MASTER'S THESIS

The data protection officers' perception on conducting a data protection impact assessment

A Belgian perspective on the harmonisation goal of the GDPR

Vandenberghe, P.M.M. (Patrick)

Award date:
2019

The Data Protection Officers' perception on conducting a Data Protection Impact Assessment

A Belgian perspective on the harmonisation goal of the GDPR.

Degree programme:	Open University of the Netherlands, Faculty of Management, Science & Technology Business Process Management & IT master's programme
Degree programme:	Open University of the Netherlands, Faculty of Management, Science & Technology Business Process Management & IT master's programme
Course:	IM0602 BPMIT Graduation Assignment Preparation IM9806 Business Process Management and IT Graduation Assignment
Student:	Patrick Vandenberghe
Identification number:	
Date:	06 december 2019
Thesis supervisor	Dr. Laury Bollen
Second reader	Dr.ir. Harry Martin
Third assessor	Not applicable
Version number:	1.0
Status:	Final version

Abstract

The General Data Protection Regulation (GDPR) is the new EU data protection legal framework. It repealed the EU Data Protection Directive in 2018. The aim of the GDPR is double: a privacy legislation which better fits the digital age and which harmonises, or bring into conformity with each other, the data protection laws of the 28 EU member states. The data protection officer (DPO) is one of the main actors under the GDPR whereby the effective and efficient conduction of a data protection impact assessment (DPIA) is part of his responsibilities.

This study aims to determine how DPO's perceive the process of conducting a DPIA, and how they see the harmonisation goal of the GDPR through this lens of the DPIA. Based on a review of the literature on GDPR, DPIA and harmonisation, semi-structured interviews were conducted.

The conclusions linked the success of harmonised DPIAs to the quality of the (inter)national guidelines and the level of service provided by the DPOs' data protection authority. It also revealed that the national exceptions imposed by the national data protection authorities and the initiatives of the sectorial federation/umbrella organisations can greatly contribute to the failure or success of harmonised DPIAs.

Key terms

General Data Protection Regulation, GDPR, Data Protection Impact Assessment, DPIA, Data Protection Officer, DPO, harmonisation.

Acknowledgement

The search for a topic for my thesis in the context of the master's programme 'Business processes and ICT' led me to the 'Data Protection Impact Assessment' (DPIA) as imposed by the EU 'General Data Protection Regulation' (EU GDPR). The GDPR is a privacy legislation applying to the processing (collecting, storing, managing and deleting) of personal data by (semi-)automated means. In order to be GDPR-compliant, a company has to assess all its existing and new business processes and IT applications related to personal data for risks that might affect the persons concerned. In this regard, conducting a DPIA could be necessary in order to decide if these processes and applications have to be redesigned.

By choosing the EU GDPR as the topic for my master thesis, I have left my comfort zone and challenged myself to explore a completely new area.

My learning journey started in 1993, when I first registered for a course at the Open University of the Netherlands. On the one hand, the Open University's flexible learning concept with regard to distance offered me the ability to make some necessary deviations from the traditional Open University path without harmful consequences. These deviations included three long United Nations and NATO missions abroad (ex-Yugoslavia, Burundi and Afghanistan), other long-term courses imposed by my employer, in-depth language courses (French, English, German) and private reasons. On the other hand, these deviations have meant that the journey has taken a long time.

I would like to thank everyone who has accompanied me on this learning path.

First, my appreciation goes to my first supervisor, Dr Laury Bollen, for his inputs that helped me to keep moving in the right direction.

Second, I would like to thank my girlfriend who supported me in any possible way and who offered much of her leisure time.

Third, I would like to express my gratitude to everyone who spent some of their valuable time to participate in the interview. Without their help and time, gathering data for the empirical part of this thesis would not have been possible.

Finally, I would like to thank the fellow students at the Open University with whom I succeeded one or more team assignments.

Thank you for walking the path with me.

I took the opportunity offered by the Open University to write the paper in UK English (instead of Dutch). This decision was taken based on some logical reasons: English is the universal language of science (in particular, of IT and Business Process Management) as well as the most commonly used language of the new privacy legislation. Moreover, this paper offered me a good opportunity to put into practise the high level of English obtained during my language courses at '*Centrum voor Levende Talen*' in Leuven (Belgium).

Summary

ICT technologies are developing at a rapid pace, and that development entails the exposure and automatic processing of personal data. These data have become an integral part of the core processes of both private and public organisations: collecting, processing, using and communicating those data. However, in turn, the availability of those data inevitably also pose more and more specific risks to the rights of individuals due to malicious phenomena, such as cyber-attacks and losses of data. Consequently, laws and regulations to protect data subjects (i.e. those whose personal data are used) are needed now more than ever before.

In this regard, 28 May, 2018, was a landmark day for data protection. On that date, the European Regulation 2016/679,[1] better known as the General Data Protection Regulation (GDPR), became enforceable in all Member States of the EU. The aim of this new data protection legal framework is twofold. First, it repealed the outdated EU Data Protection Directive 95/46/EC,[2] which was adopted when ICT was in its infancy, and replaced it with a privacy legislation which should better fit the digital age and the threats inherent to it. Second, the European Union wanted to harmonise the different fragmented and asymmetric national transposition laws of the repealed directive in order to offer EU-wide transparent protection of individuals' rights and freedoms.

The regulation is a legislative requirement to conduct a Data Protection Impact Assessment (DPIA). This DPIA is enshrined in the GDPR by means of article 35 and is advocated as one of the main rules of the regulation meant to empower data subjects' rights. Of course, not all organisations are affected in the same way by the new data protection rules of the GDPR legislation and by the possible obligation of a DPIA. In this regard, large enterprises, whose daily business relies on the systematic and extensive processing of large amounts of sensitive personal data, are more impacted by the new legislation than small firms. For the former, the consequences of a data breach is high for data subjects, but it is somewhat lower for the latter, who only gather the contact information of their clients. Furthermore, the abstract nature of the GDPR leaves room for data protection officers (DPOs), who are responsible for conducting the DPIAs, to interpret differently the relevant triggers and guidelines. This flexibility could result in an inconsistent application of DPIAs across the EU and, consequently, an uneven level of protection of personal data.

The research reported in this thesis delivers an (empirical) contribution regarding the perception of DPOs on the harmonisation goal of the GDPR through the lens of the DPIA. Based on a study of the guidelines for conducting a DPIA, as required by article 35 of the GDPR, and on the harmonisation goal of this new regulation, this thesis evaluated the perception of DPOs of different Belgian sectors on conducting a DPIA and how the harmonisation objective of the GPDR is seen through these perceptions of the DPIA.

The central research question of this research is as follows:

> *How do DPO's perceive the process of conducting a DPIA, and how do they see the harmonisation goal of the GDPR through this lens of the DPIA?*

[1] Regulation 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

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

The following sub-questions (SQ) were developed based on the central research question:

1. *What are the concepts of the GDPR, its harmonisation goal and the DPIA?*
   - *SQ1: What are the main principles of the GDPR?*
   - *SQ2: What is harmonisation?*
   - *SQ3: What are the main factors that affect the harmonisation goal of the GDPR?*
   - *SQ4: What is a DPIA?*
   - *SQ5: What are the most important requirements in the context of the execution of a DPIA, as required by the GDPR?*
2. *How do DPOs interpret and execute the DPIA?*
   - *SQ6: What are DPOs' current practices and views on the GDPR/DPIA?*
3. *How do DPOs experience the harmonisation goal of the GDPR based on their perception of the DPIA?*
   - *SQ7: How is the harmonisation goal of the GDPR seen through the lens of the DPIA*?

Any evaluation of the DPOs' perception of a DPIA and of the success of the harmonisation goal depends on what is understood by 'DPIA' and 'harmonisation'. In order to better understand these terms, the criteria for executing a DPIA and the harmonisation goal of the GDPR are addressed during the literature review of this thesis.

During the practical part of this research, qualitative data were collected during semi-structured interviews (including the discussion of a fictional case) in order to explore the DPOs' perception of the DPIA and of the harmonisation goal of the GDPR. Due to time constraints, the interviews were held within a short period of a few weeks.

Based on the literature review and the interviews with some DPOs, this study found that the interviewees view the GDPR as a good successor of the former privacy law and as a promoting harmonisation. Nevertheless, they do perceive a lack of clarity (which has to be resolved) and a number of exceptions (which have to be eliminated). One of the most cited items in this context is the DPIA.

With regard to conclusions, a 'harmonised DPIA template' consists of two parts, a common part applicable to all nations or within one nation and a second part adapted to the sector. Furthermore, the impact of the attitude of the NDPAs is somewhat two sided: on the one hand, they should explain and clarify some uncertainties and thus promote harmonisation; on the other hand, their deviating national black-and-white lists result in a non-uniform conduction of the DPIA across Member States and thus a negative influence on the harmonisation.

The answer to the central research question is that the DPOs see the DPIA as a useful tool to verify if a high-risk data processing activity is legally compliant with the GDPR. However, the GDPR itself only sets out the basic requirements of a DPIA, which may give rise to varying interpretations by the DPOs. Due to these varying interpretations, together with national Data Protection Authorities (NDPAs) having different or lacking action items, the GDPR cannot guarantee that companies all over the Member States will treat the same data risks in the same way. This situation weakens the harmonisation goal of the GDPR.

Contents

List of Figures

List of tables

List of abbreviations (A-Z)

A29WP	Article 29 Data Protection Working Party
CBPL	Commissie voor de Bescherming van de Persoonlijke Levenssfeer
CCTV	Closed Circuit Television System
Closed Circuit Television System	Chief Information Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNIL	Commission Nationale de l'Informatique et des Libertés
d.pia.lab	Brussels Laboratory for Data Protection & Privacy Impact Assessments
DIA	Data, Internet of things & Artificial Intelligence
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSGVO	Datenschutz-Grundverordnung
DSR	Design Science Research
DSRM	Design Science Research Methodology
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Cyber Security
EU	European Union
GBA	Gegevensbeschermingsautoriteit
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
ICT	Information and Communication Technology
ISIC	International Standard Industrial Classification of all economic activities
ISO	International Organisation for Standardization
ISMS	Information Security Management System
ISR	Information System Research
ISRM	Information Security Risk Management
IT	Information Technology
NDPA	National Data Protection Authority
NDPAs	National Data Protection Authorities
PDCA	Plan Do Check Act
PIA	Privacy Impact Assessment
PIAF	Privacy Impact Assessment Framework
PRIPARE	Preparing Industry to Privacy-by-design by supporting its Application in Research
RGPD	Règlement Général sur la Protection des Données
SA	Supervisory Authority
SME	Small and Medium sized Enterprises
TFEU	Treaty on the Functioning of the European Union
WP29	Working Party Article 29

1. Introduction

This chapter introduces the topic of this thesis. The general context of the GDPR and the DPIA is elaborated in section 1.1. Section 1.2 explores the research topic. Sections 1.3. and 1.4 explicate the motivation and relevance of this research project as well as the problem statement. Section 1.5 formulates the central research question, and section 1.6 explains how the research was carried out. Finally, section 1.7 provides some supplementary reading guidelines.

1.1. General context of the topic

The emergence of the TCP/IP Internet Protocol in 1973 has led to a medium for fast information exchange between individuals' computers and private and public institutions regardless of geographic location. In 1995, only 1% of the world's population used the internet, and there were limited cloud computing, smart phones and social media (Tankard, 2016). Today, the situation is completely different. Using the internet has become a daily activity for 87% of the Belgian population, 73% have a smartphone and 62% check their social media daily (Statbel, 2018). This trend is also visible in the professional domain. All employees working in a modern enterprise are included in a wide range of databases recording personal and sensitive data (such as religion and health-related information), with most of these data being processed automatically.

However, there was also a dark side to this evolution. Due to that increased connectivity, stored data became increasingly vulnerable to cyber-attacks as well as to losses and thefts. These vulnerabilities can lead to severe information security incidents. According to Doherty Associates (2018), the four most famous data breach examples are the following: First, a 2017 data breach of the payday loan company Wonga occurred due to a lack of internal security and compromised the bank details of 250,000 customers. Second, the data breach of the supermarket chain Morrison's occurred due to an internal attack and led to 100,000 employees' personal details being leaked. Third, a thief breached the data of the Brighton and Sussex University Hospital and accessed the sensitive data of patients by stealing hard drives that were supposed to have been destroyed. Finally, a data breach occurred of the social media platform LinkedIn, whereby the personal information of 165 million user accounts was compromised due to weak user passwords and a failure on LinkedIn's part to encrypt its data.

The significant examples above show that there has been a major increase in data processing activities and data security risks. On the one hand, it is common knowledge that an information system security alone is not enough and that managers must achieve a certain level of information security awareness in order to keep their company information secure. On the other hand, more than 80% of the individuals wants to know who has access to their data and expects that governments protect them with privacy legislation (Fujitsu, 2010).

At the European level, this privacy legislation has been put in place by the European Commission by means of the GDPR. The GDPR was adopted on 27 April, 2016, by the European Parliament and became applicable on 28 May, 2018. This regulation repealed the former EU Data Protection Directive 95/46/EC, which had existed for more than 20 years. The goal of the new regulation is '*to ensure a coherent application of data protection rules, taking into account the impact of new*

technologies on individuals' rights and freedoms' (European Commission, 2010). It gives power to individuals and protects their rights.[3]

For the moment, the media are fully covering the GDPR. In May, 2017, Gartner (2017) predicted that by the end of 2018, more than 50% of companies affected by the GDPR would not be in full compliance with its requirements. In March, 2019, (i.e. only a few weeks away of the first anniversary of the GDPR), IAPP (2019) still estimated this percentage at 50%, and expressed an increased need data protection strategy.

One of the principal articles of the GDPR is Article 35, which imposes a DPIA. In this regard, the concept of a privacy impact assessment (PIA) emerged during the 1980s and has become more common since then. In the EU, a DPIA became mandatory due to the introduction of the GDPR. Article 35 of the GDPR prescribes the execution of a DPIA before any processing activity that may pose a "high risk" to the rights and freedoms of individuals. This requirement is one of the key points to tackle in preparing an organisation for GDPR compliance (Barker, 2017). However, there are no official guidelines for conducting a DPIA. On a European level, the EU advisory body 'Working Party 29' has proposed some guidelines, but these are not obligatory. In the Member States, each NDPA[4] (e.g. the former Privacy Commission of Belgium) can give its own guidance and establish its own national lists which mention when a DPIA is mandatory or not necessary. In this context of uncertainties and unclear directives, DPOs must assume responsibility and advise the highest management of the organisation if an impact assessment should be conducted on the basis of the scale and the nature of the processing activities.

In light of that central role of DPOs, this research study focussed on them. The object was to study their perceptions regarding the GDPR and the execution of a DPIA. This was done by interviewing DPOs within large companies. As a first step, a 'DPIA of reference' was chosen based on results obtained from a literature review. Second, the retained DPIA was used as a reference for the interviews with some DPOs in order to find out how they perceive the harmonisation goal of the GDPR. However, it was out of the scope of this paper to conduct a practical evaluation of a DPIA by testing it on applications used within the concerned enterprises in order to verify its effectiveness and efficiency.

1.2. Exploration of the topic

With the new GDPR, the EU aims to establish legislation capable of dealing with current and future technological trends. Furthermore, the EU also seeks to harmonise the different national privacy laws. That is why the new European privacy legislation has the form of a regulation (which is directly applicable) instead of a directive (which needs a national implementation law, as was the case with the former EU Data Protection Directive). Because of the different national implementation laws, there was inharmonious implementation of that directive. However, although a regulation should lead to greater consistency in implementation, the implementation of the GDPR is not unequivocal,

[3] These rights are set down in article 12 to 22 and are dealing with the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, rights in relation to automated decision making and profiling.

[4] Writing convention: In this paper, data protection authorities and supervisory authority are used interchangeably and refer to the same organisation.
Supervisory authority is defined under article 4(21) of the GDPR as '*an independent public authority which is established by a Member State pursuant to Article 51*'.

as it can have different effects for different sectors and different sizes of companies (Tikkinen-Piri, Rohunen, & Markkula, 2018).

In the light of the modernisation goal, the GDPR introduces the concept of a DPIA. Article 35 specifies the conditions and some requirements concerning this assessment. However, the GDPR does not provide an accurate definition of a DPIA.

1.3. Motivation and relevance

1.3.1. Motivation

The study of the impact of the DPOs' perception on conducting a DPIA and on the harmonisation goal of the GDPR is motivated by the following:

In general, there is the impact of the new privacy legislation. First, as the GDPR came into force in May, 2018, it is a new focus point. As a result, experience with the regulation is lacking, and detailed guidance and advice on specific aspects of the GDPR are difficult to obtain. This lack may give rise to difficulties in applying the rules imposed by the GPDR in practical situations. Non-compliance with the GDPR may not only have legal consequences (e.g. substantial fines of up to 4% of a company's annual global turnover, or up to €20 million[5]) but may also result in a loss of customers or partners' trust. So, clarification of when the GDPR applies in practice is needed. Second, privacy is crucial in this quickly developing digital world, and protecting privacy concerns everyone of us in our daily private and professional life. In this regard, organisations process both client data (in their commercial role) and employee data (in the context of their employer-employee relationship). Third, as the GDPR is compulsory, it poses new obligations for all organisations (both governmental and private sector) regarding handling personal data.

In concrete, there is the requirement for conducting a DPIA. Article 35 of the GDPR prescribes the execution of a DPIA before any processing activity that may pose a 'high risk' to the rights and freedoms of individuals. This requirement is one of the key points to tackle in preparing an organisation for GDPR compliance (Barker, 2017).

There have been some empirical studies addressing the implementation of the privacy and data protection legislations. First, Batty, Glozier and Holland-Elliott (2009) audited '*the understanding and practice of UK occupational physicians to see if a consensus view existed*' in relation to the 'Access to Medical Reports' (1998) and the 'Data Protection Act' (1998), the latter being UK's implementation law of the former EU Data Protection Directive. This study was focused on the British health sector and on the former EU legislation. Further, Hochepied (2018) conducted qualitative research on the impact of the implementation of the GDPR in hospitals in the Belgian province of West Flanders, and Willaert (2018) focussed on the impact of the GDPR on the Belgian financial sector. Both studies treated the GDPR, but they focussed on specific Belgian business sectors. Mikkonen (2014) analysed '*the awareness and the willingness to act towards compliance regarding the proposed GDPR in Finland in 2013*.'

None of these past studies, though, has examined the perception of the DPOs on conducting a DPIA and on the harmonisation aim of the GDPR.

[5] GDPR Art 83(5)

1.3.2. Relevance

This research paper is relevant for a number of reasons. First, it contributes to closing the important knowledge gap regarding the GPDR by addressing insights in how the DPIA is interpreted and conducted by DPOs. Second, it provides a 'DPIA of reference' fulfilling all GDPR requirements, and which could be used by all DPOs. Third, it sheds some light on how diverging insights of DPOs result in different approaches to conducting the DPIA. Finally, the diverging perspectives and understandings of the practicing DPOs can help the EU in improving the defined guidelines and in making the necessary enhancements to ensure 'harmonised' data protection.

1.4. Problem statement

The goals of the GDPR are to address the new privacy threats and to align the different national privacy legislations.

In light of those goals, the GPDR imposes to conduct a DPIA when certain conditions are met. However, DPOs have the flexibility to use different approaches. Therefore, it is important to understand how DPOs perceive the purpose and process of the DPIA because they determine when and how DPIAs are conducted. Consequently, DPOs' actual attitude towards the DPIA can predict the success of the harmonisation goal of the GDPR.

1.5. Central research question

In the light of the problem statement explained above, there are two objectives in this research.

The first objective is rooted in a theoretical study on the context under which a DPIA should be conducted and on the harmonisation goal of the GDPR

> **Objective 1**: What are the requirements for conducting a DPIA within the current framework of the GDPR and what is its harmonisation goal?

The second objective focusses on the practical views and opinions of DPOs towards DPIAs and what light these opinions shed on the harmonisation goal of the GDPR.

> **Objective 2**: How do DPOs experience the harmonisation goal of the GDPR from the point of view of the DPIA?

Based on the problem statement and the objectives, the central research question which should be answered is as follows:

> **Central research question***:* What is the DPO's perception on the conduction of a DPIA, and how does he see the harmonisation goal of the GDPR through this DPIA-lens?

1.6. Main lines of approach

In order to answer the central research question, the research was divided into two parts, and the central research question was divided into sub-questions which were answered.

1.6.1. The research consists of two parts

The research was divided into two parts, with each part reflecting one of the two objectives.

The first part is linked to the first objective and involved a literature study (normative research) on the general context of the GDPR, the harmonisation goal of the GDPR and the conditions for conducting a DPIA. Additionally, a DPIA was found which reflects all requirements imposed by the GDPR, and it was thus selected as a reference for the interviews during the empirical research. The results of the literature study were further used to generate some interview questions for the empirical part.

