Designing a Process Deliverable Diagram for Privacy Impact Assessment integrated with a Privacy by Design Maturity Model

Hugo van Vliet [6205852], Friso van Dijk [Daily Supervisor], Matthieu Brinkhuis [First Exterminator], and Sietse Overbeek [Second Exterminator]

[·]Faculty of Science, Department of Information and Computing Sciences, Business Informatics, Utrecht University

September 2023

Abstract

Despite the presence of numerous Privacy Impact Assessment (PIA), there is an evident demand for a more flexible and all-encompassing framework that matches the changing data protection legislation and addresses the complexities of today's technological progress.

A PIA framework was crafted through a review of current scientific literature in this field. The method incorporated detailed coding of each step to guarantee a consistent and orderly progression. To amplify understanding and offer a graphical depiction of the process, a Process Deliverable Diagram was introduced. This Process Deliverable Diagram not only outlines the action sequence but also highlights the interconnectedness and results of each phase, presenting a complete perspective of the PIA procedure.

The result is a PIA method that is modular, adaptable, and fits into diverse organisational setups. This method provides clear directives and outlines the evolution of various growth phases.

This PIA method narrows the divide between legal mandates and real-world application, equipping organisations with a straightforward roadmap to attain data privacy conformity while at the same time help practitioners execute a PIA.

Keywords— Privacy Impact Assessment, Privacy-by-Design, Maturity, Information Science, GDPR, Process Deliverable Diagram, Data Protection Impact Assessment

Contents

List of Figures

List of Tables

Acronyms

DPIA Data Protection Impact Assessment. 4, 13, 16, 17

EDPB European Data Protection Board. 15

GDPR General Data Protection Regulation. 2, 4, 6–8, 12, 13, 15, 16, 56

PbD Privacy by Design. 6, 7, 10, 13, 14

PbDMM Privacy by Design Maturity Model. 8, 56

PIA Privacy Impact Assessment. 2, 6–9, 13, 14, 28, 56

1 Introduction

In the modern digital era, the storage and exchange of vast amounts of personal data online by individuals and organisations have led to heightened concerns about information privacy. Technological advancements have undoubtedly made information more accessible, but they have also introduced new risks and vulnerabilities for personal data [28]. Recognising information privacy as a fundamental human right is crucial in addressing these concerns. Article 12 of the Universal Declaration of Human Rights emphasise the importance of protecting personal information and the need for legal frameworks to safeguard individual privacy [6].

Breaches of information privacy pose significant risks and can result in severe consequences for individuals. A Pew Research Center study found that 64% of Americans have experienced a data breach or theft of personal information, and 79% are concerned about how businesses use their data [7]. Such breaches can lead to identity theft, financial loss, and damage to one's reputation. Moreover, data breaches may have broader societal implications, such as influencing election outcomes or facilitating cyber warfare.

To mitigate these risks, various laws and regulations have been enacted to protect personal data. In 2018, the European Union implemented the General Data Protection Regulation (GDPR), a comprehensive data protection law that mandates transparency, consent, and the right to be forgotten [85]. The GDPR has set a global standard for data protection, inspiring many countries to adopt similar legislation [51]. Non-compliance with the GDPR can result in hefty fines, such as Amazon's fine of 746 million euros for violating GDPR regulations [54]. Despite the potential for significant financial harm, many businesses remain unaware of or fail to understand the operational implications of the GDPR [82].

A key aspect of the GDPR is its emphasis on Privacy by Design (PbD) [85], a proactive approach to integrating privacy considerations into the design and development of systems, processes, products, and services involving personal data. PbD aims to prevent privacy breaches by ensuring data protection is an integral part of information systems and processes from inception [24]. To comply with the GDPR, organisations must conduct a Privacy Impact Assessment (PIA) before implementing new data processing activities that pose a potential high risk to privacy [85]. PIA is a systematic processes that identify and evaluate potential privacy risks associated with a specific project, system, or procedure. They involve assessing the impact of proposed processing activities on individuals privacy rights, identifying and evaluating privacy risks, and recommending measures to mitigate these risks [99, 25, 58]. By adopting these privacy-focused practices, organisations can proactively address potential privacy concerns and contribute to fostering a more secure digital landscape for all.

1.1 Gap in knowledge

Dr. Ann Cavoukian, the former Information and Privacy Commissioner of Ontario, Canada, first introduced the concept of Privacy by Design in her 2009 paper, "Privacy by Design: The 7 Foundational Principles" [23]. Subsequently, these best practices for privacy protection have been widely embraced, with Article 25 of the EU GDPR explicitly mandating data protection by design and by default.

PbD revolves around the seamless incorporation of privacy into the design and operation of any data processing system. This involves developing technical protocols

and tools, such as encryption and anonymization, to bolster data privacy [23]. As a result, PbD is characterised as "an engineering and strategic management approach that commits to selectively and sustainably minimise information systems' privacy risks through technical and governance controls" [78]. However, the realisation of PbD faces numerous challenges [78, 11, 10, 57, 2, 33], including:

1. Lack of awareness or understanding: A major obstacle for PbD is the insufficient awareness or comprehension of its implications among organisations. This can hinder the successful implementation of privacy protections from the outset [11]. In a later study [10], senior engineers perceived privacy requirements as burdensome, despite recognising the need to address them. Consequently, it is the lack of understanding, rather than a lack of awareness, that complicates the grasp of PbD.
2. Resistance to change: Organisations may be reluctant to alter their existing systems or processes to accommodate PbD principles, due to concerns surrounding cost, time, or implementation difficulty [57, 2]. [78] also noted that engaging management in privacy strategies presents significant challenges. High privacy standards can restrict data collection and usage for further analysis, constrain strategic options, and impact a company's bottom line, as selling this information becomes more challenging. Advocates for PbD often fail to acknowledge these economic realities.
3. Difficulty of implementation: The integration of PbD principles into systems and processes can be difficult, call for extensive resources and expertise. For instance, designing a system with privacy in mind may require proficiency in privacy law, data security, and user experience design [78, 33].
4. Inconsistent regulatory requirements: Different regulatory requirements for PbD across different jurisdictions can lead to confusion for organisations operating in multiple regions [70]. For example, the GDPR stipulates that companies offering goods or services to EU residents, even if not located within the EU, may still be subject to GDPR. This can prompt companies to test legal boundaries and risk sanctions for privacy violations to avoid business constraints [78].

In essence, PbD emphasizes the importance of embedding privacy protections into systems and processes from their inception. One method for assessing and addressing potential privacy risks is the PIA. PIA and PbD are complementary approaches to privacy protection. Organisations employ the usage of PIAs to systematically identify, assess, and effectively manage privacy risks that may arise from the collection, storage, utilisation, and disclosure of personal data [25]. Many organisations consider PIA to be a critical component of their data privacy and security strategies, and in many cases, they are mandated by law or regulation [32].

Although there is a considerable body of literature of the benefits and importance of PIA, there is a significant gap in research focusing on the specific process-level factors that contribute to the success of PIA at varying maturity levels. A systematic review of 159 articles by [37] concluded that there is a pressing need for the further development of methodological guidance for conducting PIA as required by the GDPR. This would help to establish PIA as a practical method for organisations and users with limited privacy and data protection knowledge.

There is much to discover about the maturity level of PIA practices within organisations and the frameworks outlined in the literature. To date, comprehensive studies

examining the current state of PIA maturity in organisations, the PIA frameworks presented in the literature, and the factors that contribute to the development of mature PIA practices have not been conducted. The aforementioned gaps in the literature underscore the importance of further exploration in these areas. A more thorough understanding of these issues would not only shed light on the characteristics of PIA but also enhance the effectiveness of privacy protection measures in an increasingly digital world.

1.2 Problem statement and objective

With the advancement of technology and the digitisation of various aspects of our lives, the amount of personal data collected and processed has skyrocketed [29]. While the benefits of this data expansion are numerous, it has also raised legitimate concerns about individual privacy and the potential misuse of personal data [12]. PIAs have been developed to evaluate the potential privacy risks of new initiatives and technologies before their implementation [99, 16].

However, despite the growing adoption of PIAs, there remain gaps in our understanding of their effectiveness, proper application, and the overall quality of their execution. One of the primary challenges is ensuring that PIAs are conducted in a comprehensive and meaningful manner, adequately addressing all relevant privacy concerns while providing viable recommendations to mitigate identified risks [16]. There's also a significant need for standardised guidelines and best practices to ensure consistency and quality in the application of PIAs [12].

In response to these challenges, this thesis sets out to delve into the Privacy Impact Assessment process. It aims to investigate its strengths and weaknesses and propose enhancements that can improve its effectiveness. The research will evaluate the current landscape of PIAs and explore PIAs for their refinement to better safeguard individual privacy and ensure compliance with relevant regulations. To assist organisations in developing a comprehensive and structured approach for executing a PIA, we are introducing an artefact that integrates with the Privacy by Design Maturity Model (PbDMM) [56]. This integration not only provides a clear roadmap from the initial stages of not having a PIA process to establishing a well-defined one but also empowers individuals to enhance and refine their PIA procedures over time. This approach ensures that privacy considerations are embedded from the outset, leading to more robust and effective privacy practices. This research objective aligns with the problem statement developed using the design science template proposed by Wieringa (2014) [94].

> **Improve** the PIA process and its deliverables for different maturity levels
>
> **by** designing an incremental PIA method integrated with the Privacy by Design Maturity Model (PbDMM)
>
> **that is** usable, satisfies the GDPR requirements, and displays a growth path through the maturity levels of the PbDMM
>
> **in order to** help organisations validate and incrementally improve their PIA procedures.

The findings will contribute to enhancing the efficacy and efficiency of the privacy impact assessment process. By doing so, it aims to support the protection of individual privacy rights and ensure stricter adherence to the relevant regulations. Policymakers,

privacy advocates, and other stakeholders will gain valuable insights into the effectiveness of PIA, as well as the obstacles that hinder their successful implementation. Moreover, this thesis seeks to bridge the knowledge gap in PIA, providing a comprehensive resource for those seeking to understand and improve the PIA process.

1.3 Thesis outline

In the next chapter, **Background**, concepts such as Privacy by Design, GDPR, and Privacy Impact Assessment will be explored. This section seeks to lay the groundwork, underscoring the relevance of the background investigation in relation to the central theme of the research.

In the **Research Plan** chapter, the research method and design will be explored, outlining the selected approaches for data gathering and interpretation. Ethical considerations undertaken during the research process will be highlighted.

In the **Domain Investigation** chapter, an examination of the domain relevant to the thesis topic will be conducted. The outcomes from initial research or exploratory studies will be showcased, and the current landscape of the domain will be assessed, identifying PIAs.

Subsequently, the **Privacy Impact Assessment Maturity Road Map** chapter will explain the idea of a maturity road map specific to PIA. This is achieved by integrating PbDMM into the newly developed artefact.

The chapter on **Privacy Impact Assessment Process Deliverable Diagram** will unfold the devised PIA PDD. An in-depth examination of this diagram will be conducted, detailing its elements and organisational structure.

Within the **Validation** chapter, the techniques employed to validate the Privacy Impact Assessment Process Deliverable Diagram will be detailed, along with the presentation of the validation outcomes. A discussion on the robustness and potential shortcomings of the artefact will be provided, and the implications of these results for the research will be explored.

The **Conclusion** chapter will encapsulate the pivotal findings and contributions of the research. Reflections on the research's impact will be offered, along with recommendations for future investigative paths and potential real-world applications of the research outcomes.

Lastly, the **Discussion** chapter will encompass an analysis and interpretation of the research findings. By comparing the study's results with existing academic literature, insights into the research's position in the wider academic field will be derived. The broader ramifications of the findings will be explored, and potential directions for subsequent research will be suggested.

2 Background

This section delves into the literature that forms the foundation upon which this study is constructed, providing a comprehensive understanding of related works that discuss the concepts of Privacy by Design, the General Data Protection Regulation, and Privacy Impact Assessment.

2.1 Privacy by Design

PbD is the practice of incorporating privacy concerns into the initial design of products, services, and systems. Ann Cavoukian, the former Information and Privacy Commissioner of Ontario introduced it in 1997. PbD aims to prevent data breaches and protect personal information by proactively incorporating privacy considerations into the design, development, and deployment of products and services. PbD is founded on the premise that privacy is an essential component of security and that privacy must be built into the design of information systems from the outset. This strategy aims to prevent privacy breaches before they occur, as opposed to attempting to fix them after the fact [23]. Dr. Cavoukian introduced the 7 Foundational Principles of Privacy by Design, outlined below [23]:

2.1.1 Proactive not Reactive; Preventative not Remedial

The initial principle of PbD underscores the proactive anticipation and prevention of privacy infringements prior to their occurrence, as opposed to responding to them in a retroactive manner. In order to effectively execute this idea, it is advised to consider the following three recommendations:

1. At the highest levels, there exists a distinct dedication to the establishment and implementation of privacy standards. The aforementioned criteria tend to surpass the regulations and laws set at the global level. [23].
2. The dedication to safeguarding privacy is evidently embraced by all user communities and stakeholders within a framework of ongoing enhancement [23].
3. Methods should be developed in a proactive, systematic, and innovative manner to identify inadequate privacy designs, anticipate unfavorable privacy practices and consequences, and effectively address any negative impacts well in advance of their manifestation [23].

2.1.2 Privacy as the Default

The responsibility for safeguarding privacy is not dependent upon individuals, as it is an inherent attribute of the overall system. In each given IT system or business operation, the personal information of individuals is automatically safeguarded. [23].

2.1.3 Privacy Embedded into Design

The integration of privacy into technologies, operations, and information architectures should not be seen as an afterthought, but rather approached in a creative and holistic manner. Therefore, privacy has a fundamental role in the essential operations [23].

2.1.4 Full Functionality – Positive-Sum, not Zero-Sum

The concept of full functionality in a positive-sum scenario refers to a situation where all participating entities experience advantages, and the collective gains surpass the collective costs. This stands in opposition to a zero-sum scenario, wherein the loss experienced by one party is balanced by the gain of another, resulting in an equilibrium of overall benefits and costs. Positive-sum scenarios are sometimes considered more desirable due to their ability to provide favourable outcomes for all involved parties. PbD effectively circumvents the occurrence of false dichotomies, such as the perceived conflict between privacy and security, by substantiating the feasibility and desirability of simultaneously achieving both objectives[23].

2.1.5 End-to-End Security – Lifecycle Protection

The concept of End-to-End security pertains to the implementation of a comprehensive security framework that ensures the protection of data at every stage of its existence. This implies that comprehensive security protocols are implemented starting with the inception of data, continuing throughout its many stages including storage, transfer, and utilisation, and concluding with its eventual disposal or archival. The End-to-End Security with PbD framework is a holistic approach that guarantees the safeguarding of personal data throughout its complete lifecycle. This is achieved by incorporating privacy protections into the system right from its first stages. [23].

2.1.6 Visibility and Transparency

This implies that the system and its privacy protocols are intentionally designed to facilitate users understanding of the processes involved in the collection, utilisation, and safeguarding of their personal information. This entails the provision of explicit and succinct privacy policies, facilitating user accessibility and control over their personal data, and ensuring transparency regarding the system's data collecting and processing methodologies. The importance of visibility and transparency is in their ability to empower users with the necessary information to make educated decisions regarding the utilisation of a system and to ensure its safe usage. Through the provision of visibility and openness regarding the data collection and processing procedures of the system, users are empowered to make informed decisions pertaining to the utilisation of their data and can afterwards undertake appropriate measures to safeguard their privacy. [23].

2.1.7 Respect for User Privacy

The notion of PbD places significant importance on protecting user privacy. The focal point of this security method rests in the prioritisation of safeguarding personal data starting from the initial phases of system design and development. The process entails adopting proactive measures to safeguard personal data, as opposed to adopting a reactive approach by responding to privacy breaches after they have transpired [23]. These principles conclude that PbD can be defined as "a pro-active engineering and management approach that is committed to selectively and sustainably minimise information systems' privacy risks through technical and governance controls" [78].

2.2 GDPR

On the 27th of October 1995, The European Data Protection Directive (Directive 95/46/EC) was adopted [63]. This Directive regulates the processing of personal data and is the first step in protecting the personal data of European citizens. However, the Data Protection Directive fell short of its goals and failed to standardise data protection across the EU. Therefore, the Directive required improvement [88]. As a result, the Commission adopted its proposal for a General Data Protection Regulation, abbreviated GDPR, in January 2012 [27]. The Regulation's dual purpose is to improve business opportunities by easing the free flow of personal data on the digital market and strengthening individuals' data protection rights. Directive 95/46/EC is repealed as of the 25th of May, 2018, which is the effective date of the GDPR [32].

The GDPR has two crucial distinctions: the controller and the processor. The GDPR defines the controller as follows: "a natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data," and the GDPR defines the processor as "a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller" [32]. The primary distinction between the two is that a controller holds the responsibility for ensuring compliance with the GDPR regulations, while the compliance responsibility as a processor is more limited.

The GDPR outlines six fundamental principles that organisations must follow to comply with the regulation: Fairness, lawfulness, and transparency; purpose limitation; data minimisation; Accuracy; storage limitation; Integrity and confidentiality; but data protection by design and default is at the heart of the GDPR [39]. By adhering to these six principles, organisations can guarantee that they process personal data in accordance with the GDPR and in a manner that respects individual privacy and data protection rights.

Fairness, lawfulness, and transparency The data subject must be informed of the nature of the processing (transparency), the processing must correspond to this description (Fairness), and the processing must serve one of the purposes specified in the regulation (lawfulness) [32, 85, 46, 22].

Purpose limitation Personal information must be collected for specified, explicit, and lawful purposes, and it must not be processed in a manner incompatible with those regulation [32, 46, 22].

Data minimisation The Regulation stipulates that any personal data you collect or process must be "adequate, relevant and limited to what is necessary for relation to the purposes for which they are processed" [32, 46, 22]. This implies that organisations should hold no more data than strictly necessary.

Accuracy The GDPR fourth principle stipulates that personal data must be accurate and up-to-date. Organisations must take reasonable measures to ensure the accuracy of personal data and must rectify or delete any inaccurate information. In addition to being a good business practice, this safeguards the data subject from threats such as identity theft [46, 22].

Storage limitation The fifth principle of the GDPR stipulates that personal data should not be stored for longer than required. Organisations must establish data retention periods and delete or anonymize data when it is no longer necessary. Simply put, if you no longer need the data, delete it. As you should define a purpose for all data collection, determining when the data is no longer necessary should be straightforward [46, 22].

