UNIVERSITY OF TWENTE

From Wbp to GDPR: against which burden?

On the differences in terms of obligations and conditions and their implications for organizations in the Netherlands

Bachelor Thesis
BSc European Public Administration
1st supervisor: dr. Claudio Matera
2nd supervisor: dr. Pieter-Jan Klok

Sander Boxebeld

4-7-2018

Table of Content

List of abbreviations

AP	**Autoriteit Persoonsgegevens (*'Authority Personal Data', the data protection supervisory authority of The Netherlands)***
AVG	**Algemene Verordening Gegevensbescherming (*Dutch name and abbreviation of the GDPR*)**
CFREU	**Charter of Fundamental Rights of the European Union**
ECHR	**European Convention of Human Rights**
EU	**European Union**
GDPR	**General Data Protection Regulation**
TEU	**Treaty on European Union**
TFEU	**Treaty on the Functioning of the European Union**
UAVG	**Uitvoeringswet Algemene Verordening Gegevensbescherming (*'implementing law General Data Protection Regulation'*)**
UDHR	**Universal Declaration of Human Rights**
Wbp	**Wet bescherming persoonsgegevens (*'law for the protection of personal data', the Dutch predecessor of the GDPR*)**

Abstract

The General Data Protection Regulation (GDPR), the main EU data protection law, has recently replaced the pre-existing Data Protection Directive and all national data protection legislation that implemented that Directive. In the media, the suggestion aroused that this transition in data protection legislation would have large implications for data processing organizations. In this study, the validity of that statement was assessed for personal data processing organizations located and operating in the Netherland. Firstly, the pre-existing national data protection law Wet bescherming persoonsgegevens (Wbp) and the GDPR were analyzed separately, with an emphasis on the obligations and conditions both set for data processing organizations. Consequently, these analyses were compared in order to obtain an overview of differences in terms of obligations and conditions. Finally, these differences were analyzed on their implications for data processing organizations and interviews were conducted to collect opinions on and experiences with compliance of data protection legislation. The results of the study firstly show that the differences in terms of obligations between the GDPR and Wbp are modest, and secondly suggest that the implications of these differences for data processing organizations in The Netherlands are rather limited.

Keywords: GDPR, Wbp, personal data, data protection, compliance

1. Introduction

"We don't think you should ever have to trade it [*privacy*] for a service you think is free but actually comes at a very high cost. This is especially true now that we're storing data about our health, our finances, and our homes on our devices" – Tim Cook, CEO Apple (2015)

What is at stake in times of current technological developments, working 'in the cloud' and constant data sharing between more and more devices used in one's daily life (towards even fridges and ovens sharing data online), is obvious: our right to privacy and data protection. Therefore, it is more important than ever before that efforts are being made in order to protect our fundamental freedoms in the area of (online) privacy. On the other hand, 'laissez-faire' is considered crucial in our liberal western society; Free market-functioning should be able to take care of many aspects and lead to optimal outcomes. However, as the awareness has been raised that new legislation is required in order to safeguard universal fundamental rights (established in several international and European treaties and conventions, such as the Universal Declaration of Human Rights, European Convention of Human Rights and Charter of Fundamental Rights of the European Union), the EU has decided to implement an EU-wide General Data Protection Regulation (GDPR). This Regulation, having come into force on from the 25th of May 2018, will replace the old legislation. In the former situation, all EU Member States upheld differing data protection legislations, within the broad guidelines provided by the Data Protection Directive. The GDPR will harmonize data protection legislation for the whole EU area with the aim of simplifying cross-border operations for organizations processing personal data within the EU and for organizations outside the EU operating within the EU. However, organizations processing personal data firstly needed to change their policies and operations in order to comply with the GDPR. What has changed in terms of requirements set on data processing organizations, what are the resulting consequences and what is the burden organizations consequently have to bear? As pointed out below, there is a not a single answer to that by now.

Employers' associations (*'werkgeverskoepels'* in Dutch) VNO-NCW and MKB Nederland have warned that it will take a lot of effort for (especially smaller) organizations to ensure compliance with the GDPR from the 25th of May 2018 on (MKB Nederland & VNO-NCW, 2018). In the Dutch newspaper Het Financieele Dagblad, concerns have been expressed before the GDPR entered into force. In their article, the newspaper journalists warn for upcoming sanctions as a consequence of many organizations which are expected of not complying with the new regulation from 25 May 2018 on (Het Financieele Dagblad, 2017). Also in the broader frame of the EU, there are experts who think the GDPR will have many implications and cause many changes for companies' operations (Tikkinen-Piri et al., 2018). Nevertheless, there are also other points of view; for example, in an online magazine article, the Dutch privacy-expert Marion Bout-Tapper reacts to the article by Het Financieele Dagblad. She thinks the concerns are unnecessary and, although companies need to adapt and put effort into the process of change, there is no need to panic as the authorities are not likely to fine small- and medium-sized enterprises already from the beginning on (Bout-Tapper, 2017). Because of these mixed opinions, this study will assess the implications for organizations as a result of the transition from Wbp to GDPR.

1.1 Research question and subquestions

The desire of addressing this state of confusion and panic among Dutch organizations, as well as the recognition of the limited scope and resources that come along with writing a bachelor thesis, led to the decision to focus on the situation in one of the EU Member States, the Netherlands. Within this country, attention will be paid to the consequences of the new Regulation for organizations.

The main research question addressed is therefore:

RQ:
"To what extent has the transition from Wbp to GDRP resulted in differences in terms of arising obligations and conditions that affect the operations of organizations processing personal data operating in the Netherlands?"

In this country, the pre-existing national legislation Wbp (*Wet bescherming persoonsgegevens*) is replaced by the GDPR (General Data Protection Regulation). However, since the GDPR still leaves some room for national regulations and since the national governments also need to use this room for arranging the compliance scheme regarding the data protection, the Dutch government has enacted a national law that accompanies the GDP. This law, the 'Uitvoeringswet', mainly regulates the position of the national supervisor and plays a role if it comes to special cases, exceptions and specific situations (such as the connection to the freedom of speech). This study goes into the pre-existing and replacing legislations Wbp and GDPR (accompanied by the 'Uitvoeringswet') and consequently compares them. Hereby, the research question element 'transition from Wbp to GDPR' is analyzed, after which the focus can be on the implications of potential differences for organizations. Schematically, this can be represented in the following manner:

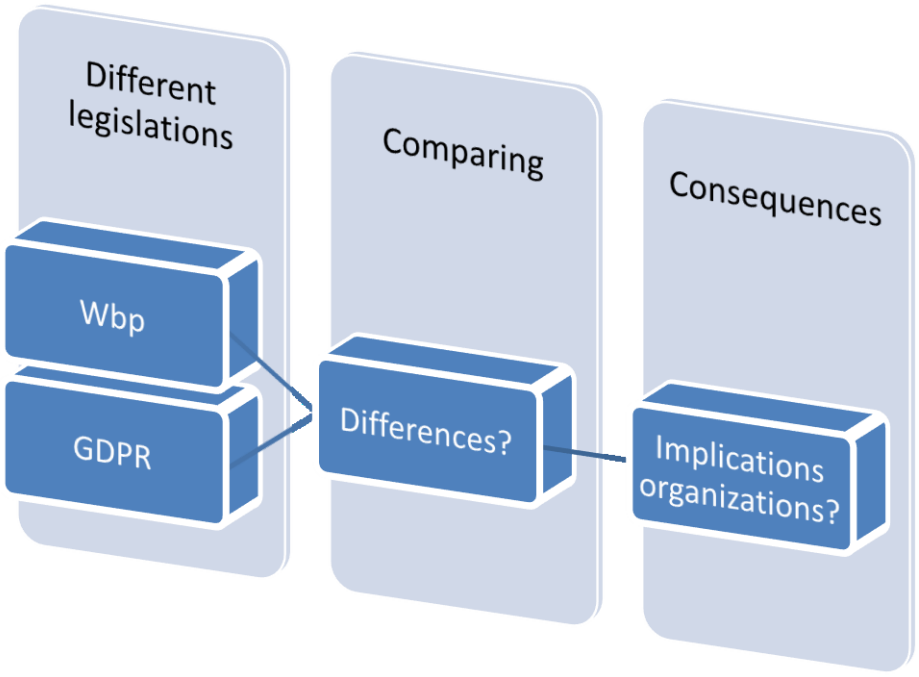

Figure 1. Schematic representation of the research steps (note that the first column does not indicate any hierarchy between the Wbp and GDPR)

Each vertical pillar is a step in the research, both a procedural order and a different type of analysis (law analysis, comparison of laws and analysing the consequences of the laws) and each blue box is an element of the overall research topic a subquestion needs to be dedicated to. The first two subquestions are placed in the same pillar as they belong to the same step; analysis of the two different legislations needs to be structured in the same way for the sake enabling a logical and structured comparison. Consequently, the first two subquestions (SQ1 and SQ2) do belong to the same phase of research. It would not make any difference if the GDPR would be analyzed as a first step and the Wbp as a second step, since the comparison of the two will only happen in the next step. Nevertheless, as the Wbp is the former legislation and the GDPR is the new one replacing it, it is only a logical order to analyze the Wbp in the first subquestion and the GDPR in the second.

Considering the arguments above, the following subquestions are formulated:

SQ1:

"What are the obligations and conditions arising from the Wbp that organizations processing personal data operating in the Netherlands had to comply with?

This first subquestion concerns an analysis of the Wbp, the data protection that the Netherlands upheld until the introduction of the GDPR. The subquestion above aims for an analysis of the Wbp on the obligations and conditions it sets for organizations to which the regulation applies, so organizations processing personal data operating in the Netherlands.

This subquestion is a descriptive one, describing the obligations and conditions resulting from the Wbp and set for the relevant organizations. The answer to the subquestion will be a description of obligations and conditions that organizations processing personal data needed to comply with.

SQ2:
"What are the obligations and conditions arising from the GDPR and the accompanying 'Uitvoeringswet' that organizations processing personal data operating in the Netherlands have to comply with?"

The second part of the analysis of data protection laws (and thus the second box in the first pillar of figure 1) is the analysis of the General Data Protection Regulation, the EU Regulation that is enforceable since the 25th of May 2018. As this Regulation leaves some room that national governments need to use in order to arrange a compliance scheme, but which can also be used to narrow the gap between the GDPR and the pre-existing national legislation, the Netherlands accompanied the GDPR with the Member State-specific 'Uitvoeringswet'. Both laws will be analyzed specifically with regards to the obligations and conditions they set for organizations falling within their scope, so organizations processing personal data operating in the Netherlands; although the GDPR is not limited to the Netherlands but applies within the whole EU, the research is limited to The Netherlands, which is the first reason why the subquestion is phrased as above. The second reason is that the Uitvoeringswet only applies to the Netherlands.

SQ3:
"To what extent are there differences in terms of their arising obligations and conditions between the pre-existing Wbp and the replacing GDPR and 'Uitvoeringswet'?"

The second pillar of this research involves the comparison of the two legislations separately analyzed under the previous pillar. The specific focus of the analysis is on the obligations and conditions arising from the legislations that apply to organizations processing personal data operating in the Netherlands. By means of a comparison, differences that may exist in terms of the obligations and conditions set by data protection legislation, that organizations processing personal data need to comply with, can be identified. Subquestion 3 develops an understanding of the differences that the introduction of the GDPR may have brought about. Ultimately, these differences are key within this study, as the following subquestion will address the consequences of these differences.

SQ4:
"To what extent did organizations processing personal data operating in the Netherlands have to change their operations in order to meet the obligations and conditions resulting from the GDPR and 'Uitvoeringswet'?"

Finally, the third and last pillar of this study (shown in Figure 1) addresses the consequences faced by relevant organizations resulting from the potential differences between the pre-existing and newly applying legislations. The underlying logic will be that in case the hypothetical situation occurs that, under the second pillar, the conclusion is that there are hardly any significant differences between the two legislations, the implications studied under the third pillar will also be of a minor nature. However, in the possible scenario that there are several significant differences between the Wbp on the one hand and GDPR and the accompanying Uitvoeringswet on the other, the likelihood of major implications for organizations will also increase. The core of this pillar's study will be the description of the effects of organizations and the efforts they need to make in order to fully comply with the GDPR and Uitvoeringswet.

1.2 Theory/concepts

In this section, the most important concepts used in the research are discussed, as well as theory hypothesizing the relationships among these concepts. Within the conceptualization part of this paragraph, a distinction is made by means of subsections (1.2.1 and 1.2.2) between data protection-concepts on one hand and data economy-concepts on the other. This distinction will be clarified in the hypothesis part of the paragraph (1.2.3).

1.2.1 Data Protection - Obligations and conditions

First, the concepts related to data protection are explained. The Wbp and the GDPR are the two main data protection legislations that will be analyzed within this study. With 'transition from Wbp to GDPR', as mentioned in the research question, the change of data protection legislation in effect is meant; while initially the Wbp was the data protection legislation in effect, this was replaced by the GDPR. In the analysis of the Wbp and GDPR, the focus will be on the obligations and conditions the

two legal documents set for data processing organizations. 'Obligations' and 'conditions', as mentioned in all subquestions, thus both need to be conceptualized. Conceptualization does not concern merely explaining the linguistic meaning of a word, but rather a cognitive understanding, a set of common characteristics which can be observed by human beings (Bajcic, 2011, p. 89). Concepts can also be called terms and characteristics can also be called facets, which are related in a way of either necessary & sufficient conditions, typologies, family resemblance or a set of similar variables (Van der Kolk, n.d.).

The conceptualization of obligation is chosen taking into account the legal nature of this study, as the focus will be on legal obligations that data-processing organizations need to comply with. The conceptualization is thus based on review of legal literature. Although an obligation might seem to be a straightforward concept, there is quite some disagreement on what this should actually entail (Himma, 2013). In the context of this study, an obligation is a duty resulting from a law that is legally enforceable. In other words, it is a duty that is established in a law and that one can enforce in court in case of a breach of this duty. This conceptualization, which is in line with several sources in legal literature (Allan, 2003; Himma, 2013; Himma, 2018; Essert, 2016) as well as with the Dutch legal framework (Book 6 Dutch Civil Code, Art. 6.1, 6.5), consists of three necessary conditions that thus all need to be fulfilled in order for a term to be an obligation. Schematically, this is presented in Figure 2.

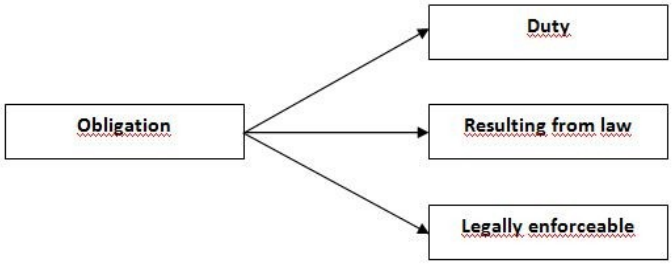

Figure 2. Schematic presentation of the conceptualization of 'condition' (*the order of facets is random and does not indicate any hierarchy*)

One might confuse an obligation with a condition, and there is also not a clear-cut distinction between the two, as courts sometimes treat a condition as an obligation (Adams, 2007). Also in this study, the conceptualization of condition is similar to the one of obligation. In this study, a condition is conceptualized as a duty resulting from a law on which an uncertain future event depends. In other words, it is a responsibility that is established in law, which needs to be fulfilled in order for a future event to be able to take place. An example of this can be formulated in the following way; Only in case an organization fulfills A, event B can take place. Event B could be, for example, persons providing their personal data to the organization. In this example, A is the condition, while B is the uncertain future event that depends on the condition. It is not enforceable in court that condition A is fulfilled, but it is required in order for event B to take place. So in case organizations want to process personal data, they need to fulfill the condition, or abstain from personal data processing otherwise. This conceptualization of a condition is in line with the explanation of Adams (2007) and again with the Dutch legal framework (Book 6 Dutch Civil Code, Art. 6.21). The schematic

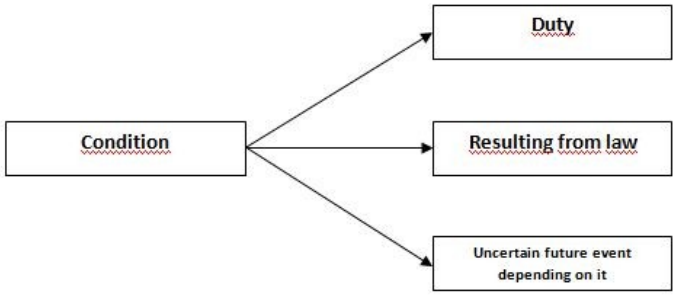

Figure 3. Schematic presentation of the conceptualization of 'condition' (*the order of facets is random and does not indicate any hierarchy)*

presentation of the conceptualization of a condition, with its three necessary conditions, is shown by Figure 3.

In the conceptualizations used in this research, there is thus a clear difference between an obligation and a condition. Nevertheless, they are mentioned together in the subquestions, as they both need to be fulfilled by organizations in order for them to be allowed to process personal data. Obligations and conditions set by the Wbp and the GDPR serve the aim of data protection. Data protection is a right established in the Dutch constitution (1983, Art. 10) as well as in the Charter of Fundamental Rights of the European Union (2000, Art. 8) and in the Treaty on European Union (2007, Art. 16). By means of the GDPR, the EU establishes a single data protection framework that covers the whole Union.