The literature study was followed by an empirical research study (using a qualitative approach) which is linked to the second objective. During this second part, the results of the literature review were used as a starting point to evaluate the perception of DPOs of the DPIA by interviewing some DPOs of inventoried Belgian organisations. The interview was primary focused on investigating how DPOs interpret and implement the directives for conducting a DPIA. As a secondary issue, it was evaluated how DPOs experience the harmonisation goal of the GDPR from the point of view of the DPIA. The results gathered via the interviews were analysed and evaluated in order to draw conclusions and to answer the main research question.

Figure 1.1 summarizes the main lines of approach conducted to carry out this research.

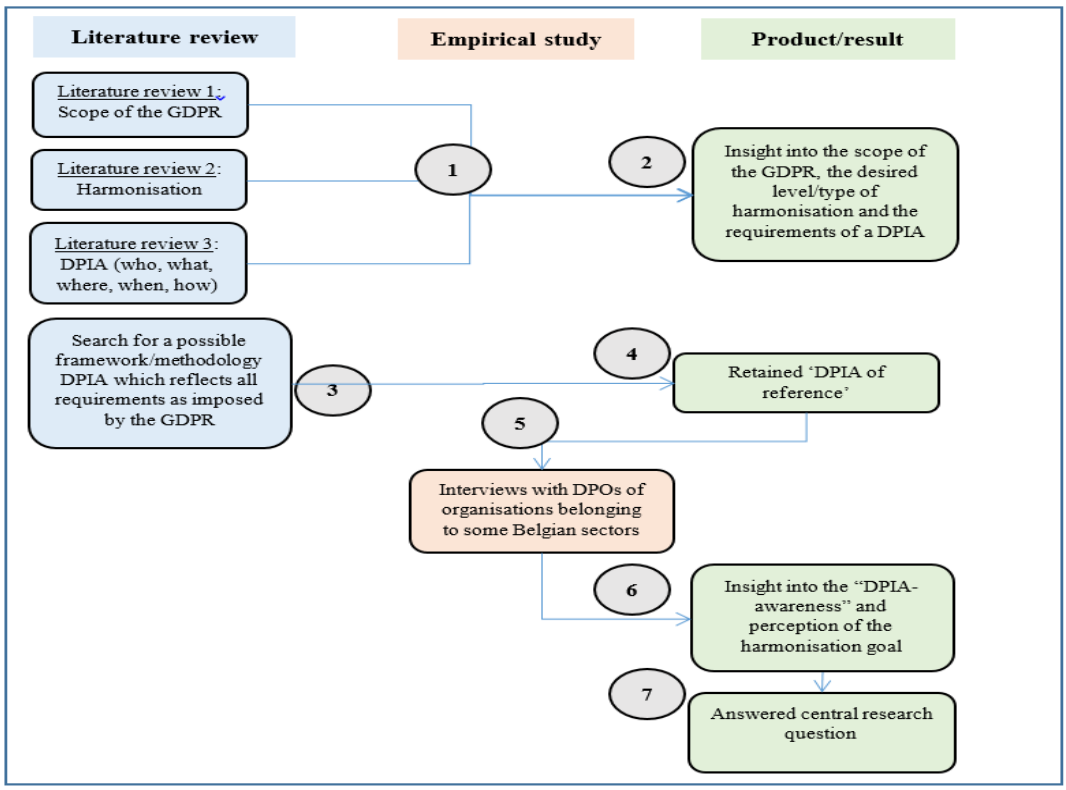


Figure 1.1
Main Lines of Approach

1.6.2. Sub-questions

In order to answer the central research question, it was used to develop nine sub-questions (SQs). Each sub-question aims at different aspects of the main question, thus enabling the main question to be answered. During the literature review, the research sub-questions listed below in Table 1.1 were the focus.

Table 1.1
Literature Review: The Sub-Questions and their Corresponding Objectives

	Sub-questions	Objective
GDPR		
SQ1	What are the main principles of the GDPR?	Gaining insight into the GDPR (description, impact, legal framework on a European and national level).
Harmonisation		
SQ2	What is harmonisation?	Finding a good definition/description of harmonisation. Gaining insight into the determining factors of harmonisation: factors favouring harmonisation and factors negatively affecting harmonisation.
SQ3	What are the main factors that affect the harmonisation goal of the GDPR?	
DPIA		
SQ4	What is a DPIA?	Finding a good definition/description of a DPIA. Gaining insight into (the requirements of) a DPIA: practical guidelines for conducting a DPIA in conformity with the directives of the GDPR and other directives: "Why", "When", "Where", "How" "Who", "What". Can a 'DPIA of reference' be identified in order to streamline the interview with the DPOs?
SQ5	What are the most important requirements in the context of the execution of a DPIA, as required by the GDPR?	

The literature review was followed by an empirical study by means of interviews and based on a retained 'DPIA of reference'. Hereby the focus was on how the DPOs perceived the DPIA. During this phase, the research sub-questions were as follows:

Table 1.2
Empirical Research: The Sub-Questions and their Corresponding Objectives

	Sub-questions	Objective
DPIA		
SQ6	What are DPOs' current practices and views on the GDPR/DPIA?	Gaining insight into the following: • Lessons learned concerning executed DPIAs? • What makes a good DPIA?
Harmonisation		
SQ7	How is the harmonisation goal of the GDPR seen through the lens of the DPIA?	Gaining insight into how DPOs experience the harmonisation in the context of conducting a DPIA.

1.7. Reading guide

This paper contains five chapters and 10 appendixes, and it is structured as follows:

Chapter 2 presents the literature review, which focusses on three parts: the GDPR, the harmonisation goal of the GDPR and the DPIA. In the third chapter, the methodology (i.e. conceptual design) is presented. This chapter explains the techniques used to gather and analyse the data. Chapter 4 sets out the analysis of the interview results and reflects on validity, reliability and ethical aspects. Chapter 5 concludes this thesis, discusses the obtained results and makes some recommendations related to the DPIA and future research.

2. Theoretical framework

This chapter describes how the literature review was conducted and how this resulted in the theoretical framework. Figure 1.1 in section 1.6 situates the literature review in the context of the overall research. The overall aim of this literature review was a detailed analysis of the literature in order to gain information regarding the GDPR, the harmonisation goal and the DPIA.

2.1. Research approach

Although snowballing is a common research approach for a literature review, this method was only appropriate for the harmonisation aspect, where the studied literature consisted of scientific articles. For an overall picture of the GPDR and the impact of article 35 (DPIA), the focus was on important official documents linked directly to the GDPR legislation and this based on the relationship between the EU and official authorities.

2.2. Implementation

The criteria used for executing the literature review can be found in Appendix C.

Based on the search results, the following legislation, official documents and overview articles were the most important documents considered in this review.

Table 2.1
Most Important Documents for Literature Review

Topic	Main reference
GDPR	• The GDPR legislation is the basis for this paper and consists of 11 chapters and 99 articles. It aims, among other things, at harmonizing the national privacy legislations. • The Recitals associated with each of the GDPR articles as they help to better understand the respective article.
Harmonisation	In the paper '*The Meaning of Harmonisation in the Context of European Community Law – a process in need of definitions*' (Lohse, 2012), the author gives a definition of harmonisation resulting from an evaluation of six 'defining' characteristics.
DPIA	• The deliverable '*Recommendations for a privacy impact assessment framework for the European Union*' (PIAF, 2012) makes recommendations with regard to policy-making and PIAs. • The deliverable '*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679*' (Article 29 Data Protection Working Party, 2017) explains article 35. It also issues guidelines on impact assessments. • The '*Recommandations d'initiative concernant l'analyse d'impact relative à la protections des données et la consultation préalable*' (Commission de la protection de la vie privée, 2018) by the Belgian Privacy Commission provides guidance on the essential elements and requirements of a DPIA.
Methodology for conducting design science research	In the paper '*A design science research methodology for information systems research'*, Peffers, Tuunanen, Rothenberger and Chatterjee (2007) present a methodology for design science research in information systems.

The whole list with references can be found at the end of this paper.

2.3. Results

2.3.1. The context of the GDPR

The GDPR is a European regulation

On 25 May, 2018,[6] the new EU GDPR repealed the Data Protection Directive 95/46/EC, which was the very first statutory regulation in the field of data protection. As a result, the GDPR became the main data protection legal framework in the EU.

Both the EU regulation and the EU directive are legislative acts which are handed down by the EU and which apply to all member states; however, they differ in binding force (European Commission, 2017). A **directive** sets out concrete objectives that must be achieved by an imposed date, but it permits individual member states to decide how to do so (incorporate their own additional features). In this respect, national authorities must transpose the directive into their national legislation, which can create differences between national implementation laws. In contrast, a **regulation** is applicable entirely and directly by all Member States without transposition into national legislation.[7] As a result, the Member States do not have the opportunity to depart from it through their national transposing legislation. However, they can create supplementary laws in order to impose additional and more rigorous requirements than those set by the regulation.

The prior directive aimed to harmonize potential disparities which might have occurred because no domestic legislation with regard to data protection existed in all Member States (Van Hoecke & Dhont, 1999). However, due to the nature of the former Directive (explained above), the harmonisation fell well short of what the EU desired. By setting a more detailed set of rules which apply to all EU Member States and by replacing the directive with a regulation, the implementation of the EU regulation within the Member States would be more tightly constrained.

The main purposes for enacting the EU GDPR were the following: First it was meant to enhance harmonisation between, or to bring more conformity to, the 28 existing but diverging data protection laws by setting a minimum 'Euro-standard' below which the Member States may not fall. Second, it established a data protection legislation which was better adapted to the current privacy concerns of the new digital age.[8]

[6] GDPR Article 99
[7] As prescribed by Article 288(2) TFEU
[8] The whole text of the GDPR can be found at http://eur-lex.europa.eu/eli/reg/2016/679/oj.

Specific terminology with regard to DPIA

Specific terminology of the GDPR can be found in the articles of the GDPR itself and in the recitals, which give further explanations about the articles.

In the context of this paper, two articles need some special attention.

First, article 4 contains various definitions. The most important key terms of the GDPR in the context of the DPIA are listed below:

- **Personal data** is '*any information relating to an identified or identifiable natural person ('data subject')'*. A natural person is said to be **identifiable** when he or she *'can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*.'[9]
- **Processing of personal data** is defined as '*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*.'[10]

Second, article 35, treats the obligations to carry out a DPIA in certain circumstances. Article 35 is reproduced in its entirety in Appendix B.

Besides the GDPR articles themselves, the recitals associated with each of the articles are also important as they help in understanding how the regulation will be interpreted by the NDPAs and as they contain important details missing in article 35.[11] The procedures and the rules involved in conducting a DPIA are clarified in recitals 84 (Risk evaluation and impact assessment), 90 (DPIA), 91 (Necessity of a DPIA), 92 (Broader DPIA) and 93 (DPIA at Authorities).

Unfortunately, neither the GDPR nor the recitals give a definition of a DPIA. According to A29WP, a **DPIA** is '*a process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data (by assessing them and determining the measures to address them)*', with **risk** being defined by as '*a scenario describing an event and its consequences, estimated in terms of severity*[12] *and likelihood*'[13] and related to the protection of personal data.

[9] GDPR Article 4(1)
[10] GDPR Article 4(2)
[11] All the recitals can be found at https://gdpr-info.eu/recitals/
[12] The following levels of likelihood/probability can be identified: negligible (= very unlikely that the threat could occur, e.g. once in a decade or less), limited (= unlikely that the threat could occur), significant (= possible that the threat could occur), maximum (= high probability that the threat could occur).
[13] The following levels of severity/impact/consequence can be identified: negligible (= no effect on data subject or only minor annoyance, e.g. waste of time), limited (= limited inconvenience that data subjects may easily overcome, e.g. extra costs, loss of service, fear, serious stress,…), significant (= significant problems that data subjects may still overcome, e.g. consequences of identity theft, loss of employment, blacklisting, …..) and maximum (= major consequences that may be irreversible or that data subjects cannot overcome, e.g. Long-term illness, inability to work, irreversible blacklisting, large scale data breach,….).

2.3.2. Harmonisation principles

Harmonisation in the context of the EU

Many definitions of **harmonisation** can be found, but a basic definition is '*a process of combination or adaptation of parts, elements or related things, so as to from a consistent and orderly whole*' (IAPP, 2018).

Within the European Union, there is a lack of a qualitative and concise definition of harmonisation established. Therefore, the definition of Lohse (2012) has been retained, stating that **harmonisation** is '*a conscious process that has the aim to lead to the insertion of a concept into the national legal orders, which triggers a process of adaptation to form a European concept as uniform as required to serve the objectives of the European Union*'. The latter definition is the result of an evaluation of six 'defining' characteristics:

- *the conscious creation of a common **Euro-standard** for political, social, economic and environmental issues which have been transferred to the European level by the Member States and whereby that standard is intended to adapt the national law in the Member States or to replace a pre-existing legal concept;*
- *the **contribution by the Member States** at three stages in the legislation, being the setting of the European standard to be harmonised (by the European legislator), the active insertion of the European concept into the national legal order (by the national legislators) and a common interpretation and application of the European concept (by the national courts);*
- ***actors involved**, being on the one hand the higher authorities (e.g. the European Commission, the European Council and European Court of Justice) and on the other hand the national actors (e.g. the Member States and their national courts);*
- ***objectives** (why harmonise?), being the elimination of existing disparities between national laws, resulting in a unified European law in order to pursue the common policy goals of the European Union;*
- ***object to be harmonised** and standard, being a law itself (the rules) and the legal practice of that law (by courts, administrative bodies, etc.);*
- ***intended result**, being a law as uniform as needed.*

Harmonisation can be achieved through several forms/mechanisms. One possible classification is the intensity of harmonisation (Kurcz, 2001) – in other words, the residual competencies left to the Member States to derogate from the imposed harmonised rules by enacting more stringent rules (i.e. setting a higher standard) on the one hand or maintaining lower standards on the other hand.

The following intensities of harmonisation can be distinguished:

- total[14]
- optional[15]
- partial[16]
- alternative[17]
- minimum[18]

[14] Total harmonisation is harmonisation whereby the Member States must ensure that everything works exactly as required at Community level without leaving them any discretion in the implementation of the harmonisation measures, unless the directive expressly permits

[15] Optional harmonisation is harmonisation whereby there exist two set of rules, one for the national territory and one for the European territory

[16] Partial harmonisation is harmonisation whereby only some aspects of the domain are treated

[17] Alternatieve harmonisation is harmonisation whereby the Member States can choose between different possible solutions provided by the EC law

Harmonisation in the context of the GDPR

As no concise definition for harmonisation in the context of GDPR was found during the literature review, an own definition of harmonisation has been established by rephrasing the above-mentioned six criteria of Lohse (2012).

Harmonisation in the context of the GDPR can be defined as:

> *The adoption of a new European privacy legislation*
> - *with the help of a directly applicable regulation (GDPR) according to Art 249(2) EC and*
> - *with the contribution of all actors involved – with an important role for the European Data Protection Board (EDPB) (which replaced the A29WP), Member States and the NDPAs*
>
> *in order*
> - *to bring the former divergent national privacy legislations (based on the EU Data Protection Directive 95/46/EC) into more conformity and*
> - *to adapt the former European legislation to current privacy issues.*

In light of these definition, the following elements influence the harmonisation goal of the GDPR.

On the one hand, the GDPR imposes harmonisation by the following 'converting' mechanisms:

- First, the new privacy legislation takes the form of a regulation.
- Second, the EDPB can issue mechanisms, guidelines, recommendations and best practices in order to ensure a consistent application of the GDPR.[19] In this regard, the EDPB replaced the A29WP since the GDPR came into force.

On the other hand, the purpose of harmonisation can be undermined by a considerable degree of 'divergence' in the application of the GDPR:

- First, there are varying degrees of legislative freedom of the Member States (Steiner and Woods, 2014):
  - First, Member States are permitted, but not obliged, to maintain higher standards than the minimum requirements.
  - Second, Member States are allowed, but not obliged, to implement the optional provisions which allows them to enact their own rules for certain subject matters.

  For example, the German, Lithuanian, Luxembourg and UK implementation law provide some specific provisions related to the DPIA, while the other Member States do not (IAPP, 2018).
- Second, there are the varying guidelines imposed by the NDPAs in order to become GDPR-compliant.
  For example, the Belgian DPA has an action plan consisting of 13 steps in order to prepare for the GDPR (Step 10 treats the DPIA), while the French and Dutch action plans consist of 6 steps and 10 steps (respectively); in both action plans, step 4 treats the DPIA. The Latvian Data State Inspectorate refers to the UK ICO's 12-step action plan (Step 10 treats the DPIA).

[18] Minimum harmonisation is harmonisation whereby the EC law establishes the minimum rules with which all Member States must comply and the Member States are entitled to impose more stringent requirements, if they wish to do so

[19] GDPR Article 70(1)(e)

The GDPR aims for minimum harmonisation by actively introducing a common legal standard with minimum clauses. These minimum clauses are indicated explicitly[20] in the preamble and in several articles and recitals (with expressions like “shall”, “may”, “margin of manoeuvre”, and “at least”). Those articles related to DPIA can be found in Appendix D.

2.3.3. Data Protection Impact Analysis

The EU has already introduced two voluntary PIA policies: the first in 2009 for ‘radio-frequency identification’ (RFID) applications and the second in 2012 for ‘smart grids’ (Kloza, Van Dijk, Gellert, Borocz, Tanas, Mantovani & Quinn, 2017). The DPIA (2018) is a mandatory policy in the area of personal data protection.

2.3.3.1. Requirements for conducting a DPIA

The DPIA is addressed in article 35 of the GDPR, which is titled ‘Data protection impact assessment’ and which lists some guidelines concerning conducting a DPIA.

The particular characteristics of personal data and the impact of the GDPR lead to specificities which have to be taken into account when conducting a DPIA. Some of these specificities are as follows (ENISA, 2016):

- specific data protection parameters (in particular, the nature, scope, context and purposes of the processing) need to be considered for an assessment;
- the risks must be assessed with regard to their impacts on the data subjects[21] and not for their potential impacts on the organisation and its activities;
- a risk with a low likelihood of occurring but with a high potential impact on particular individuals should be addressed and not simply accepted. This approach is contrary to a classical risk assessment.

In order to gain a clear view of the context of the DPIA within the GDPR, it is essential to point out the requirements imposed on conducting a DPIA. This information was gathered by answering six questions that relate to these requirements:

- Why should a DPIA be conducted?
- When is it obligatory to conduct a DPIA?
- How should a DPIA be conducted?
- Who is involved in a DPIA process?
- What are the required constitutive elements of a DPIA?
- Can a ‘DPIA of reference’ be identified in order to streamline the interviews?

The answer to each question was approached in the same way. First, the GDPR legislation was taken into account. Thereafter, because the requirements described in article 35 are rather general and loose (and consequently subject to interpretation), some further clarifications, interpretations and guidance are provided by the means of the recitals related to the GDPR, the recommendations

[20] Explicit minimum clauses are clauses which are made clear and stated plainly (while implicit minimum clauses are clauses which are implied but not stated directly).
[21] Article 35(1) GDPR

of the A29WP[22] (Article 29 Data Protection Working Party, 2017) and the Belgian Commission for the protection of privacy[23] (Commission de la protection de la vie privée, 2018).

Reasons for conducting a DPIA

The GDPR accountability principle[24] requires that an organisation that is responsible for personal data must be able to demonstrate that privacy and data protection principles are taken seriously. One way to do so is to put into place appropriate measures – for example, by conducting a DPIA. In this regard, the DPIA can function as an early warning system, identifying previously undetected risks that could lead to breaches of the GDPR and managing those risks in a cost-effective way. Failing to conduct a DPIA when required,[25] conducting a DPIA which is not in accordance with the prescriptions[26] or omitting to contact the NDPA in the cases as imposed by the GDPR[27] may result in the imposition of major penalties. For example, the administrative sanction can be '*up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher*'.[28]

While the recitals remain silent on the reasons for conducting a DPIA, the A29WP stipulates that publishing a DPIA report could demonstrate accountability[29] and transparency and thus foster trust of the data subjects in the processing operations of the controller.

The Belgian Privacy Commission states that the obligatory conduction of a DPIA in certain circumstances should be seen in light of two of the three central principles of the GDPR[30]: the above-mentioned principle of accountability and the risk-based approach. The risk-based approach requires that the implemented risk-mitigation measures must correspond to the level of the identified risks: the higher the identified risks for the rights and freedoms of the data subjects,[31] the more stringent the actions which have to be taken in order to manage those risks.

Conditions and moment for conducting a DPIA

Determining when a DPIA is obligatory has two components: the conditions under which and the moment when a DPIA must be conducted.