Integrity and confidentiality The sixth principle of the GDPR stipulates that personal data must be processed securely. Organisations must implement appropriate technical and organisational safeguards to prevent unauthorised access, modification, or destruction of sensitive data. Additionally, organisations must ensure that only authorised personnel have access to personal information. Even though violations of the other data protection principles can be detrimental to data subjects, their effects are typically limited. However, violations of this principle usually result in data breaches, which makes it very simple for supervisory authorities to prove that data was not held securely – the mere fact that a data breach has occurred is compelling evidence [46, 22].

While the GDPR is a regulation of the European Union (EU) that is directly applicable to all EU member states, individual countries may have some latitude in implementing the regulation. This is due to the fact that the GDPR permits member states to implement additional laws and regulations to supplement its provisions. For instance, the GDPR allows member states to impose additional requirements and conditions on processing personal data for scientific research, archiving in the public interest, and statistical purposes. Member states may also impose additional restrictions on using sensitive personal data for scientific research, such as health information. In addition, the GDPR permits member states to implement specific provisions regarding processing personal data by public authorities and other organisations for public interest or legal obligations. While the GDPR allows member states some leeway to introduce their additional laws and regulations, these laws and regulations must still comply with the GDPR provisions. This means that any additional laws or regulations must maintain the protections provided by the GDPR and not contradict the GDPR fundamental data protection principles [46].

2.3 Privacy Impact Assessment

PbD is an approach centred on the principle of proactively embedding privacy into the design and operation of IT systems, networked infrastructure, and business practices. The core premise is that privacy assurance must ideally become an organisation's default mode of operation [23, 75].

The practical realisation of PbD and Data Protection by Design (DPbD) is intertwined with the concept of a PIA. A PIA is a structured process used to identify and mitigate the potential privacy risks associated with a given program, policy, or technology [81, 100]. It solidifies abstract notions of privacy into tangible privacy risks, thereby necessitating the development of robust PIA and management strategies [77].

Since the introduction of the PIA and particularly since the GDPR made Data Protection Impact Assessment (DPIA) compulsory, a variety of guides, methodologies, and templates have been published. These resources are intended to assist data controllers and their organisations in carrying out PIA and DPIA effectively. However, the quality and comprehensiveness of these tools can vary significantly, which can potentially impact the effectiveness of the assessments [25].

This variance in quality and comprehensiveness of available resources leads to the first Research Question (RQ) 1: What is the state-of-the-art of literature about PIA process steps and deliverables? This question aims to critically examine the existing body of literature on PIA process steps and deliverables. It seeks to understand how these steps and deliverables have been conceptualised, operationalized, and evaluated in the literature. By exploring this question, the research aims to identify best prac-

tices, gaps, and opportunities for improvement in the PIA process and deliverables, contributing to more robust and effective privacy protection.

2.3.1 Privacy by Design Maturity Model

Maturity models consist of multiple stages or levels, each representing a progressive level of process sophistication. These levels are defined based on particular characteristics that reflect the maturity of the process. The purpose of using a maturity model is to provide organisations with a benchmark against which to evaluate their current state, establish goals for improvement, and monitor their progress over time [93]. Numerous types of maturity models have been developed over time, each tailored to a specific business or technology domain [9]. Muszynski, M. (2023) wrote his thesis, titled "Focus Area Maturity Model for Privacy by Design" [56, 55], which introduces a comprehensive maturity model that aims to evaluate and improve an organisation's Privacy by Design practices. The model consists of fourteen focus areas and sixty capabilities spanning ten maturity levels. Among these focus areas are the PIA process and the PIA report. Table 1 illustrates the focus area maturity model for PbD.

The focus area maturity model for PbD incorporates multiple focus areas that are integral parts of managing and maintaining PbD in an organisation. The model is laid out on a maturity level scale from 0 to 10, with 0 indicating no presence or attention to the focus area (represented by the symbol $\otimes$), and higher numbers indicating more mature and sophisticated practices. The letters (A, B, C, D, etc.) represent milestones or specific actions taken within a focus area to improve maturity. Each focus area (row in the matrix) has a number of capabilities, represented by consecutive letters, always starting with A. The one thing all A's have in common is that they are the first capability of their respective focus area. Each focus area progresses dependently, indicating that capabilities that depend on other capabilities are placed in a later column. For example, as shown in Table 1, capability A for the PIA report is introduced at maturity level 3 because it is dependent on the implementation of other capabilities in different focus areas.

Table 1: Privacy by Design Maturity Model [56]

	Maturity level										
Focus area	0	1	2	3	4	5	6	7	8	9	10
1. Requirements	⊗	A		B	C	D					
2. Architecture	⊗		A	B	C			D			
3. Development	⊗	A	B			C	D			E	
4. Technology	⊗	A				B		C	D		E
5. PIA Process	⊗		A	B	C	D	E		F		
6. PIA Report	⊗			A	B		C	D			
7. Risk management	⊗			A	B	C		D			
8. Processing principles	⊗	A	B			C		D			
9. Subject rights	⊗	A					B	C		D	
10. Transparency	⊗	A	B			C		D			
11. Third-party management	⊗		A		B		C				
12. Roles	⊗	A	B	C		D					
13. Awareness	⊗	A	B	C		D					
14. Monitoring	⊗					A	B	C	D	E	

2.3.2 Privacy Impact Assessment in GDPR

The General Data Protection Regulation (GDPR) created the European Data Protection Board (EDPB) as an independent body of the European Union (EU). The EDPB is responsible for ensuring that the GDPR is applied uniformly throughout the EU and for advising EU Member States, data controllers, and data processors on the interpretation and implementation of the GDPR. The EDPB is authorised to issue legally binding decisions and opinions on a range of data protection issues, such as the interpretation of the GDPR, the adequacy of data protection laws in third countries, and the imposition of fines and penalties for GDPR violations. The EDPB has issued a GDPR road map (Figure 1) with guiding principles to clarify the privacy impact assessment and promote a unified understanding of EU data protection laws [31].

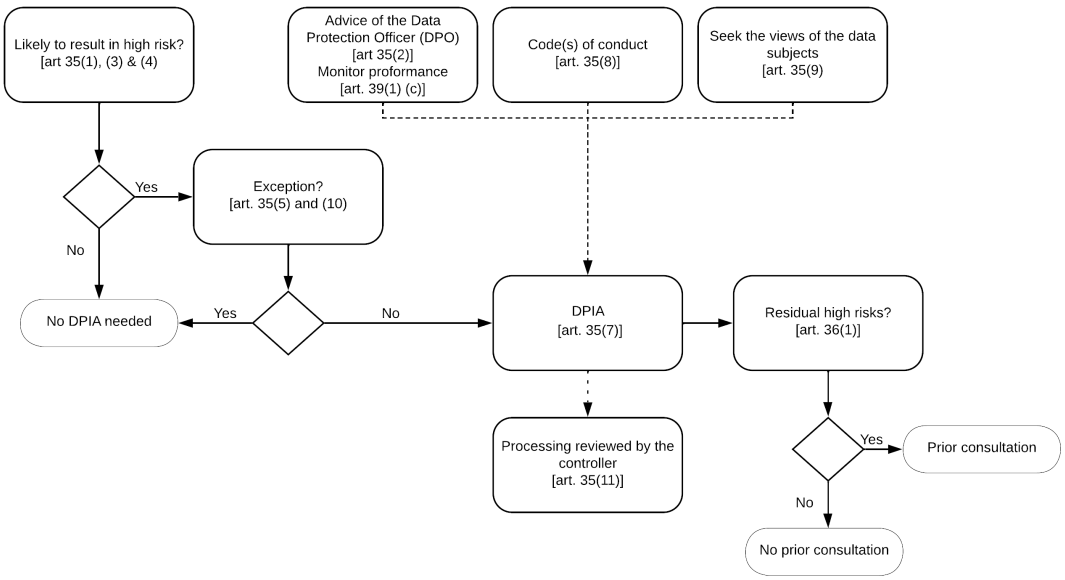


Figure 1: GDPR fundamental principles related to the DPIA [31]

The first step of the road map is determining whether a DPIA is required. The GDPR does not mandate a DPIA for every processing operation that poses a risk to individuals' rights and freedoms. Article 35(1), as illustrated by Article 35(3) and supplemented by Article 35(4), requires a DPIA only when the processing "is likely to result in a high risk for the rights and freedoms of natural persons" [85]. Article 35(1) stipulates that a DPIA must be conducted prior to processing personal data when it is likely that the processing will pose a high risk to the rights and freedoms of natural persons. This includes, but is not limited to, the use of new technologies or the processing of sensitive data at a large scale. In practice, controllers must continually assess the risks created by their processing activities to determine when a particular type of processing "is likely to result in a high risk to the rights and freedoms of natural persons" [85]. Article 35(3) provides; additional information on the content of a DPIA, stating that it should include a systematic description of the processing operations, an assessment of the necessity and proportionality of the processing, an assessment of the risks to the rights and freedoms of data subjects, and the measures in place to mitigate those risks. Article 35(4) requires authorities to compile a list of the types of processing operations which are subject to the requirement for a data protection impact assessment pursuant to article 35(1). If there is no likelihood to result in a high risk for the rights and freedoms of natural persons no DPIA is needed. The following procedure involves checking for exceptions. Article 35(10) refers to a document containing any decision-making processes related to the processing of personal data that pose a high risk to individuals' rights and freedoms. This documentation should contain a description of the processing activities, an evaluation of the processing necessity and proportionality, and an explanation of the measures taken to mitigate the identified risks. If the processing operation is on a list of exceptions (art. 35(5)) provided

by the supervisory authority, a DPIA is not required; otherwise, a DPIA is required. What a DPIA should at least contain is described in article 35(7). In cases where it is unclear whether a DPIA is required, the WP29 recommends conducting one anyway, as it is a useful tool for assisting controllers in complying with data protection law [31].

Article 35(7) does not provide specific instructions on how to conduct a DPIA, but it does provide four bullet points of what the DPIA should at a minimum include:

- a detailed description of the envisaged processing operations and purposes, including, where applicable, the controller's legitimate interest in the processing;
- an evaluation of the processing operations' necessity and proportionality in relation to the purposes;
- an evaluation of the risks to the rights and freedoms of data subjects as outlined in article 35(1); and
- the measures planned to mitigate the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

If in accordance with Article 35, the DPIA reveals that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller is required to consult with the supervisory authority prior to the processing (Article 36(1)). In practice, this means that consultation with the supervisory authority is required whenever a data controller cannot find adequate measures to reduce risks to an acceptable level (i.e., residual risks remain high) [31].

The subsequent chapter, **Research Method**, will delve into a detailed description of the research method employed for this study. It will outline the chosen approach, the various stages of the research process, and highlight the tools and techniques utilised. Additionally, the chapter will discuss how data was collected, analysed, and interpreted in the context of the study's objectives.

3 Research plan

In the forthcoming chapter, the research plan of this thesis will be detailed, serving as its foundational structure. This blueprint elaborates on the steps taken and the rationale behind each decision, aiming to provide the reader with a thorough understanding of the research process.

To begin with, the Research Questions will be presented. These questions dictate the direction and purpose of the entire study, setting forth distinct objectives.

After laying out the research objectives, the chapter transitions into the methodology, detailing the primary design method chosen for this study. This section offers insights into the selection of this specific method, ensuring the reader understands the systematic approach anchoring the research.

Following this overarching view of the methodology, the focus will shift to a more specific method design. By examining this particular method in detail, the intention is to highlight its significance within the broader research context.

Next is the literature research protocol. This section showcases the strategy employed during the literature review, from the criteria for selecting sources to the techniques used for analysis.

To emphasise the credibility of the findings, a section is devoted to the validation techniques used. This part strives to highlight the thoroughness of the research by outlining the various checks and measures instituted to confirm the results' reliability and validity.

Lastly, the ethical considerations associated with the study will be addressed. This part stresses the dedication to upholding the highest moral and ethical standards throughout the research. It will also touch upon any ethical challenges faced and the steps taken to ensure the study's integrity and responsibility.

3.1 Research questions

To address the knowledge gap, the problem statement, and the objective to structure the PIA domain, the following main research question (MRQ) is formulated:

MRQ: How to design a PIA process that is integrated with the PbDMM, that covers a constant review mechanism, is ongoing, and prevalent throughout the technology or system design life cycle by using incremental method evolution.

In order to answer the Main research question, the following Research Questions (RQ's) must be addressed.

> RQ 1: What is the state-of-the-art of literature about PIA process steps and deliverables?

This research question, seeks to identify the most recent and advanced findings in academic literature regarding the PIA process. Specifically, it focuses on understanding the latest methodologies and stages involved in conducting a PIA. Additionally, it aims to determine the expected outputs or documents produced as a result of this process.

> RQ 2: What are the process steps and/or deliverables per maturity level according to the PbDMM?

The research question, aims to explore the PbDMM [56] in depth. It specifically investigates the distinct stages or steps associated with each maturity level defined within the model. The goal is to understand how processes evolve or change as they progress through different levels of maturity in the context of the PIA.

> RQ 3: How does the revised PIA with an emphasis on incremental method engineering look like?

This research question is formulated with the intent of constructing an artefact that combines insights from both the literature study and the PbDMM. By synthesising information from these two primary sources, the aim is to produce a comprehensive and informed artefact that encapsulates the best practices and guidelines from existing knowledge, enriched with the structure and principles of the PbDMM.

> RQ4: How does the new re-designed PIA perform in practice?
>
> > RQ 4.1 How does the framework perform?
> >
> > RQ 4.2 What recommendations can be made?

This research question seeks to evaluate the practical application and effectiveness of the newly re-designed PIA. Specifically, RQ 4.1 delves into the operational performance of the framework, determining its strengths and potential areas of improvement. Meanwhile, RQ 4.2 focuses on deriving actionable recommendations based on the validation, ensuring that the PIA remains relevant and beneficial for its intended audience.

3.2 Design science

Design science focuses on the creation and examination of artefacts within their specific contexts [94]. It is an ideal methodology for studying artefacts in their natural environments, developing treatment designs, and validating these treatments. In this research, the artefact represents the PIA, while the context encompasses organisations mandated to conduct PIAs for their projects.

Wieringa (2014) engineering circle is presented in Figure 2 [94]. Design science research projects typically focus on the design cycle rather than the entire engineering cycle [64]. The design cycle, a subset of the engineering cycle, consists of three distinct activities: problem investigation, treatment design, and treatment validation.

During the problem investigation phase, the domain is thoroughly explored to facilitate treatment design by gaining a deeper understanding of the artefact requiring treatment. Once the problem is identified, a treatment is applied, and the artifact is (re)designed accordingly. The final step, treatment validation, involves evaluating the newly-created artefact to determine whether it effectively addresses the issue identified in the initial phase.

The design cycle is an iterative process, meaning that the output from one iteration serves as the input for the subsequent iteration. This cycle is repeated until the identified problem is resolved, and the established goals are achieved. This approach ensures continuous refinement and improvement, ultimately leading to more effective and robust solutions.

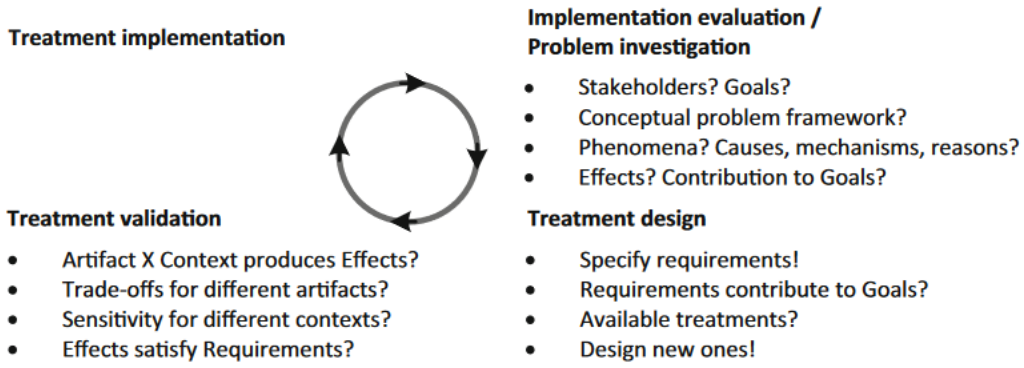


Figure 2: Engineering Cycle [94]

In Figure 3, an overview of the Research Questions in relation to Wieringa's Design Cycle phases is presented.

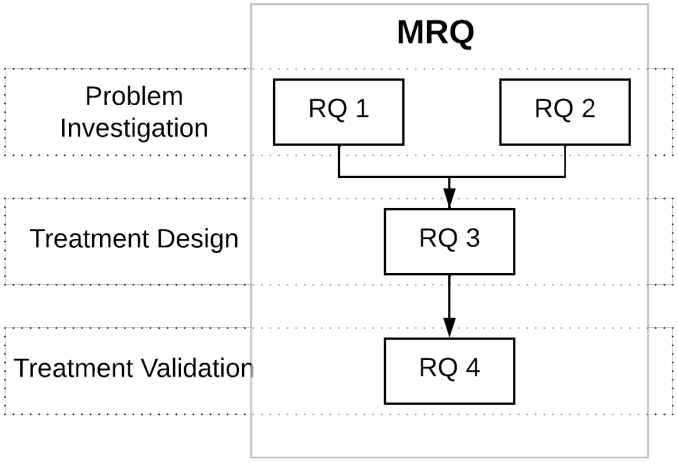


Figure 3: Research Questions Combined With Design Cycle Phases

3.3 Research Methods

The nature of our approach is demonstrated in Table 2, which presents a systematic alignment of each research question (RQ) with a corresponding research methodology.

To address Research Questions 1 and 2, we do a literature study, examining existing academic literature to acquire insights and enhance our understanding. Research Question 2 (RQ2) is specifically based on the PbDMM[56, 55], which offers a framework

to implement maturity levels into the artefact of this investigation. The ideas and conclusions obtained from the research questions RQ1 and RQ2 serve as a foundation for the creation of a new artefact.

In addressing Research Question 4 (RQ4), our primary research methodology involves conducting in-depth expert interviews. The decision to utilise expert interviews is intentional, as they provide a unique opportunity to go deeply into the subject matter and uncover nuanced aspects of the topic. Significantly, these interviews have a dual function: in addition to acquiring knowledge, they play a crucial role in validating our proposed framework, guaranteeing its resilience under examination and alignment with real-world expertise.