1.2.2 Data Economy – Organizations processing personal data and their operations

Another concept used in the research question and subquestions 1, 2 and 3 is 'organizations processing personal data'. This concept consists of three elements; 'organizations', 'processing' and 'personal data'. First there is 'organizations', which are, within this study, entities in the broad sense of the word. Krikorian (1935) would define such an organization as a 'purposive organization', a group of people that aims for accomplishing a common result. Although this definition is rather old, it is established in dictionaries to be a possible meaning of the term 'organization' nowadays (Oxford Dictionaries, 2018). Another element of the concept of 'organizations processing personal data' is 'personal data'. Within this study, 'personal data' is conceptualized as data related to facts or evaluation that can be identified to an individual. This is in line with a definition used in recent literature (Tracol, 2015), that bases its definition on an Opinion of the Advocate-General of the Court of Justice of the European Union and also corresponding to the definition of the Wbp (Wbp, Art. 1, 2017,). Examples of personal data are thus phone numbers, addresses and mail accounts, as these are types of factual information that can be retrieved to a specific individual, and also information such as someone's IQ, as that is a form of evaluative information that may be retrieved to a specific individual (Sauerwein & Linnemann, 2002). The third and last element of the conceptualization of 'organizations processing personal data' is the action of these organizations regarding personal data: 'processing'. Data processing is, within this research, as every action or set of actions that Is performed on personal data. (Taylor, 2015). All elements together, this leads to the

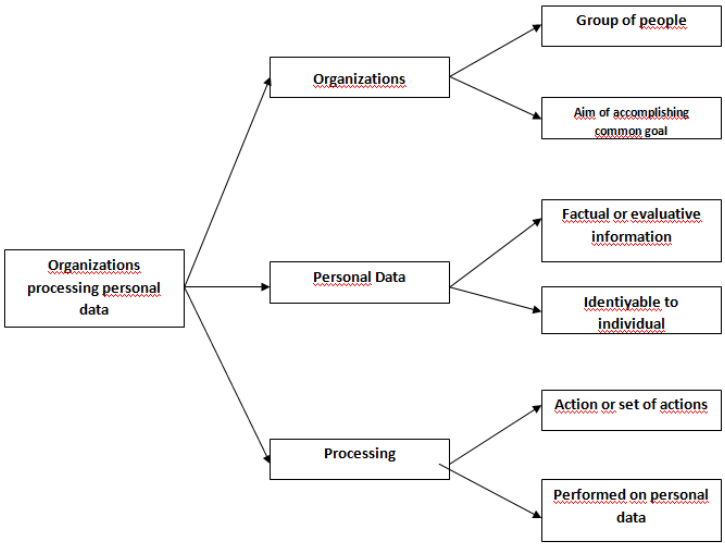

Figure 4. Schematic presentation of the conceptualization of 'organizations processing personal data' (the *order of facets is random and does not indicate any hierarchy*)

conceptualization of 'organizations processing personal data', which is schematically presented in Figure 4.

Apart from this concept, there is the concept of 'operations', mentioned in the research question and subquestion 4. In this study, 'operations' is meant as the functioning of organizations processing personal data. The study addresses the extent to which the transition from Wbp to GDPR affects this functioning of organizations. Organizations processing personal data and their operations are part of the data economy. The data-driven economy, also often referred to as digital economy, is a relatively new and rapidly increasing economic market in which personal data is considered to be an important economic tool and even called "the new currency", and in which businesses use these personal data as input in their business model and use it for commercial purposes (Crabtree et al., 2016). According to the European Commission (2017), personal data is so valuable that the total worth of European citizen's personal data could grow to almost €1 trillion per year as of 2020. Nevertheless, personal data are also often utilized not for commercial purposes but rather for information purposes, such as in organizations like municipalities and sport associations. Also this use is relevant within this study, as the Wbp and GDPR also regulate the processing of personal data for non-commercial purposes.

1.2.3 Theory on hypothesized relationships

As has been shown in sections 1.2.1 and 1.2.2, there are two sides of the same coin; On the one hand, there is the data-driven economy, in which personal data is a valuable economic tool and consumers are individual traders of their own data and on the other hand there is data protection, that regulates the use of this personal data in order to protect one's fundamental rights. Scientific literature stresses the importance of balancing these two sides, protecting individuals' fundamental rights to data protection and privacy, yet also leaving enough space for them to participate in the digital economy by trading their personal data (Crabtree et al., 2016). However, an important source of market failure exists in the digital economy, as there is a high degree of information asymmetry; many consumers, data subjects in the data-driven economy, are not aware of the extent to which personal data is collected on them and what happens to these data. Additionally, they are usually unaware of the value of their personal data, a value which is hard to determine after all (Malgieri & Custers, 2018). As a result, there is a lack of information among consumers about the value of their personal data and what is done with these data. This lack of information leads to greater uncertainty, as consumers are usually not enabled to make well-informed rational decisions regarding their privacy behavior. This uncertainty might prevent people from taking part in the digital economy at all, which reduces the economy's potential size (Kerber, 2016). If data protection legislation thus reduces this information asymmetry while at the same time leaves enough space for the trade of personal data, it might both safeguard the protection of individuals' fundamental rights as well as contribute to the data-driven economy.

This combination of safeguarding fundamental rights and strengthening the data-driven economy is exactly an objective of the GDPR, as it aims for raising the protection standards and thereby for safeguarding individuals' fundamental rights to data protection and privacy, while at the same time, it also aims for a higher degree of transparency. This greater extent of transparency might take away substantial information asymmetry effects and thus contributes to the data-driven economy as well.

Apart from this macro-economic perspective, there is also the micro-level approach that studies the impact of the GDPR on the level of organizations. Within this organization-level perspective, several questions aroused with the introduction of the GDPR, such as: 'What is the effect of the new data protection legislation on the functioning of companies that use personal data as economic tool?' and, what addresses also organizations in the broader sense, 'How does it affect the operations of other organizations, that use personal data only for non-economic purposes?' A study by Schneider (2018) suggests that the GDPR appears to significantly increase the burden for businesses regarding the generation of information about their data processing and thereby to increase their transparency in that respect.

This research would like to study that notion for not only businesses but organizations in the broader sense, as the Wbp and GDPR do not distinguish, in large parts of their provisions, between businesses and other organizations processing personal data; they simply speak of (data) 'processor' (GDPR, Art. 4, 2016; Wbp Art. 1, 2017). The setup of this research, using a comparative legal analysis followed by an analysis of the practical implications for organizations, is inspired by studies from Tikkinen-Piri et al. (2018) and Zwenne and Mommers (2016). Nevertheless, this research deviates from previously mentioned studies in two significant manners: firstly, by taking on a narrower territorial scope, focusing on data protection legislation and its consequences in the Netherlands exclusively. This brings about a different set of laws for the comparative analysis: Tikkinen-Piri et al. (2018) and Zwenne and Mommers (2016) compare the GDPR with the pre-existing Data Protection Directive, while this study compares the GDPR with the Dutch law that was enacted following the Data Protection Directive, the Wbp. On the other hand, this study has an extended material scope compared with previously mentioned studies by assessing the impact on organizations in the broad sense of the word rather than merely focusing on companies. This choice is given by the acknowledgement that various types of organizations are likely to face an increased burden in raising transparency about their processing of personal data, for the aforementioned reason of data protection legislation not distinguishing, in many provisions, between companies and other types of organizations. Given the suggestion of Schneider (2018), this study hypothesizes that the transition from Wbp to GDPR affects the operations of organizations processing personal data in a way that increases the burden for the latter.

1.3 Methodology

The research aims for answering the research question "To what extent will the transition from Wbp to GDRP change the situation for organizations processing personal data operating in the Netherlands?". This question is divided into four subquestions, that need to be answered.
The first subquestion (analyzed in Chapter 2) has explanatory, hermeneutic as well as logical elements (Matera, n.d.), as it analyses the Wbp in terms of the obligations and conditions arising from it that data processing organizations needed to comply with. A systematic approach is applied in order to identify these rules and conditions. First, by using literature review, a general introduction about the Wbp in a broader context is given, including the objectives of the law, the (legal) framework in which it operates and its history of being drawn. Subsequently , the content of the law is discussed, whereby there is (as previously mentioned) a focus on the obligations and conditions set for data processing organizations. Due to time constraints, not all provisions of the Wbp can be

analyzed, which is why the decision has been made to include those obligations and conditions that are considered to be most relevant for most organizations. This decision has been made on the basis of literature review (Engelfriet et al., 2018), and has lead to the exclusion of *inter alia* the provisions regarding sharing data with third countries. The provisions that were selected to be included in the analysis fall in the same categories for both the Wbp and GDPR, as this enables a more clear comparison of the two laws. Finally, the Wbp is discussed in terms of its enforcement; the law's supervision by supervisory authority AP is addressed. This is expected to give a clearer view of the compliance scheme and potential consequences in case of non-compliance. All together, Chapter 2 aims to give a complete understanding of the obligations and conditions set by the Wbp that organizations processing personal data had to comply with before the replacement of the Wbp by the GDPR.

The second subquestion also has explanatory, hermeneutic as well as logical elements, as the setup of the question is similar, although this subquestion is not about the Wbp but about the GDPR. Besides, the accompanying Uitvoeringswet is discussed here, which contains the legal basis for supervision and, to some extent, also application of the GDPR. This subquestion is about analysing the obligations and conditions arising from the law(s) that data processing organizations need to comply with. For the sake of enabling a well-structured comparison under the next subquestion, the structure used in this subquestion is the same as the one used in the previous subquestion. Therefore, a systematic approach is applied again. This enables the identification of differences, performed in chapter 4, with regards to the obligations and conditions that both laws set for data processing organizations. In the first section of chapter 3, the background of the law is discussed by means of a literature review. Its historical and legal contexts are analyzed (clarifying why the law was introduced, what its legal basis is and within which legal framework it operates), as this clarifies the reason for drawing the law as well as the scope of the law. In section 3.2, the content of the GDPR is examined in terms of the obligations and conditions resulting from it. Thirdly, in the last section of this chapter, the emphasis is on the enforcement of the law by the supervisory authority AP and the judicial system. All in all Chapter 3 is expected to give an understanding of the obligations and conditions set by the GDPR that data processing organizations need to comply with.

The third subquestion contains logical and explanatory elements, as it compares the Wbp and GDPR in terms of the obligations and conditions arising from them. It thereby makes use of a comparative approach. This chapter, Chapter 4, heavily relies on the findings of the previous two chapters, as their separate outcomes are compared with each other. The first section of the chapter compares the two laws themselves, thereby identifying similarities and differences in terms of obligations and conditions set. The second section of this chapter compares the interpretation and enforcement of the two laws. In both sections, the aim is as well to clarify the reasons for possible differences in terms of obligations and conditions set, as this may lead to a better understanding of them. In all sections of Chapter 4, comparative methods are used. For example, the same structures as used in chapters 2 and 3 is also used in Chapter 4, enabling a clear comparison. Also a table is drawn in order to obtain an overview of differences in terms of obligations and conditions between the two laws.

In Chapter 5, the fourth subquestion is addressed. The answer to this subquestion involves the outcomes of Chapter 4 to analyze the implications for data processing organizations in terms of the way they might need to change their operations in order to comply with the GDPR and related

Uitvoeringswet. The chapter examines the practical consequences for organizations resulting from the transition from Wbp to GDPR. Predominantly, a systematic approach is used by reviewing literature on the (expected) consequences for organizations. Of course, this partly depends on the answer to subquestion 3, that tells us the number of differences between the Wbp and GDPR. Nevertheless, a hypothesis, formulated in section 1.2.3, is that the burden for organizations has significantly increased as a result of the transition in data protection legislation.

On top of this literature study, some interviews with data processing organizations have been conducted in order to obtain an idea of the implications from the perspective of the ones facing these implications; after all, these organizations need to comply with the GDPR and they have experience with the practical implications of the transition in data protection legislation. These data processing organizations have been asked for an interview to explain the ways in which they adapted their operations in order to comply with the GDPR. Various organizations, all located in the region in which the researcher lives for practical reasons, have been approached for an interview, whereby in the process of approaching, the emphasis is on the composition of a pool of mixed organizations, such that the sample is as representative as possible for the variety of organizations existing. Some types of organizations were identified, which were: commercial private organization (business), non-profit private organization, public organization and semi-public organization. Apart from these types, organizations were also distinguished on the basis of their size, using the designations small, medium-sized and large, based on the number of employees criterion used in the categorization of companies by the Dutch government (Kamer van Koophandel, n.d.). Combining the different types and sizes, there were twelve categories in total. Considering it was difficult to have an interview for each of these organizations, taking into account the small time period available and the fact that only one chapter makes use of these interviews, the decision was taken that interviews would also be used in case not all of these categories could be interviewed. For all types of organizations, an organization was approached. If this organization was not able or willing to be interviewed within the time period that could be used for interviews, another organization within the same category was approached. In the end, for four of the nine categories (see Figure 5), an organization was willing to be interviewed.

Size	**Type**
Small	Commercial private organization (business)
Medium-sized	Public organization
Large	Semi-public organization
Small	Non-profit private organization

Figure 5. Overview of the interviewed personal data processing organizations (*the order that is used does not indicate any hierarchy among the organizations*)

Considering the variety among the organizations, both in terms of type of organization (public, semi-public, commercial private and non-profit private) and size (one-man, medium-sized and large), the sample is still considered to be representative in terms of including a variety of organizations. From these four organizations, an employee was asked who had knowledge of (and experience with compliance to) the GDPR. Three out of the four organizations were questioned via a personal interview. These personal interviews were semi-structured; although a questionnaire was prepared (see Appendix B) from which all questions were asked during the interview, there was also room for

additional remarks or questions from both the side of the interviewer and of the interviewee. The interviewee from the remaining organization, the non-profit private organization, was not able to be interviewed physically due to time constraints, which led to the decision to send the interviewee the questionnaire of Appendix B. In this way, the respondent could answer the questions as well. Moreover, it was emphasized that additional remarks or questions were also welcome.

In order to raise willingness to participate and to prevent non-complying organizations from not taking part, the first mail approaching the organizations clearly contained the guarantee of anonymous use of the interview in the final paper as well as the ability of the organization to end participation at any moment it would like to. These measures are also aimed at reducing the chance of bias in the sample or collected data. Bias in the sample may result from non-response or non-random methods of sampling, while bias in the collected data may result from the phrasing of questions, the circumstances of the interview or the interaction between interviewer and interviewee (Moser, 1951). The extent to which bias plays a role within the interviewing is discussed in section 7.2. Recognizing the potential of bias occurring, several measures have been taken, including the above-mentioned guarantee of anonymity and right to exit the study if the interviewee wishes to. Additionally, it was emphasized that all answers would be useful, with the aim of reducing social desirability effects. Finally, questions were phrased as neutral as possible. For example, even though the GDPR is hypothesized to be negatively affecting the functioning of organizations, the interviewees were asked to name both the positive and negative effects of the GDPR.

Combining the answers to the various subquestions will lead to the final conclusion, which will be the answer to the study's overall research question. This conclusion will clarify the similarities and differences between the Wbp and GDPR and the implications thereof for organizations that process personal data.

1.4 Scientific and societal relevance

The topic discussed in this study is of a clear societal relevance, as digitalization and data sharing is increasing further and further, which means it enters one's personal life more and more. With increased data sharing in the personal environment, there is a high need for a clear data protection framework. With the GDPR, the European Union sets this framework and harmonizes it for the whole European Union. However, the introduction of the GDPR also has the important effect of forcing a data processing organization to make efforts in order to comply with its standards.

Scientifically, relevance is defined in terms of which new knowledge is added by the study. In that respect, the topic gives the opportunity to generate new knowledge and needs to be examined further. Up until this point, science mainly focuses on the general implications of the GDPR, its relation to the right to privacy and general implications for companies. An example of a study that compares the Data Protection Directive with the GDPR is the study of Tikkinen-Piri et al (2018). With the case study of the Netherlands, the aim is to explore the implications for organizations operating in the Netherlands specifically, so not EU-wide and not business-specific. So far, Dutch literature has mainly compared the Data Protection Directive and Wbp on the one hand and the GDPR on the other hand in a very broad manner, such as Zwenne and Mommers (2016) do. Contrarily, this study focuses on specific changes between the Wbp and the GDPR and their implications for organizations in the

Netherlands and collects experiences and opinions of personal data processing organizations in order to test the nature and gravity of these implications.

Societally, a study is relevant in case the new knowledge added by the study has the ability to contribute to societal welfare. In that respect, this study has the ability to decrease the current state of confusion. As mentioned in the introduction, newspaper articles and employers' associations (*werkgeverskoepels*) suggest the situation of concerns and panic surrounding the introduction of the GDPR. Uncertainty and panic is always bad for economic prospects and investments, as the value of an economy is partly determined by behaviour and psychology. It is in the interest of a whole society that its economy flourishes, so this uncertainty and panic think has to be dealt with in a careful and serious manner. This research examines whether these concerns and panic are justifiable. If the study's conclusion is that this is not the case, it might calm down markets and de-stress companies. On the other hand, if the conclusion is that this truly is the case, this may be a sign for the government and employers umbrellas to think about ways to compensate organizations for the large efforts they have to make or procrastinating the enforcement of the GDPR by the AP, as was suggested in the previously-mentioned article of Het Financieele Dagblad (2017).

2. Analysis of the Wbp in the light of arising obligations and conditions

In this chapter, the Wbp is analyzed, with special attention being paid to the obligations and conditions the law sets for data processing organizations. This is an essential step of the research, as the implications of the transition in data protection regime for data processing organizations can only be determined after having identified the differences, if any, between the pre-existing Wbp and the replacing GDPR. Before this comparison can take place, the two laws need to be analyzed separately. In that respect, this chapter will discuss the context, content and enforcement of the pre-existing data protection law in the Netherlands, the Wbp.