Concerning the conditions, the GDPR provides some minimum guidelines regarding when a DPIA is mandatory. First, it is mandatory when the processing activity '*is likely to result in a high risk to the rights and freedoms of natural persons*'.[32] Although the threshold of '*high risk*' serves as the trigger for the obligation to conduct a DPIA, the GDPR remains silent on what may be understood by '*likely*

[22] Upon enactment of the GDPR, the « Article 29 Working Party » has been replaced by the « European Data Protection Board ».
[23] Is better known as « Belgian Privacy Commission ». In the context of the introduction of the GDPR, the « Belgian Commission for the protection of privacy » has been transformed to «Belgian Data Protection Authority »
[24] GDPR Article 5(2)
[25] GDPR Article 35(1), 35(3) and 35(4)
[26] GDPR Article 35(2), 35(7), 38(8) or 35(9)
[27] GDPR article 36(3)(e)
[28] GDPR Article 83(6)
[29] GDPR Article 5(2)
[30] The three key principles are : accountability, a risk-based approach and data protection by design and by default.
[31] GDPR article 24(1)
[32] GDPR article 35(1)

to result in a high risk'. Because of that silence, the GDPR gives some examples of processing activities which are considered to result in a high risk (and thus triggering a DPIA)[33]: systematic and extensive profiling with significant effects, large-scale use of sensitive data and public monitoring. Furthermore, the GDPR provides some criteria in terms of processing, type of data and consequences for the data subjects.[34]

As with most laws, the GDPR also enumerates the activities which fall outside its scope[35] and for which a DPIA is not mandatory.[36] This is the case 1) when processing is on the basis of a legal obligation or a public task, 2) when a substantially similar DPIA has already been done and 3) when the processing operation appears on the white list of the NDPA (which contains processing activities that are exempt from a DPIA under certain condition).

Based on the outcome of the DPIA, it might be necessary for some technical and organisational measures to be taken in order to protect the rights and freedoms of the persons concerned. When these measures are insufficient to reduce the identified risks to an acceptable level, the residual risks remain high (i.e. not all risks can be mitigated), and a preliminary opinion of the NDPA is mandatory.[37]

This is summarised in Figure 2.1 below:

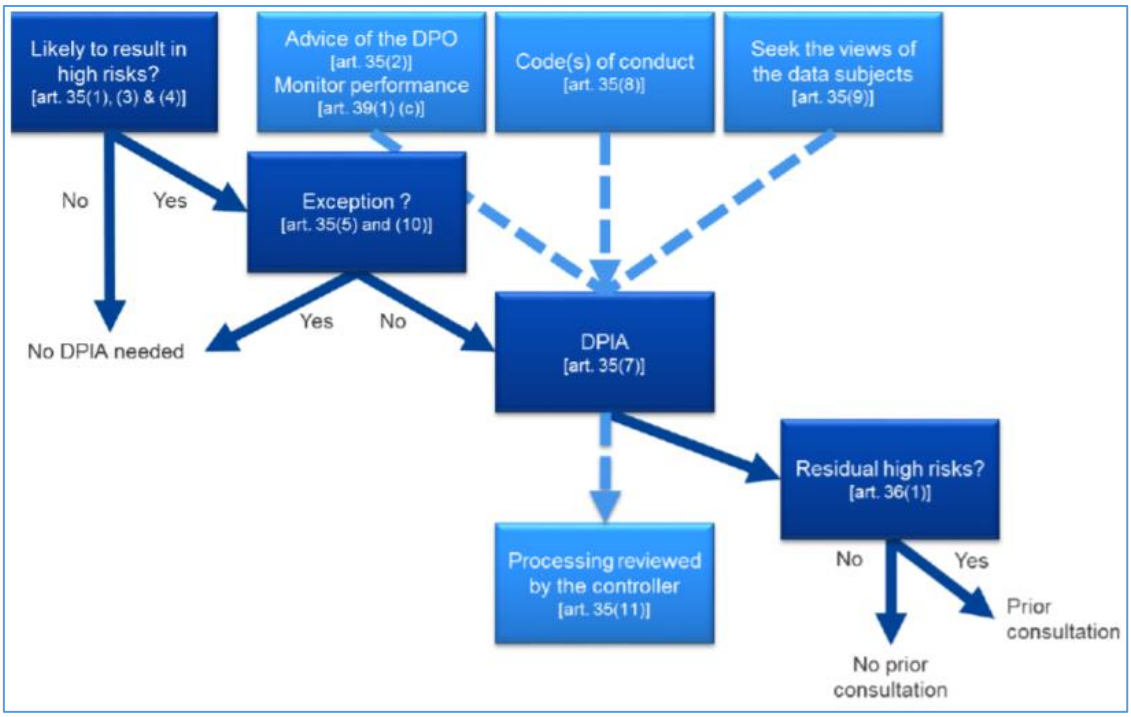


Figure 2.1
Core principles related to the DPIA in the GDPR

Source: Article 29 Data Protection Working Party (2017)

[33] GDPR Article 35(3)
[34] GDPR article 35(3)
[35] GDPR Article 2(2)
[36] GDPR Article 35(10)
[37] GPDR Article 36(1) and recitals 94-96

Recital 91 of the GDPR further explains when a GDPR is mandatory in the context of large-scale processing operations.

The A29WP interprets the list of the GDPR (with processing activities triggering a DPIA) as non-exhaustive[38] and enumerates nine criteria that should be considered when determining whether the processing of personal data raises the level of risk[39]: evaluation or scoring;[40] automated decision-making with legal or similar significant effect;[41] systematic monitoring;[42] sensitive data or data of a highly personal nature;[43] data processed on a large scale;[44] matching or combining datasets; data concerning vulnerable data subjects, such as children, employees, mentally ill persons or medical patients; use of new technologies;[45] and preventing '*data subjects from exercising a right or using a service or contract*'. On the one hand, the more of the above mentioned criteria that are fulfilled, the more likely the processing operation is to present a high risk. On the other hand, a processing operation categorised under one of those cases can still be considered by the data controller as not presenting a high risk (and so not requiring a DPIA), but this determination would have to be justified.

Contrary to the GPDR, the A29WP does give some examples of cases of high residual risk, such as illegitimate access to data leading to financial peril or even a threat to the life of the data subjects. Furthermore, the A29WP also stipulates that '*a single DPIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks'*.

For the Belgian Privacy Commission, a high-risk processing activity, '*in the absence of adequate safeguards, is likely to have significant adverse consequences for the rights and freedoms of natural persons*'. The Belgian Privacy Commission refers to the nine criteria set out in the guidelines of the A29WP. If two of these nine criteria are met, then a DPIA must be conducted. Additionally and in accordance with the prescriptions of the GDPR,[46] the Belgian Privacy Commission published on 28 February, 2018, a black-and-white list which is intended to evolve and be adapted when necessary. The black list, on the one hand, contains ten distinct processing activities that are subject to mandatory impact assessments, and it has a clear focus on sensitive data processing[47] and large scale profiling[48] of individuals.[49] The white list, on the other hand, contains processing activities

[38] As the introductory sentence of Article 35(3) GDPR stipulates: '*in particular*'
[39] GDPR Article 35(4)
[40] Is based on the GDPR Recital 71 and 91 which refer to '*aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements*'
[41] Is based on the GDPR Article 35(3)(a) which refers to '*on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person*'
[42] Is based on the GDPR Article 35(3)(c) which refers to '*a systematic monitoring of a publicly accessible area*'
[43] Is based on the Article 9 and 10 GPDR
[44] According to the WP29, the following criteria should be considered to determine whether a processing is carried out on a large scale: the number or percentage of data subjects concerned, the volume of data being processed, the duration of the processing and the geographical extent of the processing
[45] Is based on the Article 35(1) GDPR and the recitals 89 and 91
[46] *GDPR Art 35(5), Art 35(6) and the exceptions foreseen by Art 35(10).*
[47] f.e. the processing of *biometric* data[47] with the purpose to uniquely identify a person, such as facial recognition based on digital images or videos
[48] **Profiling** is defined in Article 4 as follows: '*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*'

that are exempt from a DPIA under certain conditions. The white list includes activities such as the processing of data which are necessary for the payroll of employees and general accounting purposes. Such activities can be legitimised on the basis of business interests or compliance with a legal requirement. However, this white list does not relieve the data processor of responsibility to conduct a reasonable risk assessment and risk management.

While the GDPR requires that a DPIA must only be conducted for existing processing activities when the risks change after May 25, 2018, the Belgian Privacy Commission recommends, as a best practice, also conducting a DPIA for existing processing activities if these are likely *'to result in a high risk to the rights and freedoms of natural persons'*.

Concerning the moment when a DPIA should be conducted, this should be as soon as possible in the lifecycle of the project and '*prior to the processing*'[50] of personal data, which means already during the development phase of a new project. This allows the design of the project to be influenced with minimal disruption and in the most cost-effective way instead of implementing remedial actions in a later phase (or even abandoning the whole project if the privacy risks are unacceptable). Because a DPIA is a continual process and not a single task, the DPIA should be reviewed periodically throughout the life cycle of the project in order to reflect substantial changes, for example, in the used technology, in the processing operations of personal data and in the risks for the data subjects. Such review processes make it possible to verify that the processing is still compliant with the previously performed DPIA – and thus with the GDPR.[51]

Requirements for conducting a DPIA

The GDPR offers only minor indications on how a DPIA should be performed. It only stipulates that the DPIA should be performed in compliance with established codes of conduct,[52] but the methodology, the process and the template for conducting the DPIA are not described. Moreover, no relevant information is available in the recitals.

The A29WP recommends to choose one of their proposed DPIA methodologies[53] and to implement a specific DPIA in order to ensure compliance with their imposed criteria.[54]

Apart from the directives of the GDPR, the Belgian Privacy Commission is of the opinion that the DPIA should describe the methodology used to assess the risks. The commission also advocates the favouring of existing risk management methods and recommends some minimal characteristics for appropriate risk management.

---

[49] f.e. the processing of data concerning a person's behavior with the purpose to predict that person's behavior and/or preferences for marketing goals

[50] Is based on GDPR Art 35(1), 35(10) and recitals 90 and 93

[51] GPDR Article 35(11)

[52] GDPR Article 35(8)

[53] See Par 2.3.3.2 A 'DPIA of reference'.

[54] These criteria are: a systematic description of the processing is provided, necessity and proportionality are assessed, risks to the rights and freedoms of data subjects are managed and interested parties are involved.

Parties involved in a DPIA process

Concerning the roles and responsibilities for conducting a DPIA, the GDPR mentions that it controls who should carry out a DPIA when '*a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons*'.[55]

Recitals 84 and 90 read respectively as follows: *'the controller should be responsible for the carrying-out of a data protection impact assessment'* and *'a data protection impact assessment should be carried out by the controller'.*

In line with the A29WP, the data controller, together with the DPO and the data processors, is obliged to carry out a DPIA.

According to the Belgian Privacy Commission, it is undesirable that the DPO conducts a DPIA solely behind closed doors and without involving all actors[56] who have a profound knowledge and experience of security and privacy aspects. Such an solitary approach causes risks and impacts to be overlooked.

The input/feedback of all these knowledgeable actors results in a great variety of perspectives (ethical, social, legal, etc.) and can contribute to the decision if a DPIA must be conducted. However, details pertaining to the consultative process, such as how to consult the stakeholders (such as via interviews, surveys, presentations, scenario-based workshops, public hearings) is nowhere outlined.

The required constitutive elements of a DPIA

The GDPR only lists the four primary components which a DPIA must contain[57] as a minimum: 1) a description of the process and its purpose, 2) why the process is necessary,[58] 3) how it impacts a user's data privacy and 4) how the organisation addresses those risks.[59] Furthermore, a DPIA report can also be established. This can help to document the DPIA process and can contain recommendations to be implemented. The GDPR only states that the DPIA has to be provided to the NDPA.

Recital 84 clarifies the meaning and the role of the DPIA by stating that the origin, nature, particularity and severity of such risks must be assessed.

---

[55] GDPR Article 35(1)

[56] A non-exhaustive list of possible relevant actors could be: the data controller (who is accountable for conducting a DPIA), the data processor (who *should* provide assistance to *the data controller in carrying out the DPIA), t*he project managers and application developers of new applications, representatives of data subjects (who can give their view on the intended processing), Chief Information Officer (CIO) and Chief Information Security Officer (CISO), the organisation board (for formal approval and high-level support and coordination), the National Data Protection Authority (as a regulator and in particular, as an advisor in the event of a high residual risk of the data processing), independent experts (Lawyers, IT experts, Security Experts, sociologists,…),…..

[57] GDPR article 35(7)

[58] **Necessity** is defined by the European Data Protection Supervisor as the fact that '*The processing operations, the categories of data processed and the duration the data are kept shall be necessary for the purpose of the processing*'

[59] GDPR Article 32(1) stipulates some appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

A definition of a DPIA is given by the A29WP, which defines a **DPIA** as '*a process designed to describe the processing, assess its necessity and proportionality and help manage the risk to the rights and freedoms of natural persons resulting from the processing of personal data, by assessing them and determining the measures to address them*'.

The Belgian Privacy Commission requires that a DPIA report must contain, among other elements, the purposes of processing, the stakeholders, the categories and types of private data processed in the system and a characterisation of the types of data flows.

2.3.3.2. A 'DPIA of reference'

In order to have a common reference point during the interviews with the DPOs, a 'DPIA of reference' was sought. Unfortunately, neither the GDPR nor the recitals impose a particular DPIA methodology. So, during the literature study, a method for finding a good DPIA model was considered.

First, Trilateral (a non-governmental, policy-oriented forum) aimed to provide a 'best of' DPIA (Wright, Finn, & Rodrigues, 2013). To that end, it conducted a comparative state-of-the-art study of the PIA methodologies used in the six countries with most PIA methodology experience (Australia, Canada, Ireland, New Zealand, the United Kingdom, the United States) and identified the best elements that could be used to improve the DPIA.

Second, the A29WP (2017) recommends choosing one of their proposed DPIA methodologies and implementing a specific DPIA which is compliant with their imposed criteria.[60]. Among their proposed methodologies are the '*Standard Data Protection Model*' (Federal Commissioner for Data Protection and Freedom of Information, Germany), the '*Evaluación de Impacto en la Protección de Datos Personales*' (Spanish Agency for Data Protection, Spain), the '*Privacy Impact Assessment*' (Commission nationale de l'informatique et des libertés (CNIL), France) and the '*Conducting privacy impact assessments code of practice*' (Information Commissioner's Office (ICO), (UK)).

Vandendriessche (2017) enumerates some available methodologies for conducting a DPIA, including the above-mentioned CNIL and ICO.

Both the CNIL and the ICO occur on the lists of A29WP and of Vandendriessche (2017). As the CNIL is more recent and explicitly comprises the four criteria of the A29WP, the CNIL has been retained as the reference methodology for orienting the interviews.

According to this CNIL methodology (2018), the execution process of a PIA consists of four phases: 1) study of the context in which personal data is processed, 2) study of the fundamental principles (proportionality and necessity of processing, the protection of data subjects' rights), 3) study and treatment of the privacy risks associated with data security, and 4) documentation of the validation of the PIA in order to revise the previous steps when necessary.

Besides an action plan, the French CNIL also offers open source software, which allows organisations to carry out a DPIA to ensure their compliance with the WP29 requirements.[61]

[60] Those four criteria are as follows: 1) a systematic description of the processing is provided, 2) necessity and proportionality are assessed, 3) risks to the rights and freedoms of data subjects are managed and 4) interested parties are involved.

[61] https://www.cnil.fr/en/cnil-publishes-update-its-pia-guides

2.4. Conclusion

The previously discussed answers to the first six sub-questions lead into the following conclusions:

- The GDPR is the new EU privacy law which repealed the EU Data Protection Directive and which aims to update and harmonise data protection across the EU. The GDPR is a legislative requirement to conduct a DPIA (SQ1[62]).
- Due to the lack of an existing concise definition for harmonisation in the context of the GDPR, a own definition has been established for this thesis (SQ2[63]).
- The following elements influence the harmonisation goal of the GDPR (SQ3[64]):
    - positively, the GDPR in the form of a regulation and the promoting work of the EDPB and the former A29WP.
    - negatively, the legislative freedom of the Member States and the varying guidelines imposed by the NDPAs.
- The GDPR does not define the term DPIA. However, article 35 lays down the obligation to carry out a DPIA in certain circumstances and outlines general requirements for conducting a DPIA. The GDPR provides the reason for conducting such an assessment (why), a non-exhaustive list of cases in which DPIAs must be carried out (when) and the minimum information a DPIA must contain (what). However, it does not fully clarify the roles and the responsibilities of the persons involved (who) and does not prescribe the process (how) for conducting DPIAs. Thus, many questions regarding the practical implementation of the DPIA remain unanswered. In order to streamline the interviews, the DPIA of the French CNIL has been retained as a 'DPIA of reference' (SQ4[65] & SQ5[66]).

[62] SQ1: What are the main principles of the GDPR?

[63] SQ2: What is harmonisation?

[64] SQ3: What are the main factors that affect the harmonisation goal of the GDPR?

[65] SQ4: What is a DPIA?

[66] SQ5: What are the most important requirements in the context of the execution of a DPIA, as required by the GDPR?

3. Methodology

A **methodology** can be defined as '*the theory of how research should be undertaken, including the theoretical and philosophical assumptions upon which research is based and the implications of these for the method or methods adopted*' (Saunders, Lewis and Thornhill, 2016).

This chapter is mainly devoted to the justification of the conducted empirical research during which evidence was gathered to answer the empirical questions. It justifies the chosen research method as well as the choices and decisions which were made. At the end of this chapter, a reflection on the reliability, validity and ethical aspects is given.

3.1. Research methodology

Many research methodologies exist. For this thesis, the research onion was adopted, in conjunction with design science methodology. The former was used to provide a holistic overview of the research methodology as a whole, and the latter is justified in the context of the retained artefact – that is, the 'DPIA of reference'.

3.1.1. Research onion

The research onion of Saunders et al. (2016) describes the stages ('layers') through which a researcher must pass when developing an effective methodology. It was used to justify the research strategy of this thesis because of the detailed structure. The summary table below, Table 3.1, shows the retained choices for each layer:

Table 3.1
Summary of Research Methodologies and Methods/Strategies used in this Master Thesis

	Layer	Retained choice	Justification
1	Research philosophy	Pragmatic	- Starting from reality (the GDPR entering into force), this study focusses on the problems of conducting a DPIA and contributes practical solutions and outcomes concerning the (harmonised) conducting of a DPIA. - The research problem and research question tend to a pragmatic research philosophy.
2	Approach to theory development	Inductive	- There is no clearly defined harmonisation/DPIA-framework which can be used as a starting point. - A research question and objectives were defined and served as a starting point for the development of a competent level of knowledge about the GDPR, the harmonisation and the DPIA. - Data were collected using semi-structured interviews in order to discover the DPO's perception of the DPIA, including how DPOs cope with the problems experienced and how they perceive the harmonisation goal through the DPIA.
3	Methodological choice	Qualitative	Qualitative research is usually associated with interpretivism, and, to a lesser extent, with critical realism. It also relates to pragmatism and an inductive approach to theory.
4	Strategy	Case study	- A case study is tailored for a qualitative research design. - A case study is most frequently used to answer "what", "how" and "why" questions. - The case subject of the paper is the DPO's perception on the execution of a DPIA.
5	Time horizon	[N/A]	The interviews were conducted around 28 May, 2019, about one year after the GDPR became enforceable in all Member States of the EU.
6	Techniques and procedures	[N/A]	[N/A]

3.1.2. Design science research

According to Hevner et al. (2004), **design science** '*creates and evaluates IT artefacts intended to solve identified organisational problems'*. An **artefact** includes '*any designed object with an embedded solution to an understood research problem*'.

The design science research methodology (DSRM) process model of Peffers et al. (2007) is a process model consisting of six activities organised in a nominally sequential order and covering the whole research from the start (Problem identification and motivation) to the finish (Communication). It was followed in this research for three reasons. First, empirical evidence indicates that the DSRM works in practice (Cronholm & Göbel, 2016). Second, this methodology is based on and consistent with the prior work of the above-mentioned study of Hevner et al. (2004), which can be mapped roughly to this DSRM process. Third, it can be applied as a tool to formulate the overall process for conducting research concerning the perception of the DPOs on DPIAs and for determining how the DPO sees the harmonisation goal through the conduction of a DPIA.

Because the research can be addressed by developing an artefact, the entry point for this research project is the "objective-centered solution", thus starting with activity 2 (Definition of objectives of a solution).