Each strategy employed in this study serves to enhance the overall quality and intricacy of our findings. The implementation of this method not only strengthens the validity of the results but also reinforces their trustworthiness and dependability.

Table 2: The research methods that are used to answer the RQs

Research Method	**RQ1**	**RQ2**	**RQ3**	**RQ4**
SLR	X	X	X	
Expert interviews			X	X

3.4 PIA method design

Method Engineering is defined as "[...]the engineering discipline to design, construct and adapt methods, techniques and tools for the development of information systems" [20]. Like for most methods there is not something as "one size fits all" [21], thus necessitating the creation of situational methods. These are methods designed to cater to the unique conditions of each information systems development project [20, 40]. To craft these situational methods, one needs standard building blocks and guidelines, collectively known as meta-methods, that describe their procedural and representational capabilities [20].

Since Brinkkemper's work, various approaches to Method Engineering have been proposed. One such approach involves the use of mental models to comprehend the requirements of the Design Science Research Methodology [64]. A mental model, defined as a "small scale model can be constructed from perception, imagination, or the comprehension of discourse" [48], can aid in developing a holistic understanding of the processes and their outputs. To visually represent these mental models, a process-deliverable diagram (PDD) is an ideal tool [91].

However, it is important to note that PIAs, like all other processes, are context-dependent and no two circumstances are exactly alike. As a result, a PIA Process Delivery Diagram (PDD) is proposed. This approach allows for greater flexibility and accommodates changes as the project progresses [92, 91].

3.4.1 PDD legend

A Process Deliverable Diagram (PDD), consists of two diagrams that are integrated. The left-hand side consists of activities that are conducted. The activities are depicted using the UML activity diagram. On the right-hand side are the deliverables, theses deliverables, based on a UML class Diagram, are a result of the activities, connected

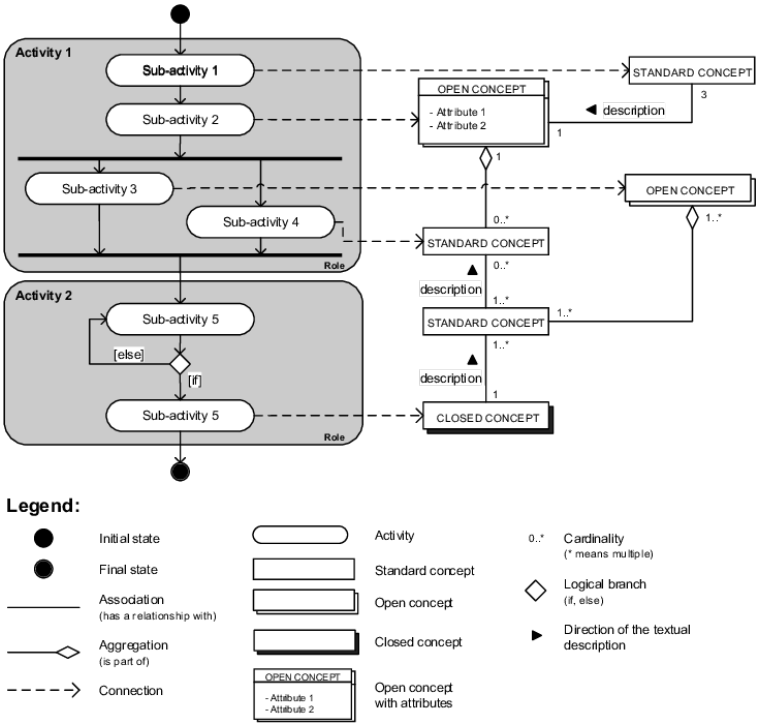
with a dashed line. These deliverables reflects the outcomes of the activity. Furthermore, the relationships among the deliverables including their cardinalities are shown, facilitating a holistic perspective.

Different shapes have different meaning when modelling a PDD. Activities are identified with a grey area whereas sub-activities are indicated by means of rounded rectangles. The diamond means that there is a logical branch based on a if-else structure, this lets a the actor decide between two courses of action based on whether a condition is true or false. In activity 1 there are two black lines. This means that the sub-activities can be executed parallel to each other but have both to be executed before continuing.

The deliverables – formally called concepts – are indicated by means of ordinary rectangles and have their names written in capital letters. There are three concepts namely, standard concept, open concept and closed concept There are three types of concepts: Standard concepts are fully defined within the PDD. Open concepts are defined in terms of other concepts. They are placeholders for more detailed definitions that are provided elsewhere. Closed concepts are a combination of standard and open concepts. Open concepts can also have attributes. This means that they can have additional information associated with them, such as a description, a value, or a list of relationships.

Furthermore, different relationship-arrows are distinguished. Fig. 3.4.1 provides an illustrative PDD and a legend of the used shapes, arrows and symbols. Input arrows (which concepts are required by an activity) are not shown, as all produced deliverables are assumed to be generally available. The activities (grey area) produces the sub-activities is partially captured by means of showing which types of actors are involved (right below: Role) [18, 20]

Figure 4: An example of a Process Deliverable Diagram including a legend [18]



3.5 Literature research protocol

Conducting a literature review is crucial for gaining a understanding of the existing body of research and establishing a solid foundation for the posed research questions. A structured approach to this task is facilitated by defining a literature research protocol. The literature review serves as the first step in understanding and analysing the context and forms the backbone of the subsequent research project.

3.5.1 PRISMA DIAGRAM

The PRISMA flow diagram [61] is utilised to identify relevant papers for inclusion in the literature review. By visually summarising the Systematic Literature Review process, the PRISMA flow diagram ensures transparency in the selection procedure, outlining the decisions made at various stages and recording the number of articles discovered. This approach enables future replication or repetition of the systematic literature review.

The PRISMA flow diagram records the number of articles at each stage. The first step involves identifying articles for review, which requires a comprehensive and reliable academic database. Numerous academic databases are available, such as Scopus, ACM, and IEEE Xplore. To make use of these databases, a search string must be formulated to find relevant papers for inclusion in the review.

The subject of this study is the PIA, which is often synonymous referred to as Data

Protection Risk Assessment. Consequently, both terms are entered into the search engine to ensure a comprehensive search. This results in the following search string, which is used as input for the search engine to identify articles relevant to the topic at hand:

`"Privacy Impact Assessment"` OR `"Data Protection Impact Assessment"`

The subsequent phase in the PRISMA flow diagram involves screening the academic databases. Table 3 outlines the inclusion and exclusion criteria employed for this process. Papers that do not contribute to answering the research questions are excluded, as well as those written in a language other than English. Furthermore, only publications from 1995 and on wards are considered. This time frame is selected based on the PIAs increasing prominence as a privacy tool from this point on wards [25]. Only papers satisfying all the inclusion criteria and not contravening any exclusion criteria are incorporated into the review.

Table 3: Inclusion and exclusion criteria.

Type	Description	Reason
Inclusion Criteria	Contributions published after January 1995	The PIA gained momentum as a privacy tool after that point
	Journal papers, conference papers	These documents are regarded as high-quality sources due to being subjected to a rigorous review process and provide accurate and reliable information.
	Contributions focusing on the PIA process and deliverable or similar frameworks	To study only articles relevant to the domains of interest.
Exclusion Criteria	Papers written not in English or Dutch	Numerous important research papers are published in English, which is the predominant language of scientific communication worldwide. This thesis is written at a Dutch government agency. Consequently, the Dutch language is included as well.
	Papers with no full-text version	A Systematic Literature Review requires reviewing the entire contents of a publication.
	Duplicated paper	All papers with the same title, keywords or content are excluded
	Paper shorter than four pages and posters	Typically, shorter papers lack the necessary depth to evaluate their contribution to the research question or topic under investigation. Without sufficient information, evaluating the paper's quality and relevance can be difficult.

In the identification phase of the PRISMA flow diagram, the previously mentioned

search string is used to query three scientific databases: 1) Scopus[1], a large abstract and citation database covering various scientific disciplines; 2) ACM Digital Library[2], a source of articles and conference proceedings in computer science and information technology; and 3) IEEE Xplore[3], a digital library for articles, conference proceedings, and standards in electrical engineering, computer science, and related fields. By employing multiple scientific databases, a more thorough literature analysis is achieved, which is crucial for high-quality research [13, 50, 19]. This approach provides several benefits:

Access to a broader range of scientific literature: Each database has unique journal coverage and publication indexing, so using multiple databases broadens the search and accesses more scientific literature [19].

Avoiding bias: Different databases may have varying editorial rules, indexing methods, and selection criteria, leading to diverse search results for the same query. Employing multiple databases reduces potential bias and offers a more comprehensive and balanced view of the research topic [73, 13].

Finding more relevant results: Leveraging several databases can help uncover more relevant results specific to the research question, as certain databases may specialised in particular fields or research areas [19].

The subsequent step involves analysing the papers discovered in the literature that provide processes and/or deliverables for PIA. This study employs A-priori coding, also known as "deductive" or "predefined" coding, is a type of qualitative data analysis where codes are established before the commencement of the analysis, typically based on theory, previous research, or the researcher's initial conceptual understanding of the phenomenon under investigation [17].

3.6 Treatment validation

The validation phase is crucial in the research process as it seeks to predict the real-world effectiveness of the proposed solution or treatment before its actual implementation. This phase, as described by Wieringa [94], is performed for a real-life problem. It doesn't rely on an existing real-world implementation but uses theoretical and practical insights to predict whether the proposed solution will contribute positively to achieving the stakeholders goals.

In Design Science Research (DSR), this validation phase corresponds to the build and evaluate activities, as conceptualised by March and Smith [65, 52]. The build activity involves creating an artefact that addresses the identified problem, while the evaluation activity assesses the artefact's ability to solve the problem. These activities align with Wieringa's engineering cycle [94], wherein the build and evaluation processes are iterative conducted until an optimal solution is achieved.

One common approach to validate an artefact in DSR, according to Wieringa [94], is to solicit expert opinion. Experts, with their extensive knowledge and experience, can predict how the proposed solution will interact with the problem context and give feedback on the anticipated effects. This method effectively uses experts as instruments to "visualise" the future application of the artefact and its potential impacts.

[1] https://www.scopus.com/
[2] https://dl.acm.org/
[3] https://ieeexplore.ieee.org/

If the predicted effects do not fulfil the requirements, the design cycle is repeated. This iterative process continues until the proposed solution is deemed to meet the stakeholders' needs [94].

To validate the PIA, this study will conduct in-dept interviews to gather the perspectives of key stakeholders. This will be instrumental in measuring the model's perceived usefulness and applicability in practical settings. The gathered feedback will also shed light on potential areas of improvement within the PIA.

The study will engage various stakeholders, including privacy professionals, data protection officers, system developers, and others who have either conducted or been a part of a PIA process in the past. A Dutch government organisation will be the recruitment ground for these participants. The objective of this is to conduct interviews with four distinct individuals to gather insights and perspectives on the matter at hand.

Interviews can take the form of structured, unstructured, or semi-structured approaches. The selection of a particular method should align with the research design and its capacity to address the research objective [30]. In the framework of this thesis, it is concluded that semi-structured interviews present specific benefits compared to structured or unstructured ones. Therefore, they will be utilised as the main data collection technique. An interview protocol will be developed to steer the interviews.

3.7 Ethics

Research ethics are vital guidelines underpinning the conduct of all scholarly investigations, ensuring responsible and integral execution. The primary goal of following ethical research principles is to safeguard participant rights, dignity, and well-being, while simultaneously expanding knowledge. These guiding principles often derive from established ethical codes and professional standards. Such codes encompass the Declaration of Helsinki, ratified by the World Medical Association, and the Ethical Principles of Psychologists and Code of Conduct, formalised by the American Psychological Association.

In this study, strict adherence to the 18 Principles for Ethical Social Research, as described by Vanclay et al. [86], is maintained. These principles provide a framework ensuring ethical research conduct, protecting participants and affirming the credibility of the findings.

This research avoids involving vulnerable groups or individuals, so no need arises for special procedures or considerations. Still, ethical principles remain consistently applied throughout the study. Details of the 18 Principles for Ethical Social Research, closely followed in this investigation, are available in Appendix A.1.

Moreover, the Ethics and Privacy Quick Scan will be conducted, a tool crafted for an all-encompassing evaluation of ethics and privacy in research[4]. This evaluation ensures the research upholds the pinnacle of ethical standards, respects privacy, ensures confidentiality, and complies with pertinent legal and institutional mandates. The Ethics and Privacy Quick Scan documentation is in Appendix A.2.

[4]For more details, visit: https://www.uu.nl/en/research/institute-of-information-and-computing-sciences/ethics-and-privacy

4 Domain investigation

The examination of the domain is composed of a systematic literature review (SLR), adhering to the PRISMA flow diagram, as delineated in section 3.6, titled "Literature Research Protocol". The objective of this SLR is to discover all accessible scholarly articles that detail the processes of PIA, employing a pertinent search string to facilitate the investigation. These PIAs are then subjected to a comparative and analytical process with the aim to enhance comprehension of existing literature solutions and to lay the groundwork for understanding what constitutes a PIA process.

4.1 Systematic literature review: Existing PIA processes

To facilitate an exploration of all relevant literature, the designated search string was entered across three distinct scientific databases. Upon introducing the search string into Scopus, a total of 254 papers were procured. Utilising the same string within the ACM database yielded a further 139 papers. Lastly, implementation of the search string within the IEEE database retrieved an additional 44 papers. This aggregates the total number of papers identified to 437. The citations corresponding to these papers were extracted and subsequently integrated into the reference management software, which possesses the capability to identify potential duplicates based on the criteria of title, author, and publication year. This action culminated in a generated list that was manually checked to affirm whether the identified papers were, indeed, duplicative in nature. Upon examination, it was ascertained that 54 papers were excluded due to their status as duplicates. Every paper was given an ID a entered into a excel sheet with the following information: Reference Type, Authors, Title, Publication Year, Links, URL and DOI. During the initial screening phase, the identified articles underwent a preliminary examination based on their respective titles and abstracts. If preliminary examination inferred that the paper potentially included a PIA process, it was subjected to a comprehensive review. Ultimately, this systematic literature review let to the inclusion of 41 papers that described a PIA process. The PRISMA flow diagram can be found in Appendix A.4. The subsequent table 4 provides a concise numeric summary of the papers that have been included in this review.

Table 4: PRISMA flow diagram in numbers

Scopus	254
ACM	139
IEEE	44
Total	437
Duplicate	54
Excluded	342
Included	41

The papers underwent a selection process based on pre-established criteria delineated in Table 3. Each inclusion and exclusion criterion is explicit and straightforward, with the notable exception of one specific inclusion criterion: "Contributions focusing on the PIA process and deliverable or similar frameworks". This criterion warrants a more nuanced interpretation, allowing for a degree of subjectivity in its application.

4.1.1 Descriptive statistics

As depicted in Figure 5, the frequency of published papers varies by year. A remarkable surge is evident from 2018 on wards, which aligns with a heightened interest in PIAs. This heightened interest was substantially influenced by the introduction of the European Union's GDPR in 2018.

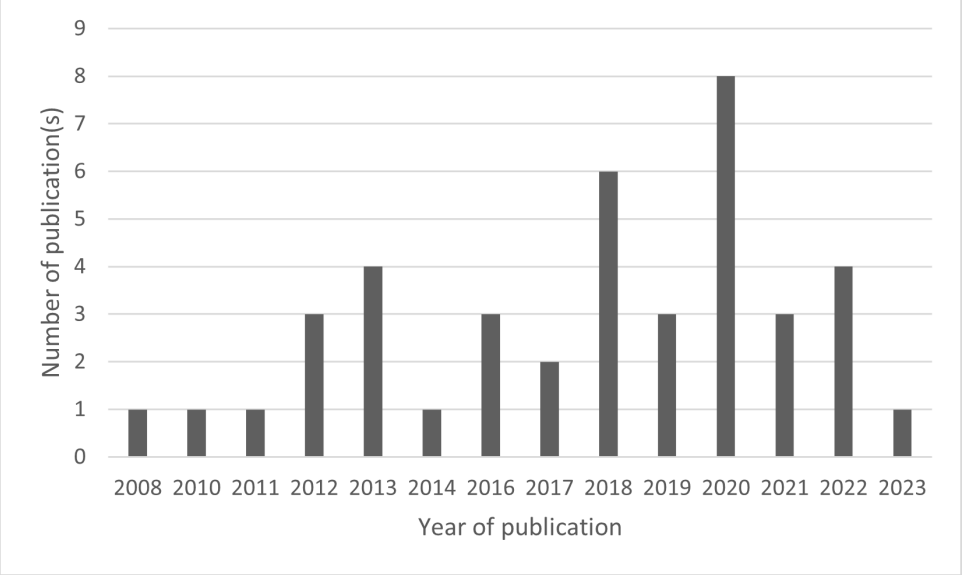


Figure 5: Distribution papers per year

4.2 Coding

A PIA should comply with the legal standards at a minimum. Compliance with data protection and privacy laws, including the GDPR in Europe, often requires fulfilling this obligation. Noncompliance may result in legal and financial sanctions, damage to the organisation's image, and loss of confidence from data subjects. Figure 1 provides an overview of the interrelation between the GDPR articles constituting the (minimal) PIA procedure. The analysis of the articles resulted in the identification of 13 steps in the PIA process. Optional process steps are outlined in the GDPR. Table 5 below summarises the GDPR Articles along with their respective subject and code.