§ 2.1 Legal context of the Wbp

The *Wet Bescherming Persoonsgegevens (Wbp)* was the main Dutch data protection law that had been in force until the GDPR came into effect. It came into effect on the first of September 2001. By means of the Wbp, the Dutch government implemented Directive 95/46/EC (*on the protection of individuals with regard to the processing of personal data and on the free movement of such data*), also known as Data Protection Directive. The Wbp found its legal foundation in Article 10 of the Dutch constitution.

> Article 10: Privacy
> *1. Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to Act of Parliament.*
> *2. Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data.*
> *3. Rules concerning the rights of persons to be informed of data recorded concerning them and of the use that is made thereof, and to have such data corrected shall be laid down by Act of Parliament.*
> (Dutch constitution, 2017)

Article 10 of the Dutch constitution concerns the right to privacy and establishes, via its first paragraph, everyone's right to privacy. The second paragraph of the article obliges the Dutch parliament, the legislator, to constitute rules regarding the recording and spreading of personal data. According to paragraph three of Article 10, the Dutch parliament also needs to constitute rules that establish the right of persons to be informed of their recorded personal data and the use made thereof, as well as the right to have these data corrected. Thus, the Wbp provided for the fulfillment of the obligations stemming from Article 10, paragraphs two and three. Without the Wbp (and before the GDPR came into force), there would have been no legal basis to hold someone responsible in case of a breach of one's right to privacy (Zwenne et al., 2007). Legally, the Wbp thus had the objective of implementing the EU Data Protection Directive and the execution of paragraphs two and three of Article 10 of the Dutch constitution. Additionally, it also executed the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Treaty No. 108, compiled by the Council of Europe that was ratified by 51 Member States including the Netherlands (Council of Europe, 1981).

By implementing and executing these legal sources, the Wbp provided for the protection of personal data and thereby safeguarded the fundamental rights to protection of one's personal data and

privacy. These rights are established, *inter alia*, in Article 12 of the Universal Declaration of Human Rights (UDHR, 1948), Article 8 of the European Convention of Human Rights (ECHR, 1950), Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU, 2000) and Article 16 of the Treaty on the Functioning of the European Union (TFEU, 2007). Besides the safeguarding of these fundamental rights, the Wbp had the objective of maintaining the trust of consumers participating in the digital economy (Zwenne et al., 2007). By regulating the collection and use of personal data, the Wbp thus aimed for raising or upholding consumer trust in the digital economy.

§ 2.2 Content of the Wbp: obligations and conditions

§2.2.1 Definitions and sphere of influence of the Wbp

The Wbp did not apply in every case. As the law concerned personal data, it should first be made clear what the Wbp defined as personal data. As already conceptualized in the introductory chapter (section 1.2.2.), personal data concerns factual or evaluative information that is identifiable to an individual. This was also established in Article 1a of the Wbp (2017). This implies that information about companies and other organizations was not considered to be personal data. Of course, information about a specific employee of an organization was personal data. Also information about organizations that is co-determining for the way in which someone is assessed or treated in society was considered to be personal data (e.g. the profit of a one-person business says something about the income of its owner). This rule also applied to information about objects (Sauerwein & Linnemann, 2002). Additionally, information that is evaluative about someone's characteristics, views or behaviors is also considered to be personal data (College Bescherming Persoonsgegevens, 2007).

In case data were considered to be personal data, the follow-up question in order to determine whether the Wbp applied, is whether the personal data were processed or not. According to the Wbp, processing concerns every action or sum of actions that is performed regarding personal data. This includes, but is not limited to: collecting, capturing, organizing, storing, updating, modifying, requesting, consulting, using, providing by forwarding, disseminating, assembling, interrelating but also fencing-off, erasing or deleting personal data (Wbp Art. 1b, 2017). Determinant in this was whether the person responsible for the data was able to have power or influence over the personal data; in case the person had not, then there was no processing in place (Sauerwein & Linnemann, 2002).

As the Wbp was a Dutch law, it applied to the processing of personal data in the context of activities of a location of the organization responsible for the processing in the Netherlands (Wbp Art. 4.1, 2017). It also applied in case the organization responsible for the processing was using resources (e.g. telephone lines) located in the Netherlands, but was itself not located in the Netherlands, neither in another EU-Member State (Wbp Art. 4.2, 2017). However, it did not apply in case resources located in the Netherlands are used, but the organization responsible is located in another EU-Member State. In that case, the relevant legislation of that EU country applied (Sauerwein & Linnemann, 2002).

Even if all previous conditions were met, the Wbp did not necessarily apply; there were some exceptions, laid down in Art. 2.2. (2017). If personal data was used exclusively for personal or home-use, the Wbp did not apply. In case personal data was exclusively used for journalistic, artistic or literary purposes, only a limited part of the Wbp's provisions was applicable. In addition, the Wbp did not apply in case personal data was processed by or for the intelligence and security agencies, for use in the execution of police tasks, by municipal governments within the municipal administration, for use in the execution of the *Wet op de justitiële documentatie en de verklaringen omtrent het gedrag* (a national law regarding the registration and providing of judicial documentation) and for the execution of the *Kieswet* (a national law that regulates all elections in the Netherlands) (Sauerwein & Linnemann, 2002). Finally, the Dutch minister of defense could exempt a case of processing of personal data by the national military forces from being subject to the Wbp for the purpose of safeguarding or promoting the international legal order (Wbp Art. 2.3, 2017).

§2.2.2 Main types of obligations and conditions set by the Wbp

In this subparagraph, a selection of the obligations and conditions set by the Wbp will be discussed. Hereby, a structure will be used of six main types or domains under which the obligations and conditions fell: objectives and foundations of data processing, time limits for storage, rights of data subjects, special types of personal data and technical and organizational security measures. These domains, the same as used in Chapter 3, are discussed consecutively with attention paid to obligations and conditions for personal data processing organizations.

Objectives and foundations of data processing and permission

The Wbp only allowed, by means of its seventh Article (2017), the collection of personal data in case the purpose was clearly defined and described before the data collection started to take place (this purpose or those purposes could not simply be adapted during the process), and the data collection had to be necessary for reaching the objective (Wbp Art. 11.1, 2017). Furthermore, data processing was only allowed by the Wbp in case it was based on one of the six foundations mentioned in Article 8 (2017). These were: (1) unambiguous permission of the person concerned, (2) necessity for the execution of an agreement conducted with the person concerned, (3) necessity for the fulfillment of a legal obligation by the data processing entity, (4) necessity for the purpose of safeguarding a vital interest of the person concerned (e.g. in case of a medical emergency), (5) necessity for the fulfillment of a task resulting from public law, or (6) necessity for the representation of a justified interest of the data processor (e.g. data processing was necessary for the proper functioning of the type of organization) (Sauerwein & Linnemann, 2002).

Time limits for storage

It was not allowed to store personal data for a time period longer than necessary for the accomplishment of the objective(s) for which the data was collected (Wbp Art. 10.1, 2017). This can vary for every case, so there was no fixed maximum time limit. Nevertheless, there could be arrangements for fixed maximum time limits in other laws on specific forms of data, e.g. regarding medical information (Sauerwein & Linnemann, 2002).

If it was no longer necessary to store the data, these data had to be removed, or all identifiable characteristics needed to be removed. Personal data was allowed to be stored longer for historical, statistical or scientific purposes (Wbp Art. 10.2, 2017). This was also true for data that was originally

not collected for these purposes, but that were provided later on for scientific research (Sauerwein & Linnemann, 2002).

Rights of data subjects

Individuals that were subject to the processing of their personal data, data subjects, had the right, resulting from Wbp Art. 33 and Art. 34 (2017), to be informed about which of their personal data is processed for which reasons. Additionally, individuals had the right to inspect whether an organization had processed their own personal data, and if so which. The organization in question had to answer in writing within four weeks, whereby it provided a complete overview of the processed information related to the person concerned, including the objectives of the data processing and all accessible information on the sources of these data (Wbp Art. 35, 2017). In case the (requested) personal data was factually untrue, incomplete or not relevant for the objective of the data processing, the person concerned had the right to let these data be corrected, completed, deleted or fenced-off (Wbp Art. 36, 2017). Additionally, someone had the right of resistance if the processing of his/her data was based on the necessity for the fulfillment of public law tasks or on the necessity of representation of justified interests and if the processing was used for direct marketing purposes (Wbp Art. 40-41, 2017). Finally, the right not be subject to automated decision-making existed. This regulated that data subjects had the right to let decisions taken on them be based on human decision-making rather than solely a computer. This right did, however, not apply in case automated decision-making was necessary for the conduct or performance of an agreement or in case the automated decision-making was authorized by law (Wbp Art. 42, 2017).

Special types of personal data

The Wbp was especially strict in case 'special personal data' was processed. 'Special personal data' included information on one's religion or (spiritual) convictions, race and ethnical background, political preference, health status, sexual activity and sexual orientation, membership of a labor union and furthermore criminal law-related data. Article 16 of the Wbp (2017) did not allow these types of personal data to be processed, apart from some very specific exceptions. Examples of these exceptions were that religious institutions, such as churches, were allowed to process personal data on one's religion (Wbp Art. 17, 2017) and hospitals were allowed to process personal data regarding one's health status (Wbp Art. 21, 2017). Even if these exceptions were not in place for a specific case, it might still have been possible to process 'special' personal data, but only in case of explicit permission, in case the data were already made public by the concerned person him-/herself, or in case of a necessity with regard to a judicial process (Sauerwein & Linnemann, 2002).

Technical and organizational security measures

The Wbp stated, somewhat vaguely, that the processor needs to take technical and organizational measures to prevent the loss of data or unjustified processing. This is because the type of data as well as the state of technology and the price of the measures were taken into account, which made it hard to determine a certain minimum degree of required protection. Nevertheless, the measures taken needed to prevent unnecessary collecting of further (unintentional) spreading of the data (Wbp Art. 13, 2017). Fifteen years after the Wbp came into force, Article 34a (Wbp, 2017) was added as from the first of January 2016. This Article added the requirement for data processors to inform supervisor AP without a delay, so as soon as possible, in case a security breach had taken

place that would or could lead to severe harmful consequences for the protection of personal data. Also added was the requirement to report all data processing activities to the AP (Wbp, Art. 27 – 32).

§ 2.3 Enforcement of the Wbp

The enforcement of the Wbp was monitored by an independent supervisory authority, the *Autoriteit Persoonsgegevens* (AP). This supervisory body is given a legal basis and is regulated in terms of organization and functions by means of Wbp Articles 51 up to and including 64 (2017). The Autoriteit Persoonsgegevens, being an independent authority, had the ability to start an investigation regarding the compliance with the Wbp either at the request of an interested party or on its own initiative (Wbp Art. 60, 2017). In case the AP noted a genuine breach of the Wbp, it had three options to sanction the data processor: first, it had the possibility to impose an administrative coercion, forcing the data processor to stop its illegal practices (Wbp Art. 65, 2017). Secondly, the AP could impose administrative fines. Such fines could amount to €20.750 at maximum in rather simple cases or at maximum €830.000 in case of severe breaches (Wbp Art. 66, 2017). Finally, the AP could also account for the detection of violations of the law or crimes committed by individuals. A violation is a less severe legal offense, that can be sanctioned with a fine of at maximum €8.300. A crime is a more severe type of legal offense, that can be sanctioned with either a fine of at maximum €20.750 or imprisonment for a maximum period of six months (Wbp Art. 75, 2017).

§ 2.4 Conclusion Chapter 2

The pre-existing national Dutch law, the Wbp, was the Dutch law that implemented the EU's Data Protection Directive and that executed the legal obligations on the Dutch government arising from Article 10 of the Dutch constitution and Treaty no. 108 of the Council of Europe. It found its legal basis in Article 10 of the Dutch constitution and aimed for safeguarding the fundamental rights to privacy and data protection, and for maintaining consumer trust in the digital economy.

The Wbp defined its use of the terms 'personal data' and 'processing'. Being a Dutch law, the Wbp applied to data processing in the context of activities of a location of the organization responsible for the processing in the Netherlands. It also applied to data processing using resources in the Netherlands by organizations not located in the Netherlands, neither in another EU-country. There were some exceptions to the applicability of the Wbp, as *inter alia* personal and domestic use and use for journalistic purposes or to safeguard national security.

The Wbp set several obligations and conditions for data processing and data processing organizations. In any case, specific objectives needed to be formulated for processing personal data and data processing had to be necessary for fulfilling these objectives. Moreover, data processing had to be based on one of the six mentioned foundations. Additionally, personal data could only be stored as long as necessary for accomplishing the predefined objectives and data processing organizations needed to take technical and organizational measures in order to prevent the loss of personal data or unjustified processing. Everyone had the right to inspect if organizations processed personal data on them and the right to correct/complete/delete/fence-off these data If these were incorrect, incomplete or unnecessary for the organizations to have stored. Furthermore, the Wbp was very strict on the processing of 'special' (sensitive) types of personal data, which was prohibited

in most cases, with only a few very specific exceptions. Finally, appropriate technical and organizational security measures needed to be taken and both all data processing activities as well as all (potential) data breaches needed to be reported to the independent supervisory authority, the Autoriteit Persoonsgegevens (AP).

Compliance with the Wbp was also monitored by the AP. This authority could start an investigation of an alleged breach with the Wbp on its own initiative or on the request of an individual concerned as a subject in the specific case of data processing. If an actual breach was found, the AP had several instruments to sanction, including administrative coercions, administrative fines and starting a criminal law procedure. In the latter case, the potential resulting (individual) sentence has the form of either a fine of maximum €20.750 or imprisonment for a maximum period of six months. In the case of administrative fines, that can be imposed on both individuals and organizations, the fines can amount to a maximum of €830.000.

3. Analysis of the GDPR in the light of arising obligations and conditions

In this chapter, the GDPR is analyzed, with special attention being paid to the obligations and conditions the law sets for data processing organizations. This naturally follows-up the analysis of the Wbp in Chapter 2. While that chapter analyzed the pre-existing national data protection law, the Wbp, Chapter 3 will analyze the replacing EU data protection law, the GDPR. This next step in the research enables a comparative analysis, as will be performed in Chapter 4.

§ 3.1 Legal context of the GDPR

The *General Data Protection Regulation* (GDPR), officially called Regulation 2016/679, is the main EU data protection law, that is enforceable since the 25th of May 2018. This followed-up a transitional period of two years, as the GDPR was signed on the 24th of May 2016. The GDPR replaces Directive 95/46/EC as well as all national data protection laws implementing that Directive, such as the Wbp. The GDPR finds its legal foundation in Article 16 of the Treaty on the Functioning of the European Union (TFEU).

> Article 16
> 1. *Everyone has the right to the protection of personal data concerning them.*
> 2. *The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.*
>
> (TFEU, 2012)

Article 16 of the TFEU establishes the right to data protection, via its first paragraph. The way this right is safeguarded is laid down by paragraph two of this article, which forces the European Parliament and the Council of the European Union, two of the main EU institutions, to adopt rules regarding the protection of individuals' personal data. Via the GDPR, the EU has adopted a law that contains such rules and that applies directly in all Member States. A Regulation is namely directly applicable and does not need to be 'translated' into national legislations, as is the case with Directives (Schutze, 2015). Naturally, this leads to greater harmonization of data protection legislation than was the case with Directive 95/46/EC and the various national data protection laws. Nevertheless, total harmonization is not the case, as the GDPR leaves room for differences in terms of exceptions for specific purposes as well as in terms of enforcement of the law (Zwenne & Mommers, 2016). As already mentioned in the introduction, national governments need to use this room to regulate the compliance scheme and to harmonize national legislation with the Regulation. Therefore, the Dutch government has enacted the *Uitvoeringswet Algemene Verordening Gegevensbescherming* (UAVG) (translated 'the implementing law GDPR'), that mainly arranges the supervision by the independent national supervisory authority, the *Autoriteit Persoonsgevens* (AP). Besides, it contains some exceptions to the GDPR when it comes to some specific purposes of data

processing (e.g. artistic, journalistic or scientific purposes). For these provisions, the Dutch government has tried to maintain as much as possible the provisions of the Wbp, which was only possible in cases where the Regulation left room for this (Schermer et al., 2018).
As mentioned above, the GDPR aims for the legal objective of fulfilling the obligation on EU institutions to adopt data protection legislation. The harmonization that took place because of the replacement of the Data Protection Directive by the Regulation is also one of the very objectives of the GDPR. Harmonization in data protection legislation strengthens the level of uniformity that contributes to the creation of the digital single market the EU is aiming for and that is expected to boost the EU's digital economy. This is because companies operating within the EU will now have to comply with one data protection regime instead of 28 different ones, thus simplifying business operations among EU countries and raising the attractiveness of operating within the EU for outside-EU businesses as they will have a large potential single market to participate in (Tikkinen-Piri et al., 2018). The European Commission calls this principle the 'one-stop-shop', which makes it simpler and cheaper for companies to be active in the EU. The Commission estimates the benefits resulting from harmonization at €2.3 billion per year (European Commission, 2017).
Apart from this harmonization objective, there is also the objective of improving the data protection standards for the whole Union. The Data Protection Directive (Directive 95/46/EC), on which the national data protection laws were based, dated from 1995. Back then, data processing technologies were way less developed and the digital economy was way smaller than nowadays. New techniques bring about new opportunities and benefit both processors and consumers, they may also pose serious privacy threats. Therefore, technological progress demands for an updated data protection regime, with the GDPR aiming to satisfy this demand (Tikkinen-Piri et al., 2018).