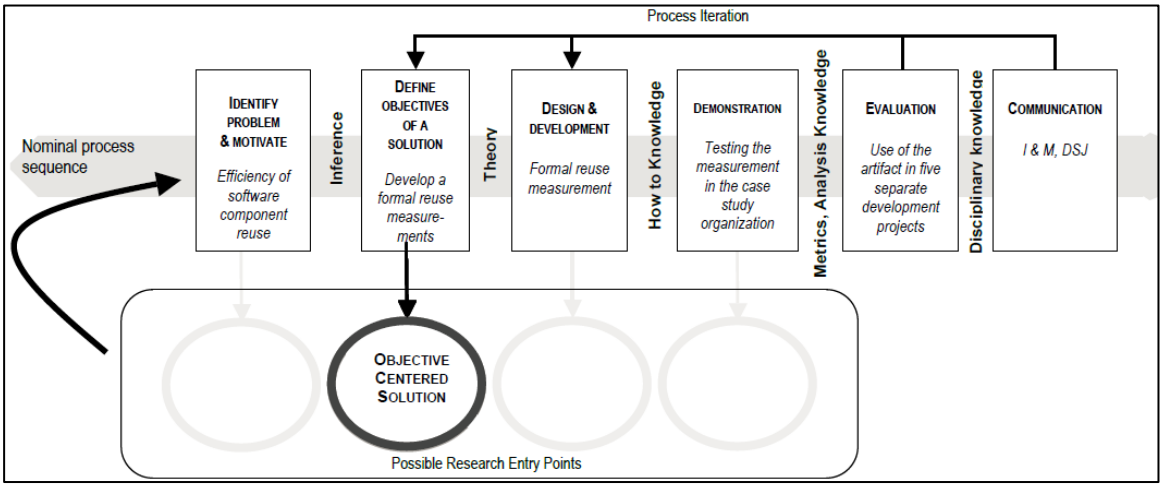


Figure 3.1
Objective-centered solution

Source: Peffers et al. (2007)

The summary table below, Table 3.2, shows how the activities were applied in this research:

Table 3.2
Activities Applied in this Research

	Activities	Application in this research	Remarks
1	Identification of the specific research problem and motivation	The new GDPR legislation aims to adapt to the new technological situation and to harmonize the national privacy legislations, leading to a better, more uniform privacy protection.	
2	Definition of the objectives for a solution	The evaluation of the perception of DPOs of the DPIA and how this perception might reflect in the harmonisation goal of the GDPR.	
3	Design and development	The main artefact is the CNIL DPIA framework.	See paragraph 2.3.3.2, A 'DPIA of reference'
4	Demonstration	After choosing the 'DPIA of reference', the artefact was used in the evaluation phase in a certain context in order study the perception of DPOs regarding the DPIA and to understand how this perception might reflect in the harmonisation goal of the GDPR. For this paper, the context is several Belgian companies for which conducting a DPIA is necessary/obligatory. As it is a 'DPIA of reference', the artefact was not adapted for use during the interviews.	
5	Evaluation	The DPOs of identified organisations were interviewed in order to go into deeper detail about their findings and their experience with the DPIA. In addition, the 'DPIA of reference' was used to compare with other DPIAs (if possible to evaluate the efficiency and effectiveness). Next, the results of the interviews were coded and compared in order to answer the central research question..	See Appendix E, Research methodologies See Appendix F, Overview of the identified sectors, Appendix G, Overview of the contacted organisations and their response, and Appendix H, Overview of the interviewed organisations.
6	Communication	The contributions are published in this paper.	See chapter 4.

A detailed elaboration of the DSRM applied to the topic of this paper can be found in Appendix E.

3.1.3. Selection of organisations and DPOs for interviews

Based on PRIPARE (2014), ENISA (2017) and Giurgiu (2017), specific sectors dealing with specific data protection operations were identified. Those sectors can be considered as having specific data protection concerns which could require a DPIA to be conducted. They are listed in Appendix F.

Due to the limited time frame reserved for the execution of this paper and due to the small response to the invitation letter for the interview, harmonisation was only evaluated with regard to eight sectors; not all sectors were covered. The eight retained sectors were retail trade, publishing activities, programming and broadcasting activities, telecommunications, financial service activities, insurance activities, management consultancy activities and public administration.

3.1.4. Data collection, data treatment and data analysis

The data collection phase consisted of two parts: a literature review and a semi-structured interview with the DPOs.

During the semi-structured interview, the DPIA and the harmonisation issues were discussed in order to explore the DPOs decisions, attitudes and opinions regarding the DPIA.

The results of the literature review and the semi-structured interviews are summarised in section 2.4 and section 4.2, respectively.

The interviews were recorded and transcribed. Due to their length, the transcribed interviews and the corresponding coding (with the respective results and conclusions) are not been retained in this paper as an appendix; however, those materials are available at the Open University as research source.

3.2. Reflection on validity, reliability and ethical aspects

The quality of empirical research depends largely on two important principles: validity and reliability. The following sections describe how these principles were pursued.

3.2.1. Validity

Validity is '*the extent to which data collection method or methods accurately measure what they were intended to measure*' (Saunders et al., 2016).

In order to pursue validity of the research design, the following principles were followed:

Validity of the interviewees

First, only 12 of the 13 interviews were evaluated – namely, those with DPOs experienced in privacy and data protection law and practices and having an adequate understanding of the DPIA.

Furthermore, those 12 DPOs were all qualified, either based on a course or on former qualifications related to privacy. Consequently, they had theoretical knowledge regarding conducting a DPIA. 11 out of 12 DPOs also had some practical experience with conducting a DPIA.

Furthermore, except for one interviewee, the function of a DPO was already somewhat established before the entry into force of the GDPR. It is mostly exercised by a person who has already held a privacy-related position in an organisation, such as a risk manager or a compliance manager. The function of such individuals has been slightly adjusted with the arrival of the GDPR to include the performance of GDPR-related tasks.

Finally, all DPOs participating in the interviews confirmed the mandatory appointment of a DPO in their organisation as their companies met the conditions under article 37 of the GPDR to designate a DPO. For most of the companies, a DPIA was required, and most DPOs reported the processing of large amounts of (sensitive) customer data. Additionally, there was also profiling in the context of personalised advertising and customer profiles. However, the latter is not considered profiling according to the GDPR, which stipulates the presence of substantial automated decision-making.

Validity of the interviews

First, although the interviews could have been held in Dutch, French, English or German, they were all conducted in Dutch, the native language of both the interviewer and the interviewee. This avoided any possible misinterpretation. Furthermore, validity was pursued by trying to explore the underlying thoughts of the interviewees. Finally, due to time constraints, the interviews were held in a short time frame (couple of weeks). This indirectly ensures that the interviews are representative as all interviewers were in the same situation (snapshot) regarding the implementation of the GDPR.

3.2.2. Reliability

Reliability refers to '*the extent to which data collection technique or techniques will yield consistent findings, similar observations would be made or conclusions reached by other researchers or there is transparency in how sense was made from raw data*' (Saunders et al., 2016).

Three points of concern must be highlighted in the context of reliability (Saunders et al., 2016).

First, the chosen interview type (semi-structured interview instead of questionnaire) had a positive and negative impact on the reliability. The reliability was affected positively by the fact that an interview gives more control over the reliability of the received data than a questionnaire; in an interview, one has more control over who answers the questions. Directly interviewing the DPO prevented another person from providing answers, as could happen in the case of a questionnaire. The potential negative effect of a semi-structured interview is that the non- standardised answers can lead to concerns about reliability. This potential problem, though, was addressed by establishing an interview protocol with short, targeted questions. Indirectly, these short questions also facilitated the coding afterwards.

Furthermore, semi-structured interviews investigating the perception of DPOs towards the GDPR/DPIAs are not intended to be repeatable since they reflect the complex reality at the time they were collected (almost one year after the GPDR came into force), a situation which is surely be subject to change. Thus, the interviews are a snapshot of the situation at a particular stage of the implementation of the GDPR, which by its nature could not be replicated by other researchers working at a later time.

Finally, although the use of personal interviews may achieve a higher response rate than using questionnaires), the response rate was rather low, which consequently had a negative impact on the reliability.

So, although reliability was pursued as much as possible, a future research could yield different results.

3.2.3. Ethical aspects

Some ethical aspects which were identified are the following. First, no cultural differences between the interviewer and the interviewees were identified. Furthermore, it was difficult to obtain consent of the contacted DPOs for an interview. However, for the DPOs who did agree to an interview, it was tried to let them feel comfortable fulfilling the interview. Hereby, a personal contact was established by assuring anonymity of the interviewed organisation and by not seeking any confidential information. In addition, the name of other participating organisations and information obtained from the other interviewees were not released.

4. Results

In this chapter, the initial aim of the study is described, followed by the results based on the interviews held with the DPOs. These results lead to the general conclusion, which is formulated in chapter 5.

4.1. Initial aim of the study

Initially, this study aimed to investigate one Belgian economic sector and to see how the DPOs of companies belonging to that sector perceive the DPIA and how the harmonisation goal might be seen through this perception. However, due to the low response rate to the invitation letter, the target of the DPOs had to be broadened to other sectors.

4.2. Results of the conducted interviews

The DPOs' answers to the questions concerning the GDPR/DPIA (SQ6[67]) yielded the following results:

All DPOs who had already conducted a DPIA reported the following:

- First, a good DPIA is '*an adapted, objective template which does not give rise to different interpretations by different actors and which results in the identification of the (most important) risks and the corresponding actions to be taken*'.
- Second, the DPOs used a personal DPIA template, whether imposed by their trade organisation or umbrella organisation, or developed by their own. These templates were mostly derived from other existing templates (e.g. CNIL) and were adapted for use within individual organisations and sectors (based on own processes, mentioning sector specific terminology,…..). Moreover, they are (constantly) adjusted based on the experiences and directives in order to have a better working version. The French CNIL DPIA was known by all interviewed DPOs, but only few had studied it thoroughly. Sometimes, they used this template as a starting point for developing their own template but the CNIIL template was not used in its original form and this for several, sometimes opposite, reasons: it is too vague, too detailed, too theoretical, not appropriate for the way of working within the organisation, it contains some imperfections (some scenarios are too small, the risks for the data subject on the moment of a data breach are not clear), it cannot be adapted to the way of working within the organisation, it is an online version, and finally, a Dutch version was needed.
- Third, on the question if they had already published their own DPIA report, all DPOs replied that they had not; most said they would not do so voluntarily. After all, the DPIA is an internal document which contains sensitive information, and the mandatory publication would lead to a slimmed down and censored version without any added value. Indirectly, it has been noticed during the interviews that the context of the sector (e.g. whether transparency is already established or not) influences the sector's openness to the publication of the DPIA report.

[67] SQ6: What are DPOs' current practices and views on the GDPR/DPIA?

The answers to the questions concerning how the harmonisation goal of the GDPR is seen through the DPIA lens[68] led to the following results:

Most DPOs confirm the conclusions of the literature review that 1) the GDPR (in the form of a regulation) is a good successor of the former privacy law and is an effective promoter of harmonisation and that 2) the lack of clarity of the GDPR has to be solved and a number of exceptions have to be eliminated.

One of the most commonly cited unclear points by the interviewees was the conduction of a DPIA:

- First, the GDPR itself only sets out the basic requirements of a DPIA and uses a vague terminology of "high risk", "likelihood" and "large scale". This vagueness is justified by the fact that the legislation applies to all sectors, but consequently, it is not always clear when (threshold) the DPO must conduct a DPIA and which DPIA template he should use. This vagueness should be translated into something more workable by means of advice coming from the WP29, clarifications and coaching by the DPA, interpretations/criteria made by the sectorial federation / umbrella organisations and a practical and objective tool (e.g. a well-though-out risk matrix) established by the individual organisation or DPO.
- Furthermore, the DPIA is a systematic process based on a risk assessment which is by definition personal and subjective, even if there are objective criteria aiming at achieving a uniform result.
- Finally, each national DPAs has the possibility of establishing a black-and-white list, resulting in such a list for each Member State. The interviewees uniformly considered this diversity of lists as negative. The GDPR can only succeed if the different privacy authorities do not try to surpass each other (in positive or negative ways); instead, the interviewees suggested that authorities cooperate and exchange information in order to arrive at a common position, as was the case in the past with the WP29. Moreover, the list with the nine criteria leaves room for interpretation.

For the interviewed DPOs, harmonisation in the context of GDPR has almost the same meaning: '*a common interpretation of discussions and directives which are integrally applicable throughout Europe*'. Only one DPO reported the fulfilment of minimum rules (as stated by minimum harmonisation).

The interviewees stated that the following approaches could promote a uniform and harmonised approach for conducting the DPIA.

- First, inside businesses, conducting a DPIA should belong to the scope of the DPO's duties whereby the DPO should be given the power to conduct business wide the same DPIA based on the preparatory work (input) from the persons involved in the data processing.

  The GDPR allows either an internal DPO or an external DPO. Internal DPOs (who are staff members of the data processor) typically understand a company and its business processes, but they are not entirely independent. In contrast, external DPOs (who are hired based on a service contract) are removed from the data processing, but they can provide new insights and perspectives and are more independent (less 'customer loyalty') than an internal DPO. An internal DPO working together with an external, government-dependent DPO or an (external) DPO working for a small number of enterprises belonging to the same legal entity

[68] SQ7: How is the harmonisation goal of the GDPR seen through the lens of the DPIA?

or to the same sector should create the best-case scenario towards a more homogenous conduction of the DPIA.

- Second, within the diverse economic sectors, the interviewees considered that a code of conduct has a (potential) positive impact on the harmonisation goal as long as it is workable and used within one sector on an international scale.

  Only one interviewed DPO mentioned that his organisation was 100% GDPR compliant, while all others stated that becoming 100% GDPR-compliant is a never-ending process. The sectors differ with regard to their level of compliance. For example, the banking sector (which already has experience dealing with financial data) seems to be more GDPR-compliant than the Telecom sector, which itself is more compliant than other sectors. The legal and medical sector have a backlog with regard getting GDPR-compliant.

  Within one sector, most DPOs work together with other DPOs – more precisely, in conducting a DPIA. There are formal meetings within individual sectors (colloquiums, workshops, meetings organised by the sectorial federation/umbrella organisation) and informal contact with other organisations. During these meetings, knowledge and high level information is shared, but no real collaboration regarding conducting a DPIA occurs as a DPIA could reveal the concerns of a certain organisation. The DPOs perceive this cooperation/partnership with other organisations within their own sector as having a positive impact on a harmonised DPIA.

- Furthermore, on the national/European level, most DPOs stated that a certified and thus formalised DPO training (e.g. ISO) promoted on a national level by the national DPA (or on a European level by the EDPB) is perceived as having a positive impact on the quality of the DPOs and on their general knowledge about the GDPR. However, it is doubtful whether such a training would positively impact the harmonisation goal of the GDPR.

- Finally, the NDPAs play an important role in helping organisations become GDPR compliant. The enterprises need some prioritisation from the DPAs. In this regard, the DPOs reported that during the starting period of the GDPR, the Belgian DPA did not provide enough guidance and had not made any interventions in their sector or issued any decisions concerning DPIAs in enterprises in their sectors. However, once the members of the Belgian DPA are appointed, the situation will likely improve. One DPO stated that the CNIL is much better than the Belgian DPA.

All DPOs were in favour of a certain common European DPIA template (one-fits-all), but there are doubts about its feasibility. A working solution could be 1) a common slimmed-down version of an existing European framework (CBNL (FR), ICO (UK)) for all sectors and completed with the specificities of each sector (e.g. specific processes, specific professional jargon) or 2) one European-wide template for each sector which is in accordance with all national legislations.

At the end of the interview, the interviewees were confronted with a fictional case concerning the purchase of a new application. This fictional case included some particularities which could all require the conduction of a DPIA[69].

- The first reaction of almost all interviewed DPOs was that they have to look at some 'alarm bells' more closely in order to find out if some potential problems can be avoided. However, there was widespread variation in their answers about what those alarm bells are. The

[69] The whole setting can be found in Appendix I, paragraph 6 (point 8 of the interview protocol).

interviewees most frequently cited the data servers located in the United States. Other alarm bells they mentioned included data processors, allergy information, birthday, the type of software, the working relationship, the fact that the data are taken out of an HR application, legitimate interest and the data processing ground.

- It is surprising to note that the interviewees responded differently to whether a DPIA should be conducted. Some DPOs said that a DPIA should be conducted, while others mentioned that a prior risk assessment should be done in order to find out if all risks are covered, before deciding if a DPIA should be conducted or not. For one DPO, it depends on the number of data subjects. For another DPO, it is has to be decided based on the guidelines of the WP29. Finally, one DPO said he would not conduct a DPIA for this case (as there is no risk for the persons concerned), although he mentioned that some contractual clauses and security measures must be taken.

All DPOs agreed that an accidental email containing unencrypted personal test data (i.e. a copy of the production data including names and addresses) to a wrong recipient can be considered a data leak. Indeed, such a mistake compromises a data subject's personal data, but it could not have been avoided by conducting a DPIA.

Aspects of this fictional case could be interpreted differently by other DPOs – for example, whether consent of the data subject is required.

5. Conclusions, discussion, recommendations and reflection

5.1. Conclusions

This section contains an overview of the objective and the conclusions based on the empirical study.

5.1.1. Objective

The GDPR replaced the EU Data Protection Directive as of 25 May 2018 and aims at updating the European data protection legislation by keeping pace with technological advances and by harmonizing the data protection laws of the 28 EU Member States. The modernised privacy law leads to a more formal way of working, which includes conducting a DPIA. Conducting a DPIA is a useful tool to verify if a high-risk data processing activity is legally compliant with this new privacy law. The higher level of harmonisation and fewer differences across Member States are guaranteed by the fact that the new privacy law has the form of a regulation rather than a directive (in contrast to the former Data Protection Directive).

This research had two objectives:

> **Objective 1**: What are the requirements for conducting a DPIA within the current framework of the GDPR and what is its harmonisation goal?
> **Objective 2**: How do DPOs experience the harmonisation goal of the GDPR from the point of view of the DPIA?

Based on the problem statement and the objectives, the central research question is as follows:

> **Central research question**: *How do DPO's perceive the process of conducting a DPIA, and how do they see the harmonisation goal of the GDPR through this lens of the DPIA?*

In order to answer the central research question, a literature review was executed, and an empirical study was conducted.

The literature review led to an enumeration of the most important requirements concerning the execution of a DPIA and the different types of harmonisation. These results were the basis for the empirical study, during which the DPOs' perception of conducting a DPIA in the context of the harmonisation goal was evaluated.

5.1.2. General conclusion

The conclusions leading to the answer of the central research question are twofold.

First of all, the DPO's perceive conducting a DPIA as necessary to verify if a high-risk data processing activity is legally compliant with the GDPR.

The DPOs cited conducting a DPIA as one of the unclear points of the GDPR which has to be clarified in the future. It is not always easy for organisations to know the criteria for conducting a DPIA (who, what, when, how). This means that the same case does not automatically result in the same reaction and subsequent measures being implemented.

Based on the lessons learned from past DPIAs, the DPOs with practical experience prefer a streamlined, short, easy-to-understand and easy-to-use template which is not static but is constantly adapted based on a "Plan-Do-Check-Act" cycle. The template should consist of two parts, a common core that is valid for all organisations and an extension consisting of a flexible, additional assessment adapted to the specific risks and requirements of individual data processing operations. This approach fits into the idea that a good DPIA is one that is best suited to an organisation while still meeting the GDPR obligations. The CNIL template (which fulfils all GDPR-requirements but does not allow the assessment to be adapted to the specific risks and requirements of individual data processing operations) could be used (partially) for the common core.

The interviews in combination with the fictional case revealed little variation in theory but only a limited consensus in DPIA-related practice among the DPOs. All DPOs were willing to comply with the GDPR by reducing risks and by conducting a DPIA when necessary, but the interpretation of when to conduct a DPIA differed from DPO to DPO. This variability illustrates that the personality and the working environment/experience of each DPO might influence the decision-making process.

Secondly, the DPOs see the harmonisation goal of the GDPR as difficult to realise.

A homogeneous execution of the DPIA, which would be applicable in an identical way in all sectors (one size fits all), is crucial for the harmonisation goal of the GDPR, but it is hard to achieve. The DPOs identified the following limitations hindering the harmonisation goal:

- First, the GDPR only sets out the basic requirements of a DPIA and uses vague terminology like "high risk", "likelihood" and "large scale", giving rise to multiple interpretations.
- Second, the DPIA is a systematic process with a risk-based approach. The geographical and cultural differences in privacy, corporate culture and the profile of an organisation/sector and the personal situation of a DPO (e.g. experience) cause risk and impact to be assessed differently by different DPOs, which influences the threshold for conducting a DPIA.
- Finally, although the GDPR aims at minimum harmonisation, the different national black-and-white lists (established by the national DPAs) and the list with the nine criteria (established by the EDPB) also give rise to divergence.

Multiple players play an important role in eliminating all uncertainties and reducing the different interpretations and thus evolving towards a harmonious conduction of the DPIA.

The most important role is reserved for the national DPAs that can achieve a certain level of harmonisation by providing guidance, support, controls; and, possibly, by promoting a certified (ISO) training regarding the GDPR/DPIA. In this context, it is important that the NDPAs closely cooperate with each other so that new national propositions achieve a prior consensus among all Member States and therefore can be easily generalised to a common guidance on a European level. However, it is striking that the different DPAs are not considered to be equally active. The Belgian DPA falls short here and is behind the CNIL and ICO who do provide guidance, execute systematic inspections and impose warnings and sanctions. Furthermore, the fines issued clearly show that the DPIA is not the priority of the NPDAs; instead, they seem to prioritise security (prevention of data breaches), the appointment of a DPO and the presence of a processing register.

