cycle (gathering, using, retaining, processing, transferring, deleting)
- Q4. How is the structure of your organization defined for privacy and data protection? Probe: relation with IT, legal, risk. DPO Probe: number of FTEs
- Q5. How often is the right of data access, update or deletion being used by your customers? Probe: how do you handle these requests? (if not answered in Q3)
- Q6. How do you take care of personal data breach notification? Probe: person in charge, time needed, budget allocated
- Q7. How do you handle privacy and data protection with your member firms outside The Netherlands? Probe: What are the similarities or differences if any? Any internal policy?

- Q8. Do you get external legal counsel, or do you talk with peers?

Questions: Future Plans

- Q9. Which parts of the changes in the EU GDPR that you consider the most troublesome?
- Q10. Have you considered any changes within your organization in the light of the new regulation? Probe: If not, why not? Probe: If yes, go to Q11.
- Q11. Have you already had a project to implement these changes? Probe: If not, why not? Probe: If yes, budget, time, number of FTEs, people involved/in charge, risk function,
- Q12. What would you want to be changed in the revision of e-Privacy directive?

CLOSING REMARKS

Is there any important questions or subjects which should be addressed to capture the current landscape and change of direction in the field of privacy and data protection that you think we missed?

This is the end of my interview. Thank you very much for your time and responses. I find them very useful for my research project. I assure you that your personal and company details will not be published without seeking your approval beforehand. I hope to keep in touch with you through email and I will get back to you at the end of my research in order to validate my findings. At last, I would like to ask you to please introduce me to other relevant persons that might be interesting to be interviewed for my project.

B

Survey Questionnaire

***1. Your organization is head quartered in**
..... *<dropdown list of countries>*

***2. Regional footprint of your organization**

☐ EU / EEA

☐ Americas

☐ Asia Pacific

☐ Other

***3. Principal industry / sector of your organization:**
as seen from your headquarters
O Automotive
O Banking
O Education
O Entertainment & Leisure
O Government
O Healthcare
O Insurance & Pensions
O IT & Security Services
O Media
O Non-profit
O Personal Transportation
O Retail
O Technology and Electronics
O Telecom
O Utilities
O Other .....

***4. Total gross revenue last year:**
as seen from your headquarters, 1 USD ~1.1 Euro
O <10 Million Euro
O 10 Million - 100 Million Euro
O 100 - 1 Billion Euro
O 1 Billion - 10 Billion Euro
O >10 Billion Euro

***5. Number of employees in your organization**
as seen from your headquarters

O 0 - 10 Employees
O 11 - 100 Employees
O 101 - 1000 Employees
O 1001 - 10,000 Employees
O >10,000 Employees

***6. Your role in the organization**
O Executive / Director
O Legal / Compliance / Privacy
O Information Technology
O Information Security
O Marketing /Sales
O Human Resources
O Corporate Communications
O Other .....

***7. What is your opinion on the following statement?**

Table B.1: Scale answer for question number 7

	Strongly Disagree	Disagree	Somewhat Disagree	Undecided	Somewhat Agree	Agree	Strongly Agree
Privacy plays an important role in my organization's strategy	O	O	O	O	O	O	O

7.1. What is your opinion on the following statement?

Table B.2: Scale answer for question number 7.1

	Strongly Disagree	Disagree	Somewhat Disagree	Undecided	Somewhat Agree	Agree	Strongly Agree
Online media plays an important role in my organization's strategy	O	O	O	O	O	O	O

7.2. What type of privacy-related information is processed by your organization?

☐ Employee data

☐ Privacy-related customer data

☐ Third party privacy-related data

☐ Other .....

7.3. Which privacy drivers are most important for your organization?
Please rank, where 1 is most important
.... Talent .... Customer .... Reputation .... Compliance .... Risk management

7.4. The GDPR may require installment of a Data Privacy Officer (DPO). In which department will the DPO (most likely) be positioned?
O Legal / Compliance
O IT / Security
O Business
O Externally
O DPO not yet positioned

O We don't need DPO
O I don't know
O Other .....

7.5. Does your organization consider any of the following changes because of EU GDPR?

☐ Growing the consumer market base within the EU

☐ Shrinking the consumer market base within the EU

☐ Changing IT suppliers (including cloud providers

☐ Changing processes and systems related to notification

☐ Changing processes and systems related to right to access

☐ Changing processes and systems related to right to data portability

☐ Changing processes and systems related to product development

☐ Changing processes and systems related to information security

☐ Changing processes and systems related to data transfers to non-EU countries

☐ Other .....

7.6. How many of the following, privacy related elements are typical for your organization?
Number of FTE working on Privacy: .....
Number of individuals with data in organization's system: .....
Number of individuals with data in organization's system added last year: .....
Number of individuals requesting access to data in organization's system: .....
Number of individuals requesting removal of data from organization's system: .....

7.7. What is the biggest challenge your organization is facing because of EU GDPR?
.....

***8. What's your opinion on the following statement?**

Table B.3: Scale answer for question number 8

	Strongly Disagree	Disagree	Somewhat Disagree	Undecided	Somewhat Agree	Agree	Strongly Agree
Our GDPR compliance gap requires us to make significant changes	O	O	O	O	O	O	O

8.1. What's your opinion on the following statements
8.2. Please share below other considerations you may have on the GDPR compliance gap.
.....

***9. What is your opinion on the following statement?**
9.1. What is your opinion on the following statements?
9.2. Please share below other considerations you may have on privacy-related investments.
.....

***10. What is your opinion on the following statement?**
10.1. What is your opinion on the following statements?
10.2. Please share below other considerations you may have on privacy-related investments.
.....

Table B.4: Scale answer for question number 8.1

	Strongly Disagree	Disagree	Somewhat Disagree	Undecided	Somewhat Agree	Agree	Strongly Agree
Our GDPR compliance gap requires us to make significant changes to the organizations governance	O	O	O	O	O	O	O
Our GDPR compliance gap requires us to make significant changes to third party management	O	O	O	O	O	O	O
Our GDPR compliance gap requires us to make significant changes to legal management	O	O	O	O	O	O	O
Our GDPR compliance gap requires us to make significant changes to data management	O	O	O	O	O	O	O
Our GDPR compliance gap requires us to make significant changes to information security	O	O	O	O	O	O	O
Our GDPR compliance gap requires us to make significant changes to IT Systems	O	O	O	O	O	O	O

Table B.5: Scale answer for question number 9

	Strongly Disagree	Disagree	Somewhat Disagree	Undecided	Somewhat Agree	Agree	Strongly Agree
My organization will be investing in privacy-related changes over the coming years	O	O	O	O	O	O	O

Table B.6: Scaling answer for question number 9.1

	Strongly Disagree	Disagree	Somewhat Disagree	Undecided	Somewhat Agree	Agree	Strongly Agree
My organization will be investing in privacy-related changes to governance	O	O	O	O	O	O	O
My organization will be investing in privacy-related changes to third party management	O	O	O	O	O	O	O
My organization will be investing in privacy-related changes to legal management	O	O	O	O	O	O	O
My organization will be investing in privacy-related changes to data management	O	O	O	O	O	O	O
My organization will be investing in privacy-related changes to information security	O	O	O	O	O	O	O
My organization will be investing in privacy-related changes to IT systems	O	O	O	O	O	O	O

Table B.7: Scale answer for question number 10.

	Strongly Disagree	Disagree	Somewhat Disagree	Undecided	Somewhat Agree	Agree	Strongly Agree
My organization will be profiting from privacy related changes over the coming years	O	O	O	O	O	O	O

Table B.8: Scale answer for question number 10.1

	Strongly Disagree	Disagree	Somewhat Disagree	Undecided	Somewhat Agree	Agree	Strongly Agree
My organization will be profiting from privacy related changes to governance	O	O	O	O	O	O	O
My organization will be profiting from privacy related changes to third party management	O	O	O	O	O	O	O
My organization will be profiting from privacy related changes to legal management	O	O	O	O	O	O	O
My organization will be profiting from privacy related changes to data management	O	O	O	O	O	O	O
My organization will be profiting from privacy related changes to Information Security	O	O	O	O	O	O	O
My organization will be profiting from privacy related changes to IT Systems	O	O	O	O	O	O	O

Thank you for taking the time to complete this survey! We truly value the information you have provided us. Your responses will play a part in our analyses of the GDPR and shed light on the state of affairs in privacy and data protection.

If you would like to contact us about the content of the survey, you can do so by emailing AnditaRahmiFaradina@student.tudelft.nl or NLRiskGDPRSurvey@deloitte.nl. You can also leave your questions, feedbacks or comments in the box below.

Many thanks,

How would you rate this survey?
Poor .... Okay .... Great

How did you find this survey?
O Direct Invitation
O Forwarded Invitation
O Social Media
O Online
O Other .....

In case you would like to receive a copy of the survey report by email, please provide your email address below
.....

Do you have any comments, questions or feedbacks?
.....