Table 5: Minimum PIA process steps according to the GDPR

GDPR Article	**Subject**	**Code**
35(1), (3), (4), (5) & (10)	Threshold analysis	Threshold analysis
35(2)	Advice of the Data Protection Officer (DPO)	Advice of DPO
39(1) (c)	Monitor DPIA performance	Monitor DPIA performance

35(8)	Code(s) of Conduct	Code(s) of Conduct
35(9)	Seek the view of the data subjects	Consult data subjects
35(7)	Systematic description of the envisaged processing operations	Processing Description
35(7)	The purposes of the processing	Processing purpose
35(7)	The legitimate interest pursued by the controller (where applicable)	Legitimate interest
35(7)	Assessment of the necessity and proportionality of the processing operations in relation to the purposes	Necessity and proportionality
35(7)	Assessment of the risks to the rights and freedoms of data subjects	Risk assessment
35(7)	The measures to address the risks	Risk measures
35(11)	Processing reviewed by the controller (Where necessary)	Review by controller
36(1)	Residual High Risk	Residual High Risk

The initial set was employed to encode the first iteration. As a result of this process, we observed the subsequent distribution:

Table 6: 1st iteration PIA process codes with their corresponding appearances in process steps from 41 PIA processes

Code	**Number of occurrences**
Threshold analysis	25
Advice of DPO	4
Monitor DPIA performance	20
Code(s) of Conduct	0
Consult data subjects	1
Processing Description	119
Processing purpose	2
Legitimate interest	6
Necessity and proportionality	7
Risk assessment	123
Risk measures	106
Review by controller	26
Residual High Risk	2
Unclassified	122

After completing the initial iteration of the analysis, some of the process steps

were found to be difficult to categorise and remained therefore unclassified. These steps were distinct because they didn't fit into any of the initial categories. This presented an obstacle since there wasn't a suitable category for these steps, making it difficult to sort or group them with the rest. To address this, five new code categories were introduced: *Implementation of measures, Residual risk, Requirements, Report, PIA preparation*. An overview of the new codes is given in Table 7

Table 7: 2nd iteration PIA process codes with their corresponding appearances in process steps from 41 PIA processes

Code	**Number of occurrences**
Implementation of measures	1
Residual risk	12
Requirements	14
Report	34
PIA preparation	61

From the initial two iterations, it became evident that certain codes recurred over 50 times. Keeping the research objective in focus, codes with such high repetition were further broken down into more detailed units. The first code to undergo this refinement was *processing description*. This led to the emergence of several new codes, such as: *describing the project, identify stakeholders, map assets, map data flows, map data, list applicable laws, list applicable policies,* and *map business processes*.

For the fourth iteration, the code *risk assessment* was subjected to a more detailed examination. This facilitated the introduction of several new codes, which are as follows: *Identify threat, Determine likelihood, Determine Impact* and *Determine risk*.

During the fourth iteration, the code *Risk measures* underwent further refinement. This in-depth analysis led to a more granulated categorisation. Consequently, we introduced several distinct codes to better capture the nuances. These newly established codes include: *Current controls, New controls, Cost-benefit analysis* and *Risk management plan*.

In the final iteration, the code *PIA preparation* was revisited. Originally, this code had emerged from those steps that were previously unclassified. Upon a more thorough evaluation, it was determined that the 61 occurrences of this code were excessive. This high frequency indicated the presence of more specific sub-codes within *PIA preparation*. Therefore, a decision was made to further dissect this code, aiming to break it down into more comprehensible and distinct segments. This let to the following codes: *PIA team, PIA scope, PIA resources, Timetable, PIA plan* and *PIA competence*.

The list of original codes and their corresponding updated codes can be referenced in Appendix A.3. This table offers a systematic comparison, ensuring clarity in understanding the transformation or modification of each code. Readers seeking detailed insights into these coding changes are encouraged to consult this table for a clear overview.

After completing these iterations, the refinement and granularity of the codes achieved a level of detail that met the research's standards. With this coding framework in place, it became feasible to initiate the development of the Process Deliverable Diagram, which aims to provide a structured visual representation of the PIA process based on the insights gathered from the literature.

5 PIA maturity road map

This thesis couples the PbDMM [56, 55], as described in Section 2.3.1, to the PIA, charting a path forward to achieve a more advanced and robust PIA process. *Note: Initially, the PIA PDD was developed. Subsequent to that, the PbDMM was integrated with the PIA. However, to enhance clarity and ease of understanding for readers in the upcoming chapter, the explanation begins with the integration of maturity levels into the PIA and the method behind it, before diving into the details of the PIA PDD itself.* To merge the PbDMM with the PIA, all capabilities associated with the PIA were examined by the first author and a second researcher. The goal was to assess whether each capability could appropriately be aligned and applied within the context of the PIA. By doing so, the goal is to create a 'PIA Maturity Road Map' which serves as a guideline for organisations to evaluate, refine, and enhance their PIA processes. The findings and offers insights into the maturity levels corresponding capabilities of the PIA. At each stage of maturity, specific focus areas are highlighted, each associated with a capability, concentrating solely on those capabilities pertinent to the PIA. This chapter presents the capabilities in conjunction with the actions undertaken in the PDD per maturity level. The subsequent chapter will detail the PDD, encompassing all the process steps and concepts with their maturity level in colour.

5.1 Maturity level 1

Requirements "Privacy requirements are formulated before the design stage based on general privacy principles and the PIA. Business and legal requirements are elicited with privacy in mind, privacy-violating requirements are discarded." [56]

This capability was implemented into the first draft of the PDD, however it was located in a other activity. "Privacy requirements are formulated before the design stage based on general privacy principles and the PIA" [56] clearly states that the requirements must be formalised of before the design stage. Therefore the decision was made to move the sub-activity *Define data protection requirements* to the activity PIA Preparation.

Development "Privacy requirements are incorporated in low-level design. Acceptance testing is used to ensure that the system meets the privacy and security requirements." [56]

This specific capability has been highlighted in the high-level summary of the PIA under the implementation phase's description. However, given that this research doesn't delve into the intricacies of the implementation phase, further details on this aspect are not provided.

Processing principles "A set of standard processing principles are applied to all processing activities (e.g., GDPR processing principles)." [56]

This capability introduces the sub-activity *Define data protection requirements* where the deliverable DATA PROTECTION REQUIREMENTS documents the related processing principles and their objective.

Roles "Stakeholders, roles, and responsibilities related to privacy activities are identified and assigned." [56]

This capability is introduced as the sub-activity *identify PIA team*, where the roles and responsibilities are formalised in the deliverable PIA TEAM.

5.2 Maturity level 2

PIA process "A PIA is performed in a methodical manner for new projects and is updated whenever there are relevant changes in the project. It considers legal, technical security, and privacy requirements and documents how these have been implemented." [56]

The initial sentence was integrated into the high-level overview by drawing a line from the monitoring phase back to the PIA. The second part was implemented by adding the legal, technical security, and privacy requirements into the description of the sub-activity *Define data protection requirements* and the deliverable DATA PROTECTION REQUIREMENTS.

Processing principles "The processing principles are documented, applied in a structured and methodical manner, and are periodically evaluated." [56]

This capability underscores the importance of ensuring that processing principles are consistently traceable throughout the design process. By formalising these principles into the deliverable named DATA PROTECTION REQUIREMENTS, it ensures a structured and systematic approach to integrating and tracking these principles at every stage of the design. This not only emphasizes their significance but also ensures compliance and adherence to the intended data protection objectives.

5.3 Maturity level 3

Architecture "The data flows for all processing activities are modelled in a data flow diagram and documented as part of the enterprise architecture. The privacy architecture viewpoints document the relationships between existing and new elements." [56]

This capability introduces the sub-activity *map data flow diagram* with as deliverable DATAFLOW DIAGRAM.

PIA process "A preliminary threshold analysis is performed to determine the necessity of a PIA when launching new initiatives or modifying existing projects. The PIA process starts in the early planning phase and carries on throughout the project's life." [56]

In the activity Pre-PIA, the sub-activity *execute threshold analysis* with as deliverable THRESHOLD ANALYSIS is introduced.

PIA report "The PIA report is reviewed and is tied to budget submissions for new projects." [56]

This capability consists of two distinct parts. Within the *Report* activity, a sub-activity named *review PIA report* has been incorporated. Simultaneously, under the *PIA preparation* activity, a new sub-activity called *create PIA plan* is introduced. The outcome of this sub-activity is the deliverable named PIA PLAN, which exclusively contains the PIA budget as its main component.

5.4 Maturity level 4

Requirements "Stakeholders are extensively involved in the formulation of privacy goals and the identification of privacy requirements. Elicited privacy requirements are related to specific threats or principles to guarantee traceability and accountability. The privacy office documents and tracks the requirements and considers privacy risks in the design phase for all processes and systems." [56]

Stakeholders play a pivotal role in shaping the privacy objectives and pinpointing the necessary privacy requirements. This is explicitly detailed within the *assessment - define data protection targets* section. The nuances of this modified step can be further understood by referencing the activity table.

Moreover, privacy requirements that have been gathered are directly linked to specific threats or principles. This connection ensures there's a clear traceability and establishes accountability. The relationship is bridged from *assessment - define data protection targets* and extends to *risk assessment - mapping threats*. A visual representation, for instance, utilise a line connecting data protection requirements to threats, e.g. "relates to".

PIA process "The logistics of the PIA process are formalised and documented: the relevant roles, responsibilities, approval process, and needed resources are assigned, and the scope and scale of each PIA is determined. A privacy control selection process is implemented which evaluates the proportionality of selected measures." [56]

This capability augments the PIA PLAN within the *PIA preparation* activity by integrating components like *PIA Scope*, *PIA Timetable*, and the *Approval process*. Concurrently, at this maturity level, the sub-activity, *Evaluate the proportionality of selected measures*, emerges, producing the deliverable named *PRIVACY CONTROL SELECTION*.

PIA report "PIA reports are stored in a centralised registry in order to create a body of knowledge that can be consulted for future projects. A mechanism is implemented for updating PIA reports and publishing PIA reports to the general public whenever significant changes are made to processing activities." [56]

At level 4 the sub-activity *create public PIA report* in the activity *report* is introduced.

Risk Management "Privacy risks are kept in an inventory, linked to specific vulnerabilities or failures, and mapped to data-flow elements. Data controllers have a complete overview of documented privacy risks and produce a control implementation plan that describes risk mitigation and the feasibility of controls through a cost-benefit analysis. Feared events are identified and their impact and severity are determined." [56]

The capability ensures in the model that their is a line from DATAFLOW DIAGRAM to THREATS (e.g. 'relates to') and the CONTROLS are checked with a COST-BENEFIT ANALYSIS

5.5 Maturity level 5

Requirements "Advice from ethical experts is gained regarding requirements for sensitive personal data." [56]

To better integrate this capability within the existing structure, a new sub-activity, termed *Ask advice from ethical experts*, has been introduced. This sub-activity finds its place within the larger activity known as *Pre-PIA*.

PIA report "The PIA process and the PIA reporting activities are decoupled. PIAs reference PIA reports from the centralised registry ensuring that subsequent changes build upon previous analysis. Privacy controls are methodically assessed using metrics. The design of the physical environment is included." [56]

To incorporate this capability, the phrase "privacy controls are systematically evaluated using metrics" is added to the activity table under the entry *identify new controls*.

Risk management "The entity has implemented documented policies and procedures to monitor and to optimise privacy risk management and control. These policies are improved by feeding back audit results into a change control process. The data lifecycle is adopted as a basis for the contextual analysis to anticipate privacy invasive events and to identify system harmful activities and risks." [56]

At this maturity stage, the sub-activity *map personal data lifecycle* is introduced within the activity *view creation*. Additionally, a connection from PERSONAL DATA LIFECYCLE to THREATS (e.g. 'relates to') is established.

Transparency "Privacy policy is defined together with data subjects who are provided information about policies, procedures, controls, and tools that allow them to determine how personal data is used and whether policies are being properly enforced." [56]

To incorporate this capability, an additional sub-activity titled *Ask advice from data subject* in the activity *PIA preparation* is integrated. This aids in formulating the deliverable DATA PROTECTION REQUIREMENTS.

Roles "Appoint a central entity responsible for privacy related issues such as a privacy committee." [56]

At this maturity stage, the sub-activity *get PIA approval* activity table is changed.

5.6 Maturity level 6

PIA process "A formalised stakeholder consultation plan is created, involving stakeholders in identifying and evaluating privacy risks. Privacy risks are identified continuously during the project and processing activity lifecycles. A senior executive is held accountable for the quality and adequacy of a PIA." [56]

The choice was made to integrate the stakeholder consultation plan within the PIA preparation phase, specifically under the sub-activity titled *create PIA plan*. This approach ensures that the PIA team possesses a systematic strategy for engaging with stakeholders prior to initiating the primary PIA process. Finally within the description of the sub-activity *get PIA approval*, it's been specified that a senior executive bears responsibility for ensuring the quality and completeness of the PIA.

PIA report "Reporting adheres to its own periodic reporting cycle independent of the PIA process and reports are submitted for audit to an independent third-party." [56]

To integrate this capability, the sub-activity *Third-party Audit* is introduced within the activity *Report*.

5.7 Maturity level 7

PIA report "Different PIA reports can exist per PIA process, these reports are adapted to their intended audience in both content and form." [56]

The capacity to customise PIA reports based on the specific PIA process means that diverse reports can be crafted for each process [56]. These reports are not only tailored in terms of content but also in their presentation, ensuring they resonate with their intended audience. Given this capability, the decision has been made to modify the sub-activity at level 4 to: *Create PIA report for different stakeholders*.

Transparency "Summaries of PIAs, TRAs, and independent third-party audit results are published." [56]

To meet the requirements of this maturity level, the sub-activity *Publish Audit Summary* is introduced within the activity *Report*.
In the upcoming chapter, a detailed exploration of the PIA PDD, integrated with the PbDMM, will be provided.

6 PIA PDD

This section delves into the detailed description of the artefact crafted specifically for this thesis. In the preceding chapter, the identified capabilities were integrated into the design framework of the PIA. This integration ensured that individual process steps and their respective deliverables were aligned with specific maturity levels. For a visual representation, refer to Figure 6, which showcases the varying maturity levels alongside their corresponding colours as they appear in the PDD.

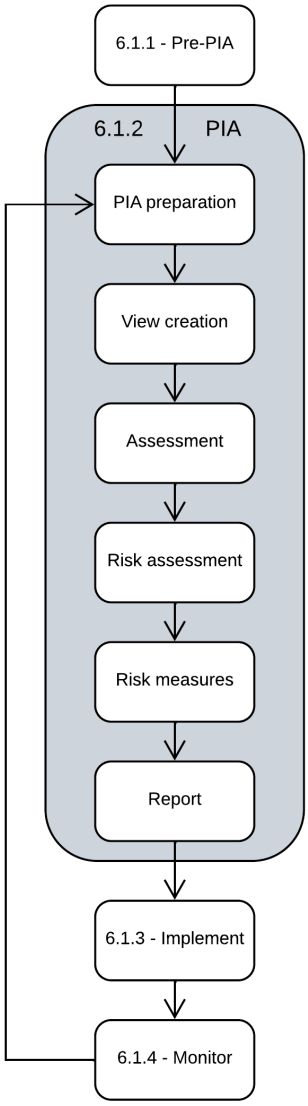
Figure 6: Maturity levels with colour as in PDD

The organisation of this chapter is presented in the subsequent manner: Firstly, an all-encompassing perspective of the entire process is presented, offering a full overview. Subsequently, the attention is redirected towards a more comprehensive examination of the pre-PIA and PIA phase. Each section is structured to initially provide a narrative description of the particular activity. Following the establishment of the contextual framework, whereas the activity and concept table of the corresponding activity can be found in the Appendix.

6.1 High level overview

The high-level overview offers an all-encompassing view of the activities integral to the effective execution of a PIA process. Acting as a guide, it outlines every step. Within the scope of this research, particular emphasis is placed on the *pre-PIA* phase, as well as the diverse activities encompassed within the *PIA* itself. Below in Figure 7 is schematic overview of the activities with a more detailed description:

Figure 7: High level overview



6.1.1 High level - Pre-PIA (Preliminary PIA)

The first activity is *Pre-PIA*. In this preliminary phase, the need to undertake a PIA (PIA) is both pinpointed and substantiated. It's not merely a procedural step; it's a foundational one, as described in the GDPR. The essence of this stage is to critically evaluate if the magnitude and potential ramifications of the project or initiative warrant a full PIA. Given the substantial costs and the considerable duration involved in

executing a full-fledged PIA, its inclusion becomes a pivotal decision point. As such, recognising and planning for it during the early stages of project planning is imperative to ensure seamless progression and resource allocation.

6.1.2 High level - PIA

Following the Pre-PIA is the actual PIA. In this core activity, a evaluation is conducted to assess how personal data is collected, stored, and managed, ensuring that it complies with privacy regulations.

6.1.3 High level - Implementation activity

After successfully completing the first two activities, the focus then shifts to the Implementation activity. It's important to note that this particular stage falls outside the boundaries of the current research. As such, it can be viewed as a 'black box,' meaning that it's unclear exactly what will be implemented and how this will be accomplished.

Improvement Actions for Maturity Level 1 Although the Implementation activity is not well-defined within the context of this research, there is one specific action recommended to attain Maturity Level 1. This involves incorporating acceptance testing procedures to ensure that the system fulfills all the necessary privacy and security requirements. This action aims to validate that the system is designed and configured to meet these standards [56].

6.1.4 High level - Monitor activity

The Monitoring activity represents a crucial part of the process and is introduced at Maturity Level 2. Just as the Monitor activity, this activity is outside the scope. It serves as a systematic way to keep a close eye on privacy issues and ensure ongoing compliance. If non-compliance or any other potential issue arises, it could set off a reevaluation of the PIA. Such issues could stem from various sources, whether they be regulatory changes, discrepancies in data handling, or unforeseen challenges. Recognising these deviations promptly is essential, as it ensures the PIA remains accurate and up-to-date. Consequently, this might necessitate a thorough revision of the PIA to address and rectify the identified concerns. This activity is designed to evolve and become more robust as the system reaches higher maturity levels.

Maturity Level 2: Ongoing PIAs Starting at Maturity Level 2, PIAs (PIAs) become a regular feature, rather than a one-time event. Whenever a new project comes into play or significant changes occur in existing projects, a methodical PIA is performed. This ensures that the privacy landscape is continually reassessed, keeping the system up-to-date and compliant with privacy regulations [56].

Maturity Level 6: Independent Reporting Cycles Once the system advances to Maturity Level 6, reporting takes on a life of its own. Rather than being tied to the PIA process, reporting follows its unique, periodic cycle. This autonomous reporting mechanism provides a dedicated channel for consistently monitoring and reporting on privacy-related metrics, separate from the PIA activities [56].

Maturity Level 7: Advanced Risk Management and Compliance At Maturity Level 7, the monitoring activity becomes significantly more advanced. First off,

data risks are automatically flagged, thanks to predictive analytics. If a high-risk operation is detected, early warnings are triggered to allow for immediate action. Additionally, a specialised privacy risk and compliance dashboard comes into play, offering a real-time overview of the system's risk landscape [56].

Maturity Level 7: Audits and Reviews Also, at this level, periodic reviews and audits are integrated into the process. These reviews scrutinise how personal data is being handled and processed, ensuring that it aligns with both legal and ethical standards. This auditing mechanism is a key pillar in the overall strategy to maintain a continuously monitored and compliant privacy environment [56].