As long as the national DPAs do not establish clear guidelines, umbrella organisations are developing their own interpretation of the vague prescriptions of the GDPR and the DPIA and are trying to achieve a uniform approach. They can do so, first, by favouring the establishment of codes of conducts, which, in turn, can facilitate the DPIAs. Additionally, they can favour cooperation and experience sharing between colleague DPOs of other organisations. Properly speaking, the activities

of the umbrella organisations and the DPOs is not harmonisation *senso stricto* but rather a conversion towards a uniform approach of conducting a DPIA within a local or sectorial context. Obviously, sectors working independently could have diverging approaches.

5.2. Discussion

This section discusses some conclusions obtained from the empirical research in relation to the literature.

Haziness in the GDPR

While one of the aims of the EU GDPR is to harmonize data protection rules throughout Europe, the overall impression is that the GDPR contains some points and concepts which can be subject to interpretation and which will need to be clarified in the future. This has also been stated by Giurgiu and Lallemang (2017).

Harmonisation

First, defining what should be understood by harmonisation in the context of the GDPR was a challenge as no definition gives a complete picture of the truth. Furthermore, the GDPR does not explicitly mention what kind of harmonisation is envisaged. Minimum harmonisation could only be deduced from the text. Finally, the DPIA template proposed by the DPOs (being a common assessment completed with an additional assessment) can fit in the '*minimum harmonisation*' approach in the case of a common national part and an additional sectorial part. A common European part and an additional national/sectorial part tend more to '*optional harmonisation*'.

NDPAs

The impact of the attitude of the NDPAs is somewhat two sided: on the one hand they should explain and clarify some uncertainties and thus promote harmonisation; on the other hand, their deviating national black-and-white lists have a negative influence on the harmonisation. Such deviation results in a non-uniform application of the GDPR (specifically of the DPIA) across Member States.

The criticism that the Belgian DPA is lagging behind the others with regard to advice and guidance is expected to be reduced since the members of the DPA have been formally appointed by the Parliament in the meantime. Moreover, the Belgian DPA is expected to increase its advisory, inspection and sanctioning activities. In the meantime, the Belgian DPA has also imposed its first administrative fine. On 28 May, 2019, a mayor was fined 2,000 EUR for misusing personal data for electoral campaign purposes (Hunton, Andrews and Kurth, 2019).

The proposed cooperation between the NDPAs is already done under the guidance of the EDPB. The NDPAs must establish a list of processing operations that trigger the DPIA requirement under the GDPR. The GDPR foresees that the EDPB sets guidelines '*to encourage consistent application of the Regulation*'[70] and to limit inconsistencies among EU Member States concerning the GDPR's DPIA requirement. In this context, the EDPB can request the NDPAs to include or remove some processing activities in their list.[71] Nevertheless, even after this process, the national lists will still not be

[70] GDPR Article 70(1)
[71] GDPR Article 35(4)

identical because the EDPB is best positioned to issue and update methods throughout the EU for conducting a DPIA, while the NDPAs are best positioned to take into account their national context and legislation with respect to the harmonisation goals of the GDPR (Hunton, 2018).

Mandatory publication of DPIA report

The DPOs are in favour of the disclosure of the DPIA report on a need-to-know basis and adapted to the goal audience. This opinion is in line with the prescriptions of the GDPR which do not specifically require the publication of DPIA reports. Nevertheless, the EDPS considers publication of DPIA reports (or at least a summary) to be a good practice. Publication should help both the organisation and others to apply and implement the GDPR (thus indirectly favouring the harmonisation goal), to reassure the stakeholders and the public and to foster trust (EDPS, 2019). However, this is contrary to the study by Wright (2013), who established a '*step-by-step guide to privacy impact assessment*'. That guide contains 16 steps which ideally should be followed in order to obtain the '*optimal PIA process*', with step 12 consisting of the preparation and publication of the report (open communication).

It remains unclear if the NDPAs should encourage organisations to publish their DPIA report and if the NDPAs should establish a list of publicly available DPIA reports.

Customer confidence

Organisations can maintain customer confidence by demonstrating compliance with the privacy and data protection requirements of the GPDR and by proving that the appropriate measures have been taken (Salami, 2017). However, conducting a DPIA and publishing the report are not seen as instruments fulfilling this objective.

5.3. Practice recommendations

Some practical results of this research that organisations could apply are the following:

First, conducting a DPIA is not a one-shot event; rather, data protection should be reviewed and updated periodically based on, for example, new requirements imposed by the NDPA or emerging technologies or risks.

Second, the process for conducting a DPIA can be the same for all processes and for all sectors; however, due to the sector- and technology-specific privacy requirements, the template of the DPIA may vary. Consequently, there is no one-size-fits-all approach to becoming GDPR-compliant because every business is different depending on the sector, the technology used and type of data processed. So, a generic approach should be adapted to the specific situation in order to provide a meaningful and useful DPIA. Moreover, this diversity of needs is also why the DPIA should contain the terminology of the sector or technology.

Finally, due to the non-uniform application of the GDPR across Member States with regard to the DPIA, there are different national black-and-white lists for conducting a DPIA. Organisations that conduct their business in multiple Member States should be aware that this situation can create difficulties in complying with the GDPR.

5.4. Recommendations for further research

This section presents recommendations for future research, for which this study can be used as a starting point for providing other insights. These guidelines are based on the limitations and the general setting of this study as discussed below.

The first recommendation concerns the time frame of the study, which was conducted around 28 May, 2018, the day the GDPR became enforceable in all Member States of the EU. Because the GDPR was completely new for many enterprises, it is advisable that this study is repeated when the GDPR is fully integrated in the enterprises and when the '*fear*' of it has subsided. This would lead to a more reliable result, and a comparison between both a future study with the present study would make it possible to study how the DPOs changed their position regarding the DPIA.[72]

The second recommendation is to interview stakeholders other than DPOs, such as data controllers and data processors, all of whom are driven by different underlying objectives.

Third, the enterprises have been identified and selected based on the current, fluid criteria for carrying out a DPIA. It is not inconceivable that these criteria will be refined in a later phase. When this is the case, it would be a good idea to repeat the same research with the new criteria.

Fourth, this study was based on the current situation in a number of enterprises situated in different sectors in Belgium. Some DPOs gave their personal ranking of the Belgian sectors in relation to their GDPR compliance. However, due to the low participation rate of DPOs within the same sector, it was not possible to thoroughly evaluate this sectoral comparison. So, further research could focus on the following:

- Enterprises of different sectors in Belgium (this could give insight into how the harmonisation goal is seen between different sectors in Belgium);
- Enterprises of the same sector in different European countries (this could give insight into how the harmonisation goal is achieved within one sector across the national borders);
- Enterprises of the same sector within one European country (this would give insight into how the harmonisation goal is seen within one country).

The interviewed enterprises were catalogued according to the ISIC, the United Nations industry classification system. This should facilitate further research (with regard to enterprises of the same sector in different European countries or enterprises of the same sector within one European country).

Finally, the GDPR offers various data protection accountability tools which can help organisations to demonstrate their compliance with the GDPR – namely, the DPIA (which is mandatory in certain circumstances) as well as the voluntary codes of conduct[73] and certification.[74] It would be interesting to see if these voluntary accountability tools give rise to the same results.

[72] In the research onion (Saunders et al., 2016) the time horizon (5th layer) will change from "cross-sectional" to "longitudinal".
[73] GDPR, articles 40 and 41
[74] GDPR, article 42

5.5. Reflection

This section contains a reflection on the quality of the research and the validity of the conclusions.

5.5.1. The impact of the process-oriented nature of the DPIA on this research

Because the DPIA is a process (and thus personal and contextual), the perception of harmonisation was difficult to analyse, in comparison with, for example, article 8 of the GDPR ('*Conditions applicable to child's consent in relation to information society services*'). This is a typical example of an explicit clause pointing at minimum harmonisation, and this based on figures. The EU determines 16 years as the default age at which a child can express valid consent to process their data (social media, applications, etc.). All Member States have to accept this minimum age of consent, but they have the ability to adopt more stringent provisions (e.g. a lower age, but not lower than 13) to protect young consumers more extensively. Many Member States have done so.[75]

5.5.2. The availability of conducted DPIAs

In order to narrow the scope, this empirical study was limited to one aspect of the GDPR: the DPIA. However, reports of performed DPIAs were hard to find because there is no requirement to make them publicly available. Trilateral Research & Consulting (2013) lists 26 publicly available PIA reports (the result of an internet search). Unfortunately, these DPIAs were executed before the publication of the GDPR. My own internet search did not result in any DPIA or DPIA reports.

Due to the limitation of resources and time restrictions, this study only evaluates the perception of 12 DPOs towards the DPIA. This could restrict the generalizability of the DPO conclusions.

Furthermore, not all identified sectors whose organisations should have to appoint a DPO (see Appendix F) were represented in the interviews.

The results of this qualitative study, which was based on data from a small non-probability sample, cannot be used to make statistical generalisations about the perceptions of all DPOs. Because of that limitation, other similar organisations should be studied.

Initially, it was planned that the interview process should be a mixed process, consisting of two types of studies: 1) an exploratory study (semi-structured interview with the DPOs) in order to explore their decisions, attitudes and opinions regarding the DPIA and 2) an explanatory study (in-depth interview with the Belgian Data Protection Authority) in order to understand the reasons for their perception towards the DPIA. However, despite several requests, the Belgian DPA was not willing to grant an interview due to time constraints. A similar reservation can be made about the Belgian professional organisation for DPOs. Although this professional organisation could have added value

[75] The Republic of Croatia has explicitly confirmed that the age of the child is at least 16, without further derogations and/or setting lower age limits. France has established the age at 15 years at which the data controller is then required to deliver the information '*in clear and easily accessible language*.' Austria, Bulgaria, Cyprus, Italy and Lithuania have set fourteen as the minimum age. Belgium, Denmark, Finland, Portugal, Sweden and UK have reduced the age to 13 years (which is the lowest so far within the EU). The adjustment of the minimum age has been justified by the importance of the Internet for young people.

to the representation and guidance of the DPOs, it was not mentioned by any of the interviewees. The professional organisation was contacted multiple times and via different methods but did not respond to a request for an interview.

5.5.3. The availability of potential DPOs to interview

This study only focused on DPOs, and other important stakeholders were not included, such as data subjects and data protection authorities. Nevertheless, the interviewed DPOs were a valid population for this study, as explained in section 3.2.1. However, due to the criteria for the selection of the DPOs and organisations, there was little variation among the characteristics of the interviewees.

Although this study provides valuable insights into the concept of executing a DPIA and points to several gaps, the following limitations concerning the availability of potential DPOs to interview should be considered. First, the interview invitations generated a response rate of only 25%. Appendix G gives an overview of this rate and the justification (if any) given by the contacted DPOs for not participating in the interview. Based on the interviews, the main reasons for the low response were: 1) the novelty of the GDPR (DPOs were afraid of giving insight into their internal guidelines and policies), 2) interview fatigue (there have been a large number of demands from students to participate in research projects, which has had an adverse impact on participants' willingness to be interviewed) and 3) a lack of time. For practical reasons, organisations/DPOs residing outside Belgium were excluded, and the focus when contacting organisations was on those who should really need a DPO according to the GDPR (see Appendix F). Second, due to the low response rate, it was not possible to evaluate the extent of harmonisation in accordance with the original aim of this thesis. In order to truly evaluate harmonisation, all DPOs should belong to the same sector (so that differences within one sector could be explored), or the response rate should be higher (so that differences between sectors could be evaluated). In general, some significant differences have been found between DPOs (especially between internal and external DPOs) and between the different sectors. However, due to the small number of DPOs within the different sectors, it is challenging but rather difficult to identify significant trends. So this evaluation is still open.

One might suggest that a survey would have been a better method for evaluating perceptions regarding the DPIA. However, in light of the low response rate for the interview requests, a similarly low response rate would likely have been achieved for the survey. Moreover, interviews make it less likely that the participants would misunderstand what is being asked than in the case of a survey. The latter would have contributed to an uncontrolled variation in results. This difference in understanding is in particular what this study evaluated.

Interviewing was a time-consuming process due to travelling to the location of the participants, the interviews themselves and the transcription of the interviews. Although the time required for the transcription of each interview could have been foreseen, the scheduling of the interviews was mainly driven by the location and the availability of the interviewees. Nevertheless, no more than two interviews were planned during the course of each day, as this appeared to be a reasonable target. Furthermore, as the use of telephone interviews contributes to access, speed and lower cost, this possibility was considered. In the end, though, telephone interviews were not used. The semi-structured interview concerning the DPIA required the engagement of the participants, and this could only be achieved in the context of a trusted personal contact (face-to-face).

It is important to note that the recent implementation of the new GPDR means that the experience of all DPOs is somewhat limited. For that reason, the assessment in this thesis is merely based on the DPOs' intentions regarding the GDPR and the DPIA.

5.5.4. The conduction of semi-structured interviews

Originally, the nature of the qualitative analysis was intended to be inductive. In the end, though, this research was a combination of an inductive and a deductive approach as some theoretical elements concerning the DPIA and the harmonisation were developed and treated during the semi-structured interviews.

Holding two interviews on the same day prevented me from conducting initial analysis on the results of the first interview before carrying out the second one. This would have been possible with only one interview a day.

The semi-structured interview, being a qualitative method, was not the ideal method to seek for differences or common features between the DPOs, such as the following: DPOs belonging to the same sector, half-time and full-time DPOs, external DPOs and internal DPOs, DPOs acting as the single DPO of an organisation and those as part of a so-called DPO office.

For example, on the one hand, the DPOs of the insurance sector varied significantly in how they perceived the impact of local cultures or traditions on the harmonisation goal. For example, one DPO saw the impact of such cultures as negative, while another saw it as positive. The third one did not perceive any possible impact. On the other hand, all interviewed DPOs of the insurance sector agreed that a common European template for conducting a DPIA, which would be applicable in an identical way in all sectors, would (possibly) have a positive impact.

Contrary to a quantitative study, this qualitative study was not able to measure consensus with a certain percentage. Because the literature review did not reveal a clear method to be used to fix the level of consensus in a qualitative study, consensus was deemed to be present when more than half of the interviewed DPOs answered in the same way. This percentage part was arbitrary based on the number of interviewees.

5.5.5. The 'DPIA of reference'

In the context of the literature review, the French CNIL template has been identified as a DPIA reference. The initial idea was to use this DPIA as an anchor point and a '*common thread*' through the interviews. However, as none of the interviewed DPOs had used this template for conducting a DPIA, the initial plan had to be adjusted. At the end, the contribution of the French CNIL template to the whole study was reduced to a supporting role.

References

As far as known, the various documents referenced in this paper are not copyright protected. So, no approval had to be sought to paraphrase or quote from the documents.
The documents have been referenced in accordance with the APA format.

Article 29 Data Protection Working Party. (2017). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679*. Brussels. Available at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236. Date accessed: 30 March 2018

Barker, J. (2017, July 27). *What does GDPR mean for you?* [Blog post]. Available at: https://digitalguardian.com/blog/what-does-gdpr-mean-for-you. Date accessed: 25 April 2018.

Batty, L., Glozier, N., Holland-Elliott, K. (2009). Interpretation of Medical Information Acts by UK Occupational Physicians. Occupational Medicine, 59(3), 153-158

Calder, S. (2017, October 29). *Heathrow's secret security data found on memory stick in London street*. The Independent. Retrieved from https://www.independent.co.uk/.

Cherdantserva, Y., Hilton, J. (2013). *A Reference Model of Information Assurance and Security*. Proceedings of the 8th International Conference on Availability, Reliability and Security (ARES), IEEE, Germany, Regesburg, 546-555.

CNIL. (2015). *Privacy Impact Assessment: Methodology (how to carry out a PIA)*. Available at https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf. Date accessed: 15 April 2018.

Commission de la protection de la vie privée. (2018). Recommandations d'initiative concernant l'analyse d'impact relative à la protection des données et la consultation préalable (CO-AR-2018-001). Available at: https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2018.pdf. Date accessed: 15 April 2018.

Commission of the European Communities. (2009). Commission Recommandation on the Implementation of Prviacy and Data Protection Principles in Applications Supported by Radio-Frequency Identification, Commission of the European Communities. Brussels.

Cronholm, S., Göbel, H. (2016). Evaluation of the Information Systems Research Framework: Empirical evidence from a Design Science Research Project.

Doherty Associates (2018), These real-world data breach examples will make you rethink your data strategy, Available at https://www.doherty.co.uk/blog/data-breach-examples-rethink-your-data-strategy. Date accessed: 20 December 2018

European Data Protection Board. (2018, July). EDPB Annual report 2018, Available at: https://edpb.europa.eu/about-edpb/board/annual-reports_en. Date accessed: 15 August 2019.

European Data Protection Supervisor. (2019, July), Available at: https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_ii_en.pdf. Date accessed: 15 August 2019.

ENISA. (2016, December). *Guidelines for SMEs on the security of personal data processing*. Available at https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing. Date accessed: 12 May 2018.

ENISA. (2017, December). *Handbook on Security of Personal Data Processing*. Available at https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing . Date accessed: 12 May 2018.

European Commission. (2010). *A comprehensive approach on personal data protection in the European Union.* COM(2010) 609 final. Brussels. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52010DC0609. Date accessed: 05 May 2018.

European Comission. (2017). Regulations, directives and other acts. Available at: https://europa.eu/european-union/eu-law/legal-acts_en. Date accessed: 05 May 2018.

Giurgiu, A., Lallemang, T. (2017, January). *The General Data Protection Regulation: A New Opportunity and Challenge for the Banking Sector*. Ace Magazine et Archives Online : Fiscalité, Comptabilité, Audit, Droit des Affaires au Luxembourg. 2017. (1). 3-15. Available at https://www.researchgate.net/publication/313114747_The_General_Data_Protection_Regulation_a_new_opportunity_and_challenge_for_the_banking_sector . Date accessed: 15 April 18.

Hevner, A., March, S., Park, J. and Ram, S. (2004). *Design Science in Information Systems Research*. MIS Quarterly, 28(1), 75-105.

Hochepied, S. (2018). *De impact van de GDPR op ziekenhuizen. Beschrijvende casestudies bij het KOM- en het E17-ziekenhuisnetwerk*. University of Ghent. Available at: https://lib.ugent.be/fulltxt/RUG01/002/508/970/RUG01-002508970_2018_0001_AC.pdf. Date accessed: 13 May 2018.

Hunton, A. (2018). EDPB adopts opinions on national DPIA lists in the EU. Available at https://www.lexology.com/library/detail.aspx?g=61be3fdf-9cd3-4d7f-a410-366e5b946df6. Date accessed: August 15, 2019.

Hunton, A. (2019). First Fine Imposed by the Belgian DPA Since GDPR. Aiblable at https://www.huntonprivacyblog.com/2019/06/04/first-fine-imposed-by-the-belgian-dpa-since-gdpr/. Date accessed: August 15, 2019

International Association of Privacy Professionals. (2019, March 26). *Privacy professionals begin to look back at year one of the GDPR. Available at* https://iapp.org/news/a/privacy-professionals-begin-to-look-back-at-year-one-of-the-gdpr/. *Date accessed: 10 April 2018.*

EU Member State GDPR Implementation Laws and Drafts. Available at https://iapp.org/resources/article/eu-member-state-gdpr-implementation-laws-and-drafts/. Date accessed: 15 August 2018.

ICO. (2014). *Conducting privacy impact assessments code of practice*. Available at https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf. Date accessed: 15 April 2018.

Inc. Garnter. (2017, May). *Gartner says Organisations are unprepared for the 2018 European Data Protection Regulation*. Available at https://www.gartner.com/newsroom/id/3701117. Date accessed: 10 April 2018.

International Association of Privacy Professionals (7 June 2018). *GDPR harmonisation: Reality or myth*? Available at: https://iapp.org/news/a/gdpr-harmonisation-reality-or-myth/. Last accessed: 18 July 2018.

International Standard Industrial Classification of all Economic Activities (ISIC), revision 4 (2008). Available at: https://unstats.un.org/unsd/publication/seriesM/seriesm_4rev4e.pdf. Last accessed: 18 May 2019.

Kloza, D., Van Dijk, N., Gellert, R. M., Borocz, I.M., Tanas, A., Mantovani, E., & Quinn, P. (2017). *Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals: d.pia.lab Policy Brief 1/2017*, d.pia.lab Policy Brief (pp. 1-4).

Kurcz, B. (2001). Harmonisation by means of Directives – never-ending story?, European Business Law Review 2001, Issue 11/12, p. 287 – 287.