C

Data Treatment

Collected survey data from the chosen platform (SurveyMonkey) is downloaded to make further processes plausible in the chosen statistics application (SPSS). This part explicates data cleaning and preparation done of the original data. Following this nature, this appendix is written in two section. The first section discusses the 'clean up' treatment. In this section, variable and individual cases removal and corrections are discussed. The second section discusses 'data preparation' needed for the next analysis and model estimation part. All recoding done and dummy variable creation is reported here.

C.1. Data Clean Up

Like most common data downloaded from a different platform, the raw data contains unnecessary or incorrectly named variables, as well as incomplete or error individual cases. Hence, data clean up is the first essential step performed before moving further to analyzing the data. This section reports the performed cleaning measures, which is divided into two subsections focusing on variables and individual cases.

C.1.1. Variable Clean Up

Table C.1: Removed Variables

Removed Variables	**Remarks**
Email Address	Auto generated by platform. Not needed.
First Name	Auto generated by platform. Not needed.
LastName	Auto generated by platform. Not needed.
Custom 1	Auto generated by platform. Not needed.

Table C.2: Renamed Variables. Asterisk (*) indicates mandatory survey questions.

Renamed Variables		
Original Name	**Updated Name**	**Question Number**
1. Your organization is headquartered in:	Headquarter	1*
2. Regional footprint of your organization : (please have this footprint in mind for remaining questions)	Region.EU	2*
V12	Region.America	2*
V13	Region.AsiaPac	2*

Continuation of Table C.2

Original Name	Updated Name	Question Number
V14	Region.Other	2*
3. Principal industry / sector of your organization: (as seen from headquarters)	Sector	3*
V16	Sector_Other	3*
4. Total gross revenue last year: (as seen from headquarters, 1 USD 1.1 Euro)	Revenue	4*
5. Number of employees in your organization: (as seen from headquarters)	TotalEmployee	5*
6. Your role in the organization:	Role	6*
V20	RoleOther	6*
7. What's your opinion on the following statement? 	PrivacyImportance	7*
7.1. What's your opinion on the following statement? 	OnlineMediaImportance	7.1
7.2. What type of privacy-related information is processed by your organization?	DataType.Employee	7.2
V24	DataType.Customer	7.2
V25	DataType.ThirdParty	7.2
V26	DataType.Other	7.2
V27	DataType.Other2	7.2
7.3. Which privacy drivers are most important for your organization? (please rank, where 1 is most important)	Driver.Customers	7.3
V28	Driver.Talent	7.3
V29	Driver.Reputation	7.3
V30	Driver.Compliance	7.3
V31	Driver.RiskManagement	7.3
7.4. The GDPR may require installment of a Data Privacy Officer (DPO). In which department will the DPO (most likely) be positioned?	DPOPosition	7.4
V33	DPOPosition.Other	7.4
7.5 Does your organization consider any of the following changes, because of the GDPR?	ConsideredChange.GrowMarketBase	7.5

Continuation of Table C.2

Original Name	Updated Name	Question Number
V35	ConsideredChange.ShrinkMarketBase	7.5
V36	ConsideredChange.ITSuppliers	7.5
V37	ConsideredChange.Notification	7.5
V38	ConsideredChange.AccessRight	7.5
V39	ConsideredChange.DataPortability	7.5
V40	ConsideredChange.ProductDevelopme	7.5
V41	ConsideredChange.InfoSec	7.5
V42	ConsideredChange.DataTransferNonEU	7.5
V43	ConsideredChange.Other	7.5
V44	ConsideredChange.Other2	7.5
7.6 How many of the following, privacy-related elements are typical for your organization?	PrivacyElement.FTE	7.6
V45	PrivacyElement.IndividualsWithData	7.6
V46	PrivacyElement.IndividualsWithDataAddedLastYear	7.6
V47	PrivacyElement.RequestToAccess	7.6
V48	PrivacyElement.RequestToRemove	7.6
7.7 What is the biggest challenge your organization is facing because of the GDPR?	BiggestEUGDPRChallenge	7.7
8. What's your opinion on the following statement?	ComplianceGap.Overall	8*
8.1. What's your opinion on the following statements?	ComplianceGap.Governance	8.1
V52	ComplianceGap.ThirdPartyMgmt	8.1
V53	ComplianceGap.LegalMgmt	8.1
V54	ComplianceGap.DataMgmt	8.1
V55	ComplianceGap.InfoSec	8.1
V56	ComplianceGap.ITSystem	8.1
8.2. Please share below other considerations you may have on the GDPR compliance gap:	ComplianceGap.Other	8.1
9. What's your opinion on the following statement?	PlannedInvestment.Overall	9*
9.1. What's your opinion on the following statements?	PlannedInvestment.Governance	9.1
V60	PlannedInvestment.ThirdPartyMgmt	9.1
V61	PlannedInvestment.LegalMgmt	9.1
V62	PlannedInvestment.DataMgmt	9.1
V63	PlannedInvestment.InfoSec	9.1
V64	PlannedInvestment.ITSystem	9.1
9.2. Please share below other considerations you may have on privacy-related investments:	PlannedInvestment.Other	9.1
10. What's your opinion on the following statement?	ExpectedBenefit.Overall	10*

Continuation of Table C.2

Original Name	Updated Name	Question Number
10.1. What's your opinion on the following statements?	ExpectedBenefit.Governance	10.1
V68	ExpectedBenefit.ThirdPartyMgmt	10.1
V69	ExpectedBenefit.LegalMgmt	10.1
V70	ExpectedBenefit.DataMgmt	10.1
V71	ExpectedBenefit.InfoSec	10.1
V72	ExpectedBenefit.ITSystem	10.1
10.2. Please share below other considerations you may have on the expected impact from GDPR:	ExpectedBenefit.Other	10.1
How would you rate this survey?	SurveyRate	n/a
How did you find this survey?	SurveySource	n/a
V76	SurveySource.Other	n/a
In case you would like to receive a copy of the survey report by email, please provide your email address below:	Email	n/a
Do you have any comments, questions, or feedbacks?	Comments	n/a

End of Table

C.1.2. INDIVIDUAL CASES CLEAN UP AND CORRECTION

A number of cases are excluded from further analyses. There are three types of cases that need to be excluded: trial cases, incomplete cases and illogical cases.

TRIAL CASES

Trial cases are cases recorded by the system when researcher makes trial inputs. Trial input was intended to ensure the logic of publicly accessed survey still works as designed and to guide the researcher in validating responses. Trial input is not intended to be recorded. However, the chosen survey system would still record any response, including the incomplete ones. The identity of excluded trial cases are as follows in Table C.3.
Total data left = 283 - 4 = 279.

Table C.3: Trial Cases

No	Respondent ID	Collector ID	Start Date	End Date	IP Address
1	6069283131	152636315	1/23/2017	1/23/2017	145.94.193.235
2	6070344282	152636315	1/24/2017	1/24/2017	145.94.197.216
3	6078662162	152636315	2/2/2017	3/21/2017	145.94.209.141
4	6203532746	152636335	5/18/2017	5/23/2017	145.94.210.74

INCOMPLETE CASES

Incomplete cases are results from initially plausible respondents not finishing the survey.

- Not filling in mandatory questions Number 8. Compliance Gap.

  Total data left: 279 – 114 = 165

- Not filling in mandatory questions Number 9. Planned Investment.

  Total data left: 165 – 4 = 161

- Not filling in mandatory questions Number 8. Compliance Gap.

  Total data left: 161 – 4 = 157

OUTLIERS AND IRRATIONAL CASES

Outliers can be easily pointed out from the 5 scale variables of: 'Total FTE', 'Total Individual Data' 'Total Individual Data Added Last Year', 'Total Access Request' and 'Total Removal Request', as well as 3 ordinal variables of: 'Overall Perceived Gap', 'Overall Planned Investment' and 'Overall Expected Impact'. Outliers can prevail as unique cases or as error/illogical inputs. Unique cases are kept while the illogical ones are deleted. To determine whether the outliers need to be excluded, the following assumptions are made.

1. The combination between 'Total FTE on Privacy', 'Total Individual Data' 'Total Individual Data Added Last Year', 'Total Access Request' and 'Total Removal Request'. Examples include too many Privacy FTE compared to total individual data; Too many Privacy FTE compared to total individual data; Too many individual data added last year compared to the existing data (more than 200%).

   If irrational, juxtapose the combination with the 'Role', 'Sector', and 'Size' of the company. Lastly, if 'Role', 'Sector', and 'Size' still do not give enough support, check the short-answer type of question if any of their remarks give support to keep or exclude the case.

2. The combination between 'Compliance Gap Overall', 'Planned Investment Overall' and 'Expected Impact Overall'. Most combinations are rational or at least can come up with a plausible reasoning. The following two combinations, however, is exceptional. These are where the planned investment does not follow the nature of the expected impact nor the perceived gap.