§ 3.2 Content of the GDPR: obligations and conditions

§3.2.1 Definitions and sphere of influence of the GDPR

As the GDPR is a data protection regime, it only applies in case of the processing of personal data.
As mentioned in Article 4 paragraph 1 (2016), 'personal data' is conceptualized as factual information that is identifiable to an individual. Following this, information about organizations is not considered to be personal data. Nevertheless, data concerning a specific employee of an organization are considered to be personal data. Also information about organizations that are identifiable to an individual are considered to be personal data (e.g. in case of a one-person business). This rule also applies to information about objects (Schermer et al., 2018).

If an organization is making use of personal data, the next step is to check whether these personal data are processed. The GDPR defines processing as any operation or set of operations that is performed on (sets of) personal data, whether or not by automated means. This includes collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destructing personal data (GDPR, Art. 4.2, 2016).

As the GDPR is an EU-Regulation, it applies in all 28 Member States of the Union. There are two possible ways the GDPR is applying (GDPR Art. 3, 2016); either the data processing organization is

located in the EU or the data processing organization is located outside the EU but data are processed from citizens of the EU. In the first instance, the organization needs to be physically located within the Union and it does not matter whose personal data is processed; even if the organization processes personal data from non-EU citizens that are also not located within the EU's territory, the GDPR still applies if the data processing organization itself is located within the Union. This sphere of influence is comparable for the UAVG, the Dutch implementing law, but then with the Netherlands as territory instead of the whole EU; the UAVG is applicable in case the data processing organization is located in the Netherlands or in case the data processing organization is not located in the Netherlands but data is processed from persons located in the Netherlands (Schermer et al., 2018).

In case that above-mentioned conditions regarding personal data, processing and the sphere of influence are satisfied, the GDPR is applicable. Nevertheless, there are some exceptions to this; Firstly, the GDPR does not apply in case of data processing for the purpose of national security, as national security-related matters fall outside the scope of Union legislation. In the Netherlands, data processing regarding the safeguarding of national security is regulated by the *Wet op de inlichtingen- en veiligheidsdiensten*, a national law on the intelligence and security agencies (UAVG Art. 3.3.b, 2018). Secondly, the GDPR does not apply in case data is processed in relation to the Common Foreign and Security Policy (CFSP) of the EU (GDPR Art. 2.2.c, 2016), as the Council of the European Union states rules regarding this type of data processing. Additionally, the GDPR does not apply in case personal data is used exclusively for personal or domestic use (GPDR Art. 2.2.c, 2016). Finally, the GDPR is not applicable in case personal data is processed for the purpose of detection and prosecution of criminal offenses (GDPR Art. 2.2.d, 2016). Regarding these activities, EU Directive 2016/680/EG applies, which is implemented in the Netherlands by the *Wet politiegegevens* and the *Wet Justitiële en strafvorderlijke gegevens* (Schermer et al., 2018).

§3.2.2 Main types of obligations and conditions set by the GDPR

In this subparagraph, a selection of the obligations and conditions the GDPR sets will be discussed. Hereby, a structure will be used of six main types or domains under which the obligations and conditions fall: objectives and foundations of data processing, time limits for storage, rights of data subjects, special types of personal data and technical and organizational security measures. These domains, the same as used in Chapter 2, are discussed consecutively with an emphasis on obligations and conditions for data processing organizations.

<u>Objectives and foundations of data processing</u>

The GDPR requires a specific beforehand-determined objective in any case of data processing. This implies that random data processing without a clear objective is not permitted. Additionally, the data processor needs to describe this objective beforehand explicitly (GDPR Art. 5.1, 2016). Finally, the data processing should fulfill one of the six legal foundations of processing personal data. These foundations are (1) unambiguous and informed consent of the concerned person for the processing of his/her personal data for a specific objective, (2) necessity for the performance of a contract with the concerned person or on request of the concerned person to take measures before the conduction of a contract, (3) necessity for compliance with a legal obligation on the data processor, (4) necessity for the safeguarding of vital interests of the person concerned or another natural

person, (5) necessity for the fulfillment of a task of common interest or of a task related to the exercise of public authority instructed to the data processor, and (6) necessity for the representation of justified interests of the data processor or of a third party, unless the interests or fundamental rights of the person concerned outweigh these justified interests (especially in the case of an infant) (GDPR Art. 6.1, 2016). Apart from the need for data processing to be based on one of these six legal foundations, there is also the requirement by the GDPR that the data processing needs to be necessary for the objectives mentioned in the legal foundations. For data processing to be necessary, it needs to be proportionate, meaning the data processing needs to be effective and reasonable. Furthermore, it needs to fulfill the subsidiarity principle, meaning that the objective could not have been fulfilled by means of less far-reaching ways (e.g. by processing no or less personal data) (Schermer et al., 2018).

Time limits for storage

The GDPR allows storage of personal data only for the time period that is strictly necessary for accomplishing the objective of the data processing (GDPR Art. 5.1.e., 2016). This provision does not contain an explicit, fixed maximum time period for storage, as this may vary for different objectives of data processing. Data processors need to determine themselves, taking into account the proportionality principle, which time limits they use for their storage of personal data. These time limits need to be established, and it must be ensured that the stored data remains to be accurate and up-to-date (European Commission, n.d.). An exception is made for data that is exclusively processed for the achievement of purposes in the public interest or for scientific, historical, or statistical research purposes, which may be stored for longer periods, provided that the data processor has implemented appropriate technical and organizational measures in order to guarantee an adequate security level and protection of the rights and freedoms of the data subject as assigned by the GDPR (GDPR Art. 5.1.e., 2016). Data that is processed for other purposes may only be stored for longer than strictly necessary in case these data are not identifiable to individuals anymore, so in case of anonymising data (European Union Agency for Fundamental Rights and Council of Europe, 2018).

Rights of data subjects

The GDPR gives several rights to the person concerned, the data subject (the person whose personal data are processed). The first right is the right to be informed about the processing of one's personal data. It regulates that data processing organizations need to provide their 'data subjects', the persons on which they collect personal data, from the start with a certain minimum of information regarding the data processing. This includes the objective and foundation of the data processing and the period for which the data is stored (GDPR Art. 13 – 14, 2016). A related right is the right of access, laid down in Article 15 (GDPR, 2016): the right for a person concerned to check if and (if so) which personal data is processed about him/her. The organization in question must answer in writing within a month, or in the situation of many or complex requests within three months.

In case the (requested) personal data is not or no longer accurate, the person concerned has the right to let these data be rectified (GDPR Art. 16, 2016). Furthermore, someone has the right to 'be forgotten'; data subjects can request from a data processing organization the erasure of his/her personal data. The data processor needs to concede such a request *inter alia* in case the personal data are no longer necessary for the objectives for which they were processed, in case the personal

data are processed in an unlawful manner or in case the data subject withdraws his/her consent (and there is no other legal foundation on which the data processing is based). In case such a request must be conceded while the data processor has shared the concerned subject's personal data, the data processor not only needs to erase the subject's personal data in its own database, but also needs to notify the parties it has shared these data with. However, the right to 'be forgotten' is no absolute right: in case there are legitimate reasons that justify the storage of personal data for a longer period, the data processing organization is allowed to reject a request to 'be forgotten'. Several exceptions in the law regulate this (GDPR Art. 17.3, 2016) (McCarty, 2018).
Additionally, someone has the right to object if the processing of his/her data is based on the necessity for the fulfillment of public law tasks or on the necessity of representation of justified interests and if the processing is used for direct marketing purposes (GDPR Art. 21, 2016). On top of this, persons concerned have the right to data portability, which means they are entitled to a copy of personal data from them processed by the organization in question (GDPR Art. 20, 2016). The objective of this right is that individuals can take these data to another organization, which makes individuals less dependent on a certain organization. Last but not least, there is the right not to be subject to automated decision-making (including profiling), that assigns the right to data subjects to have a human voice involved in decision-making they are subject to. Data subjects can thus object, in most cases, if decisions are made on them purely by a computer on the basis of their personal data. However, this right is not applicable in case data subjects give their explicit consent for automated decision-making, in case the automated decision-making is authorised by Member State law or EU law or in case the automated decision-making is necessary for the performance or conduct of an agreement between the data subjects and the data processing organization (GDPR Art. 22.2, 2016).
An example of automated individual decision-making is a computer deciding that an employee should be fired because on the basis of personal data, he/she is considered to be a risk for the organization (Schermer et al., 2018). Another example of automated decision-making is software that automatically grades a paper from a student on the basis of algorithms, without a teacher being involved (Engelfriet et al., 2018).

Special types of personal data

Under the GDPR regime, there is a distinction between 'normal' personal data and 'special' types of personal data. 'Special personal data' includes information on one's religion or (spiritual) convictions, race and ethnical background, political preference, health status, sexual activity and sexual orientation, membership of a trade union and furthermore criminal law-related data (GPDR Art. 9 – 10, 2016). It is illegal under the GDPR provision to process these special types of personal data, apart from some very specific exceptions. These exceptions are more extensively described in the UAVG and include (1) explicit permission, (2) vital interests (e.g. in case of a medical emergency), (3) data processing by and within non-profit institutions of a political, spiritual, religious or labor union-nature, (4) data that are already made public by the person concerned, (5) data processing related to a lawsuit (UAVG Art. 22, 2018), (6) data processing by the independent national supervisory authority Autoriteit Persoonsgegevens or the national ombudsman, (7) data processing under the obligation of international law (UAVG Art. 23, 2018), or (8) data processing to support historical, scientific or statistical research (UAVG Art. 24, 2018). On top of these general exceptions, there are some more specific exceptions stated in the UAVG (Art. 25 – 33, 2018) for some categories, such as medical data (Schermer et al., 2018).

Technical and organizational security measures

In its 32nd Article, the GDPR (2016) obliges data processing organizations to take appropriate technical and organizational measures in order to guarantee an appropriate level of security. What is defined as 'appropriate', depends on the case; *inter alia* the sensitiveness of the data and the scope, nature, context and purposes of the data processing are taken into account, as well as the costs of implementing the measures. Measures include, for example, the encryption of data, restriction of access to the data and ways to restore data in case of an accident (Schermer et al., 2018). If, for some reason, a 'data breach' takes place (when an intentional or unintentional failure of the security leads to the destruction, loss, modification, unauthorized provision of or unauthorized permission to processed personal data) (Schermer et al., 2018), the data processing organization needs to inform the responsible national supervisor within 72 hours (GDPR Art. 33, 2016). In the Netherlands, such breaches thus need to be reported to the Autoriteit Persoonsgegevens. In case the data processor has not done it already, the supervisory authority determines whether a breach should also be reported to the subjects of the data processing, in line with the provisions of Article 33 of the GDPR (2016).

The GDPR requires, by its 30th Article (2016), all data processing organizations to have a textual register in which they provide an insight into their data processing. Such a register does not contain the actual personal data, but it does contain, inter alia, information about the objectives of the data processing, the time limits of storing the data, the security measures that have been taken, the categories of the data that have been processed and a list of parties with whom the data have been shared. Exempted are organizations with fewer than 250 employees whose processing is occasional, is not considered to be of a high-risk nature and does not contain 'special types' of personal data (as mentioned above). Some organizations are required to appoint a data protection official, who is responsible for the compliance of the organization with the GDPR (GDPR Art. 37 – 39, 2016). This is only a requirement for public authorities and bodies (expect for courts), organizations that process special types of personal data on a large scale and organizations that require in their processing for organization's core tasks regular and systematic observation on a large scale. An example of the latter is travel data collected by a public transport company (Schermer et al., 2018).
In some cases, organizations periodically need to perform a data protection impact assessment, in which *inter alia* the type, context and objectives of data processing are described and special attention is paid to the risks of the data processing in question (GDPR Art. 35.7, 2016). Such an assessment is only required for high-risk forms of data protection. These cases of high-risk are listed by the national supervisory authorities (GDPR Art. 35.4), but the GDPR itself already gives three examples; (1) automated, systematic and extensive evaluation of personal aspects, including profiling, on which decision-making is based, (2) large-scale processing of special types of personal data and (3) large-scale and systematic observation of persons in public area (GDPR Art. 35.3, 2016) (Schermer et al., 2018).

§ 3.3 Enforcement of the GDPR

Compliance with the GDPR is supervised by an independent national supervisory authority, as prescribed by the TFEU in Article 16.2 (2007) and stated in Chapter VI of the GDPR (2016). Each of these national supervisory authorities has many tasks imposed by Article 57 (GDPR, 2016), of which some important are to monitor and enforce the application of the GDPR, to promote awareness of

the rights and obligations under the GDPR and to conduct investigations on compliance with the law. The supervisory authorities can act on their own initiative, but individuals can also submit a complaint about a specific case of data processing (GDPR, Art. 77, 2016). In case of a less severe breach of the GDPR, such as not having performed a data protection impact assessment although this was required for the organization in question, national supervisory authorities can impose an administrative fine with a maximum value of €10 million or 2% of the yearly worldwide turnover (which of the two is higher) (GDPR Art. 83.4, 2016). In case of a severe breach of the GDPR, such as data processing without a valid legal foundation or a violation of an individual's fundamental rights, the supervisory authority can impose an even higher administrative fine, with a maximum value of €20 million or 4% of the yearly worldwide turnover (GDPR Art. 83.5, 2016). Also noncompliance with orders from the supervisory authorities can result in an administrative fine of the latter category. Apart from these administrative fines, judicial sanctions can also be imposed by a court in case the 'subject' of the data processing, the person concerned, initiates a legal proceeding against the data processor (GDPR Art. 79, 2016). In the Netherlands, the national supervisory authority is the Autoriteit Persoonsgegevens (AP). The functions and structure of the AP are regulated by Chapter 2 of the UAVG (2018). The AP cooperates with the other supervisory authorities within the EU and is enabled or sometimes obliged to exchange information regarding data processing with the other authorities (UAVG Art. 19, 2018).

§ 3.4 Conclusion Chapter 3

The GDPR is the current most important data protection law within the EU, directly applying as a Regulation in the whole Union without the need for being transmuted into national legislation, and replaces Directive 95/46/EC and all national data protection regimes, thus including the Dutch Wbp. Nevertheless, the GDPR leaves room that national governments need to use, and the Dutch government therefore adopted the UAVG, that contains provisions on *inter alia* the organization and position of the national supervisory authority AP and some exceptions where the GDPR leaves room for this. The GDPR finds its legal foundation in Article 16 of the TFEU, and executes the legal obligation that this Article imposes. Apart from this aim, the GDPR also has the objective of harmonizing data protection legislation for the whole Union, thereby contributing to the realization of the digital single market in the EU. Finally, the GDPR aims for raising the data protection standards for the whole EU by being more adapted to newer data processing techniques than the previous Directive and national data protection regimes.

The GDPR states its used definitions of 'personal data' and 'processing'. As it is an EU Regulation, it applies within the territories of all 28 Union Member States. The GDPR applies both in case the data processing organization is located within the EU (regardless of whose data is processed) and in case the data processing organization is not located within the EU but data is processed from EU-citizens. The UAVG is a Dutch law and therefore only applies to data processing by organizations located in the Netherlands and to data processing by organizations outside the EU that process data from persons located in the Netherlands. There are exemptions to the applicability of the GDPR, as data processing for, *inter alia*, personal and domestic use and data processing with the objective of safeguarding national security are exempted.

There are several obligations and conditions for data processing and data processing organizations set by the GDPR. First of all, there needs to be a specific objective formulated before the GDPR allows for data processing to take place, and data processing needs to be necessary for accomplishing the objective. On top of that, it is required to fulfill one of the six legal foundations of processing personal data. Besides, data processing organizations need to provide their 'subjects' with a certain minimum level of information about the processing of their personal data. Moreover, the GDPR assigns individuals the right to access the information processed about them and let it be corrected/deleted/restricted, the right to data portability and the right not to be subject to automated decision-making. The GDPR obliges most data processing organizations to have a textual register that gives a complete overview of the organization's data processing, and it requires some data processing organizations to appoint a data protection official and to periodically perform data protection impact assessments. Furthermore, the GDPR obligates data processing organizations to take appropriate measures in order to safeguard an appropriate level of security. In case of a data breach, this should be reported to the supervisor within 72 hours. Finally, the GDPR does not allow the processing of 'special types' of personal data, except for very specific exceptions.

Compliance with the GDPR is monitored by independent national supervisory authorities. In case of the Netherlands, this is the Autoriteit Persoonsgegevens. Apart from promoting awareness of everyone's rights and duties resulting from the GDPR and monitoring and enforcing the application of the data protection regime, the supervisory authorities have the task of investigating potential non-compliance. The AP can both start such an investigation on its own or at the request of an individual concerned, someone whose data is processed, who presumes a breach of the GDPR. In case the AP establishes an actual breach, it is able to impose administrative fines that can amount to a maximum of €20 million or 4% of an organization's yearly worldwide turnover. Apart from these administrative fines, there is the possibility of initiating a legal proceeding, after which the case is dealt with by the national court system.