Lohse, E. J. (2012). The Meaning of Harmonisation in the Context of European Community Law – a process in need of definitions. Available at: https://www.academia.edu/3506314/_Th HYPERLINK "https://www.academia.edu/3506314/_The_Meaning_of_Harmonisation_in_the_Context_of_European_Union_Law_a_Process_in_Need_of_Definition"e_Meaning_of_Harmonisation_in_the_Context_of_European_Union_Law_a_Process_in_Need_of_Definition. Last accessed: 18 July 2018.

Mikkonen, T.(2014). Perceptions of controllers on EU data protection reform: a finnish perspective. Computer Law & Security Review, 30(2), pp. 190-195.

Peffers, K., Tuunanen, T., Rothenberger, M., Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45–77.

Privacy Impact Assessment Framework (2012, November). *Recommendations for a privacy impact assessment framework for the European Union*. Brussels, Belgium – London, Great-Britain: Author.

PRIPARE. (2014, December 31). Preparing industry to privacy-by-design by supporting its Application in Research. Deliverable D2.2

Salami, E. (2017, May 10). An Analysis of the General Data Protection Regulation (EU) 2016/679. Available at https://ssrn.com/abstract=2966210. Data accessed: 01 april 2018

Saunders, M., Lewis, P. and Thornhill, A. (2016). *Research methods for business students*. Harlow: Pearson Education Limited.

Statbel. (2018). ICT gebruik in huishoudens. Available at https://statbel.fgov.be/nl/themas/huishoudens/ict-gebruik-huishoudens Last accessed: 24 August 2018

Steiner and Woods (2014). 15. Harmonisation. In EU Law (12th edition, pp. 323-343). Oxford University Press. Available at: https://blackwells.co.uk/extracts/9780199279593_steiner.pdf. Last accessed: 18 July 2018

Tankard, C. (2016). What the GDPR means for businesses. Network Security, 5-8.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134-153.

Trilateral Research & Consulting. (2013, May). Privacy impact assessment and risk management. Available at https://ico.org.uk/media/1042196/trilateral-full-report.pdf. Date accessed: 30 March 2018

Van Hoecke, M. & Dhont, J. (1999). Obstacles and opportunities for the harmonisation of law in Europe: The case of privacy, University of Helsinki, Faculty of Law of Helsinki

Vandendriessche, J., Data Protection Impact Assessments under the GDPR. June 16, 2017. Available at https://www.slideshare.net/Johan_Vdd/data-protection-impact-assessments-under-the-gdpr. Data accessed: 10 April 2018.

Willaert, M. (2018). The impact of the GDPR on the financial sector. University of Ghent, Available at https://lib.ugent.be/fulltxt/RUG01/002/480/966/RUG01-002480966_2018_0001_AC.pdf. Date accessed: 13 May 2018.

Wright, D. (2013). *Making Privacy Impact Assessment More Effective.* The Information Society, 29(5), 307-315. DOI: 10.1080/01972243.2013.825687

Wright, D., Finn, R., Rodrigues, R. (2013). *A Comparative Analysis of Privacy Impact Assessment in Six Countries*. Journal of Contemporary European Research**,** [S.l.], v. 9, n. 1, jan. 2013. ISSN 1815-347X. Available at: <https://www.jcer.net/index.php/jcer/article/view/513>. Date accessed: 13 May 2018.

Appendix A: Glossary

The definitions are listed in alphabetical order.

	Definition	Source
Article 29 Working Party	The official advisory body to the European Commission in the field of personal data protection and privacy which has been established on the basis of Article 29 of the Directive 95/46/EC and which will be instituted into the European Data Protection Board on the basis of the GDPR.	Wikipedia: https://en.wikipedia.org/wiki/Article_29_Data_Protection_Working_Party
Artefact	Any designed object with an embedded solution to an understood research problem	Peffers et al. (2007)
Coding	The process of labelling of data using a code that symbolises or summarises the meaning of that data.	Saunders et al. (2016)
NL: Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL) FR : Commission de la protection de la vie privée (CPVP) (EN : Commission for the protection of privacy)	The independent federal data protection authority for Belgium whose mission is to ensure that privacy is respected when personal data are processed	Website Privacy Commissie: https://www.privacycommission.be/en/in-a-nutshel
Commission Nationale de l'Informatique et des Libertés (CNIL) (EN: National Commission on Informatics and Liberty)	The independent national data protection authority for France whose mission is to ensure that data privacy law is applied to the collection, storage, and use of personal data.	Wikipedia: https://en.wikipedia.org/wiki/Commission_nationale_de_l%27informatique_et_des_libert%C3%A9s
Data breach	Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.	GDPR, article 4
Data controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data	GDPR, article 4
Data processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller	GDPR, article 4
Data Protection Impact Assessment (DPIA)	A process to assess the risks associated with the rights and freedoms of natural persons that arise or threaten to arise in connection with the processing of personal data and to assess the possibilities for mitigating or managing these risks	Article 29 Data Protection Working Party (2017)
Data Protection Officer (DPO)	An enterprise security leadership role required by the GDPR.	Website Digital Guardian: https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required-gdpr-compliance
Data Protection Threshold Assessment	The process of establishing whether a DPIA is necessary.	Website Vulpoint: https://www.vulpoint.be/data-protection-impact-assessment-first-guidelines/
Design science	An outcome based information technology research methodology, which offers specific guidelines for evaluation and iteration within research projects.	Wikipedia: https://en.wikipedia.org/wiki/Design_science_(methodology)

	Definition	Source
European Data Protection Board (EDPB)	An independent European body, composed of representatives of the national data protection authorities, and the European Data Protection Supervisor, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities.	Website EDPB: https://edpb.europa.eu/about-edpb/about-edpb_en
European Data Protection Supervisor (EDPS)	An independent supervisory authority whose primary objective is to ensure that European institutions and bodies respect the right to privacy and data protection when they process personal data and develop new policies.	Wikipedia: https://en.wikipedia.org/wiki/European_Data_Protection_Supervisor
European Union Agency for Network and Information Security (ENISA)	A centre of network and information security expertise for the European Union, its member states, the private sector and Europe's citizens aiming to improve network and information security (NIS) within the European Union.	Wikipedia https://en.wikipedia.org/wiki/European_Union_Agency_for_Network_and_Information_Security
Harmonisation	The adoption of a new European privacy legislation • with the help of a directly applicable regulation (GDPR) according to Art 249(2) EC, and • with the contribution of all actors involved (with an important role for the European Data Protection Board (EDPB) (which replaced the Article 29 Data Protection Working Party), Member States, the NDPA and data protection officers) in order • to make the former divergent national privacy legislations (based on the EU Data Protection Directive 95/46/EC) more into conformity, and • to adapt the former European legislation to current privacy issues.	Own definition based on Lohse (2012)
Impact Assessment	A tool used for the analysis of possible consequences of an initiative on a relevant societal concern or concerns, if this initiative can present dangers to these concerns, with a view to support the informed decision-making whether to deploy this initiative and under what conditions, ultimately constituting a means to protect these concerns.	Kloza, Van Dijk, Gellert, Borocz, Tanas, Mantovani & Quinn (2017)
Information Security	A multidisciplinary area of study and professional activity which is concerned with the development and implementation of security counter-measures of all available types (technical, organisational, human-oriented and legal) in order to keep information in all its locations (within and outside the organisation's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats.	Cherdantserva & Hilton (2013)
Information Security Risk Management (ISRM)	The process of identifying, quantifying, and managing the information security risks that an organisation faces; it is a process aimed at obtaining efficient balance between realising opportunities for gains and minimising vulnerabilities and loss.	ENISA (2016)
Interviewee bias	Attempt by an interviewee to construct an account that hides some data or when she or he presents herself or himself in a socially desirable role or situation.	Saunders et al. (2016)
Interviewer bias	Attempt by an interviewer to introduce bias during the conduct of an interview, or where the appearance or behaviour of the interviewer has the effect of introducing bias in the interviewee's responses.	Saunders et al. (2016)

	Definition	Remark
International Standard Industrial Classification of all Economic Activities (ISIC)	A subdivision of the economic activities in a hierarchical, four-level structure of mutually exclusive categories.	ISIC (2018)
Methodology	The systematic, theoretical analysis of the methods applied to a field of study.	Wikipedia https://en.wikipedia.org/wiki/Methodology
Participation bias	Type of bias resulting from the nature of the individuals or organisational participants who agree to take part in a research study.	Saunders et al. (2016)
Privacy Impact Assessment Framework (PIAF)	European Commission co-funded project that aims to encourage the EU and its Member States to adopt a progressive privacy impact assessment policy as a means of addressing needs and challenges related to privacy and to the processing of personal data.	Website PIAF: Website PIAF: http://www.piafproject.eu/
PIAF consortium	Consortium consisting of Vrije Universiteit Brussel (Belgium), Trilateral Research & Consulting (UK) and Privacy International (UK) which formulated to the EC a set of recommendations on an optimised PIA Framework, based on the review of existing PIA methodologies.	Website PIAF: https://piafproject.wordpress.com/
Privacy	An ability of a socio-technical system to obey privacy legislation and to enable individuals to control, where feasible, their personal information (user-involvement)	Cherdantserva & Hilton (2013)
Research question	The key question that the research process will address, or one of the key questions that it will address.	Launders (2016)
Residual risk	Risk remaining after risk treatment.	SO 27001
Research strategy	General plan of how the researcher will go about answering the research question(s)	Launders (2016)
Risk	A scenario describing an event and its consequences, estimated in terms of severity and likelihood	Article 29 Data Protection Working Party
Risk Management	A process, aimed at an efficient balance between realising opportunities for gains and minimising vulnerabilities and losses.	ENISA (2016)
Stakeholders	A party that is or might be interested or affected by the project, technology or service: people who are internal as well as external to the organisation, such as regulatory authorities, customers, citizen advocacy organisations, suppliers, service providers, manufacturers, system integrators, designers, and academics.	Wright (2013)
Thematic analysis	A technique used to analyse qualititative data that involves the search for themes, or patterns, occurring across a data set.	Launders (2016)

Appendix B: GDPR – Article 35 "Data Protection Impact Assessment"

1. *Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.*
   A single assessment may address a set of similar processing operations that present similar high risks.
2. *The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.*
3. *A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:*
   a) *a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;*
   b) *processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or*
   c) *a systematic monitoring of a publicly accessible area on a large scale.*
4. *The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.*
   The supervisory authority shall communicate those lists to the Board referred to in Article 68.
5. *The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required.*
   The supervisory authority shall communicate those lists to the Board.
6. *Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behavior in several Member States, or may substantially affect the free movement of personal data within the Union.*
7. *The assessment shall contain at least:*
   a) *a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
   b) *an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
   c) *an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*
   d) *the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.*
8. *Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.*
9. *Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.*
10. *Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.*
11. *Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.*

Appendix C: Criteria for executing the literature review

This appendix lists the criteria used for the literature review.

1. Publication date

   For the literature review, the publication date of relevant studies was not taken into account. Given the timeliness of the topic, the consulted sources are by default recent.

2. Source references

   For the source references, the American Organisation (APA) format was used.

3. Search engines

   Initially, the following search engines were used:

   - Google
   - Google Scholar
   - EBSCO Host
   - The digital library of the Open University Netherlands. This digital library gives access to various search engines (including Google Scholar and EBSCO Host, mentioned above) and also provides access to peer-reviewed articles.

   However, Google Scholar, EBSCO Host and the digital library of the Open University Netherlands contained little information on this legislation-related topic. So, finally, Google was used as the standard search engine.

4. Languages

   Initially, literature was searched in Dutch, French, English and German. However, as the most interesting and relevant literature about GDPR is by default published in English, the search ended with only using English terms.

5. Sub-questions and used search terms:

   The search terms were selected in order to answer the sub-questions and main research question.

   A list with Dutch, French, English and German search terms was established as listed below. Single search terms and combinations of search terms were used.

Subquestion	Dutch search term	French search term	English search term	German search term
GDPR	GDPR	RGPD	GDPR	DSGVO
	privacywetgeving	législations relatives à la protection des données		
	Verordering	Réglement	Regulation	Regulierung
	conform	conforme	compliant	konform
	conformiteit	conformité	compliance	Konformität
	verwerkingsverantwoordelijke	responsable du traitement	controller	Verantwortlicher
	verwerker	sous-traitant	processor	Auftragsverarbeiter
	toezichthoudende autoriteit	autorité de contrôle	supervisory authority	Aufsichtsbehörde
	betrokken toezichthoudende autoriteit	autorité de contrôle concernée	supervisory authority concerned	betroffene Aufsichtsbehörde
	functionaris voor gegevensbescherming	délégué à la protection des données	Data protection officer	Datenschutzbeauftragte
	Gegevensbescherming	Protection des données	Data protection	Datanschutz
DPIA/PIA	Definitie	Définition	Definition	Definition
	Omschrijving	Description	Description	
	Succesfactoren	facteurs de succès	success factors	Erfolgsfaktoren
	Risico-analyse	Analyse de risques	Risk analysis	Risikoanalyse
	Framework	Framework	Framework	Framework
	Richtlijnen	Lignes directrices	Guidelines	Richtlinien
	Best practices	Bonnes pratiques	Best practices	Best practices
	Stappenplan compliancy GDPR	Étapes conformité RGPD	Action plan compliancy GDPR	Aktionsplan DSGVO
	Article 29 working party	Article 29 working party	Article 29 working party	Article 29 working party
	Gegevensbeschermingseffectbeoordeling	Analyse d'impact Relative à la Protection des Données	Data protection impact assessment	Datenschutz-Folgenabschätzung
Harmonisation	Definitie	Définition	Definition	Definition
	meten	mesurer	To mesure	messen

6. Relevant literature

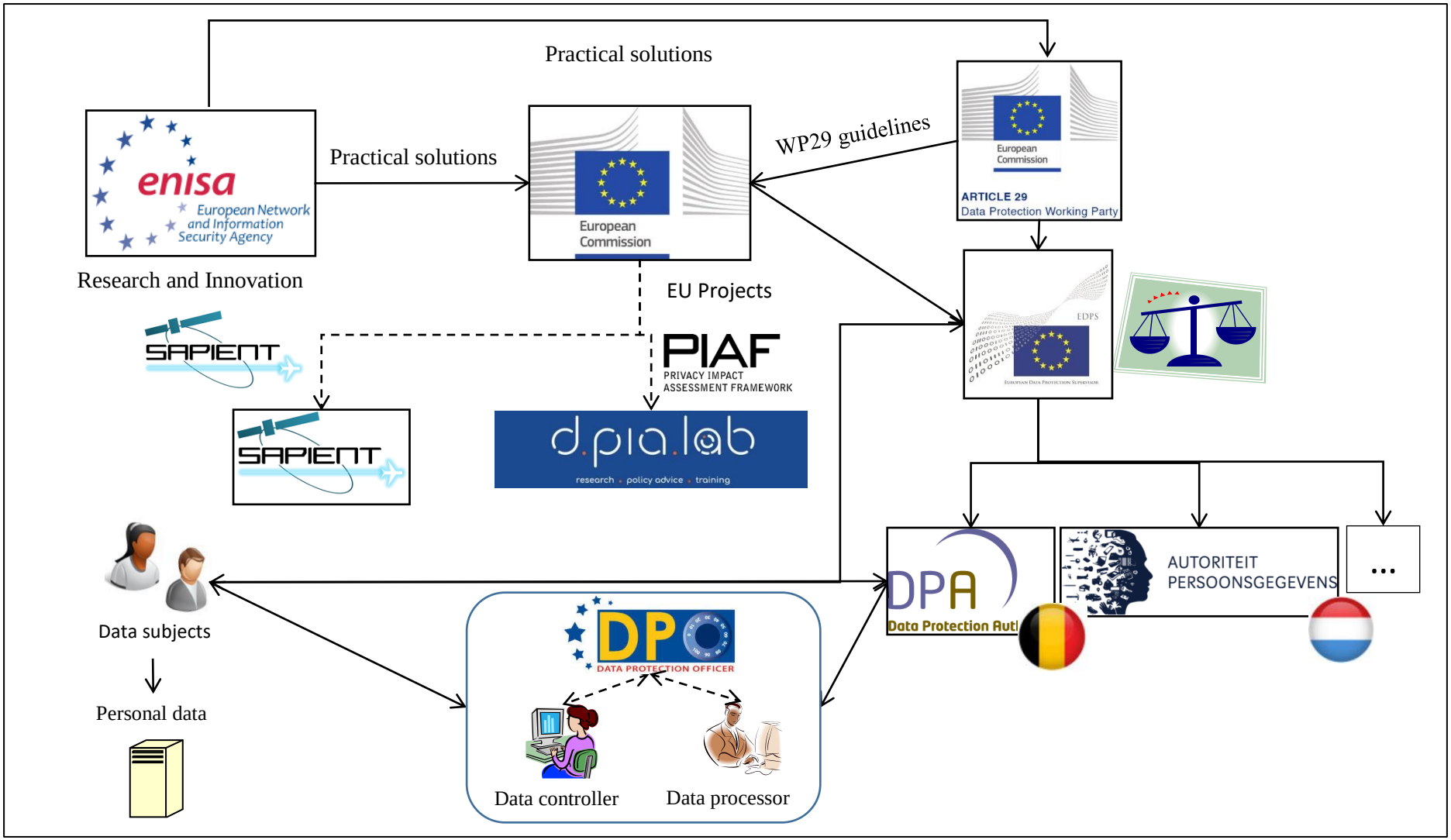
The search for influential literature pertaining to the GDPR/DPIA and the harmonisation goal was conducted in two different ways

On the one hand, official documents were consulted for information about the GDPR/DPIA. These documents could be identified by studying the relationship between the structure of the official organisations involved in the GDPR (point 7) and the publications of GDPR (point 8)

On the other hand, the harmonisation aspect was addressed by snowballing. An article was considered to be relevant if it contributed to answering one of the sub-questions. To determine this, the following steps were followed:

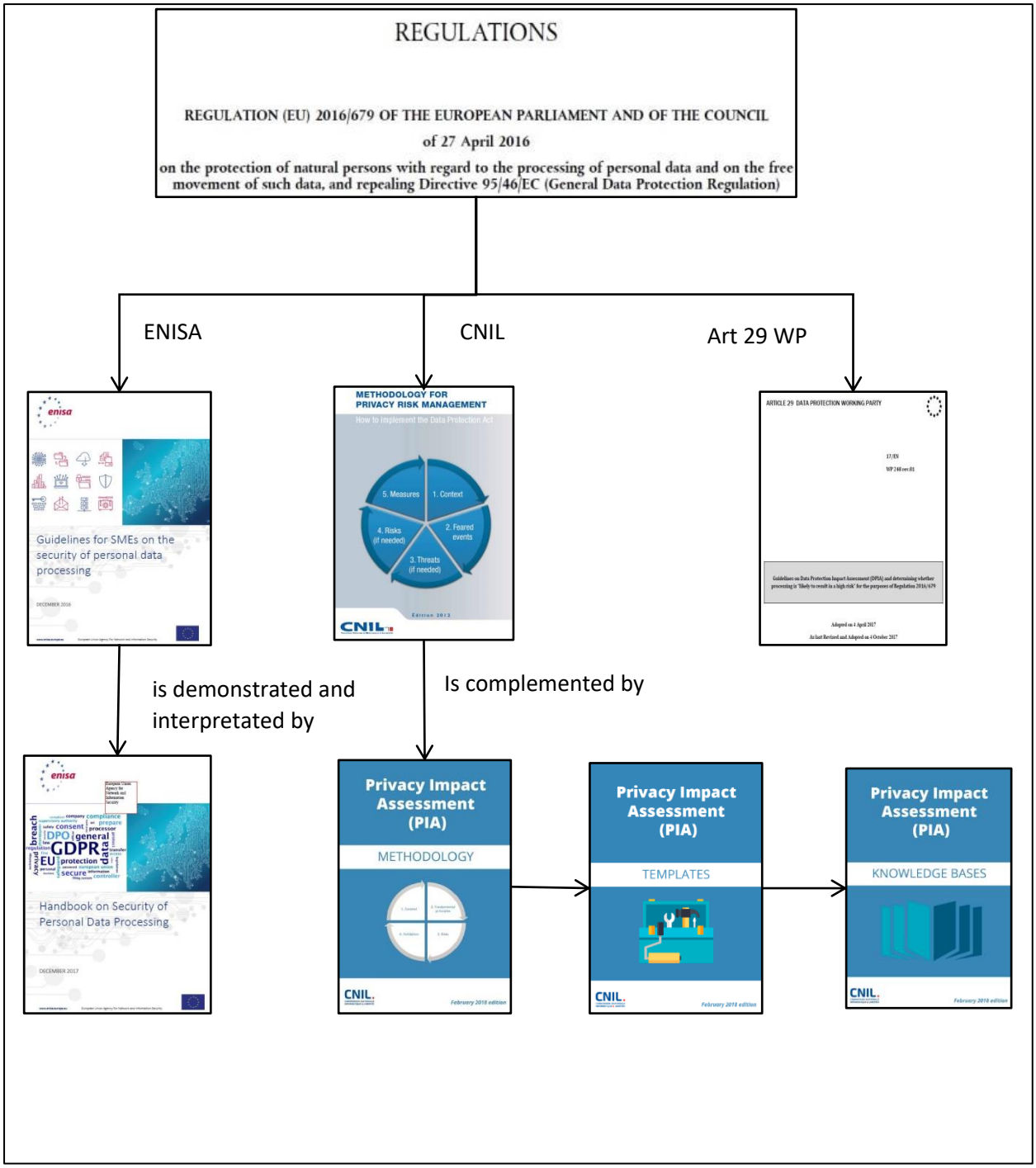
- First, consideration was given to the title, abstract and terms/keywords /entries/catchwords found in the text.
- If these related to the research topic, the whole article was read.