Table C.4: Removed Individual Cases

No	Respondent ID	Collector	Remarks
1	6314445156	Web Link 1	Lack of knowledge is detected. 480 Privacy FTE, 140 Individual Data, Has all high perceived gap, planned investment and expected impact but does not consider any changes.
2	6314749760	Web Link 1	Clearly stated that the respondent doesn't understand a lot of terms. Doesn't indicate the possession of customer data, which is unnatural for a telecom company.
3	6316845589	Web Link 1	Lack of knowledge is detected. 2000 Privacy FTE, 3000 Individual Data, Has all high perceived gap, planned investment and expected impact but does not consider any changes.
4	6316845589	Web Link Indonesia Trade Association	Clearly stated that the respondent doesn't understand a lot of terms.

Total data left: 157 – 4 = 153

C.2. DATA PREPARATION FOR ANALYSIS

C.2.1. VALUE CORRECTION

Value correction is needed to be done towards some individual cases. Mostly, the value correction is applied to mandatory question of 8, 9 and 10. There are two ways of value correction used in this study: using mean and using median. Value correction using mean is applied to mask the aforementioned mandatory questions (Number 8, 9 and 10) with the mean of each subheading questions of 8.1, 9.1 and 10.1. Subsequently, value correction of these mandatory number that still has value of 0 is masked with the median of each mandatory number. This is necessary to be done to have all the mandatory questions has a valid answer without changing the overall tendency of the data set.

D

Additional Details on Dependent Variables and Bivariate Tests

D.1. Additional Details on Dependent Variables

D.1.1. Regional Foot Print

With four values of *Regional Footprint*, namely Europe, America, Asia and Other (See Section B), there are 15 combination of footprint regions in total. The type of question to make this combination possible can be seen in Appendix C.

As can be seen in Table D.1, most respondents, with 38% amount of companies in total (58), have footprints only in European Union. The second largest regional footprint is Asia-only. A large number of companies having footprint only in Asia is highly related to the fact that many of the respondents are located in Indonesia. Following footprint regions are Other-only (8%), EU-America-Asia (7%), EU-America (5%), America Only (5%), and All Region (3%).

Table D.1: Sample Distribution In Terms of **Regional Footprint** and Their Headquarter Location. Color coding is done per row, where darker color shows higher value. A = global footprint; B = EU, America, Asia, C = America, Asia, Other; D = EU, Asia, Other; E = EU, America, Other; F = EU & America; G = EU & Asia; H = EU & Other; I = America & Asia; J = America & Other; K = Asia & Other; L = EU Only; M = America Only; N = Asia Only; O = Other Only.

Headquarter Countries	**Regional Footprint**															**Total (n)**
	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	
Netherlands	2	1		1								12				16
United Kingdom	1	2				1					1	12	1	1	1	20
France											2	5			1	8
Other EU and EEA Countries	1	2			1	2		1				24	1			32
Other European Countries		1										1			1	3
Indonesia	1											3		34	4	42
Other Asian Countries						1	2	1					1	7	3	15
United States		3				3							4	1		11
Other American Countries		1											1		1	3
Australia												1		1		2
South Africa															1	1
Total Respondents	**5**	**10**	**0**	**1**	**1**	**7**	**2**	**2**	**0**	**0**	**3**	**58**	**8**	**44**	**12**	**153**

D.2. STATISTICAL TESTS ON EACH DEPENDENT VARIABLE AND INDEPENDENT VARIABLE

D.2.1. HYPOTHESIS 1: THE INFLUENCE OF REGIONAL FOOTPRINT

Companies with footprint in EU region plan more changes related to EU GDPR.

INDEPENDENT VARIABLE STATISTICS

Independent Variable to be tested with the Dependent Variables is *RegionalFootprint*. The variable is recoded into 3 categories of *EUOnly*, *EU and Other*, and *Non-EU*.

The statistics of the *RegionalFootprint* are shown in Table D.2 with histogram in Figure D.1.

Table D.2: *RegionalFootprint* Statistics

Variable	N	Mean	Std. Dev	Min	Max
RegionalFootprint	153	2.0588	0.90492	1	3

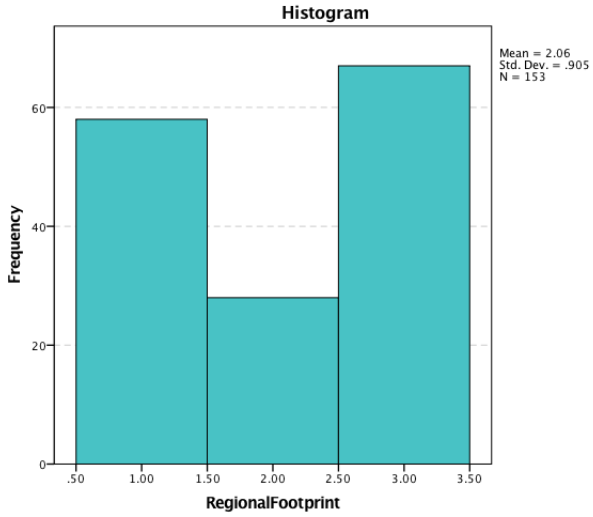


Figure D.1: Histogram of Regional Footprint

TEST RESULTS

For testing the association between a non-normal categorical independent variable (with 3 values) and an ordinal dependent variable, a non parametric test of Kruskal Wallis is chosen.

Table D.3: Bivariate Analyses - RegionalFootprint

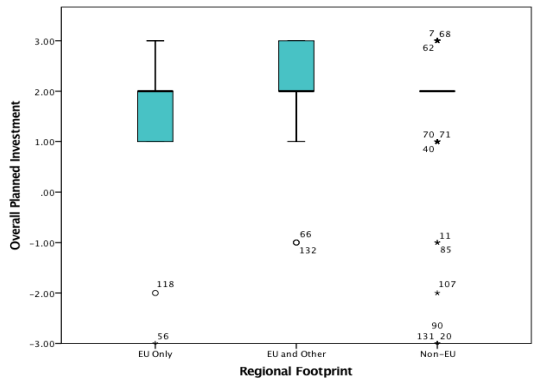
Dependent Variable	Chi-Square	Asyp.Sig.	Mean Rank
Planned Investment	3.334	0.189	EU and Other >Non-EU >EU Only
Considered Internal Changes	5.337	0.069	EU and Other >EU Only >Non-EU

The test results (Table D.3) show that there is no significance difference (0.05 level) among the three groups of region in terms of *PlannedInvestment* nor *ConsideredInternalChanges*. Figure D.2 shows the boxplots of the independent variable for each of the dependent variables.

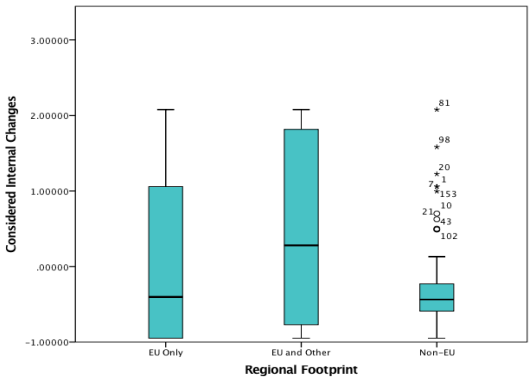
Decision: Reject first hypothesis.

D.2.2. HYPOTHESIS 2: THE INFLUENCE OF SIZE

Larger companies will have more planned changes related to EU GDPR



(a) Boxplot RegionalFootprint x Planned Investment



(b) Boxplot RegionalFootprint x Considered Internal Changes

Figure D.2: Boxplots of Regional Footprint

INDEPENDENT VARIABLE STATISTICS

Independent Variable to be tested with the Dependent variables is *Revenue*. *Revenue* is an ordinal variable with five values. The histogram of this variable is reported in Figure 5.4a. The statistics of *Revenue* are as follows (Table D.4).

Table D.4: Revenue Satistics

Variable	N	Mean	Std. Dev	Min	Max
Revenue	153	1.2418	1.32301	0	4

TEST RESULTS

To test the association between an ordinal independent variable and an ordinal dependent variable where normality is not found, a non parametric test of Spearman is chosen.

The test results (Table D.5) show that there is no significance difference (0.05 level) in *Planned Investment* for different company sizes. However, a significant difference in *Considered Internal Changes* is found between different company sizes. Figure D.3 shows the boxplots of the independent variable for each two dependent variables.