Chapter 4: Comparative analysis of the Wbp and GDPR in the light of arising obligations and conditions

In this Chapter, the pre-existing data protection legislation in the Netherlands, the Wbp, will be compared with the current EU data protection regime, the GDPR (also the UAVG will be addressed when comparing material scopes, provisions regarding 'special' types of personal data and supervision mechanisms). Special attention will hereby be paid to the (potential) difference in obligations and conditions that both laws set for data processing and data processing organizations. In this Chapter, the structure of the analyses of the separate laws as discussed in Chapters 2 and 3 will be used to obtain an overview of differences between the two data protection regimes. This will be supplemented by making use of additional literature. After this chapter, the consequences of these potential differences will be analysed in Chapter 5.

§4.1 Comparison of legal contexts

As the two laws are different in nature, the Wbp being a Dutch law and the GDPR an EU-Regulation, they are based on different legal foundations: the Wbp is mainly based on Article 10 of the Dutch constitution and the GDPR is mainly based on Article 16 of the TFEU. Nevertheless, both Articles obligate the relevant legislator (the Dutch government and the European Parliament together with the Council of the European Union respectively) to enact legislation that regulates the protection of personal data. In that respect, both laws fulfil the obligation of enacting data protection legislation. Also, both laws aim for safeguarding the fundamental rights to privacy and data protection, that are established in several sources of international and European law. The Wbp, and EU Directive 95/46/EC it is based upon, have the additional objective of maintaining consumer trust in the digital economy. The GDPR builds upon this, with the aim of setting up an updated framework for data protection that fits the recent technology, larger digital economy and new data processing techniques better. Besides, the Wbp lacks the harmonization objective of the GDPR, which is logical considering the national nature of the aforementioned law.

§4.2 Comparison of content

§4.2.1 Comparison of definitions and spheres of influence

First of all, the definitions used in the Wbp and GDPR will be compared (the UAVG refers to the definitions of the GDPR), as they determine in which instances the laws are applicable. The two central definitions in both laws are 'personal data' and 'processing'. Regarding personal data, both the Wbp and the GDPR use the definition of factual information that is identifiable to an individual. The underlying rules that determine in which instances information about organizations and objects is considered to be personal data also correspond. Also the used definitions of processing essentially correspond, as both the Wbp and the GDPR define processing as an action or set of actions performed on personal data.

For the GDPR, the territorial sphere of influence, so when and where the rules of the Regulation are applicable, is extended compared with the Wbp. Of course, the Wbp, having been a Dutch law, was

applicable to the territory of the Netherlands. The GDPR, being an EU Regulation, is applicable to the territory of the whole European Union. The UAVG is a Dutch law, which is thus applicable within the territory of the Netherlands. Apart from the territory in which the laws apply, the UAVG and GDPR are equal regarding to which data processing cases they apply, so wherever 'GDPR' is mentioned within this indention, the UAVG is meant as well. Both the Wbp and GDPR applied or apply to data processors that process data in the context of the operations of that organization's location(s) within the territory the law applies to. As discussed earlier, the territories in which the two laws apply differ. Nevertheless, as this study focuses on the practical implications of the transition in data protection legislation for data processing organizations in the Netherlands, the only relevant territory of application is the territory of the Netherlands. In this indention, we thus ignore the application of the GDPR in the other 27 EU Member States. Apart from the earlier-mentioned application of both the Wbp and the GDPR to data processors that process data in the context of the operations of that organization's location in the Netherlands, the GDPR extends the territorial sphere of influence with two additional cases in which it applies, where the Wbp does not: firstly, the GDPR applies as well in case of third parties that process data on behalf of the responsible for the data, such as a CRM-system in the cloud or an email-application or online storage service. Secondly, the GDPR also applies in case the data processor does not have a location in the Netherlands or another EU-country, but is processing data from Dutch citizens for the purpose of providing goods and services or when observing their behavior within the Netherlands. This means that, for example, an Asian online-store that processes addresses for delivery of goods now also has to comply with the same data protection legislation, just like an American website that uses cookies processing personal data (Zwenne & Mommers, 2016).This was not the case under the Wbp regime, and thus the two additional cases in which the GDPR applies form an extension of the territorial scope.

On the basis of the analysis in Chapters 2 and 3, one can conclude that the material sphere of influence, that determines for which activities the law is applicable, does not differ significantly for both data protection regimes: both are applicable in case of data processing, also if automated or partly automated. The exceptions that both contain also correspond, with *inter alia* data processing for personal and domestic uses and for the purpose of safeguarding national security exempted under both regimes. Also Zwenne and Mommers (2016) conclude that the material sphere of influence has not changed in the transition from Wbp to GDPR.

§4.2.2 Comparison of main types of obligations and conditions

Objectives and foundations of data processing and permission

Both the Wbp and GDPR require data processors to establish clear and pre-determined objectives of the data processing, and the data processing needs to be necessary for achieving these objectives. Also the six legal foundations, of which at least one needs to be fulfilled in order for data processing to be allowed for, correspond for both legal documents

Time limits for storage

The Wbp states, just like the GDPR does, that data cannot be stored for longer than strictly necessary for accomplishing the specific objectives. Nevertheless, both laws do not specify this maximum period, as this may vary for different objectives. They also both contain exceptions for data storage

of data processed for scientific, historical or statistical research purposes or for purposes in the public interest, as long as adequate measures are taken to safeguard the level of security.

Rights for data subjects

The Wbp and GDPR both assign individuals the right to be informed, but the content of these rights differs for both laws; under the Wbp is was sufficient to inform the data subject about the purpose of the data processing and the identity of the data processor (and more information only if the need exists on the basis of the nature of the data, the circumstances of the data collection or the use made of the data) (Wbp Art. 33 – 34, 2017). Contrarily, the GDPR is more explicit and requires way more information to be provided to the data subject by default, such as the legal foundation for the data processing, the time period for which the data will be stored, the rights of the data subject and the ways in which the data processor deals with requests regarding the assertion of these rights (GDPR Art. 13 – 14, 2016). Another right for data subjects in both laws is the right to access what personal data is processed about them. In contrast with the right to be informed, this right has a similar content in both laws. Both laws also contain the corresponding right to correct, complete or restrict one's personal data in case these are incorrect. Concerning the right to 'be forgotten', there is a difference between both laws: while the Wbp mentions the right of erasure together with the right to correct, complete or restrict one's personal data in its 36th article, the GDPR has a separate article thereon, Article 17 (2018). Nevertheless, apart from this difference in terms of formulation, there is no significant difference in content: the right to 'be forgotten' of the GDPR, Article 17, should merely be seen as a bundling of various rights that were already existing under the Wbp, but spread out over multiple different articles (Jansen, 2018). Both laws contain the right not be subject to automated decision-making, from which the contents only differ in one aspect that is less relevant for the scope of this study (the addition of explicit consent as a possible exception to the applicability of this right) (Naudts, 2016). Moreover, the GDPR contains an additional right that is not included in the Wbp: the right to data portability, that for example simplifies the transfer of a customer from one energy supplier to another.

Special types of personal data

The Wbp and GDPR are just as strict on the processing of 'special types' of personal data, which they define similarly: they both prohibit the processing of these data. They both, however, contain exceptions to this prohibition. As the exceptions to the GDPR's provisions regarding special personal data needed to be specified in the national implementing law, the UAVG, the Dutch government had the ability to maintain as much as possible the already existing exceptions that were applicable under the Wbp. And indeed, it maintained the exceptions that were already there under the Wbp, resulting in no significant differences in this domain.

Technical and organizational security measures

Both the Wbp and GDPR oblige data processors to take appropriate technical and organizational security measures, taking into account the sensitivity of the data, he objectives, context and nature of the data processing and financial aspects of the implementation of these measures. Under both regimes, the duty exists to report a data breach to the supervisory authority, the AP. The GDPR is somewhat more strict in this respect, as data breaches always need to be reported, while the Wbp only obligates this when there is the likeliness of potentially very harmful consequences. On top of

this, the GDPR sets a deadline of 72 hours for informing the AP, while the Wbp did not mention a specific deadline for this (although a data breach needs to be reported without any delay according to both legislations).

Furthermore, there are some elements that are new under the GDPR regime; the first is the introduction of the obligation to have a textual register in which data processing organizations record details on the type of data processing they perform. This obligation is in place for most organizations, with only smaller organizations processing non-special, low-risk types of personal data on an occasional basis being exempted. In fact, this requirement to register replaces the requirement to report data processing activities to the AP, which was in place under the Wbp (Juridict, n.d.).

On top of those measures, some organizations are required to appoint a data protection official, that is responsible for the organization's compliance with the GDPR. Such a data protection officer also existed in the Wbp's provisions, but then on a voluntary basis. Under the GDPR, this is an obligation for some organizations and again voluntary for others. Moreover, some organizations periodically need to perform data protection impact assessments, that mainly assess the potential risks of the data processing. This is a novelty of the GDPR, that did not exist in the Wbp.

§4.3 Comparison of enforcement

The independent supervisory authority with the task of monitoring the compliance with the data protection legislation is the same for both laws. This authority, the AP, had and remains to have the ability to start investigations both on its own initiative or on the request of a data subject. Comparing the AP under the Wbp and the GDPR, the AP now has more of a legal basis for cooperation with other national supervisory authorities, and even the duty to do so. Apart from this, the maximum sanctions are also much higher: while administrative fines could amount up to €20.750 in case of less severe breaches of the Wbp and €830.000 in more severe cases, these maximum fines went to a maximum of €10 million or 2% of the yearly worldwide turnover (whichever of the two is higher) in less severe cases up to €20 billion or 4% in more severe breaches of the GDPR. Indeed, the administrative fines related to the enforcement of the GDPR are more than twenty times higher than the ones related to the enforcement of the Wbp (Klekovic, 2017).

§4.4 Conclusion Chapter 4

Having compared the context of both the Wbp and GDPR, it can be concluded that although they are based on different legal foundations, they share most of their objectives: both fulfil the obligation imposed by either the Dutch constitution (in case of the Wbp) or the TFEU (in case of the GDPR) on the legislator to adopt data protection legislation, they both aim for safeguarding the fundamental rights to privacy and data protection. Additionally, the Wbp has the aim of maintaining consumer trust in the digital economy, on which the GDPR builds further by setting an updated framework that better fits recent technology, the larger digital economy and new data processing techniques. On top of this, the GDPR has the aim of harmonizing data protection legislation within the EU, while the Wbp lacks this objective as a consequence of its national nature.

Consequently, comparing the content of both laws, one can conclude that the definitions used in both legal documents correspond. The material sphere of influence also corresponds and thus has not changed significantly. Also the territorial scope of influence partly corresponds, as both the Wbp and GDPR apply to data processors that process data in the context of the operations of that organization's location(s) within the territory in which the law is applicable. The GDPR nevertheless expands the territorial sphere of influence, by adding two additional cases in which it applies. The first is the case of third parties processing personal data on behalf of the responsible for the data. The second is the case of data processors without a location within the GDPR's territory, that processes personal data from citizens within the GDPR's territory for the purpose of providing goods and services or when observing their behaviour within the GDPR's territory. Focusing on the Netherlands, the transition in data protection legislation has thus resulted in a larger territorial sphere of influence, with more data processing organisations that now need to comply.

When comparing the main types of obligations and conditions set by the Wbp and GDPR, it is striking that both data protection regimes require pre-determined and explicit objectives before personal data processing is allowed to place. Processing personal data needs to be necessary for obtaining these objectives under both regimes, and the six legal foundations correspond as well. Apart from that, both do not specify explicit maximum time periods for the storage of personal data. From the rights assigned to data subjects, five occur in both laws: the right to be informed, the right to access, the right to complete/correct/restrict one's personal data, the right to 'be forgotten' and the right not to be subject to automated decision-making. While the right to access, the right to complete/correct/restrict, the right to 'be forgotten' (right to erasure) and the right not to be subject to automated decision-making correspond in terms of their contents in the Wbp and GDPR, the right to information has a different content in both laws; under the GDPR regime, the information-provision to data subjects needs to be more extensive in comparison with the Wbp. On top of the five rights mentioned in both laws, the GDPR assigns an additional right to data subjects compared with the Wbp: the right to data portability. Both data protection legislations in general prohibit the processing of 'special' types of personal data and personal data of a criminal law nature, apart from some specific exceptions. Thanks to the UAVG, these exceptions are similar for both data protection regimes. In terms of technical and organizational measures, both the Wbp and the GDPR require an 'appropriate' level of security, with 'appropriate' varying for every individual case. Under both data protection legislations, data breaches need to be reported to supervisor AP, with the GDPR being a bit stricter in terms of the rules regarding this. Furthermore, the GDPR adds some requirements that did not exist under the Wbp regime. These are upholding a textual register of processing activities (replacing the requirement to report data processing activities to the AP), appointing a data protection officer and performing data protection impact assessments.

The enforcement schemes for both data protection legislations include similarities, as the independent supervisory authority that enforces compliance is the same for both: the Autoriteit Persoonsgegevens (AP). This authority has, under both laws, the ability to start investigations both on its own initiative and on the request of a person concerned. There are, nevertheless, two differences regarding the enforcement of the data protection legislations; the first difference is that the AP has more legal basis and the duty of cooperation with other national supervisory authorities in the EU under the GDPR compared with the Wbp. The second, perhaps more influential difference is the drastic raising of the maximum fines in case of non-compliance. These maximum fines are more than twenty times higher than the maximum fines were under the Wbp.

On the basis of these comparisons, the third subquestion (SQ3) can be answered. There are a few differences in terms of arising obligations and conditions between the pre-existing Wbp and the replacing GDPR and UAVG, as also supported by IT lawyers (Dagblad van het Noorden, 2018). The GDPR namely maintains all obligations and conditions that were already there under the Wbp, but adds several new obligations and conditions. Schematically, this is presented in the table of Appendix A.

The GDPR has a different content, compared with the Wbp, for the right to be informed and requires more extensive information-provision to data subjects. It also has a different content for the right to be forgotten', enabling data subjects to withdraw their consent. Furthermore, it assigns a new right to data subjects: the right to data portability. Data processors have the obligation to honour these rights in case data subjects send them a request. Additionally, the GDPR contains a different content concerning the duty to report data breaches; it is a bit more strict if it comes to the time in which this needs to take place, as it sets a deadline of 72 hours for reporting (while the Wbp did not set an explicit deadline) and it requires reporting in more cases than the Wbp. Finally, the GDPR adds some completely new conditions that are compulsory for some data processors, regarding the upholding of a textual register with processing activities (instead of reporting these activities to the AP), the appointment of a data protection officer and the performance of data protection impact assessments. So all in all, there are some differences in terms of obligations and conditions, as the GDPR contains additional obligations and conditions. Furthermore, these obligations and conditions also apply to more data processors under the GDPR than before under the Wbp, as third parties processing personal data on behalf of the responsible for the data and, in many, cases also non-EU data processors now need to comply with the GDPR. Finally the maximum fines in case of non-compliance have increased drastically.

Chapter 5: Analysis of the practical implications for the operations of data processing organizations

In chapter 5, the practical implications of changes between the Wbp and GDPR for personal data processing organizations will be analyzed. Therefore, the results of Chapter 4, containing the differences in terms of obligations and conditions between the Wbp and GDPR, will be used. These differences need to be analysed in terms of the implications they could have for personal data processing organizations. It is possible that the few changes existing have significant implications for data processing organizations. If this is the case, it could explain the earlier-mentioned state of confusion and panic. The implications of specific changes in data protection legislation will be analysed by making use of scientific and non-scientific literature will be used. Additionally, a few interviews are conducted with several different types of organizations that process personal data. As these organizations are the ones that had to implement certain measures to ensure compliance with the GDPR, they can indicate to what extent they have experienced large implications for them. In the end, the combination of both the literature study and the interview analysis enables the answering of the fourth subquestion.

§5.1 Analysis of implications resulting from specific changes

In Chapter 4, an overview of changes in data protection legislation is provided. This is presented in the form of a table in Appendix A. The underlying logic hereof is that only these changes are relevant for the efforts that organizations need to make in order to comply with the GDPR; for example, if an obligation was already existing under the Wbp and continues to be there under the GDPR, an organization thus does not need to change its operations in order to comply with the GDPR. An assumption in this logic is that organizations complied with the Wbp when that regime was in effect. It is therefore important to realize that the method of explaining the implications for personal data processing organizations using the table of differences between the Wbp and GDPR cannot explain the number and gravity of implications for organizations that did not comply with the Wbp before. For the rest of this paragraph, it will be assumed that organizations did comply with the Wbp before, as they were obliged to. Below, the implications of the changes and novelties in obligations and conditions, resulting from the transition in data protection legislation, will be analyzed.

As has been revealed before, the right to be informed has a different content under the two data protection regimes, with the GDPR requiring a more extensive provision of information to data subjects. The implication hereof is that data processing organizations need to organize their information provision to data subjects. Of course, in case of many different data subjects, it would be a large burden for personal data processing organizations to inform all subjects individually about the data processed on them. However, this is not the only way in which the right to be informed can be respected. In practice, a data processing organization can satisfy this requirement by placing a privacy statement on its website and pointing out to data subjects from the start of its processing of personal data where this statement can be found (Autoriteit Persoonsgegevens, n.d.). A privacy statement has to be written using simple and understandable language, corresponding level B1 or B2 of the Common European Framework of Reference for Languages (Engelfriet et al., 2018), and needs to contain the contact information of the data processing organization, the contact information of the data protection officer within the organization (if applicable), the objective(s) and

foundation(s) of the data processing (including motivation), the time period of storage, information about the sources from which personal data are retrieved and with which parties they are shared and why, and information about the rights of data subjects and the way in which the data processing organization deals with these rights and requests regarding these rights (Autoriteit Persoonsgegevens, n.d.). In this manner, data subjects know where they can find information about the organization's processing of personal data and can consequently invoke their right to be informed by reading the privacy statement. If organizations collect data offline by means of, for example, a registration form, it could refer to its online privacy statement by including the URL of the statement on the registration form. Another possibility, in case the organization does not have a website, is to print the privacy statement on the registration form or hand it out together with the form (Engelfriet et al., 2018).