In the sections that follow, a examination of each activity within the PDD is presented. The organisation of the content is structured systematically:

1. An initial description detailing the flow of the PDD, coupled with explanatory notes to enhance understanding.
2. A visual representation in the form of the PDD figure, which provides a graphical overview of the processes.
3. The table related to the PDD activity, which details its associated activities and concepts, is available in the appendix for reference.

6.2 Pre-PIA activity in PDD

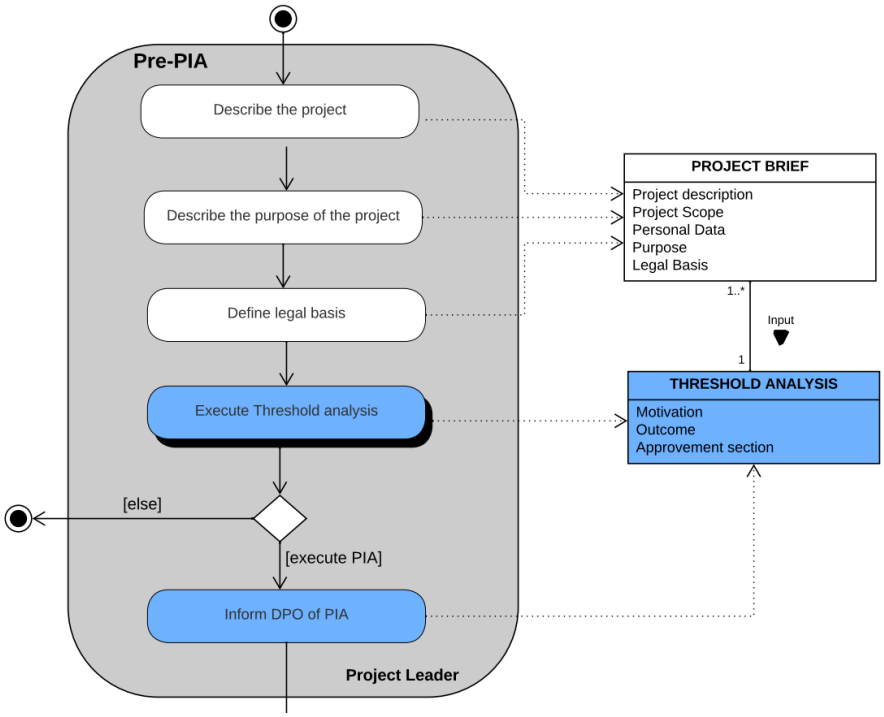
In the initial activity of the PIA process, we commence with the Pre-PIA activity, which is illustrated in Figure 8. The primary objective during this preliminary activity, the Pre-PIA, is to determine whether there's a necessity to proceed with a PIA. The sub-activities of the *pre-PIA* are: *describing the project*, *describe the purpose of the project*, and *define the legal basis*, the main output or deliverable that emerges is the PROJECT BRIEF. This document, the PROJECT BRIEF, encapsulates key details about the personal data that is intended to be processed. It answers pertinent questions such as: What kind of personal data will be managed? Why is there a need to process it? And, what legal grounds justify this data processing?

Following the formulation of the PROJECT BRIEF, the subsequent sub-activity is to *execute threshold analysis* which is introduced at maturity level 2. This sub-activity is instrumental in determining the necessity for a PIA. The output from this analysis is encapsulated in a document called the THRESHOLD ANALYSIS. The THRESHOLD ANALYSIS documents the reasoning and the eventual verdict on the appropriateness of conducting a full PIA.

Following this sub-activity, a decision branch emerges. The outcome of the THRESHOLD ANALYSIS effectively dictates whether a full PIA is warranted. If the decision leans towards the need for a PIA, the subsequent step entails *inform the DPO of the PIA*. The DPO's endorsement is sought, confirming the necessity of the full PIA. This affirmation is also recorded within the THRESHOLD ANALYSIS document.

Alongside the PDD (Figure 8), the activity table (Table 11) and the concept table (Table 12) are presented in Appendix A.5. The activity table delineates each activity, its related sub-activities, and their connection to the deliverables they produce and utilise. Meanwhile, the concept table provides a list of deliverables, categorising them as concepts, each accompanied by a reference and a clear definition.

Figure 8: Pre-PIA activity in PDD



6.3 PIA Preparation activity in PDD

After concluding the pre-PIA activity, there may arise a need to undertake a thorough PIA. The next activity in this PDD is labelled as the PIA preparation. This activity identifies all necessary organisational resources essential for a successful PIA.

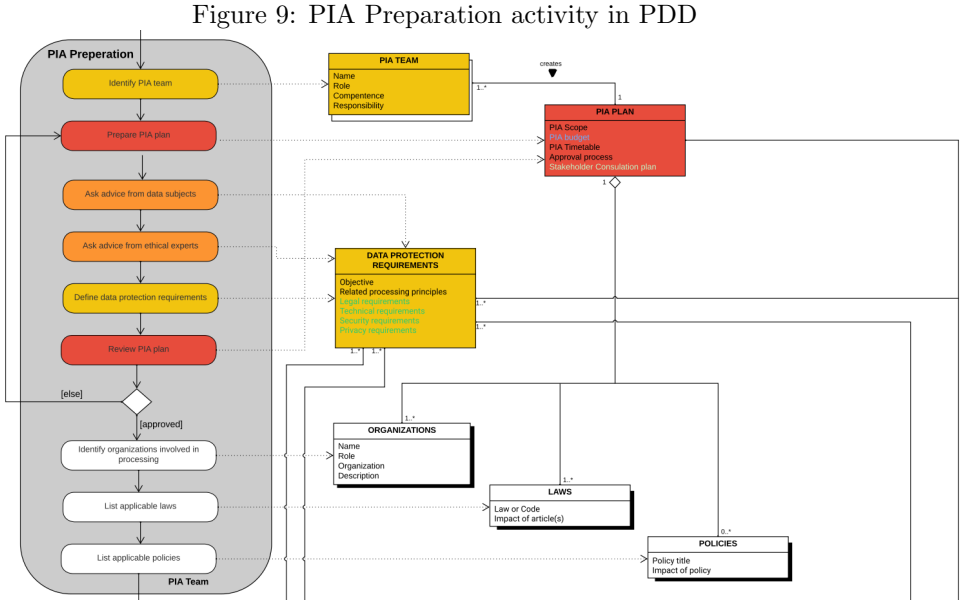
Within the activity PIA preparation, the first sub-activity is to *identify PIA team*. This involves assembling a list, termed the PIA TEAM, that outlines all team members, detailing their names, roles, areas of expertise, and respective responsibilities. Subsequent to team identification, the focus shifts to crafting the PIA PLAN. This document, drafted by the constituted PIA team, offers an overview of the project's scope, allocated budget, proposed timeline, approval mechanisms, and a strategy for engaging stakeholders. Importantly, this PIA PLAN also finds a place within the concluding PIA REPORT.

The next stages encompass seeking advice from data subjects, ethical experts, and outlining data protection requirements. These activities cumulatively result in the DATA PROTECTION REQUIREMENTS document, which elucidates specific requirements and foundational principles of data processing. Thereafter, a review of the PIA PLAN is undertaken. Depending on the outcome of this review, the PIA PLAN is either approved for execution or sent back for revisions.

Further tasks involve the identification of all organisations involved in the data processing chain, producing an list titled ORGANISATIONS. Following this, a listing of laws pertinent to data processing is created, named LAWS. This document not only

lists the relevant laws but explicates the nuanced impact each might have on processing activities. The final activity is to curate a list of the policies the data processor abides by, which is captured in the POLICIES list, highlighting each policy's ramifications on data processing. Alongside the PDD (Figure 9), the activity table (Table 13) and the concept table (Table 14) are presented in Appendix A.6.

Figure 9: PIA Preparation activity in PDD



6.4 View creation activity in PDD

Initiating the activity view creation involves several planned sub-activities:

Map Personal Data: The first step is geared towards tracing the footprint of every piece of personal information. The culmination of this activity is the PERSONAL DATA REGISTER, a structured log or repository that encapsulates details of all personal data in use or storage.

Map Personal Data Flows: To understand how personal data traverses through the system, it's essential to chart out its flow. This leads to the creation of the DATAFLOW DIAGRAM, a visual representation delineating the movement of personal data within the organisation's ecosystem.

Map Software and Hardware: Equally crucial is the knowledge of infrastructural assets supporting data processing. The outcome of this sub-activity is ASSETS, a list or diagram detailing all software and hardware components involved in data handling.

Map Business Process: To further deepen understanding, it's imperative to diagram the various business processes. The BUSINESS FLOW DIAGRAM does just this, offering a visual guide to the processes that underlie and dictate the flow of personal data.

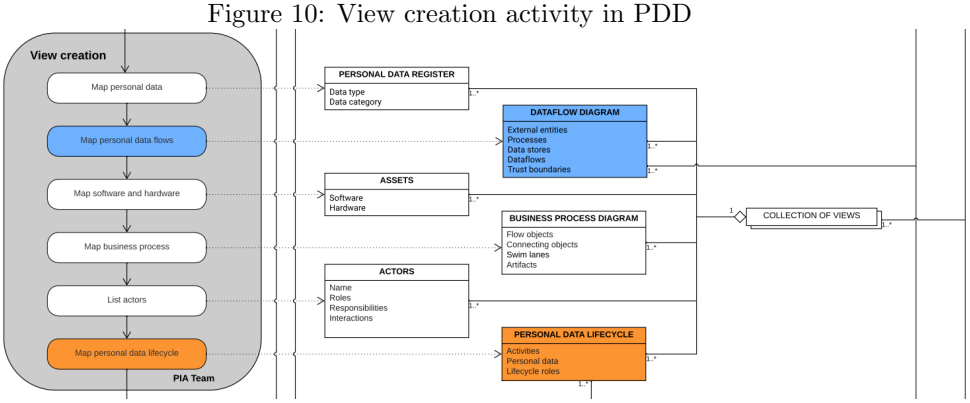
List Actors: Identifying the key players or entities that interact with, or influence, personal data is essential. This leads to the compilation of ACTORS, an list specifying all individual entities, their roles, and their interactions with the data.

Map Personal Data Lifecycle: This sub-activity delves into the entire lifespan of personal data, from its inception to disposal. The PERSONAL DATA LIFECYCLE is a visual or documented representation that traces the stages of data from collection, processing, storage, to eventual deletion.

Lastly, to ensure that these various perspectives are easily accessible and organised, they are consolidated into the COLLECTION OF VIEWS. This becomes a one-stop repository that holds all of diagrams and lists, offering a view of personal data management within the organisation. This consolidated approach aids stakeholders in making informed decisions and ensures data integrity and protection throughout the organisation.

Alongside the PDD (Figure 10), the activity table (Table 15) and the concept table (Table 16) are presented in Appendix A.7.

Figure 10: View creation activity in PDD



6.5 Assessment activity in PDD

After the creation of the views, the progression leads to the assessment activity. Central to this activity is the objective of critically evaluating the necessity, proportionality, and legal compliance of data practices within the organisation. Rather than taking a broad approach, this evaluation becomes more precise by focusing on a specific view with a chosen ACTOR, thus creating a detailed USE CASE.

These USE CASEs function as descriptive scenarios that simulate how specific ACTORS interact with the data in certain situations, allowing the organisation to:

Assess Necessity: By observing how an actor interacts within a particular view, the organisation can determine whether the underlying data practices are necessary. It aids in understanding if the data being handled is truly essential for the actor's intended purpose or objective.

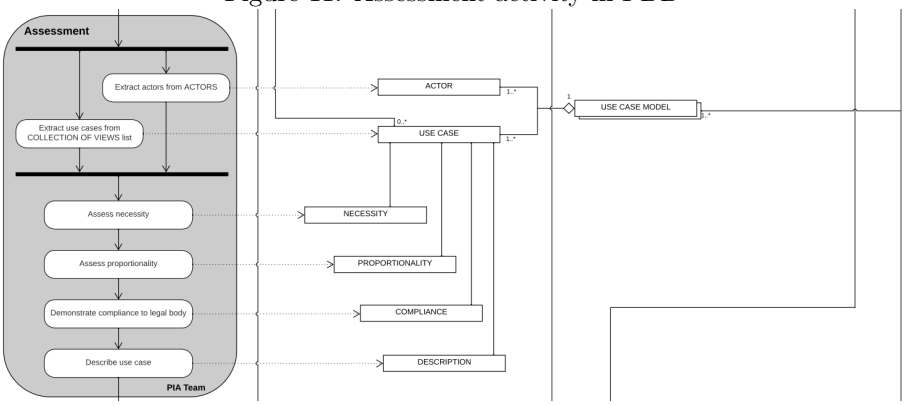
Assess Proportionality: The use case provides insights into whether the data practices within that view are balanced and relevant concerning the actor's objectives. This ensures that data interactions are not excessively broad or restrictive for the actor's needs.

Demonstrate compliance to legal body: By using the use case as a model, the organisation can investigate if the interactions of the actor within the view adhere to prevailing legal standards and regulations. This step is paramount as it directly ties to the organisation's legal responsibilities and potential liabilities.

Following their creation, these use cases are systematically archived in a USE CASE MODEL. This model serves as a structured repository, housing all the USE CASEs generated during the assessment activity. By collecting these USE CASEs in a unified model, the organisation ensures that insights and evaluations derived from them are easily accessible and can guide future data practices and decisions, ensuring they remain purposeful and compliant.

Alongside the PDD (Figure 1), the activity table (Table 17) and the concept table (Table 18) are presented in Appendix A.8.

Figure 11: Assessment activity in PDD



6.6 Risk assessment activity in PDD

Following the initial assessment, the PDD progresses to the risk assessment activity. This activity is instrumental in identifying potential vulnerabilities and determining their potential implications for the organisation.

Map the Threat: The commencement of this activity is characterised by a focused effort to pinpoint potential threats. This involves an in-depth exploration and analysis of the various factors and vulnerabilities that could compromise data integrity and security. The culmination of this sub-activity is a documented list or representation named 'THREATS'.

Determine Likelihood and Impact: Once threats are mapped, it's necessary to assess two key dimensions - the probability of the threat materialising (LIKELIHOOD) and the potential repercussions if it does (IMPACT). This nuanced understanding equips the organisation with a clearer perspective on which threats could be most harmful.

Determine Risk: By multiplying the determined impact with the assessed likelihood, one can calculate the overall risk associated with each identified threat. This computation provides a quantifiable metric, making it easier to understand the severity of each threat.

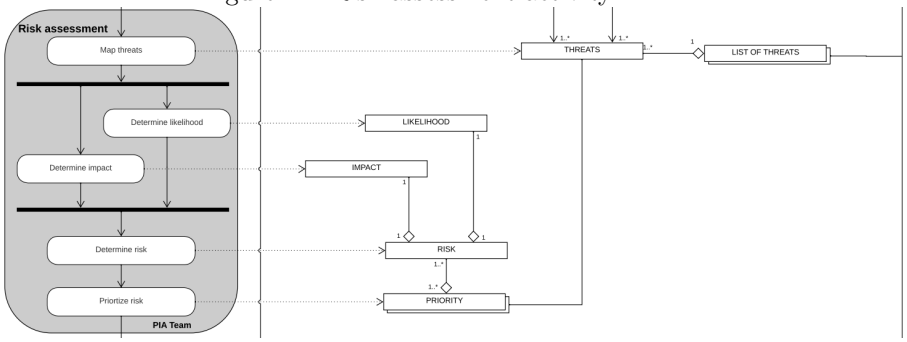
Prioritize Threats: Based on the calculated risk, threats are then ranked. Those with the highest potential risks, derived from their impact and likelihood, are accorded higher priority. This prioritisation facilitates informed decision-making, guiding the organisation on where to focus its mitigation efforts first.

To ensure that all the identified and evaluated threats are easily accessible for

future reference and action, they are catalogued in the LIST OF THREATS. This structured repository becomes a crucial resource, enabling the organisation to revisit, review, and update its threat landscape as and when required.

Alongside the PDD (Figure 13), the activity table (Table 19) and the concept table (Table 20) are presented in Appendix A.9.

Figure 12: Risk assessment activity in PDD



6.7 Risk measures activity in PDD

Transitioning from the initial activities, the next activity is risk measures. Within this activity, the emphasis is on recognising and refining controls that safeguard the organisation from potential threats. Each sub-activity builds on the previous, ensuring a comprehensive approach to risk mitigation.

Identify Current Controls: As a starting point, it's essential to take stock of the already-existing protective measures in place. This involves a meticulous review of all procedures, protocols, and safeguards currently employed by the organisation to fend off risks. The culmination of this sub-activity is the CURRENT CONTROLS artefact, which serves as a detailed inventory of all current protective measures.

Identify New Controls: Recognising that the threat landscape is dynamic, there's a need to explore potential new safeguards that address evolving risks. This sub-activity zeroes in on identifying novel, more effective, or supplementary protective measures. The outcome of this process is documented as NEW CONTROLS, which details these new safeguards.

Execute Cost-Benefit Analysis: With both current and new controls at hand, the next sub-activity is to weigh their economic implications against their potential benefits. The COST-BENEFIT ANALYSIS evaluates the financial costs of implementing and maintaining each control against the projected benefits, mainly in terms of risk reduction and potential damage mitigation. This analysis provides clarity on which controls offer the most value and should be prioritised.

Prioritize controls: Post-analysis, both current and newly identified controls are collated and ranked. Their prioritisation is largely influenced by the cost-benefit analysis, ensuring that the most impactful and cost-effective controls are implemented first. All these controls, organised by priority, are archived in the LIST OF CONTROLS.

Evaluate the Proportionality of Selected Measures: It's imperative to assess the suitability and proportionality of the chosen measures. This means ensuring that each control or safeguard is not too strict or not strict enough in relation to the specific

risks they are designed to mitigate. It's about striking the right balance, ensuring that measures are effective without being unnecessarily burdensome. The outcome of this evaluation is captured in the PRIVACY CONTROL SELECTION deliverable, which documents the controls deemed proportionate and suitable for implementation.

Create Plan for Risk Management: With the right controls in hand, the focus then shifts to devising a strategic plan detailing the how and when of implementation. This involves determining timelines, allocating resources, and setting milestones for the roll out of each control. It's a roadmap that ensures a systematic and efficient deployment of the selected measures. This strategy is enshrined in the RISK MANAGEMENT PLAN deliverable.