Table D.5: Bivariate Analyses - Revenue

Dependent Variable	Correlation Coefficient	Sig. (1-tailed)
Planned Investment	-0.044	0.293
Considered Internal Changes	0.182	0.012

Decision: Inconclusive. The hypotheses is proven with *Considered Internal Changes* as dependent variable but not with *Planned Investment.*

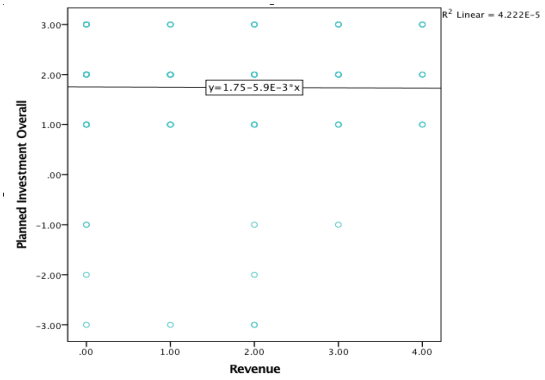
D.2.3. HYPOTHESIS 3: THE DIFFERENCES PER INDUSTRIAL SECTOR

The magnitude of planned changes by companies differs across industrial sectors

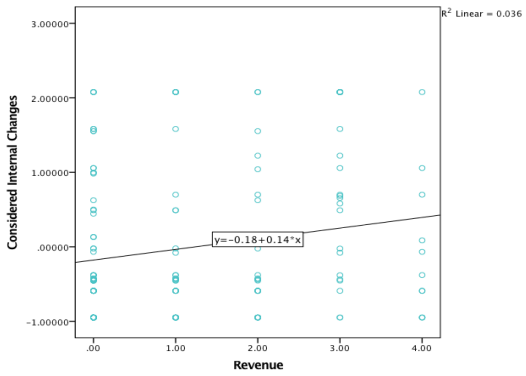
INDEPENDENT VARIABLE STATISTICS

Independent Variable to be tested with the Dependent variables is *IndustrialSector*. The sample distribution can be seen in Figure 5.3. As stated in the previous section, *IndustrialSector* is recoded into five categories to put in the model. Those categories are Media, IT/Information Security, Government, Finance, and Others.

The statistics of the *IndustrialSector* are shown in Table D.6.



(a) Scatterplot Revenue x Planned Investment



(b) Scatterplot Revenue x Considered Internal Changes

Figure D.3: Scatterplot of Revenue

Table D.6: *IndustrialSector* Statistics

Variable	N	Mean	Std. Dev	Min	Max
IndustrialSector	153	3.4118	1.33540	1	5

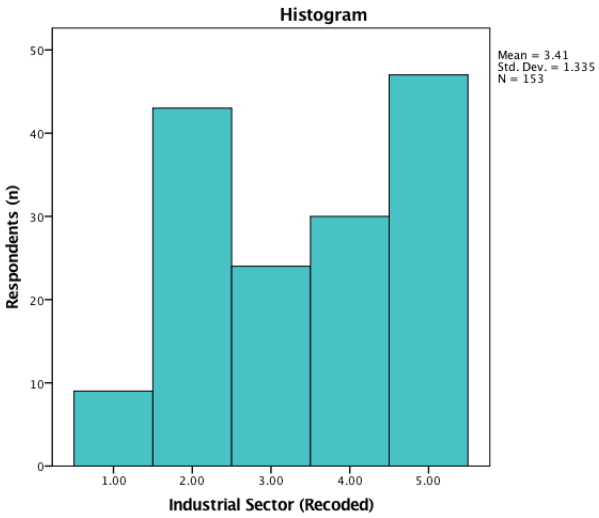


Figure D.4: Histogram of Industrial Sector

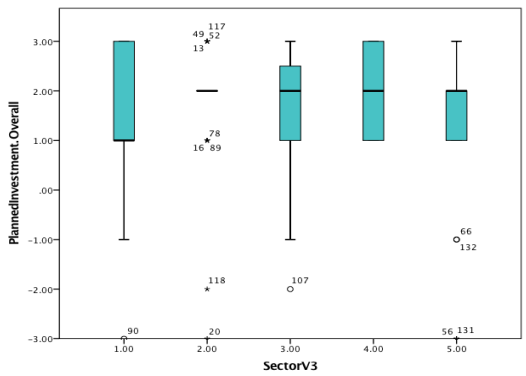
Table D.7: Bivariate Analyses - Industrial Sector

Dependent Variable	Chi-Square	df	Asyp.Sig.	Mean Rank
Planned Investment	1.351	4	0.853	Finance >IT/InfoSec >Government >Others >Media
Considered Internal Changes	3.348	4	0.501	IT/Infosec >Media >Finance >Other >Government

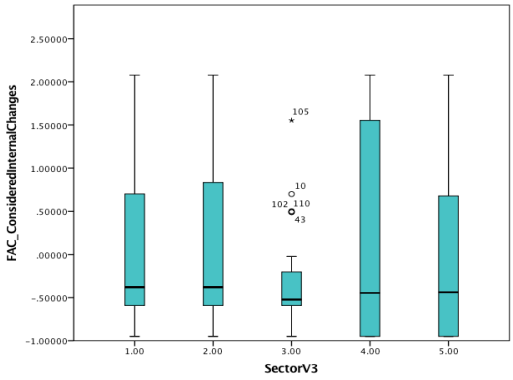
TEST RESULTS

For testing the association between a non-normal categorical independent variable (with 5 values) and an ordinal dependent variable, a non parametric test of Kruskal Wallis is chosen.

The test results (Table D.7) show that there is no significance difference (0.05 level) among the industrial sectors in terms of *PlannedInvestment* nor *ConsideredInternalChanges*. Figure D.5 shows the boxplots of the independent variable for each two dependent variables.



(a) Boxplot Industrial Sector x Planned Investment



(b) Boxplot Industrial Sector x Considered Internal Changes

Figure D.5: Boxplots of Industrial Sector

Decision: Reject third hypothesis.

D.2.4. HYPOTHESIS 4: THE INFLUENCE OF DPO EXISTENECE

The existence of DPO will lessen the changes planned by the companies

INDEPENDENT VARIABLE STATISTICS

Independent variable to be tested with the Dependent variables is *DPOExistence*. The statistics of this variable are shown in Table D.8

Table D.8: *DPOExistence* Statistics

Variable	N	Mean	Std. Dev	Min	Max
DPO Existence	153	0.6471	0.47945	0	1

TEST RESULTS

For testing the association between the categorical independent variable (with 2 values) and an ordinal dependent variable, a non parametric test of Mann-Whitney is chosen.

Table D.9: Bivariate Analyses - DPO Existence

Dependent Variable	Mann-Whitney	Z	Asymp.Sig. (2-tailed)	Mean Rank
Planned Investment	1839.5	-3.492	0.000	Has DPO >No DPO
Considered Internal Changes	2265.5	-1.573	0.116	Has DPO >No DPO

In terms *Planned Investment*, the test results (Table D.9) show that there is a significant difference (0.05 level) among the groups with DPO and no DPO. However, in terms of *Considered internal changes*, the test results show an *almost* significant difference (0.058) between the two groups. Figure D.6 shows the boxplots of the independent variable for each two dependent variables.

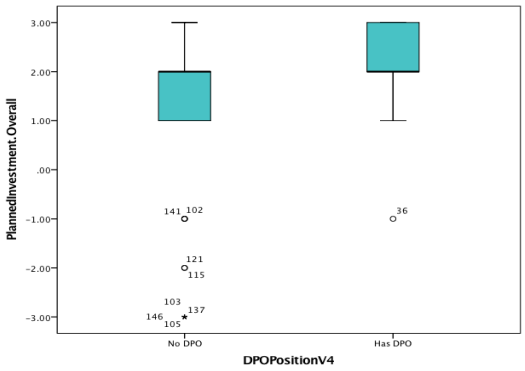
Decision: Accept the fourth hypothesis with a note that towards the *Considered Internal Changes*, the significant value is slightly missed.

D.2.5. HYPOTHESIS 5: THE INFLUENCE OF PERCEIVED GAP

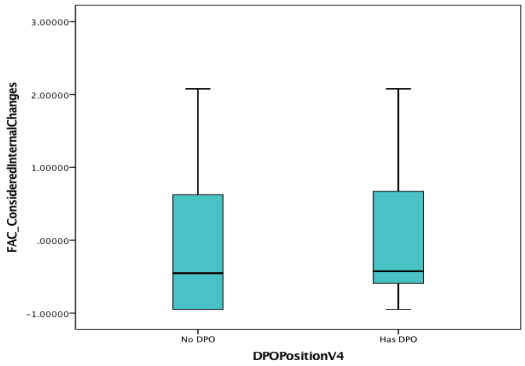
Companies that perceive higher compliance gap with EU GDPR have more planned changes to EU GDPR

INDEPENDENT VARIABLE STATISTICS

Independent Variable to be tested with the Dependent Variables is *PerceivedGap*. The statistics of this variable are shown in Table D.10 while the histogram in Figure **??**



(a) Boxplot DPO Existence x Planned Investment



(b) Boxplot DPO Existence x Considered Internal Changes

Figure D.6: Boxplots of DPO Existence

Table D.10: *PerceivedGap* Statistics

Variable	N	Mean	Std. Dev	Min	Max
PerceivedGap	153	1.5229	1.33813	-3	3

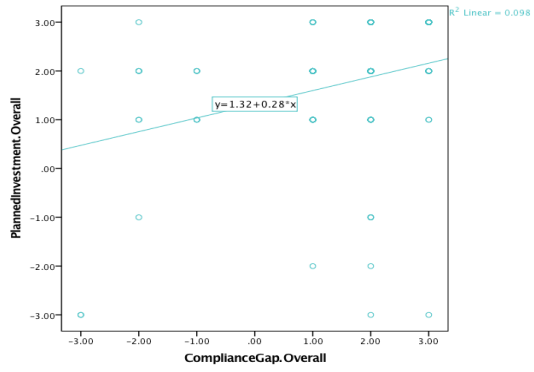
Table D.11: Bivariate Analyses - PerceivedGap

Dependent Variable	Correlation Coefficient	Sig. (1-tailed)
Planned Investment	0.000	0.306
Considered Internal Changes	0.073	0.184

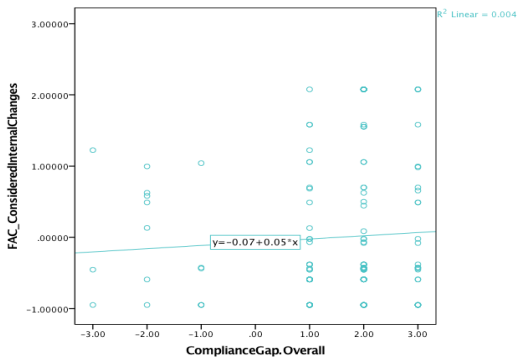
TEST RESULTS

For testing the association between the ordinal independent variable and an ordinal dependent variable, a non parametric test of Spearman is chosen.