Altogether, there are several ways of respecting the right to be informed and thus fulfilling the obligation of informing data subjects without having to inform every subject separately, so without structurally having to make a lot of effort: once an organization has compiled a privacy statement and has become accustomed to referring this statement before every collection of personal data, it has complied with this requirement. The interviewed organizations, except for the one-man business who does not comply yet with this requirement, all uphold an online privacy statement and they also indicated that it was not a lot of work to compile this. All in all, the practical implication of this difference between the Wbp and GDPR seems to be rather limited.

A new right added by the GDPR is the right to data portability. This right enables data subjects to obtain a digital copy with their personal data processed by the concerned organization. This right only applies for data that is provided by the data subject himself or directly by his personal devices, and that is digitally processed, which implies that the right to data portability is inapplicable in case of data processing on paper (such as by the earlier-mentioned registration forms). Also, the privacy of others may not be risked by invoking this right. The right can be invoked in case the processing on the legal foundation of consent or of an agreement, and its aim is to enable data subjects to reuse their data elsewhere or publish them. This theoretically simplifies the transfer of customers among companies. (Engelfriet et al., 2018). It nevertheless also requires organizations to implement technical measures in order to be able to concede requests regarding data portability. It is hard to estimate what the burden of such measures will be, but this is definitely a considerable implication.

Most personal data processing organizations need to have an overview of their data processing, resulting from the requirement to uphold a textual register with data processing activities. This register can be used in order to answer in a fast and adequate way to requests regarding the exercise of rights assigned to data subjects (Engelfriet et al., 2018). Nevertheless, the Wbp instead contained the requirement to report all data processing activities to the Autoriteit Persoonsgevens, which was a similar responsibility. All in all, the implications for personal data processing organizations are very limited and the administrative burden can be considered to be equal.

The requirement to appoint a data protection officer only applies for large organizations and organizations that process 'special' types of personal data on a large scale or organizations that require in their processing for organization's core tasks regular and systematic observation on a large scale. In practice, such organizations usually already have employed experts in the field of law, IT or

both, that have to deal with the implementation of the GDPR as their core task. This was also the case for the medium-sized public organization and large semi-public organizations that were interviewed. Their data protection officers only needed little additional training in order to be able to fulfill their tasks. In their opinion, the burden resulting from this requirement is insignificant. Similarly, the requirement of performing data protection impact assessments has a small implication in practice. Both the public and semi-public organization indicated to have performed these assessments before the GDPR introduced this as a requirement, for they saw the value of such assessments for data protection in general and thought it is just logical to map the potential risks of one's data processing activities. This can, according to the large semi-public organizations, also have a simple form, such as a checklist that is used for the determination of risks arising from a certain case of personal data processing.

In general, all interviewed organizations had the opinion that their functioning in terms of performing their core tasks is not limited as a result of the transition in data protection legislation. The GDPR namely does not modify which personal data are allowed to be processed in what way; this remains relatively the same as it was under the Wbp regime. The largest overall change is the larger degree of transparency and accountability that needs to be realised by data processing organizations, which implies that these organisation have to raise their own level of awareness by mapping and recording their processing activities. All interviewed organizations recognize the resulting burden in terms of administrative requirements, but they think this burden is limited in terms of its gravity. Nevertheless, especially for small organizations, the right to data portability might have serious implications in terms of the adjustment of ICT facilities. Contrarily, one of the interviewees added the idea that, intuitively, the transition in data protection legislation might have even benefit the functioning of organizations. The underlying logic is that, as personal data processing organizations need to rethink their data processing activities, they become more aware of the organization of their core tasks as well, which might lead to an optimization of these core tasks. Additionally, one might also take measures in order to prevent the loss of important data, which would also contribute to the functioning of the organization.

§5.2 Conclusion Chapter 5

On the basis of the analysis of Chapter 5, the fourth subquestion (SQ4) can be answered. From most of the differences in obligations and conditions between the Wbp and GDPR, the implications seem to be limited, both considering the transition in data protection legislation in general and with regard to specific changes. Most obligations and conditions can be complied with in ways that burden the personal data processing organizations only minimally. The interviewed organizations also indicate that the burden on them is well-bearable, apart from overdue work that still needed to be done as a result of non-compliance with the Wbp. The most important exception to this is the right to data portability, that may have somewhat further-reaching implications, that could be examined further in future research (see §7.3). Nevertheless, neither of the interviewed organizations raised their concern about this. Moreover, all organizations also had the opinion that the transition in data protection legislation has had no effect on the performance of their core tasks. Thus, they did not need to change their operations for the performance of their core activities, but they had to change their operations to some extent for compliance with the GDPR.

Chapter 6: Conclusion

Before the overall research question can be answered, first all subquestions need to be answered separately, using the analysis of Chapter 2 up to and including Chapter 5.

SQ1: "What are the obligations and conditions arising from the Wbp that organizations processing personal data operating in the Netherlands had to comply with?

The Wbp, a Dutch law implementing the former EU Data Protection Directive, was legally based on Article 10 of the Dutch constitution and aimed for safeguarding the fundamental rights to privacy and data protection and for maintenance of consumer trust in the digital economy. The Wbp set several obligations and conditions for data processing organizations, of which the main ones were divided over five categories within this study; firstly, the Wbp required specific and pre-determined objectives as well as fulfilment of at least one of the six legal foundations as a condition for personal data processing. Additionally, the data processing needed to be necessary for the accomplishment of the objectives. Secondly, the Wbp restricted the storage of personal data. Thirdly, the Wbp assigned data subjects several rights that needed to be respected by personal data processing organizations. Fourthly, the Wbp contained separate rules for the processing of 'special' types of personal data and data of a criminal law nature, as processing these types of date was usually prohibited. Fifthly and finally, organizations needed to take appropriate technical and organizational security measures and needed to report both all of their processing activities as well as all (potential) data breaches to the supervisory authority AP. This supervisory authority had the possibility of sanctioning in cases of non-compliance with the Wbp, by imposing administrative coercion, administrative fines or by starting a criminal law procedure.

SQ2: "What are the obligations and conditions arising from the GDPR and the accompanying UAVG that organizations processing personal data operating in the Netherlands have to comply with?"

The GDPR, an EU Regulation that has replaced the former Data Protection Directive and all national data protection laws resulting from the Directive, is legally based on Article 16 of the TFEU and aimed for the harmonization of data protection legislation in the EU and thus for contributing to the digital single market in the EU and for raising the data protection standards by answering the more advanced technological possibilities of today with a newer data protection regime. The GDPR sets several conditions and obligations for personal data processing organizations, of which the main ones were divided over five categories: firstly, the GDPR requires specific and pre-determined objectives as well as fulfilment of at least one of the six legal foundations as a condition for personal data processing. Additionally, the data processing needs to be necessary for the accomplishment of the objectives. Secondly, the GDPR restricts the storage of personal data. Thirdly, the Wbp assigns data subjects several rights that needed to be respected by personal data processing organizations. Fourthly, the GDPR contains separate rules for the processing of 'special' types of personal data and data of a criminal law nature, as processing these types of date is usually prohibited. Fifthly and finally, organizations need to take appropriate technical and organizational security measures and need to report, in some cases, data breaches within 72 hours to the supervisory authority AP. Furthermore, most data processing organizations need to uphold a register of data processing activities, while some also need to appoint a data protection official and to perform data protection impact assessments. The AP has the possibility of sanctioning in cases of non-compliance with the

GDPR, by imposing administrative coercion, administrative fines or by starting a criminal law procedure. The compliance scheme is arranged in the UAVG.

SQ3: "To what extent are there differences in terms of their arising obligations and conditions between the pre-existing Wbp and the replacing GDPR and UAVG?"

The Wbp and GDPR correspond mostly in terms of their contents, as the GDPR maintains all obligations and conditions that already existed under the GDPR, but contains a different content for a few obligations and conditions and added some new obligations. The conditions with regard to specific and pre-determined objectives and foundations and necessity condition remain the same. Also the obligation regarding the time period of data storage exists in the same form in both laws. Both laws also correspond in terms of their strict requirements with regard to the processing of 'special' types of personal data and personal data of a criminal law nature. The UAVG plays a role in this, as it contains the exceptions under which processing of these types of personal data is allowed. These exceptions are adopted from the Wbp. Regarding the rights assigned to data subjects, the GDPR modifies the content of one right, the right to be informed. This right imposes a condition on personal data processing organizations to inform their data subjects beforehand. Under the GDPR, this information-provision needs to be more extensive, containing more information, than under the Wbp. The GDPR also assigns an additional right to data subjects: the right to data portability. Furthermore, the Wbp and GDPR both obligate personal data processing organizations to take appropriate technical and organizational security measures. The obligation to report data breaches exists in both laws, even though this obligation is slightly adapted under the GDPR regime, as data breaches now need to be reported within 72 hours. The obligation of the Wbp to report all data processing activities to the supervisory authority is replaced, under the GDPR, by the obligation for most data processing organizations to document all data processing activities. Finally, the GDPR adds two new obligations, that only apply to some organizations, depending on their type and size and the nature of their data processing activities: the obligation to appoint a data protection official and the obligation to periodically perform data protection impact assessments. The AP remains to have the same tasks and composition under the GDPR and UAVG as under the Wbp, albeit the AP has now more ability as well as the duty to cooperate with other national supervisors. Moreover, the maximum heights of the fines that can be imposed have drastically increased under the GDPR.

SQ4: "To what extent did organizations processing personal data operating in the Netherlands have to change their operations in order to meet the obligations and conditions resulting from the GDPR and 'Uitvoeringswet'?"

The differences in terms of obligations and conditions were analyzed on their implications for personal data processing organizations. The modified content of the right to be informed has limited implications, as it is well-possible to standardize the information-provision process by upholding a privacy statement, to which can be referred before every case of data processing. The implications of the new right to data portability are still unclear, as it might be possible that significant technical changes have to be made in order to be able to answer requests related to this right. Nevertheless, neither of the organizations interviewed raised concerns about this. The obligation to report data processing activities is replaced by the obligation to document data processing activities. As these obligations are estimated to impose similar burdens to personal data processing organizations, the implications of this difference are very limited. The new obligations to appoint a data protection official and to perform data protection impact assessments only apply to some organizations. These

organizations are, considering their size, type or nature of their data processing activities, usually already equipped with experts in the field of IT, law or both. For these experts, data protection is part of their core responsibilities, so that compliance with these new obligations is expected to be easily-realizable, which is also supported by the interviewed organizations that need to comply with these obligations. All in all, the changes that organizations processing personal data operating in the Netherlands had to make in order to meet the obligations and conditions resulting from the GDPR and UAVG are limited.

Combining the answers to the different subquestions and interrelating them enables this study to answers its overall research question:

RQ: "To what extent has the transition from Wbp to GDRP resulted in differences in terms of arising obligations and conditions that affect the operations of organizations processing personal data operating in the Netherlands?"

The Wbp and GDPR are both data protection regimes, that set obligations and conditions with regard to data processing and data processing organizations. Most of these obligations and conditions are similar for both regimes, but there are some differences (see Appendix A for a schematic overview). These differences include an adapted right to be informed, that demands a more extensive information-provision to data subjects, the new right to data portability, the obligation to document all data processing activities that replaces the obligation to report all data processing activities and the new obligations for some data processing organizations to appoint a data protection official and to perform data protection impact assessments. Apart from these differences in obligations and conditions, there is an important difference in enforcement, as the GDPR drastically raises the maximum heights of the fines (by a factor twenty) that can be imposed compared with the Wbp.

The differences in terms of obligations and conditions have only limited implications for personal data processing organizations, as most differences can easily be addressed by data processing organizations in order to comply with the GDPR and UAVG. Regarding this, it should be noted, however, that it remains unclear what the implications of the new right to data portability are. These implications should thus be studied further (see §7.3). Apart from that specific change, the other implications seem to be limited in terms of their gravity for data processing organizations. The major change that data processing organizations need to make is to map and document all of their data processing activities and inform their data subjects accordingly. According to the interviewed organizations, this administrative burden is well-bearable. Apart from these (few) changes that data processing organizations need to make in order to comply with the GDPR and UAVG, no changes need to be made in their operations; the interviewed organizations all indicate that the GDPR does not limit the performance of the organization's core tasks, so there is no need for these organizations to change their operations for the sake of their core activities.

All in all, on the basis of this study, it can be concluded that the differences in obligations and conditions resulting from the transition from Wbp to GDPR affect the operations of organizations processing personal data operating in the Netherlands only to a limited extent.

Chapter 7: Discussion

§7.1 Implications of the study

On the basis of a legal comparison of the Wbp and GDPR, this study ascertains a (low) number of differences in terms of obligations and conditions, of which the implications are both assessed using literature as well as tested on their practical occurrence by means of experiences and opinions collected by the conduction of interviews with personal data processing organizations. The combination of the comparison of laws, the review of literature and the conduction of interviews is a novelty that generates knowledge about the implications of the transition in data protection legislation for personal data processing organizations.

Considering the study's conclusion that the implications of the differences in terms of obligations and conditions arising from the transition from Wbp to GDPR are only limited, it is unlikely that these implications can explain the state of confusion and panic mentioned in Chapter 1. Consequently, on the basis of this study, there is no incentive for the government to compensate organizations for the efforts they make or to procrastinate the enforcement of the GDPR, as suggested by Het Financieele Dagblad (2017). Nevertheless, further research might be desirable in order to assess the actual causes of the state of confusion and panic (see §7.3).

The study's conclusion that there are only a few significant differences in terms of obligations and conditions between the Wbp and GDPR is not to say that there are also few differences in terms of the offered level of data protection. It could well be that the GDPR, in accordance with its objectives, raises the standards of data protection, but it is not within the scope of this study to assess that.

§7.2 Limitations

There are doubts with regard to the generalizability of the study's findings, and thus the study's external validity, due to various reasons: first, the organizations selected were all physically located in the region in which the researcher lives, which may have had an effect on the study's outcomes. Theoretically, it could be possible that compliance with and opinions about data protection legislation within that region differ from compliance and opinions in other regions. If this would be the case, the study's findings are representative for the region only, and not for the Netherlands in total. Besides, the non-response that had to be dealt with could have been related to the level of compliance, which would have lead organizations that were compliant to be more willing to participate and others not. This might have had an influence on the representativeness of the interviewed sample of organizations. Finally, only four organizations have been interviewed, which is quite a limited number.

Due to time constraints, the decision has been made (as also explain in section 1.3) to focus on the provisions of the Wbp and GDPR that were considered to be most important in the context of this analysis. Furthermore, due to these time constraints as well as due to a lack of economic knowledge, the study has not considered to include economic modeling as a method of mapping the costs and benefits of the transition in data protection legislation. Consequently, the implications for data processing organizations are only analyzed in a qualitative manner, a quantitative approach is not used.

§7.3 Recommendations for future research

Reflecting on the limitations of this study, future research has various ways to start from. First, future research could use the exact same research design, including the same questionnaire, but with a large number of respondents. This would enable the study to come to a more representative sample by including more variety among organizations in terms of categories and regions, which would increase the study's generalizability.

Besides, future research could analyze the Wbp and GDPR more extensively, by analyzing and comparing all provisions rather than a set of provisions. This would map all differences and could form the basis for an analysis on the implications of all changes. Future research could also include a quantitative approach in the analysis of differences between the obligations and conditions set by the Wbp and GDPR. There have been studies attempting to estimate the costs for organizations arising from the GDPR, such as the study by Christensen & Etro (2013), but these do not start from differences between the Wbp and GDPR and do not include a qualitative approach. The combination of qualitative and quantitative methods would substantially wide, and potentially strengthen, the analysis of implications for data processing organizations, especially with regard to the implications of the new right to data portability, of which the impact could not be determined in this study.

Alternatively, further research could build upon the conclusions of this study; although it was expected that the transition in data protection legislation would significantly increase the burden for personal data processing organizations, the study's literature study and its conducted interviews both indicate limited implications. Consequently, it is unlikely that these implications can explain the state of confusion and panic there is (or at least had been). The interviewees suggest other possible explanations, such as non-compliance with the Wbp before (so that significantly more effort has to made in order to comply with the GDPR) or the deterrent effects that the high sanctions under the GDPR regime may have. If future research would like to address the state of confusion and panic and its causes, it thus has reasons to study the former rate of compliance with the Wbp or the psychological effects that higher sanctions may have.