Identify Threats with Residual Risk: This step involves pinpointing threats that still pose a risk even after identifying the selected controls. It acknowledges the reality that no system is entirely foolproof, and some threats will continue to exist. The key is to recognise these risks to ensure that they are continuously monitored and addressed as needed.

Hereafter is a logical branch. If there are any THREATS that continue to pose a residual high risk, it is imperative that these are clearly described. This ensures that all stakeholders are aware of the potential dangers and can take appropriate measures to address them

Identify Threats with Residual High Risk: With a broader understanding of threats with residual risks, the focus narrows down to those that pose a significantly high risk. These are threats that, despite all measures, still have the potential to inflict considerable harm or damage if they materialise. Identifying these threats is crucial as it indicates areas where extra vigilance or additional measures might be required.

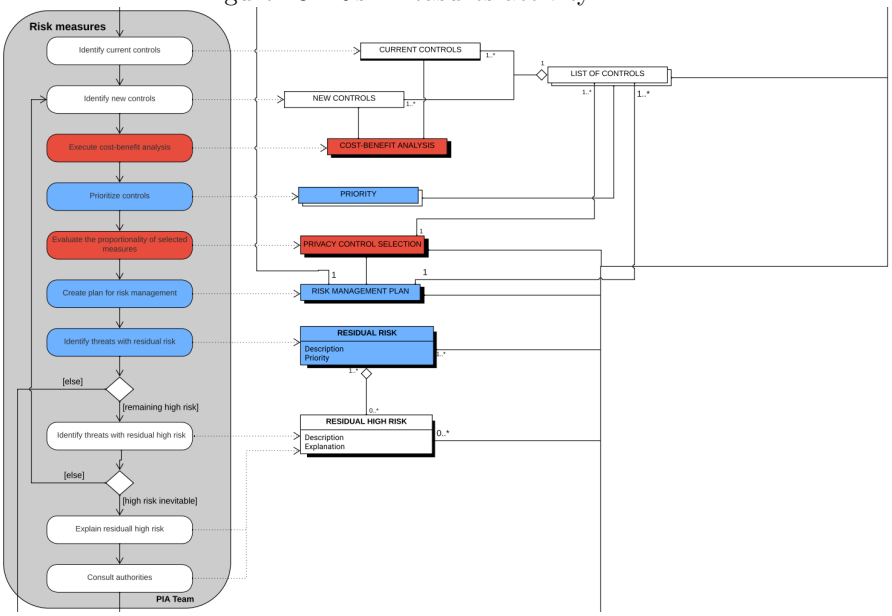
Hereafter is another logical branch. If the residual high risk is inevitable the high risk should be explained and the authorities contacted as required by the GDPR. Otherwise new controls should be taught of to minimise this high risk.

Explain Residual High Risk: Beyond mere identification, it's vital to comprehend the reasons behind the persistence of such high risks. This involves a deep dive into understanding why the existing controls might not be fully effective against these threats and the potential consequences of these threats materialising. This insight aids in refining strategies or seeking alternate solutions.

Consult Authorities: Given the severity and implications of high residual risks, it's required to consult with external authorities. This could mean liaising with regulatory bodies or seeking guidance from industry experts.

Alongside the PDD (Figure 14), the activity table (Table 21) and the concept table (Table 22) are presented in Appendix A.10.

Figure 13: Risk measures activity in PDD



6.8 Report activity in PDD

Create PIA Report: This initial sub-activity entails the detailed documentation of the entire PIA process. From the methodologies used, risks identified, to the measures proposed, everything is meticulously recorded. This report serves as the definitive record of the organisation's PIA journey.

Review PIA Report: Before the report gains wider visibility, it undergoes a rigorous internal review. This ensures that the content is accurate, comprehensive, and aligned with organisational standards and objectives. Any inconsistencies, gaps, or errors identified are rectified at this stage.

Consult DPO (Data Protection Officer): Given the importance of data protection, the Data Protection Officer (or a similar role within the organisation) is consulted. Their expertise is invaluable in validating the PIA report's content, ensuring its alignment with data protection principles, and confirming that all regulatory requirements are addressed.

Audit by Third Party: To further ensure the PIAs robustness and objectivity, an external audit by a third party is conducted. This brings an outside perspective, which can identify overlooked areas, suggest improvements, or validate the thoroughness of the PIA.

Publish Third Party Audit Summary: Upon completion of the external audit, a summarised version of the findings is made public. This promotes transparency, builds trust with stakeholders, and showcases the organisation's commitment to privacy and data protection.

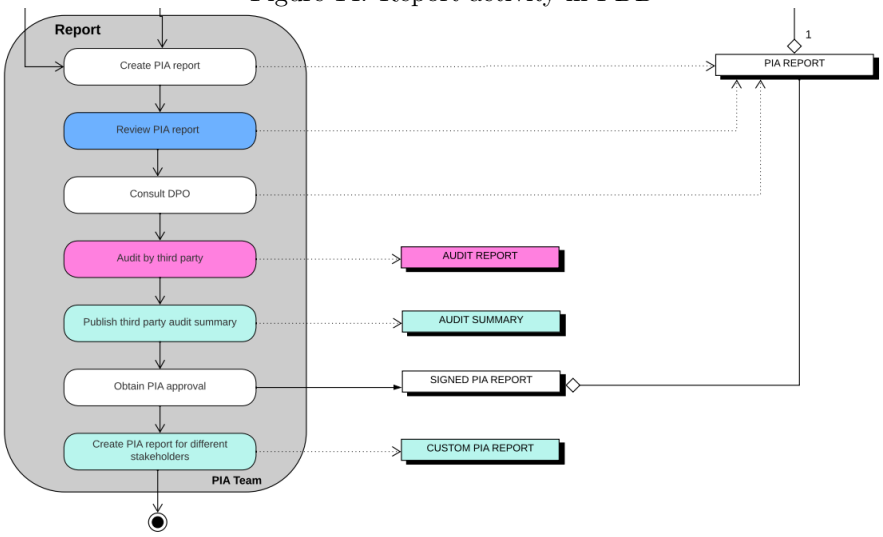
Obtain PIA Approval: With all the reviews and audits completed, the PIA report is presented for formal approval, typically by a senior management committee or board. Their endorsement signifies the organisation's collective agreement with and

commitment to the PIAs findings and recommendations.

Create PIA Report for Different Stakeholders: Recognising that different stakeholders have varying needs and interests, specialised versions of the PIA report are crafted. Tailored to address specific concerns or provide relevant insights, these versions ensure that every stakeholder, from employees to partners to regulators, is adequately informed.

Alongside the PDD (Figure 14), the activity table (Table 23) and the concept table (Table 24) are presented in Appendix A.11.

Figure 14: Report activity in PDD



7 Validation

This chapter explores the research's validation process through interviews with professionals in the government sector. The **Validation process** provides a breakdown of the interview approach, and **Validation Results** presents firsthand feedback from the participants. The chapter wraps up with **Points for Recommendation**, which identifies proposed refinements to the research.

7.1 Participants

For the validation of this thesis, four in-depth interviews were conducted with working professionals actively engaged in roles within a governmental context. These individuals, with their unique perspectives and experiences, offered invaluable insights that enriched the overall understanding and analysis. Each interview was semi-structured to capture a comprehensive view of the challenges, nuances, and intricacies faced when executing a PIA. Through these discussions, a diverse range of viewpoints and experiences was gathered, ensuring a holistic exploration of the topic. Table 8 provides a concise summary of the interviewees roles, as well as their theoretical and practical expertise.

Table 8: Overview of the interview participants

Number	**Role**	**Theoretical knowledge**	**Practical knowledge**
Participant 1	Privacy officer	High	Low
Participant 2	Senior Project leader	Low	Medium
Participant 3	Chief information security officer	High	High
Participant 4	Privacy officer	High	High

7.1.1 Privacy officer

A privacy officer is an individual who is appointed within an organisation to assume responsibility for the oversight and administration of personal data privacy. The primary responsibility of this position entails ensuring that a company adheres to relevant data protection requirements when handling the personal data of its employees, customers, suppliers, and other individuals (often referred to as data subjects). [5].

7.1.2 Project leader

In a organisation setting, a project leader assumes the role of overseeing and coordinating a designated project or a collection of tasks. The individuals in this role are responsible for supervising the process of planning, implementing, and finalising the project, with the aim of achieving the established goals within the designated time frame and financial limitations. The primary duties frequently encompass the coordination of team members, establishment of objectives and timelines, oversight of progress, resolution of challenges, and dissemination of updates to relevant stakeholders. The individual assuming the role of project leader assumes the primary responsibility of serving as the central point of contact for the project. Additionally,

[5] https://www.indeed.com/career-advice/finding-a-job/what-does-privacy-officer-do

they are tasked with the responsibility of ensuring that the project is in alignment with the objectives and standards set out by the firm. [6].

7.1.3 Chief information security officer

The role of a Chief Information Security Officer (CISO) inside a organisation encompasses the responsibilities of a high-ranking executive who is accountable for the development and sustenance of the organisation's strategy, vision, and program aimed at ensuring the sufficient safeguarding of information assets and technology. Primary responsibilities typically encompass the formulation and execution of security policies and protocols, supervision of regulatory adherence, leadership of security personnel, evaluation and mitigation of risks, facilitation of incident response strategies, and collaboration with senior management to harmonise security endeavours with overarching corporate goals. [7].

7.2 Validation process

The validation process began with prospective participants receiving an email invitation that contained a comprehensive information letter, the details of which can be found in Appendix A.14. The primary purpose of this letter was twofold: to provide a clear overview of the research objectives and to ascertain the recipient's willingness to participate in an interview session.

While preparations for reaching out to potential participants were underway, an interview protocol was created. This document, which is accessible in Appendix A.15, served as more than just a list of questions. It was designed as a strategic blueprint, guiding the interviewer in extracting insightful details about the proposed model and obtaining a hands-on understanding of practical implementations.

When participants expressed an interest in contributing to the research, the next steps were set into motion. An official interview invite was dispatched to them, bundled with a detailed consent form, ensuring they were well-informed and comfortable with the interview's procedures and terms. For reference, both these integral documents can be consulted in Appendix A.14 and A.13.

To cater to the convenience of the participants and maintain a structured research process, interviews were organised by determining a date and time that best suited both the researcher and the participant. These sessions took place on-site, providing an environment conducive to candid and comprehensive discussions. Post the confirmation of participant's consent, the interview was recorded, ensuring every detail was captured. However, in a commitment to participant privacy and as explicitly outlined in the consent form, once the valuable insights from these recordings were transcribed, the original audio files were deleted.

7.3 Validation results

In the following subsection, the findings obtained from the interviews are detailed and discussed. The feedback and insights gathered during the interviews were originally articulated in Dutch. These comments were translated into English by a native Dutch speaker. This translation process was carried out with guarantee that the nuances,

[6]https://www.indeed.com/career-advice/finding-a-job/project-leader-vs-project-manager

[7]https://www.cisco.com/c/en/us/products/security/what-is-ciso.html# ciso-role-explained

context, and intent of the original statements remained intact, thus providing an authentic representation of the participants perspectives. This section is organised in a systematic manner to provide an overview of the feedback obtained from the interviews. Initially, the structure of the interviews was designed to follow the sequence of the PDD chronicle, ensuring that each activity was thoroughly discussed. For each activity, the primary insights and takeaways from the participants are presented to offer a clear understanding of their perspectives and experiences. These insights capture the essence of the participants feedback and shed light on their views regarding the effectiveness, relevance, and potential areas of improvement for each activity. Subsequently, in the subsection titled "Points for Recommendation," specific improvement steps are delineated. These recommendations are derived from the collective feedback of the participants and are aimed at enhancing the overall efficacy and applicability of the PIA PDD.

7.3.1 Validation of activity Pre-PIA

Government's Pre-PIA Template: The participants highlighted the existence of a Pre-PIA template employed by the government. This template, enriched with a threshold mechanism, guides the employees in determining if a full PIA is warranted.

Participant 1 shared, "In our government setup, the Pre-PIA serves as a threshold analysis. An employee completes the Pre-PIA, and based on the results, the template indicates whether a full-blown PIA is necessary. Subsequently, the Data Protection Officer (DPO) is informed."

Echoing this, Participant 2 remarked, "I frequently utilise the Pre-PIA template provided by our government."

Ambiguity Surrounding 'PROJECT BRIEF': The term 'PROJECT BRIEF' in the Pre-PIA elicited some confusion among participants. Both Participant 2 and Participant 4 felt that the terminology could be misleading.

Delving into this, Participant 2 expressed, "The term 'PROJECT BRIEF' is somewhat ambiguous. As a project leader, there are instances where I'm handed a specific project, making the name potentially misleading."

Participant 4 elaborated on this sentiment, explaining, "The process typically starts with a briefing. As the project unfolds through its stages, it's logical to refer to it using this term. However, there are times when the task at hand isn't a structured project but more of a straightforward data processing activity."

Iterative Approach to 'PROJECT BRIEF': A suggestion to adopt a more iterative approach to the 'PROJECT BRIEF' was introduced, emphasising the importance of recurrent threshold analyses.

Participant 3 recommended, "While crafting the project letter, it's imperative to revisit it frequently or perhaps carry out a threshold analysis. Such a practice ensures that the decision to proceed is rooted in concrete information. If there's any uncertainty, it might be prudent to halt the process."

Clarity on Notification and Approval: The term 'notify', especially in the context of the DPO, posed some challenges in interpretation.

Participant 3 elucidated, "Securing approval is paramount. But there seems to be a mix-up. The Pre-PIA mentions notifying the DPO, suggesting mere communication, while the actual intent seems to be seeking enhancements or permissions. Generally, 'informing' doesn't inherently mean 'seeking consent.' This nuance can lead to confusion."

7.3.2 Validation of activity PIA-preparation

The participants think it is a good idea to formalise a formal PIA team.

Participant 1: "Currently, this process is carried out in an ad hoc manner. It's the responsibility of the management to allocate the necessary resources. Once the manager identifies the right individual, they know that this person should be a part of the team to execute the PIA. However, if the selection remains arbitrary, it's like they're just picking someone randomly from here and there. These individuals are then placed together, as if they were simply positioned in a hallway, left to complete the tasks. Personally I think it is a good idea to formalise a PIA team. "

Participant 2 : "The involvement of the team can vary. Typically, one or two individuals handle this, with one person filling out the form and perhaps another team member reviewing it. Then it's sent to the privacy office. What's crucial, and potentially relevant for your research, is that the realisation of needing a PIA often comes too late. So, there's a delayed recognition that a PIA should be prepared."

The second sub-activity *create PIA plan* participant 1 says: "I would expect there to be a PIA plan in place. With this plan, we can make an estimate of the time required for the project. It's wise to have a broad estimate to ensure we stay within the desired timeline. It's also crucial to account for the necessary approvals; these must be obtained in a timely manner. When making a PIA there is support document, I miss that very much"

For the third deliverable Participant 1 says: "I can not place, to ask data subject and ethical experts" for input in the DATA PROTECTION REQUIREMENTS. "This is not something we do"

Participant 2 says "It's always somewhat ambiguous and elusive. As project leaders, we suddenly face this challenge. A PIA then needs to be prepared. But honestly, it's not our strong suit."

The sub-activities *List applicable laws* and *List applicable policies* participant 1 say "It's only logical that they be included. Yes."

participant 4: "I appreciate that in your model you differentiate by seeking advice from the data subjects—the individuals the data pertains to. It's also commendable that you consider consulting an ethical expert."

7.3.3 Validation of activity view creation

The process of view creation in the system, as described, drew varied reactions from the participants, particularly in terms of comprehensiveness and clarity.

Component Inclusion and Omissions: Participant 1 provided detailed feedback on the components that are included and those that are missing within his own organisation. "While the DATA PROTECTION REGISTER is well-integrated, I observed that a data flow diagram is missing from the views. The inclusion of assets is commendable, but the lack of a business process diagram is a noticeable gap. Furthermore, while actors are generally seen as third parties, their specific roles, responsibilities, and interactions with the system. Another missing piece in this puzzle is the personal data lifecycle, which remains unaddressed."

Ambiguity in Terminology: Participant 4 expressed reservations regarding the terminology used, particularly the term 'view creation'. "The phrase 'view creation' seems vague to me. Its abstract nature makes it hard for me to grasp its essence. Could you possibly provide an alternative description or clarify its intent?"

7.3.4 Validation of activity Assessment

The assessment component of the system garnered feedback from the participants, emphasising the depth, clarity, and structure of the process.

Depth and Clarity in Evaluation: Participant 1 delved deep into the intricacies of the assessment, providing insights on the approach and its efficacy. "The assessment process prompts one to question the functioning of the process and the nature of data involved. It gives a view of the personal data in play, its indispensability, and its proportionality. These examinations are grounded in the basic tenets of the case at hand. What stands out are the recurring themes that emerge, shedding light on patterns and consistencies. The lucidity in your explanation aids in navigating through this complexity, offering me a lens into your thought process. It's evident that such a methodical approach would elevate the quality of the PIA."

Integration of Use Cases: Participant 3 highlighted the integration of use cases, which enriches the assessment process. "The concepts of 'necessity' and 'proportionality', though summarised in one line, are now enveloped by a use case. This use case demystifies the 'how' and 'why' behind the assessment, albeit at an elevated level. From my vantage point, this direction feels promising."

7.3.5 Validation of activity risk assessment

The participants imparted their knowledge and perspectives on risk assessment, touching upon the fundamental principles of consistency, as well as the distinction between threats and vulnerabilities.

The Imperative of Consistency: Participant 4 shed light on the cornerstone of an effective risk assessment: consistency. "As diverse cases present themselves, it's vital to employ the same risk assessment technique across the board. Such a disciplined approach guarantees that risks are identified, evaluated, and documented in a standardised fashion. Deviating from this method introduces disorder, culminating in inconsistent and potentially unreliable results."

Delineating Threats and Vulnerabilities: Further, Participant 4 delved into the distinction between threats and vulnerabilities, particularly within the context of information security. "While threats are a significant aspect of information security, one cannot overlook the importance of identifying vulnerabilities. Picture a scenario where there's a door that cannot be secured. The imminent threat in this situation is an unauthorised person, perhaps a burglar, capitalising on this vulnerability to gain entry. Drawing a clear line between threats and vulnerabilities is essential. Recognising a specific vulnerability, like the aforementioned unsecured door, and its potential threat, such as the burglar, sets the stage for crafting various mitigate strategies."

7.3.6 Validation of activity Risk Measures

The participants provided their perspectives on risk measures, emphasising the importance of specificity, the contrast between technical and organisational solutions, and the differing approaches between governmental and commercial entities.