The test results show in Table D.11 there is a significant difference (0.05 level) in terms of *Planned Investment* but not in terms of *Considered internal changes*. Figure D.7 shows the scatterplots of the independent variable for each two dependent variables.



(a) Scatterplot Perceived Gap x Planned Investment



(b) Scatterplot Perceived Gap x Considered Internal Changes

Figure D.7: Scatterplots of Perceived Gap

Decision: Inconclusive. Accept hypothesis in terms of Planned Investment; Reject in terms of Considered Internal Changes.

D.2.6. HYPOTHESIS 6: THE INFLUENCE OF EXPECTED IMPACT

Companies that expect more impact from EU GDPR have more planned changes related to EU GDPR

INDEPENDENT VARIABLE STATISTICS

Independent Variable to be tested with the Dependent Variables is *Expected Impact*. The statistics of this variable are shown in Table D.12 while the histogram in Figure **??**

Table D.12: *Expected Impact* Statistics

Variable	N	Mean	Std. Dev	Min	Max
Expected Impact	153	0.9281	1.71719	-3	3

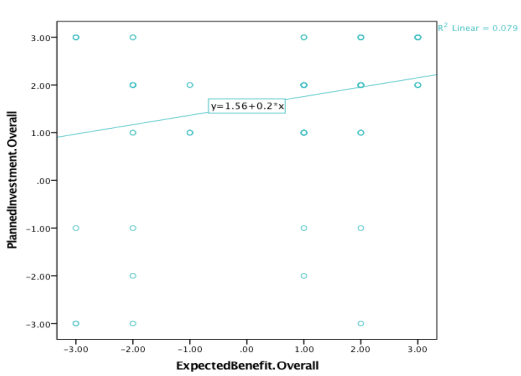
TEST RESULTS

For testing the association between the ordinal independent variable and an ordinal dependent variable, a non parametric test of Spearman is chosen.

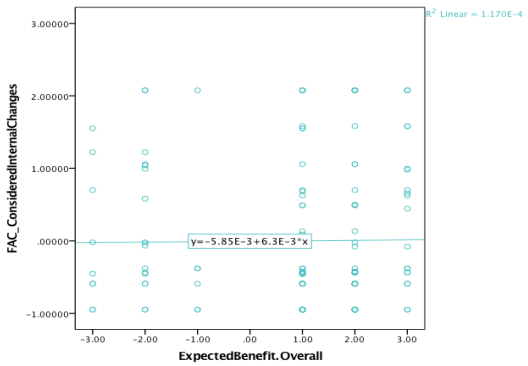
Table D.13: Bivariate Analyses - Expected Impact

Dependent Variable	Correlation Coefficient	Sig. (1-tailed)
Planned Investment	0.000	0.306
Considered Internal Changes	0.053	0.258

The test results show in Table D.13 there is a significant difference (0.05 level) in terms of *Planned Investment* but not in terms of *Considered internal changes*. Figure D.7shows the scatterplots of the independent variable for each two dependent variables.



(a) Scatterplot Expected Impact x Planned Investment



(b) Scatterplot Expected Impact x Considered Internal Changes

Figure D.8: Scatterplots of Expected Impact

Decision: Inconclusive. Accept hypothesis in terms of Planned Investment; Reject in terms of Considered Internal Changes.

D.2.7. HYPOTHESIS 7: THE INFLUENCE OF VALUE ON PRIVACY IMPORTANCE

Companies that place higher value on data privacy plan more changes related to EU GDPR

INDEPENDENT VARIABLE STATISTICS

Independent Variable to be tested with the Dependent Variables is *PrivacyImportance*. The statistics of this variable are shown in Table D.14 while the histogram in Figure 5.6a

Table D.14: *Privacy Importance* Statistics

Variable	N	Mean	Std. Dev	Min	Max
Privacy Importance	153	2.0654	1.14520	-3	3

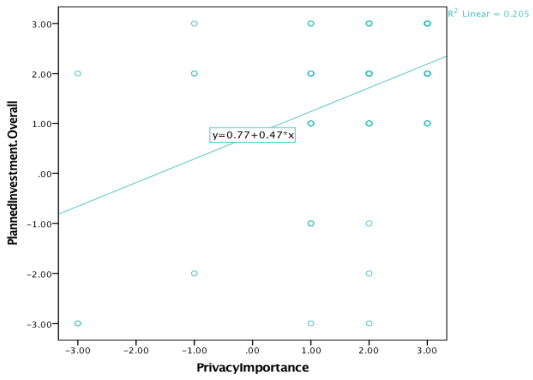
TEST RESULTS

For testing the association between the ordinal independent variable and an ordinal dependent variable, a non parametric test of Spearman is chosen.

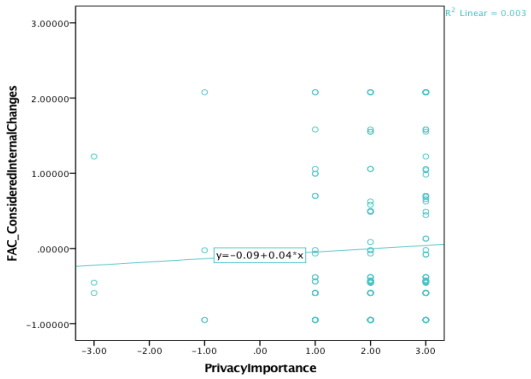
Table D.15: Bivariate Analyses - Privacy Importance

Dependent Variable	Correlation Coefficient	Sig. (1-tailed)
Planned Investment	0.000	0.356
Considered Internal Changes	0.117	0.097

The test results show in Table D.15 there is a significant difference (0.05 level) in terms of *Privacy Importance* but not in terms of *Considered internal changes*. Figure D.9shows the scatterplots of the independent variable for each two dependent variables.



(a) Scatterplot Privacy Importance x Planned Investment



(b) Scatterplot Privacy Importance x Considered Internal Changes

Figure D.9: Scatterplots of Privacy Importance

Decision: Inconclusive. Accept hypothesis in terms of Planned Investment; Reject in terms of Considered Internal Changes.

D.2.8. HYPOTHESIS 8: THE INFLUENCE OF DEPENDENCY ON PERSONAL DATA PROCESSING

Companies that place higher dependency on personal data processing consider less changes related to EU GDPR

INDEPENDENT VARIABLE STATISTICS

Independent variable to be tested with the Dependent variables is *ProcessThirdPartyData*. The statistics of this variable are shown in Table D.16

Table D.16: *Processing Third Party* Statistics

Variable	N	Mean	Std. Dev	Min	Max
Processing Third Party Personal Data	153	0.8235	0.38247	0	1

TEST RESULTS

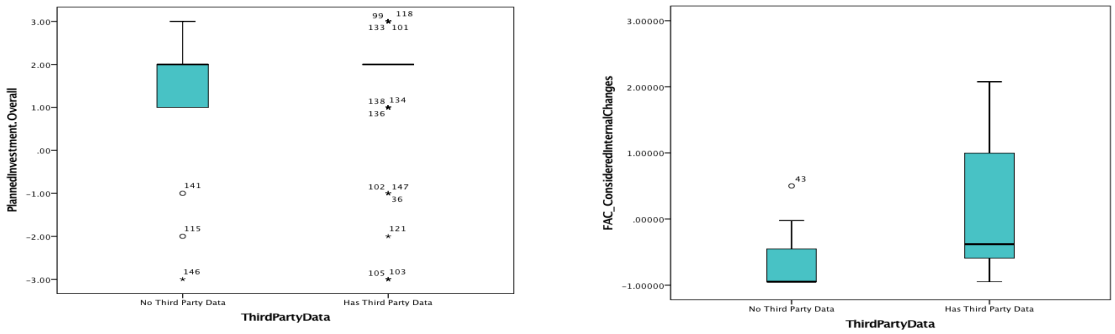
For testing the association between the categorical independent variable (with 2 values) and an ordinal dependent variable, a non parametric test of Mann-Whitney is chosen.