Bibliography

Journal Articles

Bajcic, M. (2011). 'Conceptualization of Legal Terms in Different Fields of Law: The Need for a Transparent Terminological Approach'. *Research in Language*, 9(1): 81 – 93

Crabtree, A,. et al. (2016). 'Enabling the new economic actor: data protection, the digital economy, and the Databox'. *Personal and Ambitious Computing,* 20(6): 947 – 957

Essert, C. (2016). *A Theory of Legal Obligation*. In: Waluchow, W.J. and Sciaraffa, S. (2016). *The Legacy of Ronald Dworkin*. New York (NY), U.S.A.: Oxford University Press

Himma, K.E. (2013). 'The Ties that Bind: An Analysis of the Concept of Obligation'. *Ratio Juris*, 26(1): 16 – 46

Himma, K.E. (2018). 'Is the Concept of Obligation Moralized?'. *Law and Philosophy,* 37: 203 – 227

Krikorian, Y.H. (1935). 'The Concept of Organization'. *The Journal of Philosophy,* 32(5): 119 – 126

Malgieri, G. and Custers, B. (2018). 'Pricing privacy – the right to know the value of your personal data'. *Computer Law & Security Review*, 34: 289 – 303

Moser, C.A. (1951). 'Interview Bias'. *Review of the International Statistical Institute*, 19(1): 28 – 40

McCarthy, H. (2018). 'GDPR series: the Right to be Forgotten'. *Data Protection Ireland*, 11(1): 15 – 17

Schneider, G. (2018). 'European intellectual property and data protection in the digital-algorithmic economy: a role reversal (?)'. *Journal of Intellectual Property Law & Practice*, 13(3): 229 – 237

Simitis, S. (1995). 'From the Market To the Polis: The EU Directive on the Protection of Personal Data'. *Iowa Law Review,* 80(3): 445 – 469

Tankard, C. (2016). 'What the GDPR means for businesses'. *Network Security*, 2016, June, pp 5 – 8

Taylor, M. (2015). 'The EU's human rights obligations in relation to its data protection laws with extraterritorial effect'. *International Data Privacy Law,* 5(4): 246 – 256

Tikkinen-Piri, C., Rohunen, A., and Markkula, J. (2018). 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies'. *Computer Law & Security Review,* 2018, 34: 134 – 153

Tracol, X. (2015). 'Back to Basics: The European Court of Justice further defined the concept of personal data and the scope of the right to data subjects to access it'. *Computer Law & Security Review*, 31: 112 – 119

Zwenne, G.J. & Mommers, L. (2016). 'De tien belangrijkste veranderingen die de Algemene Verordening Gegevensbescherming gaat brengen'. *Tijdschrift voor Compliance.* 2016, august

Books

Engelfriet, A., Chew-Meij, L., and Kager, P. (2018). *Handboek AVG Compliance in de praktijk. Editie 2018*. Amsterdam, The Netherlands: Ius Mentis

Schutze, R. (2015). *An Introduction to European Law.* Cambridge, UK: Cambridge University Press

Webpages

Adams, K.A. (2007). *How a Court Determines Whether Something is an Obligation or a Condition.* Lastly consulted on 16 April 2018 from: http://www.adamsdrafting.com/how-a-court-determines-whether-something-is-an-obligation-or-a-condition/

Autoriteit Persoonsgegevens. (n.d.). *Rechten van betrokkenen: Is een privacyverklaring volgens de AVG verplicht?* Retrieved on June 2, 2018 from: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/rechten-van-betrokkenen#is-een-privacyverklaring-volgens-de-avg-verplicht-6253

Autoriteit Persoonsgegevens. (n.d.). *Rechten van betrokkenen: Hoe stelt u een privacyverklaring op?*. Retrieved on June 2, 2018 from: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/rechten-van-betrokkenen#hoe-stelt-u-een-privacyverklaring-op-6255

Christensen, L. and Etro, F. (2013). *European data protection: Impact of the EU data-protection regulation*. Retrieved on June 28, 2018 from: https://voxeu.org/article/european-data-protection-impact-eu-data-protection-regulation

European Commission. (n.d.). *For how long can data be kept and is it necessary to update it?* Retrieved on June 12, 2018 from: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_en

European Commission. (2017). *Questions and Answers – Data protection reform package*. Retrieved on June 23, 2018 from: http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm

Het Financieele Dagblad. (2017). *Bedrijven in paniek over Europese privacywet*. Retrieved on March 17, 2018 from: https://fd.nl/economie-politiek/1213263/bedrijven-in-paniek-over-europese-privacywet

H.R. Praktijk. (2017). *Werkgevers onderschatten nieuwe privacywetgeving.* Retrieved on March 15 2018 from: https://www.hrpraktijk.nl/topics/arbeidsvoorwaarden/nieuws/werkgevers-onderschatten-nieuwe-privacywetgeving

Jansen, M. (2018). *Recht op vergetelheid de grootste vernieuwing die de AVG biedt?*. Retrieved on June 20, 2018 from: https://www.dirkzwager.nl/kennis/artikelen/recht-op-vergetelheid-de-grootste-vernieuwing-die-de-avg-biedt/

Juridict. (n.d.). *De meldplicht van de Wbp wordt binnen de AVG vervangen door een documentatieplicht*. Retrieved on June 14 2018 from: https://juridict.nl/blog/article/16707/de-meldplicht-van-de-wbp-wordt-binnen-de-avg-vervangen-door-een-documentatieplicht

Kamer van Koophandel. (n.d.). *Waaruit bestaat de jaarrekening?* Retrieved on June 26, 2018 from: https://www.kvk.nl/inschrijven-en-wijzigen/deponeren/jaarrekening-deponeren/waaruit-bestaat-de-jaarrekening/

Klekovic, I. (2017). *EU GDPR vs. European data protection directive.* Retrieved on June, 12 from: https://advisera.com/eugdpracademy/blog/2017/10/30/eu-gdpr-vs-european-data-protection-directive/

Naudts, L. (2016). *The Right not to be Subject to Automated Decision-Making: The role of explicit consent.* Retrieved on June 20, 2018 from: https://www.law.kuleuven.be/citip/blog/the-right-not-to-be-subject-to-automated-decision-making-the-role-of-explicit-consent/

Oxford Dictionaries. (2018). *Organization.* Lastly consulted on 16 April 2018 from: https://en.oxforddictionaries.com/definition/organization

Other Publications

Bout-Tapper, M. (2017). *Paniek bij MKB rond Europese privacywet is onterecht.* Amsterdam, The Netherlands: OverOndernemen

Centrum voor Informatiebeveiliging en Privacybescherming. (2017). *Tussen Wbp en Avg: Over de invoering van de Avg.* Amsterdam: CIP

College Bescherming Persoonsgegevens. (2007). *CPB Richtsnoeren: Publicatie van persoonsgegevens op internet*. The Hague, The Netherlands: College Bescherming Persoonsgegevens

Dagblad van het Noorden. (2018). *Privacywet? Geen paniek*. 24 mei 2018, Dagblad van het Noorden.

European Union Agency for Fundamental Rights and Council of Europe. (2018). *Handbook on European data protection law, 2018 edition*. Luxembourg, Luxembourg: Publication Office of the European Union

ICTRecht B.V. (2017). *De Algemene Verordering Persoonsgegevens: Wat verandert er echt?* Amsterdam, The Netherlands: ICTRecht B.V.

Jongers, T.S. (n.d.). *Algemene Verordening Gegevensbescherming.* The Hague, The Netherlands: PEP

Kerber, W. (2016). *Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection*. Marburg, Germany: Marburg Centre for Institutional Economics

Krzysztofek, M. (2017). *Post-reform personal data protection in the European Union: general data protection regulation (EU) 2016/679.* Alphen aan den Rijn, The Netherlands: Wolters Kluwer

Lemsom, M. (2017). *Bedrijven en overheden niet klaar voor nieuwe privacywet.* Hilversum, The Netherlands: NOS

Matera, C. (2016). *Writing the bachelor thesis in law in the EPA programme at the University of Twente.*

MKB Nederland & VNO-NCW. (2018). *Een knellend probleem: privacy versus goed werkgeverschap. Leg in UAVG vast welke gegevens voor welk doel wél mogen worden verwerkt.* The Hague, The Netherlands: MKB Nederland & VNO-NCW

Sauerwein, L.B. and Linnemann, J.J. (2002). *Handleiding voor verwerkers van persoonsgegevens. Wet Bescherming Persoonsgegevens*. The Hague, The Netherlands: Ministerie van Justitie

Schermer, B.W., Hagenauw, D. & Falot, N. (2018). *Handleiding Algemene verordening gegevensbescherming (en Uitvoeringswet Algemene verordening gegevensbescherming.* The Hague: Ministerie van Justitie en Veiligheid.

Van der Kolk, H. (n.d.). *Conceptualization: Constructs as combinations of facets and terms.* Enschede, The Netherlands: University of Twente [microlecture]

Zwenne, G.J., Duthler, A.W., Groothuis, M.M., Kielman, H.H., Koelewijn, W.I. and Mommers, L. (2007). *Eerste fase evaluatie Wet bescherming persoonsgegevens. Literatuuronderzoek ten behoeve van onderzoeksopzet en vraagarticulatie.* The Hague, The Netherlands: WODC

Legislation

Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, available at: http://www.refworld.org/docid/3ae6b3b70.html

Civil Code for the Kingdom of the Netherlands Book 6, Contract law, 1 September 2017, *Stb.* 2016, 290, available at: http://wetten.overheid.nl/BWBR0005289/2017-09-01

Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, *OJ* [2012] C 326, 26 October 2012, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT

Constitution for the Kingdom of the Netherlands *,* 17 November 2018, Stb. 2017, 426, available at: http://wetten.overheid.nl/BWBR0001840/2017-11-17

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Convention 108, 28 January 1981, CETS No 10, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, available at: http://www.refworld.org/docid/3ae6b3b04.html

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 4 May 2016, *OJ* L119, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC

Universal Declaration of Human Rights, 10 December 1948, 217 A (III), available at: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf

Wet bescherming persoonsgegevens, 1 June 2017, *Stb.* 2016, 373, available at: http://wetten.overheid.nl/BWBR0011468/2017-07-01

Appendix A: Table with differences in obligations and conditions

Obligation or condition	Wbp Art.	GDPR Art.	Corresponding content?
Objectives and foundations of data processing			
Pre-defined and explicit objectives for data processing	7	5.1	Yes
Necessity for the achievement of the objectives	11.1	5	Yes
Based on at least one of the six legal foundations	8	6.1	Yes
Time limits for storage			
Storage for as long as necessary for the accomplishment of the objectives + Exceptions	10.1 + 10.2	5.1.e + 5.1.e	Yes
Rights for data subjects			
Right to be informed	33 -34	13 – 14	No
Right to access	35	15	Yes
Right to correct/complete	36	16	Yes
Right to resist	40 – 41	21	Yes
Right to 'be forgotten'	36	17 – 18	Yes
Right to data portability	-	20	No
Right not be subject to automated decision-making	42	22	Yes
Special types of personal data			
Prohibition of processing special types of personal data or personal data of a criminal law nature +Exceptions	16 + 17 – 23	9 – 10 + UAVG 22 – 33	Yes
Technical and organizational security measures			
Appropriate technical and organizational security measures	13	32	Yes
Reporting of data breaches	34a	33	No
Reporting/registering personal data processing activities	27 – 30	30	No
Appointment of a data protection official	-	37 – 39	No
Performance of data protection impact assessments	-	35	No

This table schematically presents the various obligations and conditions, together with the articles in which they are mentioned. Red text indicates an obligation or condition that is stated in only one of the laws or of which the content does not correspond for both laws.

Appendix B: Questionnaire

The questionnaire below is used in the three personal interviews, as all questions were asked during the interviews. Additionally, one organization filled in this questionnaire. This (anonymized) answered questionnaire, as well as a translated version of the questionnaire and the audio recordings of the personal interviews can be found in the separate Data Appendix.

After the first questions that give an impression of the personal data processing activities of the interviewed organizations, there are several questions that show the organization's awareness of and compliance with the Wbp and GDPR. Finally, various questions are included that ask for the interviewee's opinion and experience regarding the (transition from the Wbp to the) GDPR. An summarizing matrix of answers to the twenty questions by the respondents can be found in Appendix C of this paper.

Questionnaire (Dutch version)

Zoals u reeds bekend naar aanleiding van ons contact, bent u volledig vrij in uw beantwoording van onderstaande vragen. Het zijn achttien vragen, allemaal voorzien van een beknopte toelichting en sommige vragen ook van de context van de wet (u waarschijnlijk reeds bekend). Uw antwoorden zullen in mijn onderzoek geanonimiseerd worden gebruikt. Deze zullen dus niet herleidbaar zijn op u als persoon, noch op uw organisatie. In alle gevallen waarbij in de vragen de woorden 'u' en 'uw' worden gebruikt, wordt verwezen naar de organisatie waarvoor u werkzaam bent en niet uw persoon.

Informatie organisatie (*aanvullen graag*):

- Type organisatie (*publiek/semi-publiek/privaat*): …….
- Commericeel of non-profit (*met of zonder winstoogmerk*): ……..
- Omvang organisatie (*zal slechts worden gebruikt om de organisatie te categoriseren als klein, middelgroot of groot*)
  - Aantal werknemers: …….
  - Indien van toepassing en publiekelijk bekend (*bij bijvoorbeeld grote organisaties*) - jaarlijkse totale omzet: …..

Vragen

1. **Welke persoonsgegevens verwerkt u? Waarom verwerkt u deze?**
   - *Context wet*

   *De AVG verstaat onder persoonsgegevens **feitelijke informatie herleidbaar naar individuen**. Denk hierbij bijvoorbeeld aan adressen, telefoonnummers en mailadressen. Ook **waarderende informatie** valt onder persoonsgegevens, bijvoorbeeld informatie over iemands functioneren. Volgens de AVG moet u verder een duidelijk en vooraf omschreven doel of doelen hebben voordat u persoonsgegevens mag verwerken.*
   - *Toelichting vraag*

   Wat voor persoonsgegevens worden door uw organisatie verwerkt en van wie (bijvoorbeeld klanten, leden, medewerkers, etc.)? Welke doelen heeft u voor welke verwerking? Is het voor deze doelen noodzakelijk dat persoonsgegevens verwerkt worden?

2. **Hoe verwerkt u deze persoonsgegevens?**
   - *Context wet*
     De AVG omschrijft verwerken als elke bewerking of geheel van bewerkingen met betrekking tot persoonsgegevens. Voorbeelden van verwerking zijn verzamelen, vastleggen, opslaan, wijzigen, opvragen, raadplegen, gebruiken, verstrekken en wissen en vernietigen van persoonsgegevens.
   - *Toelichting vraag*
     Welke vorm(en) van verwerking worden door uw organisatie uitgevoerd?

3. **Hoe bent u op de hoogte gesteld van de verplichtingen die de AVG met zich meebrengt? Denkt u dat de verplichtingen en rechten die de AVG stelt in het algemeen bekend genoeg zijn?**
   - *Toelichting vraag*
     Hoe weet u wat de AVG inhoudt en hoe u hieraan moet voldoen? Was u ruim op tijd geïnformeerd om aan de AVG te kunnen voldoen voor de ingangsdatum van 25 mei 2018? Denkt u dat het voor iedereen duidelijk is wat zijn/haar rechten en plichten zijn wat betreft (de verwerking van) persoonsgegevens?

4. **Voldoet uw organisatie nu aan de AVG, naar uw mening?**
   - *Toelichting vraag*
     De AVG is van toepassing sinds 25 mei 2018. Voldoet uw organisatie aan alle eisen die door de AVG gesteld worden?

5. **Voldeed uw organisatie daarvoor aan de Wbp?**
   - *Context wet*
     De AVG vervangt de Wet bescherming persoonsgegevens (Wbp), de Nederlandse wet die van toepassing was op verwerking van persoonsgegevens van 1 september 2001 tot 25 mei 2018. Tussen september 2001 en mei 2018 moest uw organisatie bij het verwerken van persoonsgegevens dus voldoen aan de Wbp.
   - *Toelichting vraag*
     Voldeed uw organisatie aan de eisen die de WBP stelde?

6. **Op welke juridische grondslag baseert u uw gegevensverwerking?**
   - *Context wet*
     Volgens de AVG moet u, naast het bij vraag 1 genoemde doel, ook een grondslag hebben waarop u uw gegevensverwerking baseert. U moet dus voldoen aan minstens één van de zes grondslagen die de AVG noemt voordat u persoonsgegevens mag verwerken. Deze zes grondslagen zijn (beknopt omschreven):
     a. *Toestemming van de betrokkene wiens persoonsgegevens worden verwerkt (let op: dit moet vrijwillige, specifieke, geïnformeerde en ondubbelzinnige toestemming zijn)*
     b. *De verwerking is noodzakelijk voor het uitvoeren van een overeenkomst met de betrokkene of op verzoek van de betrokkene vóór het sluiten van de overeenkomst) (bijv. iemands adres bij een online bestelling die bezorgd moet worden)*

c. *De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting waar uw organisatie aan moet voldoen (bijv. u moet een kopie van het identiteitsbewijs van uw werknemers bewaren om te voldoen aan de Wet op de loonbelasting)*
d. *De verwerking is noodzakelijk om de vitale belangen van de betrokkene of een ander persoon te beschermen (bijv. in een medisch noodgeval)*
e. *De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag (bijv. door de Raad voor de Kinderbescherming, de Reclassering, etc.)*
f. *De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van uw organisatie of van een derde, indien die belangen zwaarder wegen dan de belangen of grondrechten van de betrokkene (e.g. bij direct marketing of ter voorkoming van fraude)*

- *<u>Toelichting vraag</u>*
  Kunt u voor uw verwerkingen van persoonsgegevens aangeven op welk van de zes grondslagen ze zijn gebaseerd?

7. Bewaart u de persoonsgegevens? Heeft u procedures omtrent de tijdslimiet voor het bewaren van persoonsgegevens?

- *Toelichting vraag*
  De AVG stelt regels aan het bewaren van persoonsgegevens. Heeft u een termijn vastgelegd hoe lang u persoonsgegevens bewaart, en richtlijnen hoe u deze verwijdert of anonimiseert?