The Need for Specificity: Participant 1 highlighted the importance of precision when discussing identifiers in risk measures. "Identifiers are not just recommended; they are essential. Should one detail them? Absolutely. They must not only be mentioned but also clearly described and named."

Technical vs. Organisational Solutions: Participant 2 presented a pragmatic approach to challenges in risk measures. "There's a boundary to what can be achieved

technically. If we hit a wall on the technical front, but there's room for an organisational solution, then it's imperative to come to a mutual agreement on the way forward."

Government vs. Commercial Approaches: Participant 3 outlined the contrasting strategies between government institutions and commercial entities when addressing risks. "There's a pronounced difference in how risk measures are approached by governmental bodies compared to commercial enterprises. Governments tend to prioritise accuracy and compliance, often irrespective of the associated costs. On the other hand, commercial organisations operate within set budgets. They aim to achieve their objectives within these financial constraints, and once the budget is depleted, the resources cease."

7.3.7 Validation of activity report

The participants shared their perspectives on the reporting aspect, emphasising the need for external audits based on project size and the importance of giving due attention to the PIA.

Role of External Audits: The first participant brought forward the idea that the magnitude of a project should influence the decision to engage a third party for an audit. "The scale of the project ought to dictate whether an external audit is necessary. Larger projects, given their potential impact and complexity, may benefit from an impartial third-party review."

Underestimation of PIA: Participant 2 highlighted a concerning trend observed in some organisations regarding the treatment of PIAs. "From my observations, PIAs tend to be sidelined in many organisations, not receiving the prominence they warrant. In an era with privacy challenges, and with entities like our works council keeping a eye, it's paramount that PIAs are prioritised. Regrettably, they are frequently relegated to being mere footnotes in project plans."

7.3.8 Points for recommendation

The participants found the PIA process, along with its associated deliverables, to be coherent and logical. They felt that the proposed sequence of steps, complemented by the specified deliverables, was apt and didn't see a need for any alterations.

The participants observed that within the government, the PROJECT BRIEF and THRESHOLD ANALYSIS are combined into a single document. However, it is worth noting that this practice may not be universal across other organisations. To ensure a broader applicability, the decision was made to maintain these two deliverables as separated entities.

The term PROJECT BRIEF has led to some confusion among the participants. To ensure clarity en eliminate any ambiguity it is recommended to rename this concept to a more descriptive and straightforward term. Therefore it is recommended to change PROJECT BRIEF to PRE-PIA BRIEF.

The sub-activity *inform DPO of PIA* is somewhat ambiguous. This is because, in addition to being informed the DPO is also required to provide permission. As a result, the use of the word *inform* may not fully capture the essence of the process. To ensure clarity and avoid any misunderstanding, it is recommended to replace the term *inform* with a more descriptive and accurate term that encompasses the entire scope of the sub-activity. Therefore it is better to call the activity *Consult DPO of PIA* instead of *Inform DPO of PIA*

The concept of *view creation* could be unclear or vague. To effectively reconcile the gap between theoretical concepts and their actual implementation, it is crucial to employ vocabulary that is both accurate and comprehensible. This would guarantee that even persons lacking an understanding of the process may nevertheless establish a connection with and realise its significance. Therefore, it is advisable to substitute the phrase *view creation* with a terminology that possesses a broader comprehension and appeals to a more extensive range of individuals. Other terms that are considered include Architecture Viewpoints, System Models, and Processing Diagrams.

This PIA is primarily focused on threats. However, one of the participants pointed out the importance of differentiating between threats and vulnerabilities. By delineating and addressing both threats and vulnerabilities, a more robust model can be developed. This distinction not only enriches the assessment but also provides a more holistic understanding, ensuring that potential weaknesses are identified and addressed effectively.

Incorporating the option to only conduct a third-party audit by determine the necessity could be achieved by introducing a logical decision branch. This would empower participants by giving them the choice to determine whether they wish to proceed with such an audit. Providing this flexibility ensures that participants can tailor the process to their specific needs and preferences, enhancing the overall model.

8 Conclusion & Discussion

This chapter offers an overview of the study's primary outcomes, addresses the research questions, highlights key theoretical and practical insights, and suggests potential directions for subsequent research.

8.1 Conclusion

This study was initiated by identifying a gap in carrying out a detailed-level PIA. This observation gave rise to the subsequent problem statement:

> **Improve** the PIA process and its deliverables for different maturity levels
>
> **by** designing an incremental PIA method integrated with the Privacy by Design Maturity Model (PbDMM)
>
> **that is** usable, satisfies the GDPR requirements, and displays a growth path through the maturity levels of the PbDMM
>
> **in order to** help organisations validate and incrementally improve their PIA procedures.

To tackle this problem statement a main research question was created: *How to design a PIA process that is integrated with the PbDMM, that covers a constant review mechanism, is ongoing, and prevalent throughout the technology or system design life cycle by using incremental method evolution?* This main research question further breaks down into four distinct questions, each of which is explored and answered in the succeeding four subsections.

8.1.1 Research question 1

The objective of the first research question was to examine existing literature pertaining to the PIA process steps and associated deliverables. This extensive review aimed to establish a foundational understanding and a solid operational base from which subsequent explorations and enhancements could be constructed. This resulted into the following research question.

> RQ 1: What is the state-of-the-art of literature about PIA process steps and deliverables?

To address this research question, a thorough literature review was conducted as outlined in our research plan. This study led to the selection of 41 papers, each detailing a complete PIA. Upon analysing these documents, we identified 577 process steps and 167 deliverables. It was anticipated that these two figures would differ. The discrepancy arises from the observation that existing literature often provides a broad overview of the PIA, lacking granularity at the detail level. Consequently, many process steps are presented in a generic manner without being paired with a specific deliverable. After identifying all the process steps and deliverables, they were systematically coded using an a-priori coding technique. This method allowed for a more organised and structured categorisation of the data. As a result, distinct and concrete process steps were determined, each paired with its corresponding deliverable. This approach ensured precision and clarity in understanding the relationships between the steps and their associated outputs. By leveraging a-priori coding, the research was able to establish a foundation for the PIA PDD.

8.1.2 Research question 2

The aim of this particular research question was to develop a structured roadmap that practitioners can initially utilise, guiding them progressively in maturing their organisation's practices and strategies. This step-by-step guide intends to foster growth and refinement within organisational processes, enabling a clear path from inception to advanced levels of proficiency.

> RQ 2: What are the process steps per maturity level?

To address the posed research question, the newly crafted PIA was then compared with a Focus Area Maturity Model specifically tailored for Privacy-by-Design, as detailed in [56].

A thorough examination of the capabilities inherent within the PbDMM was conducted. The objective was to pinpoint best practices corresponding to each maturity level. This examination made it possible to document these practices, ensuring they are actionable and relevant for organisations at various stages of maturity.

Following this examination, the insights were integrated into the PIA. The process steps and deliverables within the PIA were coloured and organised. This not only enhanced the visual appeal of the PIA but also facilitated a more streamlined understanding of its contents, ensuring that stakeholders can easily navigate and implement the provided recommendations.

8.1.3 Research question 3

The primary objective of this research question was to develop a new artefact. After an analysis of the included papers, we translated our findings into a coding scheme. Using this structured coding scheme, we then constructed a Process Deliverable Diagram. This diagram served as a visual representation, aiding in the better understanding and interpretation of the entire process. Through this methodical approach, we ensured that the resulting artefact was both meaningful and aligned with the insights garnered from research question 2.

> RQ 3: How does the revised PIA with an emphasis on incremental method engineering look like?

The revised PIA commences with a broad, high-level overview. This overarching view is organised into four strategic steps: the Pre-PIA phase, the PIA phase, the Implementation phase, and the Monitoring phase. For the purposes of our research, our attention is predominantly concentrated on the initial two phases: Pre-PIA and PIA.

From this focus, we derived a set of 7 main activities, each with its unique sub-activities and deliverables:

Pre-PIA Activity: This is the foundational step and contains 5 sub-activities. At the end of this activity, two key deliverables are produced, ensuring that the groundwork is appropriately laid out for the subsequent phases.

PIA-Preparation Activity: Serving as a bridge to the actual assessment, this activity involves 9 specific sub-activities. The meticulous process within this activity results in 6 crucial deliverables, preparing the ground for a thorough impact assessment.

View Creation Activity: This activity, with its 6 sub-activities, is pivotal in shaping the perspective of the assessment. By its conclusion, there are 7 significant deliverables that provide a clearer visualisation of the data under assessment.

Assessment Activity: A central component of the PIA, this activity comprises 6 sub-activities. The outcome of this rigorous assessment phase is 7 essential deliverables that form the legal ramification that the processing activity is lawful, necessary and proportional.

Risk Assessment Activity: This activity delves into identifying potential risks, with 5 sub-activities. The in-depth analysis culminates in 6 vital deliverables, highlighting the possible vulnerabilities and areas of concern.

Risk Measures Activity: Acting as a responsive phase to the prior activity, this segment consists of 10 sub-activities. The exhaustive process leads to the generation of 9 critical deliverables, outlining the measures and strategies to mitigate identified risks.

Report Activity: The culmination of the entire PIA process, this activity contains 7 sub-activities. Its primary purpose is to document and present findings, and it achieves this through 5 definitive deliverables, providing stakeholders with a report on the assessment's findings and recommendations.

Through this detailed breakdown, the revised PIA offers a structured, step-by-step approach, ensuring that each phase and activity is addressed with utmost precision and clarity.

8.1.4 Research question 4

Research question 4 was formulated to verify the efficacy of the newly developed artefact. The primary objective of this phase is to determine the extent to which the actual outcomes of the artefact align with its anticipated advantages. This gave rise to the subsequent research question:

RQ4: How does the new re-designed PIA perform in practice?

RQ 4.1 How does the framework perform?

RQ 4.2 What recommendations can be made?

The evaluation of the PIA was carried out using a qualitative approach, specifically through four semi-structured interviews involving experts in the field. These practitioner experts provided insights that were pivotal in measuring the effectiveness and utility of the PIA.

The first sub-research question, labelled as *RQ 4.1: How does the framework perform?*, sought to understand the reception and applicability of the newly devised model. Encouragingly, the feedback was overwhelmingly positive. Every interviewee expressed a favourable view of the model, highlighting its potential benefits. They were particularly impressed by the process steps and their respective deliverables, noting that these elements are instrumental in facilitating the execution of a PIA.

However, it's worth noting that a significant number of interviewees were unfamiliar with some of the steps outlined in the PIA. Despite this lack of recognition, they opined that these steps were valuable additions that should be incorporated. This feedback further underscores the PIAs multifaceted role. Not only does it serve as a guide for conducting assessments, but it also acts as a roadmap, illuminating the path towards achieving varying maturity levels in the realm of privacy practices.

The secondary sub-research question, denoted as *RQ 4.2 What recommendations can be made?*, was integrated with the intent of identifying specific areas of enhancement within the PIA process. This exploration aimed to derive actionable recommendations that could bolster the effectiveness and efficiency of the PIA process. As a

result, several concrete improvement steps were proposed, emphasising areas that were pivotal to refining the overall method and execution of the PIA.

8.2 Discussion

The discussion primarily revolves around two central themes, both of which emerged prominently during the validation interviews. These themes not only captured the essence of the feedback received but also stood out due to their recurring nature, highlighting their significance in the broader context of the discussions.

8.2.1 Underestimation of PIA

The concept of "End-to-End Lifecycle Protection" is considered a fundamental premise in the framework of PbD. The aforementioned principle highlights the significance of incorporating privacy considerations at the early stages of a system or project's existence, even before any data is collected. It is crucial to maintain these considerations throughout the entire lifecycle of the data, starting from its inception and continuing until its ultimate conclusion [24].

When applying this principle to the context of a PIA, it emphasizes the need of initiating the PIA from the outset of the project and consistently utilising it to inform privacy-related decisions and evaluations throughout the project's entirety. The thoughts expressed in a research conducted by [43] align with the aforementioned concerns, highlighting the potential compromise of privacy safeguards due to the delayed implementation of PIAs in various projects.

During the course of the research interviews, participants expressed similar feelings, with one interviewee explicitly drawing attention to the widespread occurrence of delays in commencing PIAs. The aforementioned delays not only undermine the efficacy of the PIA, but also have the potential to lead to subsequent modifications and escalated expenses.

One potential approach to guaranteeing the prompt commencement of PIAs is to establish a clearly defined PIA procedure that is firmly integrated into the operational framework of the organisation. In order to enhance the effectiveness of this procedure, it is recommended to supplement it with periodic instructional workshops that are designed to raise awareness among employees about the importance of conducting early and ongoing PIAs. By cultivating a culture that recognises privacy considerations as essential rather than secondary, companies can effectively communicate that PIAs are not only administrative procedures but vital mechanisms that protect both the organisation and its stakeholders.

8.2.2 Significance of concrete improvement steps for a PIA

The defined model provides companies with a framework that encompasses a range of stages, from basic to complex, allowing them to assess their capabilities and identify areas for development. According to a study conducted by [77], the existing methodologies for assessing privacy risks and impacts are mostly designed for static environments, including the stages of requirement formulation, design, and implementation.

During the process of validation, participants acquired significant insights through an exploration of various degrees of maturity. The implementation of the structured

classification technique enabled an examination of the PIA process and empowered participants to critically evaluate their procedures.

The aforementioned input underscores the necessity of clearly defining and assigning duties within the process of PIA. The task at hand involves more than simply allocating responsibilities; it necessitates ensuring that every stakeholder, ranging from the privacy officer to the business units, possesses an understanding of their position within the larger framework and possesses the requisite tools and skills to effectively carry it out.

The efficacy of a PIA is contingent not only upon its theoretical underpinnings but also on the actual competence of its implementation. As organisations delve further into the domain of privacy and data protection, it is crucial to guarantee that all entities involved, irrespective of their position within the organisational structure, possess an understanding of their responsibilities and are equipped with the necessary expertise and education to fulfil them effectively.

Within a broader framework, this could entail implementing a more formalised on-boarding procedure for those engaged in PIAs, offering targeted training sessions tailored to specific needs, or organising recurrent seminars aimed at addressing issues and reinforcing fundamental understanding. organisations can achieve optimal efficacy in their PIA processes only by implementing comprehensive and holistic methodologies.

8.3 Threats to validity

The integrity of a study is judged by its validity, which speaks to how truthful its outcomes are, devoid of bias or the researchers' personal views [72]. The potential constraints of this study are discussed in line with the four main threats to validity in case studies: construct validity, internal validity, external validity, and reliability [95, 72, 101].

8.3.1 Construct Validity

Construct validity deals with ensuring that the measures under investigation align with the research objectives and questions. Challenges to this validity arise when there's a mismatch in understanding the constructs between the study participants and the researcher [96]. In the context of this study, the primary goal was evaluating the PIAs efficacy. To bolster the research's construct validity, a validation interview was held to identify and rectify any discrepancies and to refine the PIA to fit the intended framework.

To strengthen the study's construct validity, multiple research methods were leveraged, encompassing both literature reviews and expert consultations. This multifaceted approach provided an view of the subject, enhancing the overall credibility of the findings. By tapping into both methodologies, the research addressed their individual limitations, leading to a more nuanced understanding of the PIA. However, it's worth noting that broadening the research methodologies or sourcing data from an even wider array of resources could have further solidified the construct validity.

In qualitative research forms like expert interviews, researcher bias can compromise construct validity. This study made a conscious effort to minimise such influences. Instead of using leading questions, experts were actively incorporated into the research, creating a space for them to share their authentic opinions. This approach not only minimised bias but also promoted open and honest discussions, bolstering the study's credibility.

8.3.2 Internal Validity

Internal validity is critical when establishing causal relationships. When assessing the influence of one element on another, there might be a third unseen factor also impacting the study's subject. Unawareness of this third factor can harm the study's internal validity [96].

A systematic literature review poses certain challenges. Its legitimacy relies on transparency and replicability. To counter potential risks, it's essential to delineate the processes used to formulate and implement search terms. By being transparent, other researchers can reproduce the same search and achieve similar results. Additionally, to ensure a consistent selection process, a subset of the papers was reviewed by two researchers. This collaborative approach reduced potential biases in paper selection.

Data coding discrepancies can further hinder internal validity. Subjective interpretations during qualitative data analysis can result in varied outcomes. To counteract this, a clear coding strategy is paramount. Even with detailed protocols, human interpretation can differ. To counter this, dual coding was employed, allowing for the comparison of results, ensuring consistent interpretation. If disagreements arose, discussions between researchers aimed to reach a consensus.

Potential biases in participant selection, especially when relying on interviews, can also harm internal validity. By focusing on government officials, the study may have limited its broader applicability. To address this, a diverse set of participants within the government sector was interviewed, ensuring an understanding within the chosen domain.

8.3.3 External Validity

External validity assesses if a study's outcomes can be generalised to other scenarios or groups. The study's generalizability is an indicator of its external validity [96]. With the introduction of the GDPR, PIAs became mandatory, making this study pertinent for organisations handling personal data within the EU.

However, it's crucial to recognise that the study's broader applicability might be limited since the validation was conducted in an EU state. Different jurisdictions might have unique laws and cultural nuances affecting privacy assessments. To broaden the study's scope, the term "Privacy Impact Assessment" was used, reflecting a global understanding of privacy concerns. The inclusion of non-EU articles ensured a wider range of viewpoints, making the findings more universally applicable.

8.3.4 Reliability

Reliability pertains to the study's consistency irrespective of the researcher [96]. If varied outcomes emerge, the PIA method's reliability could be questioned.

For this study, it was vital to ensure that the PIA method produced consistent evaluations. One reliability concern was the limited participant number for the validation case study. To enhance future research's reliability, multiple validation case studies are recommended, ensuring diverse participant involvement.

8.4 Study Limitations

The PIA research revealed several limitations. A major limitation was the sample's scope and diversity. While our findings are insightful, a larger, more diverse sample could have provided more globally applicable results. The study's EU-centric focus

raises questions about its applicability outside the EU, especially in regions with different data protection norms.

Limiting the participant pool to the government sector might not capture other industries' views. Methodologically, our reliance on literature and expert opinions might have introduced biases. Employing diverse data collection techniques might have offered a more rounded view.

Data protection standards and technology are ever-evolving, adding a time-sensitive limitation. Our research offers a snapshot of the current state of PIAs, which might change with technological or regulatory advancements. Research biases, either from the team or the participants, are always a concern. Our primary PIA focus might have overshadowed broader trends. The dynamic nature of PIAs demands continuous adaptation, and while our core findings are robust, alternate models could offer different insights.