The test results (Table D.17) show that there is a significant difference (0.05 level) among the groups in terms of *Planned Investment* and *Considered Internal Changes*. Figure D.10 shows the boxplots of the independent variable for each two dependent variables.

Decision: Accept the eighth hypothesis.

Table D.17: Bivariate Analyses - Processing Third Party Personal Data

Dependent Variable	Mann-Whitney	Z	Asymp.Sig. (2-tailed)	Mean Rank
Planned Investment	1316.5	-2.020	0.043	Processing 3rdPty Data >Not Processing
Considered Internal Changes	799.5	-4.362	0.000	Processing 3rdPty Data >Not Processing



(a) Boxplot Processing 3rd Party Personal Data x Planned Investment

(b) Boxplot Processing 3rd Party Personal Data x Considered Internal Changes

Figure D.10: Boxplots of Processing 3rd Party Personal Data

D.3. MORE DETAILS ON THE MULTIVARIATE TESTS

D.3.1. *PlannedInvestment* AS DEPENDENT VARIABLE

MODEL ESTIMATION

An iterative process was performed using SPSS to estimate a linear regression model for the investment planning in preparing for EU GDPR. The method selected was the Stepwise estimation: it eliminates or adds one variable in each step until the best model is found. The variables are added according to their contribution to the explanation of the variance of the dependent variable and are eliminated if their contribution lacks statistical significance. The iterative process ends when all independent variables with significant contribution in explaining the variance are included in the model. Additionally, backward and forward method from SPSS were also executed but both of them gave similar results with stepwise method.

A disfigurement was discovered after estimating a preliminary model. A multicollinearity exist between some variables *Revenue* and *#TotalEmployee* (with correlation coefficient of 0.66). Both of the variables indicate the size of the surveyed companies. Additionally, the *Revenue* is associated well with the dependent variable compared to the *#TotalEmployee* with the dependent variable when tested individually. Hence, it is decided to exlude *#TotalEmployee* and keep the *Revenue* inside the model.

The model obtained has a practical significance (R^2) equal to 31.5%, which means that 31.5% of the total variance of the dependent variable that can be explained by the model. The statistically significant variables that influence the model are listed in Table D.18.

EXCLUDED VARIABLES

Not all independent variables are found to be statistically significant in influencing *Planned Investment*. The exluded variables are *Revenue, ProcessExtData, ExpectedImpact, DummyEUnOther, DummyEUOnly, DummyMedia, DummyIT, Dummy Government, DummyFinance, DummyExecutives, DummyITInfoSec, DummyLegal, DummyMarketing.*

The ones that are significant in bivariate test but excluded in multivariate test are *Expected Impact, ProcessExtData.* Meanwhile, *size* and the two categorical variable (*regional footprint* and *industrial sector*) represented by the dummies, are kept excluded as expected.

REGRESSION ASSUMPTION

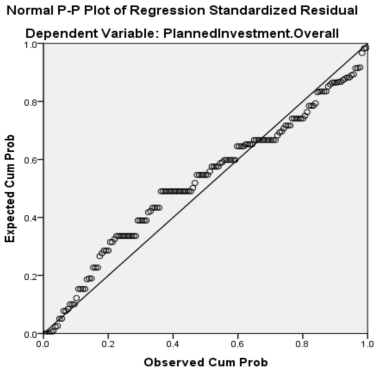
Before moving further to analyze the result of the model, regression assumptions of the models are checked. First, the homoscedastic residual error is not proven. The heteroscedasticity is found in the model as found in Figure D.11b. This figure hints that the prediction for lower value is not consistently accurate. Second, the

Table D.18: Multiple Regression Model (DV = Planned Investment)

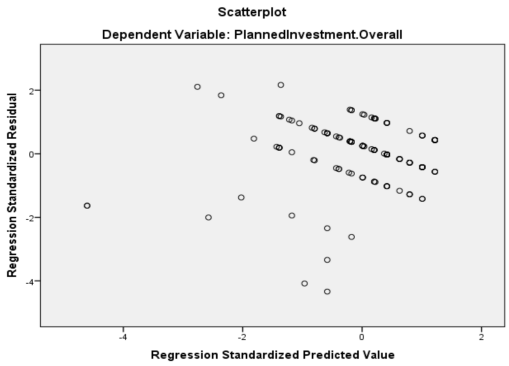
Variable	Mean (sd)	Unstandardized Coefficients		P >|z|	Collinearity Statistics	
		Coefficient	Std. Error		Tolerance	VIF
Privacy Importance	2.0654 (1.14520)	0.399	0.074	0.000	0.930	1.075
DPO Existence	0.6471 (0.4794)	0.674	0.174	0.000	0.953	1.049
Perceived Gap	1.5229 (1.33813)	0.143	0.064	0.027	0.902	1.109
Constant		0.267	0.196	0.176		

R Square = 0.315 ; Adjusted R Square = 0.301

normality can be seen in Figure D.11a. The deviation from the normal distribution is found to be moderate. Lastly, the multicollinearity can be checked from the VIF or the critical value. All of the VIF are lower than 10. Hence, there is no multicollinearity in the model.



(a) Residual Plot for the Regression Model with *Planned Investment* as Dependent Variable



(b) QQ Plot for the Regression Model with *Planned Investment* as Dependent Variable

Figure D.11: Residual Plots for the Regression Model with *Planned investment* as Dependent Variable

INTERPRETATION

As previously mentioned, the final regression model included three different variables: *Privacy Importance*, *Existence of DPO* and *Perceived Overall Gap*. On top of their statistically significant contribution to the dependent variable, the effect of these variables are in the same direction with varying scale. For the sample under study, the following statements can be derived from the analysis of the variables' correlation coefficient:

- The higher companies' perception on *Privacy Importance*, the more likely it is for them to *Planned* more Investment.
- The *existence of DPO* increases the tendency of planning higher investment.
- The higher companies' perception on compliance gap, the higher the tendency of planning large investment.

The first and third findings above fit with our hypotheses. However, the second finding related to existence of DPO influences the dependent variable in the opposite direction. It was assumed that the absence of DPO would mean higher compliance gap, which would eventually increase the planned investment. However, the result shows a different phenomenon. Instead of the absence of DPO, the existence of DPO is the factor that would increase the tendency to invest more to prepare for the EU GDPR. A plausible reason for this is the knowledge of the company induced by the existing DPOs. The existing DPOs have probably managed to make their companies more aware regarding the EU GDPR. Hence, more awareness on the gap with EU

GDPR is prevalent. Consequences of not meeting the EU GDPR also might has been alerted. In result, the tendency to plan large investment is higher for the companies with DPO.

There are much less independent variables that are found to be significantly associated the dependent variable. Despite the fact of their individual association with the dependent variable, a different result of multivariate model might still exist. As the multicollinearity is confirmed to be non existant, there are two plausible reasons left. First is the significantly small number of data compared to the independent variables. There are 153 number of cases in the sample, while there are 25 variables (as a result from recoding category variables to dummy variables). Only a small number of cases can be significantly explained by the number. Removing the variables did not give much difference as the iterative stepwise method had left out the insignificant independent variables at the first place. Second is the large gap of statistical significance of the included and excluded independent variables. An independent variable that are individually significant in explaining the dependent variable might be less significant compared to other independent variables. As a result of multiple regression, the not significant independent variables are left out. Hence, only the three independent variables can be seen to be influential to the dependent variable in this model.

The influences of the non-significant independent variables towards the dependent variable are still interesting to find out. For this purpose, the Enter method in the SPSS was chosen. Across the *Headquarter*, Indonesia is found to has the highest tendency to plan large investment, followed by US and countries in Europe. Across the *Regional Footprint*, companies that have footprint globally (i.e. EU, America, and Asia) is positively more correlated to the investment plan compared to the companies in EU Only. Interestingly, the companies in EU-only has a negative effect compared to the global ones. Across the *Industrial Sector*, media and advertisement is related negatively strong with the investment plant with the highest score. On the contrary, Finance is related positively with the dependent variable. Across the *Role of Respondents*, IT and Legal have a higher tendency to think the planned investment of their companies is high. Marketing, on the other hand has a low and even negative prediction on the number of investment planned. A more elaborated discussion on the plausible explanation behind these findings can be found in the next Discussion Chapter.

D.3.2. COMPARING THE TWO MODELS WITH BOTH DEPENDENT VARIABLES

Another multivariate regression to compare the two dependent variables were also performed. It is done by taking all significant variables from each previous models. Instead of stepwise method, enter method is chosen. The purpose is to not exclude the insignificant ones and see how these independent variables affect the dependent variables simultaneously. The resulting regression models can be seen in Table D.19.

The regression models are consistent with the earlier findings. The independent variables are consistently not overlapping for each regression model. The different IVs for each DVs hints that *Planned Investment* and *Considered Internal Changes*. This assumption is proven by the low spearman correlation between the two variables (coeff. 0.046). The scatterplot of these DVs can also be seen in Figure D.12. This can be interpreted that the two DVs measure two different dimension of companies way in planning changes.