7. Structure of the official organisations involved in the GDPR



Source: own design

8. Relationship between publications



Appendix D: GDPR = minimum harmonisation

1. Preamble

The **preamble** states that:

> "*.....Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States* ***SHOULD BE ALLOWED*** *to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a* ***MARGIN OF MANOEUVRE*** *for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including* ***DETERMING MORE PRECISELY*** *the conditions under which the processing of personal data is lawful.* "

which means that the Regulation contains a clause explicitly stating that the Member States have some freedom in adopting the GDPR, as long as they accept the minimum conditions.

2. Recitals

Recital 10 of the GDPR offers the opportunity for diversity by stating:

> *"… Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation…. This Regulation also provides a* ***MARGIN OF MANOEUVRE*** *for Member States to specify its rules ….*"

3. Articles of the GDPR

Concerning the DPIA, **Article 35 of the GDPR**, entitled Data protection impact assessment, states:

> "*7. The assessment shall contain* ***AT LEAST****:....."*
> ....
> "*11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment AT LEAST when there is a change of the risk represented by processing operations*."

meaning that an organisation is at liberty to decide that an assessment should contain more elements and that a review of the processing should not only be carried out when there is a change of the risk represented by processing operations, but also in the case of other situations.

And **Article 39** - Tasks of the data protection officer - mentions:

> "*1. The data protection officer shall have* ***AT LEAST*** *the following tasks:...."*

meaning that an organisation is mandated to attribute more tasks to the data protection officer.

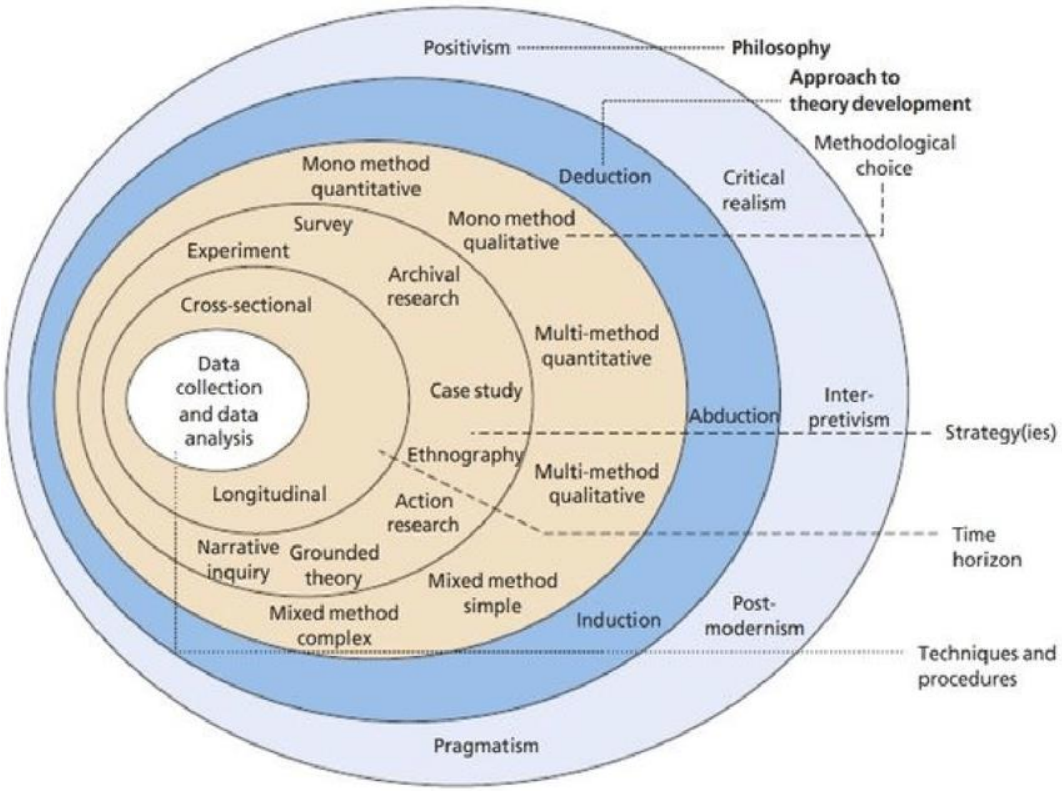
Appendix E: Research methodologies

This appendix contains a detailed elaboration of the DSRM and the research onion, both of which were applied in this research.

1. Research onion

The research onion (Saunders et al., 2016) describes the stages through which a researcher must pass in order to formulate an effective methodology.

This onion has six layers which have to be 'peeled off' in order to get at the core, which represents the data collection and data analysis.



For the purpose of this research, the following choices were made.

a. Research philosophy (layer1)

Saunders et al. (2016) define a research philosophy as '*a system of beliefs and assumpions about the development of knowledge in a particular field*'.

From research onion of Saunders, the five most commonly adopted research philosophies are positivism, critical realism, interpretivism, postmodernism and pragmatism.

Research philosophy	Description/Definition	Applicability to this study? Justification
Positivism	Works with an observable social reality to produce law-like generalisations.	- No. - The research question cannot be answered by observing social reality.
Critical realism	Explains what is seen and experienced in terms of the underlying structures of reality that shape observable events.	- No - The research question cannot be answered by observing events.
Interpretivism	Studies the meanings created by humans.	- No. - The GDPR/DPIA is not a meaning created by humans.
Postmodernism	Emphasises the role of language and of power relations.	- No - No language elements were involved in this study.
Pragmatism	Argues that concepts are only relevant where they support action. It considers research as starting with a problem and aiming to contribute practical solutions that inform future practice.	- Yes - Starting from the reality (the GDPR entering into force), this study focusses on the DPIA and aims to contribute practical solutions and outcomes concerning the (harmonised) conducting of a DPIA. - The research problem and research question tend to a pragmatic research philosophy.

For this study, pragmatism was retained.

b. Approach to theory development (layer 2)

Saunders et al. (2016) state that research commences from either a deductive or an inductive approach.

Approach to theory development	Description/Definition	Applicability to this study? Justification
Deduction	Approach to theory development whereby a theoretical proposition is tested through the collection of data.	- No - There were no hypotheses for this study..
Abduction	Aproach to theory development whereby data is collected to explore a phenomenon, identify themes and explain patterns, to generate a new – or modify an existing – theory which is subsequently tested.	No
Induction	Approach to theory development whereby a theory is developed as the data are collected and analysed.	- Yes - There is no clearly defined harmonisation/DPIA-framework which can be used as a starting point. - A research question and objectives were defined and served as a starting point for the development of a competent level of knowledge about the GDPR and the DPIA. - Data were collected using interviews with open questions designed to enable an understanding of each DPO's perception of the DPIA, such as how they cope with the problems and the possible impact on the harmonisation.

For this study, induction was retained.

c. Methodological choice (layer 3)

Methodological choice	Description/Definition	Applicability to this study? Justification
Mono quantitative method	One quantitative data collection technique and corresponding analytical procedure is used to generate or use numerical data.	- No - There were no numerical data available. - Quantitative research is usually associated with positivism, and, to a lesser extent, critical realism and pragmatism and with a deductive approach to theory development.
Mono qualitative method	One qualtitative data collection technique and corresponding analytical procedure is used to generate or use non-numerical data.	- Yes - Qualitative research is usually associated with interpretivism, and, to a lesser extent, critical realism and pragmatism and with a inductive approach to theory.
Multi-method quantitative method	More than one quantitative data collection technique and corresponding analytical procedure is used to generate or use numerical data.	- No - The multi-method quantitative approach was not appropriate because there were no numerical data available.
Multi-method qualitative method	More than one qualtitative data collection technique and corresponding analytical procedure is used to generate or use non-numerical data.	- Yes, this approach was possible.
Mixed method	A combination of quantitative and qualitative data collection techniques and corresponding analytical procedures are used.	- No - The mixed method approach was not appropriate because there were no numerical data available.

For this study, the mono qualitative method was retained.

d. Research strategy (layer 4)

Saunders et al. (2016) define a research strategy as '*a plan on how a researcher will go about answering her or his research question*' and distinguish the following research strategies for the execution of an empirical study: experiment, survey, archival and documentary research, case study, ethnography, action research, grounded theory and narrative inquiry.

These possible research strategies are listed below, together with their description and with an analysis of whether they were applicable for this study.

Research strategy	Purpose	Applicability to this study? Justification
Experiment	To study the probability of a change in an independent variable causing a change in a dependent variable.	- No. - Experiment is tailored for a quantitative research design and for exploratory and explanatory studies. - This research question could not be answered by executing an experiment.
Survey	The structured collection of data from a sizeable population using questionnaires, structured observation and structured interviews.	- No. - Survey is tailored for a quantitative research design and for exploratory and descriptive studies. - Survey is most frequently used to answer "what", "who", "how much" and "how many" questions. - The research question could not be answered by executing a survey.
Case study	The empirical investigation of a particular contemporary phenomenon within its real-life setting, using multiple sources of evidence.	- Yes - Case study is tailored for a qualitative research design. - Case study is most frequently used to answer "what", "how" and "why" questions. - The case subject of the paper is DPOs' perception of the DPIA.
Archival and documentary research	To analyse administrative records and documents as principal sources of data.	- No - The research question could not be answered by executing archival and documentary research.
Ethnography	To study the culture or social world of a group using field research.	- No - Ethnography is used for studying groups. - The research question could not be answered by executing an ethnographic study.
Action research	To obtain practical outcomes for a change of the organisational context and to generate knowledge/theory	- No - Action research is used for studying changes within an organisation. - Action research is most frequently used to answer "how" questions. - The research question could not be answered by executing an action report.
Grounded theory	To develop theoretical explanations of social interactions and processes	- No - Grounded theory is used for studying behaviour. - The research question could not be answered by executing a grounded theory study.
Narrative inquiry	To analyze the experiences of participants, using their narratives to interpret an event	- No - Narrative inquiry is used for studying events based on narratives. - The research question could not be answered by executing a narrative inquiry.

For this paper, the case study approach was retained.

e. Time horizon (layer 5)

Time horizon	Description/Definition	Applicability to this study? Justification
Cross-sectional	A particular phenomenon (or phenomena) are studied at a particular time.	- Yes - The interviews were conducted over a short period of time – namely, around 28 May, 2019, one year after the GDPR became enforceable in all Member States of the EU.
Longitudinal	A particular phenomenon (or phenomena) are studied over an extended period of time.	- No - Because this master thesis is constrained by time, changes and developments could not be studied.

For this paper, the time horizon is cross-sectional.

f. Techniques and procedures (layer 6)

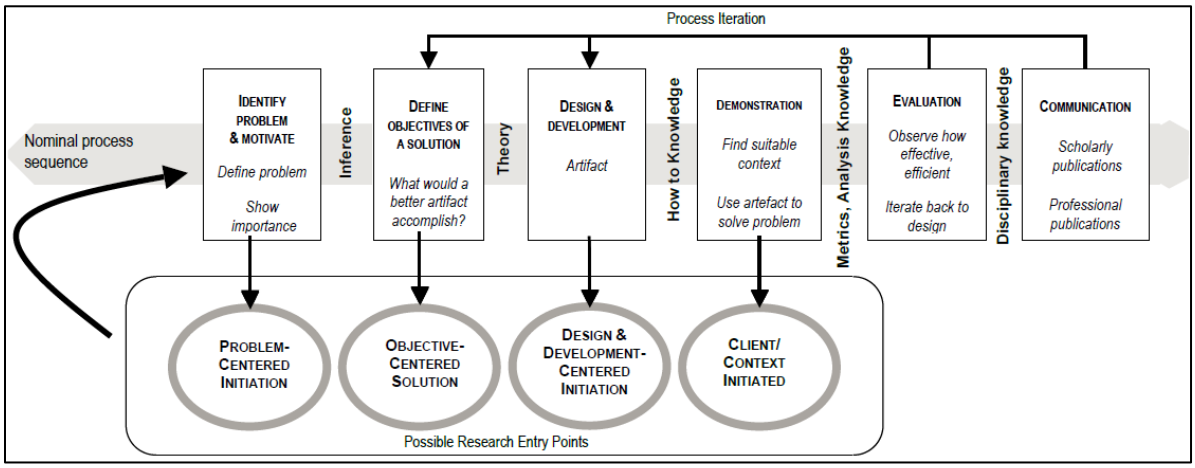
This concerns the data collection techniques and analysis procedures, but has not been elaborated in the scope of this study.

2. Design science research

The design science research methodology (DSRM) process model of Peffers et al. (2007) is a process model consisting of six activities organised in a nominally sequential order and covering the whole research from the start (Problem identification and motivation) to the end (Communication).

The six steps are as follows and are illustrated in the figure below:

1. Problem identification and motivation
2. Definition of the objectives for a solution
3. Design and development
4. Demonstration
5. Evaluation
6. Communication



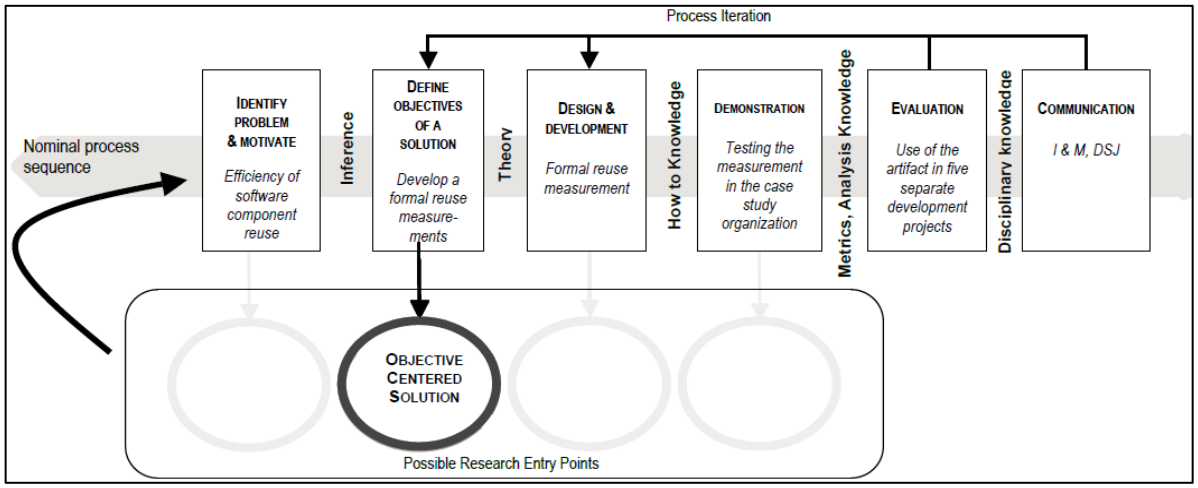
The fact that step three consists of the creation of the artefact and that this artefact (the DPIA) already exists does not make DSRM less applicable or less valid for this case. The study of the level of harmonisation can still be framed in light of the DSRM. As stressed by Peffers (2007), '*for design in practice, the DSRM may contain unnecessary elements for some contexts, while being much too general to support design in others*'.

The six-step process is structured in a nominally sequential order. However, there is no need to always proceed from activity one to activity six in a sequential order. Instead, four approaches/solutions are possible, depending on the starting point:

1. **Problem-centered approach** (starting with activity one): the research is triggered from the observation of a problem (e.g. finding a research gap in the literature).
2. **Objective-centered solution** (starting with activity two): the research can be addressed by developing an artefact (e.g. industrial projets).
3. **Design and development-centered approach** (starting with activity three): the research uses an existing artifact that has not yet been formally evaluated for the concerned problem domain.
4. **Client/context initiated solution**: the research starts with the observation of a practical solution that worked, and then the process is applied backwards (e.g. real-world consulting projects).

For this research project, the entry point is the “objective-centered solution”.

As the aim of this thesis was to improve existing methods, the approach for this paper resembles an objective-centered solution. So, the nominal sequence as indicated in the Figure below was followed.



Appendix F: Overview of the identified sectors

Based on PRIPARE (2014), ENISA (2017) and Giurgiu (2017), specific sectors dealing with specific data protection operations were identified. Those sectors can be considered as having specific data protection concerns, which could require a DPIA to be conducted or a DPO to be appointed.

The retained sectors have been classified based on the International Standard Industrial Classification of all Economic Activities (ISIC, 2008). This classification should facilitate the comparison between companies/sectors within the European Union in the context of further studies of the DPIA.

Some of these groups are not explicitly discussed in this paper. This is due to the fact that for certain groups no DPO could be interviewed (see also Appendix G).

Short name in this paper	ISIC		Specific data protection processing operations which could require to carry out an DPIA and/or to appoint a DPO*
	Code	Description	
Vehicles	C-29	Manufacture of motor vehicles, trailers and semi-trailers	
Public	O-84	Public administration and defence; compulsory social security	Large amount of (customer) data
Membership	S-94	Activities of membership organisations	
Retail	G-46	Wholesale trade, except of motor vehicles and motorcycles	- The overview of the goods and services bought by the customers may reveal sensitive data about their health and preferences relating to sexuality, politics and religion. - Intelligent data analytics on customers' data give insight into their consumption behavior, habits and preferences.
Finance	K-64	Financial service activities, except insurance and pension funding	
Insurance	K-65	Insurance, reinsurance and pension funding, except compulsory social security	
Publishing, Radio & TV	J-58	Publishing activities	- Marketing campaigns may reveal sensitive information about the customers' health, race or ethnic origin, and preferences relating to sexuality, politics and religion. - Intelligent data analytics on customers's data give insight in their consumption behavior, habits and preferences.
	J-60	Programming and broadcasting activities	
Telecom	J-61	Telecommunications	- Intelligent data analytics on customers' data give insight in their consumption behavior, habits and preferences.
Legal Consultancy	M-69	Legal and accounting activities	- Large amount of data - In the case of DPO-as-a-service, the risks are linked to the data protection processing operations of the concerned sector
	M-70	Activities of head offices; management consultancy activities	
Education	O-85	Education	A webplatform for the follow up of the students (contact information, school results) and for the communication between professors/administration and the students (announcements, digital course materials, assessments) may reveal sensitive data about the studens (health/disability/ ethnic background/religion).
Hospital	Q-86	Human health activities	The webplatform for the exchange and sharing of patients' health information reveals sensitive personal information. In the case of vulnerable categories of data subjects (e.g. data subjects with specific diseases or handicaps or minors) the loss of this information could constitute a very high risk for the concerned persons.

* The loss of confidentiality, integrity and availability of these data could constitute a high risk for the customers.

Appendix G: Overview of the contacted organisations and their response

This appendix gives a numerical overview of the contacted organisations , the interviewed organisations and their given reasons for not participating

The organisations are listed according to the ISIC.