8. Hoe gaat u om met de rechten van betrokkenen? Heeft u hier een procedure voor opgesteld?

- *<u>Context wet</u>*
  De AVG verleent de betrokkene diverse rechten, waaronder het recht om geïnformeerd te worden, het recht op inzage in hoe zijn/haar persoonsgegevens worden verwerkt, het recht om deze gegevens te verbeteren of aanvullen indien deze onjuist of incompleet zijn, het recht om 'vergeten te worden' (zijn haar gegevens te laten verwijderen of afschermen)en het recht op dataportabiliteit (het recht op een kopie van zijn/haar gegevens om die mee te kunnen nemen bij bijv. de overstap naar een andere provider).
- *<u>Toelichting vraag</u>*
  Hoe informeert u betrokkenen over de verwerking van hun persoonsgegevens? Hoe gaat u om met verzoeken in het kader van hierboven genoemde rechten; wie handelt deze verzoeken af en hoe antwoordt u?

9. Verwerkt u 'bijzondere' soorten persoonsgegevens of persoonsgegevens van strafrechtelijke aard?

- *<u>Context wet</u>*
  De AVG onderscheidt enkele soorten 'bijzondere' persoonsgegevens, die gezien hun aard extra gevoelige informatie bevatten. Het gaat hierbij om gegevens gerelateerd aan iemands religieuze of levensbeschouwelijke overtuigingen, ras en etnische achtergrond, politieke opvattingen, gezondheid,seksueel gedrag en seksuele oriëntatie en lidmaatschap van een vakbond en genetische en biometrische gegevens.
  De AVG is erg strikt wat betreft de verwerking van deze gegevens en in de meeste gevallen is

het dan ook verboden om 'bijzondere' persoonsgegevens te verwerken. Er zijn slechts enkele specifieke uitzonderingen hierop. Ook voor persoonsgegevens van strafrechtelijke aard geldt dat ze slechts in zeer specifieke uitzonderingssituaties verwerkt mogen worden.

- *Toelichting vraag*
  Verwerkt u 'bijzondere' persoonsgegevens of gegevens van strafrechtelijke aard? Zo ja, op basis waarvan denkt u deze te mogen verwerken?

10. Houdt u een register van verwerkingsactiviteiten bij? Wat heeft u hierin opgenomen?

- *Context wet*
  Volgens de AVG bent u verplicht een register bij te houden waarin u al uw verwerkingsactiviteiten bijhoudt. Uitgezonderd op deze verplichting zijn kleine organisaties (minder dan 250 werknemers), tenzij hun gegevensverwerking niet-incidenteel (en dus stelselmatig) is, een hoog risico met zich meebrengt of 'bijzondere' persoonsgegevens bevat.
- *Toelichting vraag*
  Houdt u een dergelijk register bij? Indien ja: wat heeft u hierin opgenomen? Wie houdt het register bij?

11. Heeft u een functionaris gegevensbescherming aangesteld?

- *Context wet*
  Sommige organisaties zijn verplicht om een functionaris gegevensbescherming aan te stellen. Organisaties zijn dit verplicht indien ze (1) een overheidsorganisatie zijn, of ten behoeve van hun kerntaken (2) regelmatige en stelselmatige observatie op grote schaal vereisen in hun verwerking (bijv. vervoersbedrijven die reisgegevens verzamelen) of (3) 'bijzondere' gegevens en/of persoonsgegevens van strafrechtelijke aard op grote schaal verwerken. Overige organisaties zijn niet verplicht om een functionaris gegevensbescherming aan te stellen, maar mogen dit op vrijwillige basis toch doen.
- *Toelichting vraag*
  Heeft u functionaris gegevensbescherming aangesteld? Indien ja, beantwoord u dan a.u.b. ook de volgende deelvragen:
  a) *Bent u op grond van één van bovenstaande criteria verplicht om een functionaris gegevensbescherming aan te stellen of heeft u dit op vrijwillige basis gedaan?*
  b) *Welke hoofdfunctie binnen de organisatie heeft de persoon die tot functionaris gegevensbescherming is benoemd? Waarom is specifiek deze persoon functionaris gegevensbescherming geworden?*
  c) *Heeft deze functionaris voor de uitoefening van zijn/haar taken een training gevolgd of anderzijds inspanningen geleverd om op de hoogte te zijn van zijn/haar taken en plichten?*

12. Verricht u gegevensbeschermingseffectbeoordelingen?

- *Context wet*
  De AVG verplicht sommige organisaties om periodiek een gegevensbeschermingseffectbeoordeling uit te voeren. Dit is alleen verplicht voor verwerkingen die (potentieel) een hoog risico inhouden. De toezichthouder Autoriteit Persoonsgegevens zal een lijst bijhouden met types verwerkingen die een hoog risico inhouden, maar in de wet staan in ieder geval drie gevallen van verwerkingen die een hoog

risico inhouden: (1) geautomatiseerde, systematische en uitgebreide evaluatie van een individu's persoonlijke aspecten, waaronder profilering, waarop besluitvorming wordt gebaseerd, (2) op grote schaal verwerken van 'bijzondere' persoonsgegevens of persoonsgegevens van strafrechtelijke aard, en (3) het grootschalig en stelselmatig observeren van mensen in openbaar toegankelijke ruimten.

- *Toelichting vraag*
  Bent u op basis van bovenstaande criteria of de lijst van de AP verplicht om gegevensbeschermingseffectbeoordelingen uit te voeren? Indien ja: hoe voert u deze beoordelingen uit? Wie binnen de organisatie is daarvoor verantwoordelijk?

13. Welke technische en organisatorische maatregelen heeft u getroffen om de gegevens te beveiligen? Waren deze makkelijk of moeilijk te realiseren?

- *Context wet*
  U wordt, als verwerker van persoonsgegevens, geacht om passende technische en organisatorische maatregelen te nemen ten behoeve van de beveiliging van uw persoonsgegevens. Wat wordt beschouwd als 'passend', verschilt per geval: de gevoeligheid van de gegevens die u verwerkt wordt hierbij in beschouwing genomen, evenals de aard, context en doelen van de verwerking en de kosten die uitvoering van maatregelen met zich meebrengen. Technische maatregelen omvatten bijvoorbeeld encryptie, firewalls en het beveiligen van de computersystemen. Organisatorische maatregelen omvatten bijvoorbeeld het beperken van de toegang tot bepaalde persoonsgegevens en het specificeren wie waartoe toegang heeft.
- *Toelichting vraag*
  Welke technische en organisatorische maatregelen heeft u getroffen? Waren deze makkelijk complex te realiseren? Kostte dit veel tijd en/of geld of niet, of waren de benodigde maatregelen reeds genomen vóór invoering van de AVG?

14. Was het voor u eenvoudig of complex om aan de AVG te voldoen? Heeft u een inschatting van tijd/moeite/geld/middelen die gebruikt zijn om ervoor te zorgen dat u aan de AVG voldoet?

- *Toelichting vraag*
  De AVG kent, zoals u ook hierboven al hebt kunnen zien, een hele reeks vereisten aan verwerkers van persoonsgegevens. Was het voor uw organisatie eenvoudig om aan al deze wettelijke eisen te voldoen, of was (en is) dit complex? Kunt u inschatten hoeveel tijd en moeite werknemers van de organisatie kwijt zijn geweest met de implementatie van de AVG, en hoeveel financiële middelen of middelen van andere aard nodig zijn geweest om te voldoen aan de AVG?

15. Denkt u dat het voor uw type organisatie makkelijker of moeilijker dan gemiddeld is om aan de AVG te voldoen?

- *Toelichting vraag*
  Denkt u, gelet op de persoonsgegevens die u verwerkt, de verwerking zelf en uw organisatie, dat het voor uw organisatie makkelijker of moeilijker is om aan de AVG te voldoen dan voor de gemiddelde organisatie? Waaraan ligt dat volgens u?

16. In hoeverre is de verandering in databeschermingswetgeving een bijdrage aan of belemmering voor het functioneren van uw organisatie?

- *Toelichting vraag*
  Of het nou de verkoop van goederen of diensten, het verrichten van een publieke taak of iets anders is: uw organisatie heeft ongetwijfeld een bepaalde kerntaak. Draagt de verandering in databeschermingswetgeving (van Wbp naar AVG) bij aan het functioneren van uw organisatie, en dus de uitvoering van haar kerntaak? Of belemmert de verandering in databeschermingswetgeving juist het functioneren van uw organisatie, en dus de uitvoering van haar kerntaak? Op welke manieren is dit het geval?

17. Vindt u het gerechtvaardigd dat er eisen worden gesteld aan uw gegevensverwerking?

- *Toelichting vraag*
  Vindt u dat de doelen van de AVG (het beschermen van persoonsgegevens en privacy, het harmoniseren van databeschermingswetgeving binnen de EU en het behouden van consumentenvertrouwen in de digitale economie) rechtvaardigen dat de wet eerdergenoemde eisen stelt? Denkt u dat de AVG wat die doelen betreft een verbetering is ten opzichte van de Wbp?

18. Bent u op de hoogte van de boetes die opgelegd kunnen worden bij het niet voldoen aan de AVG? Wat vindt u hiervan?

- *Context wet*
  De maximumboetes die kunnen worden opgelegd onder de AVG zijn substantieel hoger dan onder de Wbp (tot wel twintig keer hoger).
- *Toelichting vraag*
  Bent u op de hoogte van deze verhoging en van de maximumboetes? Wat vindt u van deze verhoging? Is het een reden voor uw organisatie om zich meer te bekommeren om het al dan niet voldoen aan de AVG?

19. Als u dit zou moeten benoemen, wat vindt u dan de voor- en nadelen van de AVG ten opzichte van de Wbp voor u als verwerker?

- *Toelichting vraag*
  Is de AVG wat u betreft, los van de doelen uit voorgaande vraag, een verbetering ten opzichte van de Wbp voor u als verwerker van persoonsgegevens? Is het makkelijker of moeilijker om aan de AVG te voldoen ten opzichte van de Wbp? Heeft de AVG voordelen voor u als verwerker? Heeft de AVG nadelen?

20. Wat kan volgens u verbeterd worden aan de AVG?

- *Toelichting vraag*
  Gelet op uw beantwoording van voorgaande vragen, uw implementatie van de AVG en uw (weliswaar nog korte) ervaring met het opereren onder de AVG, wat kan er dan nog verbeterd worden aan de AVG?

Appendix C: Matrix of answers by respondents

The following matrix gives an overview of answers by the interviewees. The question numbers refer to the questions of the questionnaire.

Question	Answer organization			
	Small commercial private organization (business)	**Medium-sized public organization**	**Large semi-public organization**	**Small non-profit private organization**
1 Which personal data + objectives	Contact information of customers, bank account number Objectives: information provision, financial administration	Many types of personal data. Also for many objectives	Many types of personal data (more than can be listed). Also for many objectives.	Various personal data, mostly contact information. Objectives: members administration, information provision, sending invitations for activities, promotion
2 Forms of data processing	Recording, storing, using	Many different forms of processing	Many different forms of processing	Recording, storing, using
3 How informed about rights and duties	Informed in time, in this case via other job for which I am also involved in implementation GDPR, but otherwise I would have heard it in the news. Informed about specific content GDPR via documents AP and a handbook about compliance with the GDPR	There is a department of legal affairs that informs the rest of the organization, many people followed a training, personally I am mainly informed via self-study with AP instructions and a book	Already three years ago informed about the coming GDPR. In terms of content, both internal and external lawyers provided the organization with the specific content	Informed late (a few weeks before the GDPR became enforceable) by umbrella organizations
4 Compliance with GDPR	Not compliant with the GDPR	Not fully compliant yet with the GDPR, but on the right way. Roughly complying with	Compliant with the GDPR, although it is an ongoing process; it could be that on the basis of	Not fully compliant yet with GDPR

		the GDPR for about 70%	case law, we will find out that we still need to improve things	
5 Compliance with Wbp	Not compliant with the Wbp before, also unaware of its existence	Not fully compliant with the Wbp before, and unaware of its content. There were also never inspections	Compliant with the Wbp before, although there were never inspections	Not compliant with Wbp before
6 Foundations	Permission, necessity for the performance of an agreement, necessity for the fulfillment of a legal obligation (such as the duty to store invoices for a certain amount of time)	Necessity for the performance of an agreement, necessity for the fulfillment of a legal obligation, mostly because of the necessity for performance of a public task	Permission, necessity for the performance of an agreement, necessity for the fulfillment of a legal obligation, necessity for the representation of legitimate interests (e.g. marketing)	Permission, necessity for the performance of an agreement
7 Storage + procedures time limits	Data is stored, but no procedures yet regarding time limits	There are procedures regarding data storage, that also has to do with other laws we have to comply with, such as the *Archiefwet*	Procedures are made by departments and teams, the data protection officials only check to what extent these procedures comply with the GDPR. Nevertheless, everybody is responsible him-/herself for his/her data storage	No procedures yet regarding time limits
8 Rights data subjects	No procedures regarding requests from data subjects (and requests are also	The department of legal affairs is working on procedures to	No procedures regarding requests from data subjects.	No procedures regarding requests from data subjects.

	not expected). Information-provision still inadequate	ensure a timely answer. Information provision via online privacy statement	Information will be provided via an online privacy statement	Information will be provided via an online privacy statement
9 'special' personal data	No	Yes, for health-related data. Necessary for the provision of healthcare. Very strict security measures therefore	Yes, for scientific purposes	Yes, information regarding diets and allergies. Necessary for the preparation of meals
10 Register processing activities	No, not yet at least	Yes, all required information	Yes. Not more included than necessary for the law	No
11 Data protection official	No	Yes, since a few weeks officially. That person's main task include connecting governance with communication, so that fits with this duty. The official followed a course from a consultancy agency.	Yes, in the form of a team of four people with different expertise and backgrounds. Members followed various trainings from external lawyers, but were already involved in data protection as they are either lawyers or IT experts	No
12 Data protection impact assessments	No	Not yet, but it is planned	Yes, once via a computer system and now a checklist is developed to assess the potential risk of each processing activity	No
13 Security	Technical measures are there, as the computer	Technical measures,	Both technical and	No measures yet. Plans to take

measures	systems are secured (and also a secured mailbox is planned). Organizational measures were also already in place (such as passwords for administrative systems containing personal data)	including a secured network, firewalls. Organizational measures, including restricting access. There measures were mostly already there before the introduction of the GDPR	organizational measures in place, but already before the introduction of the GDPR	organizational measures; storing all data at one place, restricting access
14 Efforts to comply, resources	No financial resources were used, only a few hours of time	Not difficult, it mostly requires a different way of thinking, being more aware of your data processing. Also technically, it was not difficult. We already had a high level of security. Nevertheless, difficult to fully comply, as employees also use their personal devices for mails etc.	Technically not difficult, as the measures were already there. Interpretation is a challenging part, as you never know when you fully comply. Finally, it is difficult to convince everybody within the organization to cooperate, that requires quite some time (but also the case before the introduction of the GDPR)	No financial resources were used, in terms of time roughly thirty hours spent on ensuring compliance
15 Difficulty of compliance	It would be rather easy for this organization to comply, as it is really small, so that all processing activities are well-known and well-considered	More difficult to comply than for a company, as our organizations processes many more personal data due to the performance of public tasks	It is more difficult to comply due to the large size and decentralization of the organization, with many different projects and activities going on.	Easier to comply than for the average organization, due to its small size. On the other hand, due to a lack of compliance with the Wbp before,

			On the other hand, the organization was already compliant with the Wbp and various measures were already in place	it is still more difficult
16 Contribution or hindrance	The GDPR has no influence on the performance of the organization's core tasks	No contribution or hindrance to the organization's core tasks, it just requires a different way of thinking	The GDPR does not hinder the performance of the core tasks of the organization. It also does not directly contribute, but intuitively might contribute as it forces the organization to rethink and map their processes, which might lead to optimization of these processes	No influence on the organization's core tasks, as long as data subjects do not complain with the way their data is used
17 Justifyable	Yes, sometimes people process data without having thought out the process and that leads to misconducts. Therefore, personal data were already handled with care	Yes, and especially for a public organization, as it collects a lot of data	Yes, certainly	Yes, also within the organization, the GDPR contributes to the level of data protection.
18 Sanctions	Good that the fines are there and are that high, as data protection is a serious matter. This organizations will not be checked and not be fined either, as goodwill can be demonstrated	Aware of the fact that there are high fines possible, but not aware of the exact numbers. Very good that these fines are there, otherwise compliance	Good that the fines are that high. These sanctions force compliance, in contrast with the Wbp, that was not taken seriously by many organizations.	Expect the fines to be imposed seldomly. Could have a (good) deterrent effect for large organizations. Our organization will never be checked and

		levels would be low		certainly not fined, so less relevant
19 Advantages and disadvantages GDPR compared with Wbp	No idea, as the organization did not comply with the Wbp before and is unaware of its content	Although not really aware of the content of the Wbp, I already found out there are only little differences between the Wbp and GDPR.	An advantage is the height of the fines. For data protection officials, those fines make it easier to persuade others within the organization. No disadvantages experienced. All in all, there are hardly any differences for us between the Wbp and GDPR	No idea, as we did not comply with the Wbp before and are not aware of its content
20 Improvements GDPR	I cannot think of an improvement by now	The AP could be more clear in terms of when it is going to inspect organizations, how these inspections work, etc.	Some things are still vague, such as the difference between the data responsible and the data processor. Case law is needed to address those issues. Furthermore, it is unclear what the AP formally thinks of having a data protection team rather than a single official	Sometimes it is still vague what is allowed or not. Lack of case law. The AP could accompany small and inexperienced organizations more