One way to define the relation between the two dependent variables is as follows: *Considered Internal Changes* as the metrics measuring the initial decision (i.e., change or no change?), while *Planned Investment* as the metrics measuring the magnitude of investment planned (if change is decided, how large the investment is planned?). This is plausible because *Considered Internal Changes* is the latent variable resulting from nominal variables measuring what kind of changes are considered. Furthermore, as defined, *Planned Investment* is the ordinal variable measuring companies' level of agreement on investing in privacy-related changes.

Table D.19: Regression Models for DVs With Previously Significant IVs

Variable	Mean (sd)	DV = Planned Investment			DV = Considered Internal Changes		
		Coefficient	Std Error	P >|z|	Coefficient	Std Error	P >|z|
Constant		0.086	0.264	0.746	-1.059	0.242	0.000
DPO Existence	0.6471	**0.674**	**0.178**	**0.000**	0.098	0.162	0.547
Value on Privacy	2.0654	**0.385**	**0.075**	**0.000**	-0.021	0.068	0.760
Dependency on Personal Data Processing	0.8235	0.156	0.218	0.476	**0.782**	**0.200**	**0.000**
Perceived Gap	1.5229	**0.148**	**0.064**	**0.021**	0.053	0.059	0.368
Dummy EU and Other	0.1830	0.270	0.230	0.241	**0.697**	**0.210**	**0.001**
Dummy EU Only	0.3791	0.063	0.181	0.727	**0.492**	**0.166**	**0.04**
R Square / Adjusted Square		0.325 / 0.297			0.187 / 0.154		

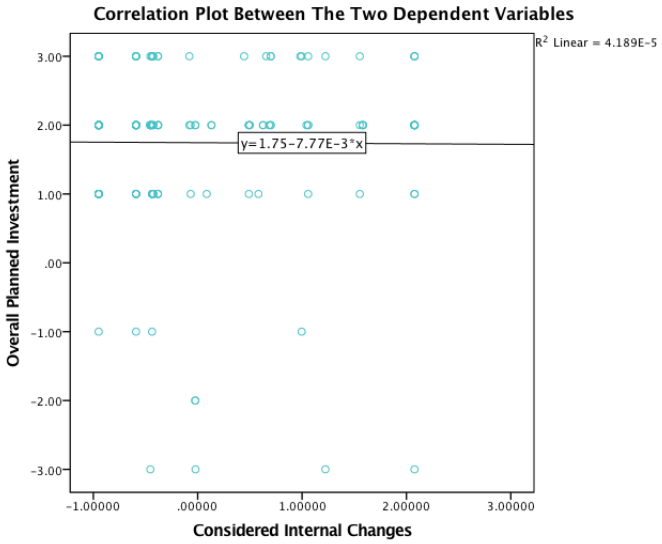


Figure D.12: Scatterplot for Planned Investment and Considered Internal Changes

BIBLIOGRAPHY

Ajigini, O. A. (2015). *Exploring security strategies for enterprise data protection in organisations*. Retrieved from http://hdl.handle.net/10500/20175

Ajzen, I. (1991). EU data protection policy. *Organizational Behavior and Human Decision Processes*, *50*, 179–211.

Akerlof, G. A. (1970). The market for "lemons
: Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics*, *84*(3), 488. doi:10.2307/1879431

Allianz. (2015). A guide to cyber risk: Managing the impact of increasing interconnectivity. Retrieved from http://www.agcs.allianz.com/insights/white-papers-and-case-studies/cyber-risk-guide/ on 08/05/2016.

Altman, I. (1976). *Environment and social behaviour*. Brooks/Cole Publishing Co. Retrieved from https://www.amazon.com/Environment-Social-Behaviour-Irwin-Altman/dp/0818501685?SubscriptionId=0JYN1NVW651KCA56C102&tag=techkie-20&linkCode=xm2&camp=2025&creative=165953&creativeASIN=0818501685

Anastasopoulou, K., Kokolakis, S., & Andriotis, P. (2017). Privacy Decision-Making in the Digital Era: A Game Theoretic Review. In *Hum. asp. inf. secur. priv. trust* (pp. 589–599). Springer International Publishing. doi:10.1007/978-3-319-58460-741

Armerding, T. (2017). The 15 biggest data breaches of the 21st century | cso online. http://www.csoonline.com/article/2130877/data-protection/data-protection-the-15-worst-data-security-breaches-of-the-21st-century.html. (Accessed on 08/06/2017).

Arrow, K. J. (2001). Uncertainty and the welfare economics of medical care. *Journal of Health Politics, Policy and Law*, *26*(5), 851–883. doi:10.1215/03616878-26-5-851

Ashford, W. (2012). Big changes expected as ec publishes data protection review. Retrieved from http://www.computerweekly.com/news/2240114258/Big-changes-due-in-revised-EC-data-protection-rules on 08/05/2016.

Banisar, D. & Davies, S. (1999). Global Trends In Privacy Protection: An International Survey of Privacy, Data Protection and Surveillance Laws and Developments. *Journal Of Computer And Information Law*, *18*(1).

Batty, L., Glozier, N., & Holland-Elliott, K. (2009). Interpretation of medical information acts by UK occupational physicians. *Occupational Medicine*, *59*(3), 153–158. doi:10.1093/occmed/kqp012

Bélanger, F. & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Q.* *35*(4), 1017–1042. Retrieved from http://dl.acm.org/citation.cfm?id=2208940.2208951

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, *11*(3-4), 245–270. doi:10.1016/s0963-8687(02)00018-5

Beldad, A. D., Jong, M. D., & Steehouder, M. F. (2009). When the bureaucrat promises to safeguard your online privacy: Dissecting the contents of privacy statements on dutch municipal websites. *Government Information Quarterly*, *26*(4), 559–566. doi:10.1016/j.giq.2009.05.002

Bennett, C. (2001). Privacy in the political system: Perspectives from political science and economics. *SSRN Electronic Journal*. doi:10.2139/ssrn.2230389

Berkgamp, L. (2002). The privacy fallacy: Adverse effect of europe's data protection policy in an information-driven economy. *Computer Law Security*, *18*(1).

Best, S. J., Krueger, B. S., & Ladewig, J. (2006). Privacy in the information age. *Public Opinion Quarterly*, *70*(3), 375–401. doi:10.1093/poq/nfl018

Borghi, M., Ferretti, F., & Karapapa, S. (2013). Online data processing consent under EU law: A theoretical framework and empirical evidence from the UK. *International Journal of Law and Information Technology*, *21*(2), 109–153. doi:10.1093/ijlit/eat001

Boyd, D. & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, *15*(8). doi:10.5210/fm.v15i8.3086

Bryman, A. (2006). Integrating quantitative and qualitative research: How is it done? *Qualitative Research*, *6*(1), 97–113. doi:10.1177/1468794106058877

Burghardt, T., Böhm, K., Buchmann, E., Kühling, J., & Sivridis, A. (2010). A study on the lack of enforcement of data protection acts. In *Next generation society. technological and legal issues* (pp. 3–12). Springer Berlin Heidelberg. doi:10.1007/978-3-642-11631-5_1

Bygrave, L. A. (2010). Privacy and data protection in an international perspective. *Scandinavian Studies in Law*, (56).

Bygrave, L. A. (2014). *Data privacy law: An international perspective*. Oxford University Press. Retrieved from https://www.amazon.com/Data-Privacy-Law-International-Perspective/dp/0199675554?SubscriptionId=0JYN1NVW651KCA56C102&tag=techkie-20&linkCode=xm2&camp=2025&creative=165953&creativeASIN=0199675554

Carson, A. (2015). The gdpr is here: What's a privacy pro to do next? Retrieved from https://iapp.org/news/a/the-gdpr-is-here-whats-a-privacy-pro-to-do-next/ on 07/08/2016.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*. SAGE Publications, Inc.

Creswell, J. W., Hanson, W. E., Plano, V. L. C., & Morales, A. (2007). Qualitative research designs. *The Counseling Psychologist*, *35*(2), 236–264. doi:10.1177/0011000006287390

DNews. (2013). How facebook sells your personal information - seeker. https://www.seeker.com/how-facebook-sells-your-personal-information-1766411494.html. (Accessed on 08/06/2017).

Duri, S., Elliott, J., Gruteser, M., Liu, X., Moskowitz, P., Perez, R., … Tang, J.-M. (2004). Data protection and data sharing in telematics. *Mobile Networks and Applications*, *9*(6), 693–701. doi:10.1023/b:mone.0000042507.74516.00

EC. (2012). Reform of eu data protection rules. Retrieved from http://ec.europa.eu/justice/data-protection/reform/index_en.htm on 01/02/2016).

EC. (2015). Eprivacy directive: Assessment of transposition, effectiveness and compatibility with proposed data protection regulation. Retrieved from https://ec.europa.eu/digital-single-market/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data on 01/07/2016).