Sector	Contacted	Interview	Raisons for not participating				Remarks
			Internal privacy guidelines	Too many request from students and too time consuming	Not the right person/ organisation	No answer (after reminder)	
Vehicle	05	00	01	00	00	04	
Retail	05	01	01	00	01	03	
Publishing	02	01	00	00	00	01	
Radio&TV	02	01	00	00	00	01	
Telecom	04	02	00	00	00	02	
Finance	07	01	01	01	00	04	
Insurance	13	03	02	01	01	06	
Legal	01	00	00	00	01	00	
Consultancy	04	02	00	00	00	02	One consultancy agency represented the membership company as a external DPO.
Public	01	01	00	00	00	00	
Education	04	01	01	01	01	00	Has been interviewed, but finally, not retained
Hospital	04	00	00	01	01	02	
Membership	01	00	00	00	00	00	Represented by Consultancy02
TOTAL (#)	**53**	**13**	**06**	**04**	**05**	**25**	
TOTAL (%)	**100 %**	**24,6 %**	**11,3 %**	**7,5 %**	**9,4 %**	**47,2 %**	
TOTAL retained interviews	**--**	**12**	**--**	**--**	**--**	**--**	

Appendix H: Overview of the interviewed organisations

Code derived from ISIC*	Description	Type DPO	Type of interview (number of interviewed persons)
Retail01	A retailer with tens of thousands of employees and millions of customers, offering different concepts in Belgium and some neighbouring countries.	Half-time Internal	Face-to-face (DPO and two collaborators)
Publishing01	A Belgian publishing and broadcasting company with more than 1.200 employees and a consolidated turnover of 277 million euros, offering newspapers, magazines and TV activities in Belgium, the Netherlands, and Germany.	Half-time Internal	Video-conference (DPO)
Radio&TV01	A Belgian broadcaster with globally more than 2000 employees, offering radio, television and online services	Half-time Internal	Face-to-face (DPO)
Telecom01	A Belgian telecoms company with more than 1.400 employees and more than 3 million clients, offering fixed and mobile telephony, broadband and TV to residential customers in Belgium, and on the other hand mobile and fixed telephony and broadband to business customers all across Belgium and Luxembourg.	Full-time Internal	Face-to-face (DPO)
Telecom02	A Belgian provider with more than 3.500 employees offering of on the one hand digital cable television and fixed and mobile telephone services to residential customers in Flanders and Brussels, and on the other hand voice, data and Internet services to business customers all across Belgium and in Luxembourg.	Full-time Internal	Face-to-face (DPO)
Finance01	A Belgian bank and insurance company offering financial services (attracting savings, granting loans, distribution of collective investments) and life and non-life insurance products.	Full-time Internal	Face-to-face (DPO)
Insurance01	Belgian branch of a French insurance Company with 200 employees, offering various insurance products to individuals, self-employed persons, companies, and institutions in Belgium. It distributes its products and services through a network of agents.	Full-time Internal	Face-to-face (DPO)
Insurance02	An independent Belgian health insurance fund with more than 600 employees and +/- 500.000 customers, offering reimbursement of medical costs, the payment of a replacement income, health insurance funds and supplementary insurance (such as hospitalisation insurance, dental care insurance and insurance for medical costs) in Flanders and the Dutch part of Brussels.	Half-time Internal	Face-to-face (DPO)
Insurance03	Belgian subsidiary of a French insurance company, having approximately 200 employees and offering roadside and travel assistance all over the world to over 200 000 clients, operating mainly in Belgium.	Half-time Internal	Face-to-face (DPO)
Consultancy01	Consultancy agency in the domain of compliance with 15 employees and different organisations as a client offering among other things “DPO as a service”.	Part-time External	Face-to-face (DPO)
Consultancy02	Lawfirm with three employees offering among other things “DPO as a service”.	Part-time External	Face-to-face (DPO)
Public01	Government organisation with 23.000 employees.	Part-time Internal	Written answers (DPO)
Education01	Adult Education Center specialised in language education.	Not a real DPO.	Face-to-face

* Organisations are listed according to the ISIC.

Appendix I: Semi-structured interview

1. For the preparation and execution of the interview, the guidelines of Saunders et al. (2016) were followed.

2. Justification for semi-structured interview:
   a. The semi-structured interview was chosen for this study. First, this approach made it possible to infer causal relationships between variables and to understand the reasons for the decisions that the DPOs had taken as well as their attitudes and opinions. Second, it made it possible to ask interviewees to explain their answers and to probe the meaning of specific words or ideas. Third, as privacy legislation is rather sensitive, it was important to establish personal contact with the interviewees. Furthermore, as DPOs from different organisations had to be interviewed, it would not have been meaningful to ask exactly the same questions to each interviewee (as would be the case with a questionnaire); in this regard, each organisation could have had a different approach to the questions surrounding the GDPR, the DPIA or DPOs. Nevertheless, many organisations responded similarly to many questions. Differences between the organisations could only be identified during the interviews. Thus, semi-structured interviews made it possible to adapt the questions while still ensuring consistency between the different interviews (Saunders et al., 2016).
   b. A qualitative study was chosen over a quantitative study as the aim was to explore, to explain and to provide insights rather than to provide statistical generalisations.
   c. Saunders et al. (2016) found that managers are more likely to agree to be interviewed rather than to complete a questionnaire, especially when the interview topic is seen to be interesting and relevant to their current work. This preference is due to the following reasons:
      - On the one hand, an interview provides the research participants the opportunity not only to reflect on events without needing to write anything down but also to receive feedback and personal assurance about the way in which their information will be used.
      - On the other hand, interviewees might be reluctant to complete a questionnaire because they do not feel it is appropriate to provide sensitive and confidential information to someone they have never met or because they have to provide written explanatory answers (if requested) when the question is not entirely clear.
   d. All data were gathered in real time (interviews), except for one case in which the questions were answered by mail due to an incompatibility of agendas.
   e. Furthermore, due to the complexity of issues to be covered (i.e. their number and variety), an interview was the best means of collecting data.
   f. As the topic (GDPR) is rather sensitive and as eight to ten organisations initially had to be interviewed, it could be expected that the response rate for a questionnaire would be much lower.

3. Preparation
   a. As qualitative research interview type the semi-structured interview has been selected.
   b. An interview protocol was established (see 6. Interview protocol).
   c. Regarding selection of the interviewees, an invitation email was sent to plausible DPOs, inviting them to take part in the interview. These DPOs belonged to companies which were

required to assign a DPO and to carry out a DPIA. Consequently, it was expected that they would have some expertise in DPIAs.

d. In order to increase the response rate, a reminder mail was sent out a few weeks after the initial request for interview. An evaluation of the final responses can be found in Appendix G). A positive response was received from 13 DPOs, a response rate of less than 25% (with reminder).
e. A pre-arrangement was made with the DPOs willing to do the interview to meet at an appropriate interview location (normally hosted by the interviewee) at a specific time (when the interviewee was under least pressure) for an agreed period (1.5 hours).
f. Prior to the interview, the website of the interviewee's organisation was browsed for organisational information about the topic of privacy in general and the GDPR in particular.

4. Execution
   a. The interview with the DPOs was carried out between end of April, 2019, and the beginning of June, 2019, using the interview protocol.
   b. Except for two interviews which involved two and three interviewees, all other interviews were conducted on a one-on-one basis, comprising myself and a single participant. One interview was conducted with two interviewees. The presence of two or more interviewees allowed divergent views.
   c. With the permission of the interviewee, the interview was recorded.
   d. During the interview, I avoided imposing my own beliefs and frame of reference through comments, tone or non-verbal behaviour (interviewer bias). Moreover, by establishing a personal contact, assuring anonymity and not seeking confidential information, I encouraged the interviewee to provide a full picture of the situation. I also did not name other organisations that had participated in the research or talk about the data obtained from the other interviewees (interviewee bias).
   e. The interview protocol can be found further under paragraph 6. Interview protocol.

5. Data treatment and data analysis
   a. The interviews were transcribed using a question-and-answer format in "clean verbatim" style, meaning that stutters, filler speech (um, uh), non-speech sounds (laughing, coughing, throat clearing) and false starts which were self-corrected by the speakers were removed; these elements did not constitute an added value for this study. Furthermore, slight edits to correct sentence structure and grammar were applied. Finally, irrelevant information, such as ordering coffee or answering an important phone call, was not transcribed.
   b. In order to make the transcripts easier to read, topic headings were put in capital letters, questions in *italics* and responses in normal font.
   c. Because some interviewees insisted on anonymity, the following procedure was followed:
      (1) The interviewed organisation is not mentioned in the transcripted interview (this transcription is not added to this thesis but was transferred to the Open University as a source).
      (2) Without mentioning the interviewed organisation by name, a description of the interviewed organisation is included in the thesis, with the name of the sector according to ISIC.
      (3) If reference is made in the thesis to individual results or answers from the interviewed organisation that are important in the elaboration of the results, these are also mentioned under the name of the sector according to ISIC.

(4) A separate “mapping table” was drawn up making the link between the interviewed organisation and the name of the sector according to ISIC (this was not added to the thesis itself, but it was transferred to the Open University as a separate source).

d. After transcription, the transcripts were presented to the interviewee for further adjustments, comments and final approval.
e. Afterwards, the whole data set was thematically analysed in order to answer the research question.

6. Interview protocol

As this paper is written in English, the interview protocol has been established in English. However, the interview itself can be held in Dutch, French or English depending on the agreement between the interviewer and the interviewee.

No currently available assessment tool for the harmonisation topic *was identified from the literature or from canvassing key opinion leaders in the field*. That is why a list of questions was specifically created for these interviews.

If possible and with the agreement of the interviewee, the interview will be recorded.
Duration: approximately 1,5 hours.

Part 2 contains general questions about the characteristics of the organisation, part 3 contains professional questions about the interviewee. The other parts test the insights of the DPO towards the GDPR/DPIA.

Interview questions and their correspondance to research questions

Topic list and questions

1. Introduction

Link with research sub-question: none

a. First, thank you for accepting the request for an interview.
b. I am currently following the Master's degree in Business Process Management and IT at the Open University of the Netherlands.
This master's degree is aimed at evaluating and improving the business processes and IT.
This interview is part of my master's thesis on the GDPR and more specifically on how the DPOs perceive the DPIA and the possible impact of this on the harmonisation objective of the GDPR.
c. I will explain how the interview will go:
d. The interview will last approximately 1,5 hours and consists of three parts:
(1) The first part contains some general questions about your organisation, about you as DPO, and the general perception on the GPDR.
(2) The second part focuses on the DPO and the DPIA and the harmonisation goal of the GDPR.
(3) The third part is a small theoretical 'case'.
e. If you don't know the answer to a question, that question will be skipped.
f. Of course you have also the right to decline any question I ask.
g. A word about confidentiality
(1) During the interview, no confidential information will be sought.
(2) In this context, it is absolutely not the intention to evaluate specific DPIAs within your organisation.
(3) In the context of my commitment to confidentiality, on the one hand, I will not name the other interviewees and I will not talk about the data I obtained from them and, on the other hand, I will not pass your name and your input to them.
h. Non-verbal reactions will not be registered.
i. If you agree, the interview will be recorded.
j. What happens after the interview:
(1) the text will be transcribed and sent to you for approval.
(2) The data collected during the different interviews will be analysed in order to find out how the DPOs perceive the GDPR/DPIA and to formulate some potential improvements.
(3) If you wish, you can remain anonymous.
k. Before we continue, do you have any questions or comments regarding this interview?

2. Characteristics of the interviewee's organisation

Link with reseach sub-question: Validity of the research study (were the right people interviewed?)

a. Which industry / sector does your organisation belong to?
b. What is the number of employees in your organisation?

3. Professional characteristics of the interviewee

Link with reseach sub-question: Validity of the research study (were the right people interviewed?)

Now some questions about you as a DPO.

a. What is your current role within the organisation?
b. Are you a full-time or part-time DPO?
If part-time, what is your other/main function/role within the organisation?
c. Are you an internal or external DPO for this organisation?
d. How long are you in place as DPO?
e. What are your tasks, activities and responsibilities in the context of the GDPR?
f. For your organisation, who are the data subjects, the data controllers and data processors?
g. How would you describe your function as DPO in relation to the data subjects, the data controllers and the data processors?
How would you describe your function as DPO in relation to the Data Protection Authority?
How would you describe your function as DPO in relation to the Data Protection Authority?
Do you work closely with the Belgian Supervisory Authority and the EDPB (European Data Protection Board)?
Do you have the impression that you were guided/supported by the Belgian Supervisory Authority and the EDPB?
h. Do you have theoretical knowledge of DPIA?

If Yes: How have you acquiered this knowledge? (Self-study/Autodidact; Online course; training, resulting in a certificate (ISO, ….)

4. <u>The DPO's organisation and the GDPR</u>

<u>Link with research sub-question:</u>

a -> f: SQ6: What are DPOs' current practices and views on the GDPR/DPIA?

g: Validity of the research study (were the right people interviewed)

a. Generally speaking, has the corporate strategy changed since the introduction of the GDPR?

b. Are there specific threats/vulnerabilities for your organisation/sector in the context of the GDPR?

   If Yes: What could be the impact and consequences? E.g. current and emerging technologies which can have an impact on privacy and other fundamental rights? Have specific measures been taken in order to reduce the risks?

c. Are there also certain advantages to the entry into force of the GDPR?

d. Is your organisation already 100% GDPR-compliant?

e. What are the biggest practical problems in getting GDPR compliant?

f. Besides the GDPR, are there currently specific laws or private initiatives at national or European level concerning privacy in your sector?

   If Yes: Which ones? Do some of these sector-specific rules present inconsistencies with the GDPR and in which case does the GDPR prevail?

g. Why does your company or sector have to appoint a DPO? Based on which article/guideline of the GDPR?

5. <u>DPO's perception on the GDPR in general:</u>

<u>Link with research sub-question:</u> SQ6: What are DPOs' current practices and views on the GDPR/DPIA?

a. What is your general opinion about the GDPR?

b. Do you have the impression that the GDPR in general contains some points and concepts which are unclear and can be interpreted differently by you and a collegue DPO and so need to be clarified in the future?

c. Has the GDPR changed your way of working in comparison with the period before the GDPR?

6. <u>DPO's perception on the DPIA</u>

<u>Link with research sub-question:</u> SQ6: What are DPOs' current practices and views on the GDPR/DPIA?

We have just treated your perception as DPO on the GDPR in general. What follows are a few questions about your perception as DPO on the DPIA itself.

a. What is your general view on DPIAs?

b. From your point of view, what makes a good DPIA?

c. According to the GDPR, a DPIA is required whenever processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA is required <u>at least</u> in the following cases:

   (a) a systematic and extensive evaluation of the personal aspects of an individual, including profiling;
   (b) processing of sensitive data on a large scale;
   (c) systematic monitoring of public areas on a large scale.

   Which case is applicable for your company/sector?
   The GDPR mentions the expression "At least" three cases, so there may be more cases. In your opinion, are there other cases for which a DPIA is/should be required, in general and for your organisation?

d. What do you think about the vague terminology used in the GDPR: 'high risk', 'likelihood', 'large scale'…..

   The GDPR does not define the notion of "risk" or "high risk", it only provides some examples of processing situations where such an assessment should be carried out. What is your opinion about that?

e. The GDPR establishes the general requirements where a DPIA must be conducted. Member States may impose additional requirements where they believe a DPIA is necessary. Additionally, the supervisory authority of each Member State must make and publish lists regarding what types of processing require DPIAs and what kind of activities do not.

   What do you think of that?

f. Are there specific opportunities and challenges for your sector in terms of conducting a DPIA?
   If not already treated: One of the objectives of a DPIA is to 'strengthen the confidence of customers or citizens in the way personal data is processed and privacy is respected'. How can a DPIA 'strengthen the confidence'?
   Do you see it as a burden or do you see it as an advantage in order to increase your competitiveness on the market by acting in a data protection friendly manner?

g. According to Art 39 of the GDPR, conducting a DPIA is one of the tasks of the DPO.
   (1) What is your point of view on that?
   (2) Do you consider it as your main task?

h. We have already spoken about the theoretical knowledge of conducting a DPIA.
   But you also have practical experience with conducting a DPIA.
   Do you have practical experience with conducting a DPIA?
   (1) If Yes:
      (a) The DPIA has been conducted based on which article of the black and white list of the former Privacy Commission?
      (b) What was your experience?
      (c) What are the results ('lessons learned') of the earlier performed DPIAs which could be used in order to improve the future DPIAs?

i. DPIA of reference
   (1) Have you created your own one or do you use a DPIA template published by a national data protection authority or another organisation?
   (2) What are the advantages or inconveniences of your template?
   (3) If already mentioned above: You are familiar with the French DPIA established by CNIL. I conducted a study myself and it became clear that the CNIL methodology was the only template that met all the requirements of the GDPR legislation. However, finally, you didn't choose this template. Why?
   (4) If not mentioned above: Are you familiar with the French DPIA established by CNIL?

j. DPIA report
   Besides conducting a DPIA itself, you have also the DPIA report. Are you in favour of a DPIA report being published so that it is accessible for everybody?
   Have you published your own DPIA report?

k. Codes of conduct
   The GDPR also treats the codes of conducts. Are there currently national or European codes of conduct in your sector?
   If yes, could this code of conduct facilitate the execution of a DPIA?
   If No, do you think that a national or European code of conduct in your sector should be necessary in order to facilitate the execution of a DPIA?

l. Should the appointment of a single DPO or a single DPO-office for a group of undertakings facilitate the execution of a DPIA?

m. Do you cooperate with other organisations in the context of conducting a DPIA?
   How are the privacy-problems introduced and resolved?

n. Do you think that there is a need for a common template for conducting a DPIA, which would be applicable in an identical way in all sectors? (one size fits all)
   In how much detail should a DPIA be regulated?
   <Discussion>: Regulation of only core elements give a lot of flexibility to the Member States, but on the other hand, too much legislation could lead to a useless DPIA.

o. Are there local cultures or traditions in your sector that complicate the correct application and integration of GDPR/DPIA?

7. DPO's perception on the harmonisation goal of the GDPR

Link with research sub-question: SQ7: How is the harmonisation goal of the GDPR seen through the lens of the DPIA?

We have just treated your perception as DPO on the DPIA itself. Now we will focus on the harmonisation itself.

a. The GDPR has a double aim: first, establishing a legislation in agreement with the current and future technological trends. Furthermore, harmonising the different national privacy laws.
   A definition for harmonisation in the context of GDPR has not been found during the literature review, but what does harmonisation in the context of the GDPR/DPIA mean to you and to your sector specifically?

b. What are the enabling and disabling factors of the harmonisation goal of the GDPR/DPIA? Or, in other words, how can the harmonisation goal of the GDPR be influenced positively and negatively?

c. Are there points and guidelines of the DPIA which can be subject to interpretation or which are incoherent and which have to be solved in order to achieve a certain level of harmonisation?

d. We have already discussed a number of factors in the context of the conduct of a DPIA. Now we will focus on harmonisation. I will ask for all the following factors, how you perceive their impact on the harmonisation goal (positively, negatively, no impact)?

(1) The GDPR in the form of a regulation instead of the former directive.

(2) The vague terminology used in the GDPR: 'high risk', 'likelihood', 'large scale' and the absence of a definition of the notion of "risk" or "high risk".

(3) A close cooperation/guidance/support by the national privacy commission and the EDPB.

(4) A close cooperation/partnership with other organisations within your sector concerning the GDPR/DPIA.

(5) A national or European code of conduct in your sector.

(6) Local cultures or traditions in your sector.

(7) A common European template for conducting a DPIA, which would be applicable in an identical way in all sectors (one size fits all).

(8) The mandatory publication of a DPIA report.

(9) A kind of certification (ISO,...) regarding the GDPR/DPIA/the formation of DPO.

(10) The GDPR allows having either an internal DPO (who is a staff member of the data processor) or an external DPO (who is hired based on a service contract). Might an external (and thus more independent) DPO facilitate the harmonisation goal?

(11) The appointment of a single DPO for a group of undertakings.

(12) Do you think that if one Member State requires a stricter privacy protection than another Member State, this may in the long term have a positive or negative impact on harmonisation?

8. Case

Link with research sub-question: SQ6: What are DPOs' current practices and views on the GDPR/DPIA?

A final item concerns a fictive case.The aim is to have an open discussion with you. It is a hypothetical case, so not focused on your organisation.
You are DPO of a company based in Belgium. A new application is being implemented by a company based in the Netherlands with Data Centres in the US. The application stores personal data relating to employees, staff members and customers and is NOT meant to process special categories of data referred to in Art. 35 paragraph 3 GDPR on a large scale. It is only meant to enable staff members and customers to organise birthday parties and wedding anniversaries. To be able to use the service, date of birth, wedding date and gender of the staff members are introduced in the application via an interface with the human resources application. Missing and additional information such as allergies etc are filled in by the staff members and customers. The staff members and customers also need to provide their phone number, etc..
You are the project owner for this service.

a. If this case should emerge within the company, what would be your first reflex?

b. Should a DPIA be conducted or not? Why?

c. How should the DPIA be performed, from start to finish?

d. What measures should be taken and how should those measures be managed?

e. Should there be a difference if the data subject has given explicit consent to the processing of his or her personal data for one or more specific purposes?

Still the same case. Suppose that during the testing phase, one of the testers emailed accidently some unencrypted personal test data to a wrong recipient. These test data are a copy of the production data and included names and addresses.

a. Can this be considered as a data breach compromising the data subject's personal data?

b. What are the key considerations for the actions to be undertaken?

c. Could this have been avoided with a DPIA?

Are there aspects of this case which could be interpreted differently by other DPOs?

9. Closing remarks

Link with research sub-question: none

a. We have reached the end of the interview.

b. As a feedback for me, what do you think about the interview?

c. Do you think we have considered all the important aspects of DPIA/harmonisation? Is there something missing?

d. Do you have any additions to what we have discussed?

e. What could be improved in the following interviews?

f. Do you think that an online questionnaire instead of an interview would have been better?

g. Concerning the way ahead: a full record of the interview will be compiled. You will receive this record so that you can still check this for inaccuracies.

h. The response rate for the invitation mail was low.
Do you have an idea why?

i. Thank you for your time.

Appendix J: Transcription and coding of interviews

Due to their volume, the transcripted interviews and the corresponding coding have not been retained in this paper as an appendix, but are available at the Open University as a research source.