Egelman, S., Felt, A. P., & Wagner, D. (2013). Choice architecture and smartphone privacy: There's a price for that. In *The economics of information security and privacy* (pp. 211–236). Springer Berlin Heidelberg. doi:10.1007/978-3-642-39498-0_10

Eisenhardt, K. M. (1989). Agency Theory: An Assessment and Review. *Acad. Manag. Rev. 14*(1), 57–74.

Enserink, B., Hermans, L., Kwakkel, J., Thissen, W., Koppenjan, J., & Bots, P. (2010). *Policy analysis of multi-actor systems*. Eleven International Publishing.

EU. (2017). Regulations, directives and other acts. Retrieved from https://europa.eu/european-union/eu-law/legal-acts_en on 14/12/2017).

European Union. (2016). Regulation 2016/679 of the European parliament and the Council of the European Union. *Off. J. Eur. Communities*, *2014*(March 2014), 1–88. doi:http://eur-lex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf. arXiv: arXiv:1011.1669v3

Gellman, R. (2014). Fair information practices: A basic history. *SSRN Electronic Journal*. doi:10.2139/ssrn.2415020

Grande, A. (2016). Top privacy cases of 2016: Midyear report - law360. https://www.law360.com/articles/813134. (Accessed on 08/06/2017).

Greene, J. C., Caracelli, V. J., & Graham, W. F. (1989). Toward a conceptual framework for mixed-method evaluation designs. *Educational Evaluation and Policy Analysis*, *11*(3), 255–274. Retrieved from http://www.jstor.org/stable/1163620

Harris, L. (1990). *The equifax report on consumers in the information age: A national opinion survey conducted for equifax inc. by louis harris ...* Equifax. Retrieved from https://books.google.nl/books?id=zu4gngEACAAJ

Hartlapp, M. & Falkner, G. (2009). Problems of operationalization and data in EU compliance research. *European Union Politics*, *10*(2), 281–304. doi:10.1177/1465116509103370

Husted, B. W. (2006). Agency, Information, and the Structure of Moral Problems in Business. *Organ. Stud. 28*(2), 177–195. doi:10.1177/0170840606067990

Jang-Jaccard, J. & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. doi:10.1016/j.jcss.2014.02.005

Jensen, M. C. & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, *3*(4), 305–360. doi:10.1016/0304-405x(76)90026-x

Katz, J. E. & Tassone, A. R. (1990). A report: Public opinion trends: Privacy and information technology. *Public Opinion Quarterly*, *54*(1), 125. doi:10.1086/269188

Kenny, S. & Borking, J. (2002). The value of privacy engineering. *Journal Of Information, Law And Technology*.

Kokolakis, S. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. doi:10.1016/j.cose.2015.07.002

Koops, B.-J., Cuijpers, C., Nouwt, S., Roosendaal, A., & Cehajic, S. (2009). EU fundamental rights agency: 'thematic study on assessment of data protection measures and relevant institutions' - country report on the netherlands. *TILT - Tilburg Institute for Law, Technology, and Society*.

Kuner, C. (2009). An international legal framework for data protection: Issues and prospects. *Computer Law & Security Review*, *25*(4), 307–317. doi:10.1016/j.clsr.2009.05.001

Kuzma, J. (2011). Empirical study of privacy issues among social networking sites. *J. Int'l Com. L. Tech*, *6*(74).

Lee, D.-j., Ahn, J.-H., & Bang, Y. (2011). Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection. *MIS Q. 35*(2), 423–444. Retrieved from http://www.jstor.org/stable/pdf/23044050.pdf

Leenes, R. & Kosta, E. (2015). Taming the cookie monster with dutch law – a tale of regulatory failure. *Computer Law & Security Review*, *31*(3), 317–335. doi:10.1016/j.clsr.2015.01.004

Leichtenstern, K., Bee, N., André, E., Berkmüller, U., & Wagner, J. (2011). An empirical evaluation of the compliance of game-network providers with data-protection law. *Trust Management*, *5*, 149–164.

Luftman, J. & McLean, E. R. (2004). Key Issues for IT Executives. *MIS Quarterly Executive*, *3*(2), 89–104.

Lynskey, O. (2014). Deconstructing data protection: the "added-value"of a right to data protection in the EU legal order. *Int. Comp. Law Q. 63*(3), 569–597. doi:10.1017/S0020589314000244

Mikkonen, T. (2014). Perceptions of controllers on EU data protection reform: A finnish perspective. *Computer Law & Security Review*, *30*(2), 190–195. doi:10.1016/j.clsr.2014.01.011

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science*, *11*(1), 35–57. doi:10.1287/orsc.11.1.35.12567

Milgrom, P. & Roberts, J. (1992). *Economics, organization and management*. Pearson.

Miltgen, C. L. & Peyrat-Guillard, D. (2013). Cultural and generational influences on privacy concerns: A qualitative study in seven european countries. *European Journal of Information Systems*, *23*(2), 103–125. doi:10.1057/ejis.2013.17

Mitroff, I. I. (1983). *Stakeholders of the organizational mind (jossey-bass management series/jossey-bass social and behavioral science series)*. Proquest/Csa Journal Div.

Morris, J. & Lavandera, E. (2012). Why big companies buy, sell your data - cnn. http://edition.cnn.com/2012/08/23/tech/web/big-data-acxiom/index.html. (Accessed on 08/06/2017).

Niglas, K. (2004). The combined use of qualitative and quantitative methods in educational research.

Pavlou, P., Liang, H., & Xue, Y. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal- Agent Perspective. *MIS Q. 31*(1), 105–136. doi:10.2307/25148783. arXiv: /ehis.ebscohost.com/

Peguera, M. (2015). In the aftermath ofGoogle spain: How the 'right to be forgotten' is being shaped in spain by courts and the data protection authority. *International Journal of Law and Information Technology*, *23*(4), 325–347. doi:10.1093/ijlit/eav016

Pfeifle, S. (2015). Gdpr: We have agreement. Retrieved from https://iapp.org/news/a/gdpr-we-have-agreement/ on 01/02/2016.

Poullet, Y. (2009). Data protection legislation: What is at stake for our society and democracy? *Computer Law & Security Review*, *25*(3), 211–226. doi:10.1016/j.clsr.2009.03.008

Raab, C. D. (1998). The distribution of privacy risks: Who needs protection? *The Information Society*, *14*(4), 263–274. doi:10.1080/019722498128719

Rudgard, S. (n.d.). Origins and historical context of data protection law. Retrieved from https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf.

Schoeman, F. (1984). Privacy: Philosophical dimensions. *American Philosophical Quarterly*, *21*(3), 199–213. Retrieved from http://www.jstor.org/stable/20014049

Shirer, M. (2016). Double-digit growth forecast for the worldwide big data and business analytics market through 2020 led by banking and manufacturing investments, according to idc. International Data Corporation. Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS41826116

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167. doi:10.2307/249477

Smith, Dinev, & Xu. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989. doi:10.2307/41409970

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477–560.

Solove, D. J. (2016). A brief history of information privacy law. *George Washington University Law School, Public Law Legal Theory Research Paper Series*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=914271

Son & Kim. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, *32*(3), 503. doi:10.2307/25148854

Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems*, *75*, 49–62. doi:10.1016/j.dss.2015.04.011

Tashakkori, A. & Teddlie, C. (2010). *Sage handbook of mixed methods in social & behavioral research*. The Sage handbook of. SAGE Publications. Retrieved from https://books.google.nl/books?id=v4wJF5hZhKgC

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2017). EU general data protection regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*. doi:10.1016/j.clsr.2017.05.015

TRUSTe. (2015). Data privacy is a major concern for consumers. Retrieved from http://www.truste.com/blog/2015/01/28/data-privacy-concern-consumers/

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, *22*(2), 254–268. doi:10.1287/isre.1090.0260

UN. (2016). *Data protection regulations and international data flows: Implications for trade and development*. Retrieved from http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1468

W., C. J. & Clark, V. L. P. (2010). *Designing and conducting mixed methods research*. SAGE Publications, Inc.

Wakefield, R. (2013). The influence of user affect in online information disclosure. *J. Strateg. Inf. Syst.* *22*(2), 157–174. doi:10.1016/j.jsis.2013.01.003

Walczuch, R. M. & Steeghs, L. (2001). Implications of the new EU directive on data protection for multinational corporations. *Information Technology & People*, *14*(2), 142–162. doi:10.1108/09593840110695730

Warren, S. D. & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193. doi:10.2307/1321160

Weaver, M. (2017). Uk public faces mass invasion of privacy as big data and surveillance merge | uk news | the guardian. Retrieved from https://www.theguardian.com/uk-news/2017/mar/14/public-faces-mass-invasion-of-privacy-as-big-data-and-surveillance-merge on 08/06/2017.

WEF. (2012). Personal data: The emergence of a new asset class. Retreived from https://www.weforum.org/reports/personal-data-emergence-new-asset-class on May 2016.

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*. 20th ser., *25*(1), 166. Retrieved from http://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431–453. doi:10.1111/1540-4560.00072

Zeldin, W. (2012). Online privacy law: Netherlands | law library of congress. https://www.loc.gov/law/help/online-privacy-law/netherlands.php. (Accessed on 07/26/2017).