Despite these limitations, our research's value remains intact. These findings pave the way for more in-depth future studies. This research followed Wieringa's (2014) design cycle once, with time constraints defining the scope. With more time, multiple design cycle iterations could have been pursued, further validating the results. Future endeavours would benefit from long-term observations, especially regarding validation of improvements, an aspect not fully covered in our study.

8.5 Further Research

The research conducted serves as a step towards understanding of the PIA. Given the outcomes and limitations of the study, the following avenues for further research are proposed:

1. **Cross-industry Analysis:** This research primarily focused on the government sector. Future studies could delve into PIAs' application and nuances in various industries such as healthcare, finance, and technology. Each sector has unique data protection challenges that a PIA would need to address specifically.
2. **Global Perspective:** While this study had an EU-centric lens, it would be invaluable to explore PIAs from a global perspective. Understanding how different jurisdictions and cultures approach privacy assessments could lead to a more universally adaptable PIA framework.
3. **Evolution of PIAs:** As data protection standards and technologies evolve, PIAs need to adapt. A longitudinal study tracking the evolution of PIAs over time, especially in response to technological advancements and changing regulations, would provide insights into the dynamic nature of data protection.
4. **Implementation Challenges:** Future research could focus on the practical challenges organisations face when implementing PIAs. This could lead to the development of tools, best practices, and strategies to assist organisations in effectively conducting PIAs.
5. **Educational Initiatives:** Given the importance of early and ongoing PIAs, research could explore educational strategies to raise awareness and competence in organisations. This could range from on-boarding procedures, training sessions, to seminars focusing on PIAs.
6. **PIA Automation:** With the increasing role of technology in data protection, exploring the potential for automating certain aspects of the PIA process could

be an avenue for future research. This could include tools for risk assessment, monitoring, and reporting.

The outlined suggestions are by no means complete but represent a starting point for delving deeper into the multifaceted domain of PIAs. Given the ever-increasing importance of data protection in today's digital age, continued research in this domain is not only beneficial but essential.

References

[1] Saeed Abu-Nimeh and Nancy R Mead. "Combining Privacy and Security Risk Assessment in Security Quality Requirements Engineering". en. In: ().

[2] Alessandro Acquisti, Curtis Taylor, and Liad Wagman. "The Economics of Privacy". en. In: *Journal of Economic Literature* 54.2 (June 2016), pp. 442–492. ISSN: 0022-0515. DOI: 10.1257/jel.54.2.442. URL: https://pubs.aeaweb.org/doi/10.1257/jel.54.2.442 (visited on 03/01/2023).

[3] Amir Shayan Ahmadian et al. "Supporting privacy impact assessment by model-based privacy analysis". en. In: *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*. Pau France: ACM, Apr. 2018, pp. 1467–1474. ISBN: 978-1-4503-5191-1. DOI: 10.1145/3167132.3167288. URL: https://dl.acm.org/doi/10.1145/3167132.3167288 (visited on 05/01/2023).

[4] Rehab Alnemr et al. "A Data Protection Impact Assessment Methodology for Cloud". en. In: *Privacy Technologies and Policy*. Ed. by Bettina Berendt et al. Vol. 9484. Series Title: Lecture Notes in Computer Science. Cham: Springer International Publishing, 2016, pp. 60–92. ISBN: 978-3-319-31455-6 978-3-319-31456-3. DOI: 10.1007/978-3-319-31456-3_4. URL: http://link.springer.com/10.1007/978-3-319-31456-3_4 (visited on 05/01/2023).

[5] Majed Alshammari and Andrew Simpson. "Privacy Architectural Strategies: An Approach for Achieving Various Levels of Privacy Protection". en. In: *Proceedings of the 2018 Workshop on Privacy in the Electronic Society*. Toronto Canada: ACM, Jan. 2018, pp. 143–154. ISBN: 978-1-4503-5989-4. DOI: 10.1145/3267323.3268957. URL: https://dl.acm.org/doi/10.1145/3267323.3268957 (visited on 11/16/2022).

[6] General Assembly. "Article 12". In: (). URL: http://nations-united.org/Universal_Declaration_Of_Human_Rights/Articles_Human_Rights/Articles_12_Human_Rights_Universal_Declaration_Nations_United_Twelve.htm.

[7] Brooke Auxier et al. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information". In: *PEW RESEARCH CENTER* (Nov. 2019), p. 63. URL: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[8] M. Bas Seyyar and Z.J.M.H. Geradts. "Privacy impact assessment in large-scale digital forensic investigations". en. In: *Forensic Science International: Digital Investigation* 33 (June 2020), p. 200906. ISSN: 26662817. DOI: 10.1016/j.fsidi.2020.200906. URL: https://linkinghub.elsevier.com/retrieve/pii/S2666281720300263 (visited on 05/01/2023).

[9] Jörg Becker, Ralf Knackstedt, and Jens Pöppelbuß. "Developing Maturity Models for IT Management: A Procedure Model and its Application". en. In: *Business & Information Systems Engineering* 1.3 (June 2009), pp. 213–222. ISSN: 1867-0202. DOI: 10.1007/s12599-009-0044-5. URL: http://link.springer.com/10.1007/s12599-009-0044-5 (visited on 03/01/2022).

[10] Kathrin Bednar, Sarah Spiekermann, and Marc Langheinrich. "Engineering Privacy by Design: Are engineers ready to live up to the challenge?" en. In: *The Information Society* 35.3 (May 2019), pp. 122–142. ISSN: 0197-2243, 1087-6537. DOI: 10.1080/01972243.2019.1583296. URL: https://www.tandfonline.com/doi/full/10.1080/01972243.2019.1583296 (visited on 03/01/2023).

[11] Bélanger and Crossler. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems". en. In: *MIS Quarterly* 35.4 (2011), p. 1017. ISSN: 02767783. DOI: 10.2307/41409971. URL: https://www.jstor.org/stable/10.2307/41409971 (visited on 03/01/2023).

[12] Colin J. Bennett and Charles D. Raab. "Revisiting the governance of privacy: Contemporary policy instruments in global perspective". en. In: *Regulation & Governance* 14.3 (July 2020), pp. 447–464. ISSN: 1748-5983, 1748-5991. DOI: 10.1111/rego.12222. URL: https://onlinelibrary.wiley.com/doi/10.1111/rego.12222 (visited on 02/27/2023).

[13] Ana P Betrán et al. "Effectiveness of different databases in identifying studies for systematic reviews: experience from the WHO systematic review of maternal morbidity and mortality". en. In: *BMC Medical Research Methodology* 5.1 (Dec. 2005), p. 6. ISSN: 1471-2288. DOI: 10.1186/1471-2288-5-6. URL: http://bmcmedresmethodol.biomedcentral.com/articles/10.1186/1471-2288-5-6 (visited on 03/27/2023).

[14] Felix Bieker et al. "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation". en. In: *Privacy Technologies and Policy*. Ed. by Stefan Schiffner et al. Vol. 9857. Series Title: Lecture Notes in Computer Science. Cham: Springer International Publishing, 2016, pp. 21–37. ISBN: 978-3-319-44759-9 978-3-319-44760-5. DOI: 10.1007/978-3-319-44760-5_2. URL: http://link.springer.com/10.1007/978-3-319-44760-5_2 (visited on 05/01/2023).

[15] Felix Bieker et al. "Data Protection Impact Assessment: A Hands-On Tour of the GDPR's Most Practical Tool". en. In: *Privacy and Identity Management. The Smart Revolution*. Ed. by Marit Hansen et al. Vol. 526. Series Title: IFIP Advances in Information and Communication Technology. Cham: Springer International Publishing, 2018, pp. 207–220. ISBN: 978-3-319-92924-8 978-3-319-92925-5. DOI: 10.1007/978-3-319-92925-5_13. URL: https://link.springer.com/10.1007/978-3-319-92925-5_13 (visited on 05/01/2023).

[16] Reuben Binns. "Data protection impact assessments: a meta-regulatory approach". en. In: *International Data Privacy Law* 7.1 (Feb. 2017), pp. 22–35. ISSN: 2044-3994, 2044-4001. DOI: 10.1093/idpl/ipw027. URL: https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipw027 (visited on 02/28/2023).

[17] Erik Blair. "A reflexive exploration of two qualitative data coding techniques". en. In: ().

[18] Vincent Blijleven et al. "A meta-modeling technique for analyzing, designing and adapting healthcare processes: A process-deliverable perspective". en. In: *2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI)*. Las Vegas, NV, USA: IEEE, Feb. 2016, pp. 316–319. ISBN: 978-

1-5090-2455-1. DOI: 10.1109/BHI.2016.7455898. URL: http://ieeexplore.ieee.org/document/7455898/ (visited on 09/18/2023).

[19] Wichor M. Bramer et al. "Optimal database combinations for literature searches in systematic reviews: a prospective exploratory study". en. In: *Systematic Reviews* 6.1 (Dec. 2017), p. 245. ISSN: 2046-4053. DOI: 10.1186/s13643-017-0644-y. URL: https://systematicreviewsjournal.biomedcentral.com/articles/10.1186/s13643-017-0644-y (visited on 03/27/2023).

[20] Sjaak Brinkkemper. "Method engineering: engineering of information systems development methods and tools". en. In: *Information and Software Technology* 38.4 (Jan. 1996), pp. 275–280. ISSN: 09505849. DOI: 10.1016/0950-5849(95)01059-9. URL: https://linkinghub.elsevier.com/retrieve/pii/0950584995010599 (visited on 10/20/2021).

[21] Tobias Bucher et al. "Situational Method Engineering". en. In: ().

[22] Alan Calder. *EU GDPR: an international guide to compliance*. en. OCLC: 1203021495. Ely, Cambridgeshire: ITGP, 2020. ISBN: 978-1-78778-254-9.

[23] Ann Cavoukian. "Privacy by Design The 7 Foundational Principles". en. In: (2009). URL: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

[24] Ann Cavoukian. *Privacy-by-design: The 7 Foundational Principles*. 2011. URL: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

[25] Roger Clarke. "Privacy impact assessment: Its origins and development". en. In: *Computer Law & Security Review* 25.2 (2009), pp. 123–135. DOI: https://doi.org/10.1016/j.clsr.2009.02.002.

[26] Joshua Coles, Shamal Faily, and Duncan Ki-Aries. "Tool-Supporting Data Protection Impact Assessments with CAIRIS". en. In: *2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE)*. Banff, AB: IEEE, Aug. 2018, pp. 21–27. ISBN: 978-1-5386-8420-7. DOI: 10.1109/ESPRE.2018.00010. URL: https://ieeexplore.ieee.org/document/8501328/ (visited on 05/01/2023).

[27] Council of the and European Union. *Interinstitutional File: 2012/0011 (COD)*. 2015. URL: https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf.

[28] Deloitte. "Are data privacy concerns driving consumer behavior? Not yet." In: (Aug. 2021). URL: https://www2.deloitte.com/us/en/insights/industry/technology/protecting-consumer-data.html.

[29] Tamara Dinev, Paul Hart, and Michael R. Mullen. "Internet privacy concerns and beliefs about government surveillance – An empirical investigation". en. In: *The Journal of Strategic Information Systems* 17.3 (Sept. 2008), pp. 214–233. ISSN: 09638687. DOI: 10.1016/j.jsis.2007.09.002. URL: https://linkinghub.elsevier.com/retrieve/pii/S0963868707000492 (visited on 02/27/2023).

[30] Owen Doody and Maria Noonan. "Preparing and conducting interviews to collect data". en. In: *Nurse Researcher* 20.5 (May 2013), pp. 28–32. ISSN: 1351-5578, 2047-8992. DOI: 10.7748/nr2013.05.20.5.28.e327. URL: http://rcnpublishing.com/doi/abs/10.7748/nr2013.05.20.5.28.e327 (visited on 09/21/2023).

[31] EDPB. *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*. 2017. URL: https://ec.europa.eu/newsroom/article29/items/611236.

[32] European Parliament and Council of the European Union. *Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. May 2016. URL: http://data.europa.eu/eli/reg/2016/679/2016-05-04.

[33] Simone Fischer-Hübner et al., eds. *Privacy Enhancing Technologies: 12th International Symposium, PETS 2012, Vigo, Spain, July 11-13, 2012. Proceedings*. en. Vol. 7384. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012. ISBN: 978-3-642-31679-1 978-3-642-31680-7. DOI: 10.1007/978-3-642-31680-7. URL: https://link.springer.com/10.1007/978-3-642-31680-7 (visited on 03/01/2023).

[34] Michael Friedewald et al. "Data Protection Impact Assessments in Practice: Experiences from Case Studies". en. In: *Computer Security. ESORICS 2021 International Workshops*. Ed. by Sokratis Katsikas et al. Vol. 13106. Series Title: Lecture Notes in Computer Science. Cham: Springer International Publishing, 2022, pp. 424–443. ISBN: 978-3-030-95483-3 978-3-030-95484-0. DOI: 10.1007/978-3-030-95484-0_25. URL: https://link.springer.com/10.1007/978-3-030-95484-0_25 (visited on 05/01/2023).

[35] P. Garbacz and O. Kutz. *Formal Ontology in Information Systems: Proceedings of the Eighth International Conference (FOIS 2014)*. EBSCO ebook academic collection. IOS Press, 2014. ISBN: 978-1-61499-438-1. URL: https://books.google.nl/books?id=oG7YBAAAQBAJ.

[36] Ayo Gbadeyan, Sergey Butakov, and Shaun Aghili. "IT governance and risk mitigation approach for private cloud adoption: case study of provincial healthcare provider". en. In: *Annals of Telecommunications* 72.5-6 (June 2017), pp. 347–357. ISSN: 0003-4347, 1958-9395. DOI: 10.1007/s12243-017-0568-5. URL: http://link.springer.com/10.1007/s12243-017-0568-5 (visited on 05/01/2023).

[37] Georgios Georgiadis and Geert Poels. "Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review". en. In: *Computer Law & Security Review* 44 (Apr. 2022), p. 105640. ISSN: 02673649. DOI: 10.1016/j.clsr.2021.105640. URL: https://linkinghub.elsevier.com/retrieve/pii/S0267364921001138 (visited on 06/26/2023).

[38] Dimitra Georgiou and Costas Lambrinoudakis. "Data Protection Impact Assessment (DPIA) for Cloud-Based Health Organizations". en. In: *Future Internet* 13.3 (Mar. 2021), p. 66. ISSN: 1999-5903. DOI: 10.3390/fi13030066. URL: https://www.mdpi.com/1999-5903/13/3/66 (visited on 05/01/2023).

[39] Michelle Goddard. "The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact". en. In: *International Journal of Market Research* 59.6 (Nov. 2017), pp. 703–705. ISSN: 1470-7853, 2515-2173. DOI: 10.2501/IJMR-2017-050. URL: http://journals.sagepub.com/doi/10.2501/IJMR-2017-050 (visited on 02/13/2023).

[40] Frank Harmsen, Sjaak Brinkkemper, and Han Oei. "Situational Method Engineering for Information System Project Approaches". en. In: ().

[41] Jane Henriksen-Bulmer, Shamal Faily, and Sheridan Jeary. "DPIA in Context: Applying DPIA to Assess Privacy Risks of Cyber Physical Systems". en. In: *Future Internet* 12.5 (May 2020), p. 93. ISSN: 1999-5903. DOI: 10.3390/fi12050093. URL: https://www.mdpi.com/1999-5903/12/5/93 (visited on 05/01/2023).

[42] Jane Henriksen-Bulmer, Shamal Faily, and Sheridan Jeary. "Implementing GDPR in the Charity Sector: A Case Study". en. In: *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*. Ed. by Eleni Kosta et al. Vol. 547. Series Title: IFIP Advances in Information and Communication Technology. Cham: Springer International Publishing, 2019, pp. 173–188. ISBN: 978-3-030-16743-1 978-3-030-16744-8. DOI: 10.1007/978-3-030-16744-8_12. URL: https://link.springer.com/10.1007/978-3-030-16744-8_12 (visited on 05/01/2023).

[43] Jaap-Henk Hoepman. *Privacy Design Strategies (The Little Blue Book)*. 2022. URL: https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf.

[44] Christina Höfer et al. "POPCORN: privacy-preserving charging for emobility". en. In: *Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles*. Berlin Germany: ACM, Nov. 2013, pp. 37–48. ISBN: 978-1-4503-2487-8. DOI: 10.1145/2517968.2517971. URL: https://dl.acm.org/doi/10.1145/2517968.2517971 (visited on 05/01/2023).

[45] Christopher Irvine, Dharini Balasubramaniam, and Tristan Henderson. "Short Paper: Integrating the Data Protection Impact Assessment into the Software Development Lifecycle". en. In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Ed. by Joaquin Garcia-Alfaro, Guillermo Navarro-Arribas, and Jordi Herrera-Joancomarti. Vol. 12484. Series Title: Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, pp. 219–228. ISBN: 978-3-030-66171-7 978-3-030-66172-4. DOI: 10.1007/978-3-030-66172-4_13. URL: https://link.springer.com/10.1007/978-3-030-66172-4_13 (visited on 05/01/2023).

[46] IT GOVERNANCE PRIVACY TEAM. *EU General Data Protection Regulation (GDPR) – An implementation and compliance guide, fourth edition*. IT Governance Publishing, Oct. 2020. ISBN: 978-1-78778-249-5 978-1-78778-248-8. DOI: 10.2307/j.ctv17f12pc. URL: http://www.jstor.org/stable/10.2307/j.ctv17f12pc (visited on 03/16/2023).

[47] Leonardo Horn Iwaya et al. "Mobile Health Systems for Community-Based Primary Care: Identifying Controls and Mitigating Privacy Threats". en. In: *JMIR mHealth and uHealth* 7.3 (Mar. 2019), e11642. ISSN: 2291-5222. DOI: 10.2196/11642. URL: http://mhealth.jmir.org/2019/3/e11642/ (visited on 05/01/2023).

[48] Philip Nicholas Johnson-Laird. *Mental models: Towards a cognitive science of language, inference, and consciousness*. Issue: 6. Harvard University Press, 1983. ISBN: 0-674-56882-6.

[49] Inga Kroener and David Wright. "A Strategy for Operationalizing Privacy by Design". en. In: *The Information Society* 30.5 (Oct. 2014), pp. 355–365. ISSN: 0197-2243, 1087-6537. DOI: 10.1080/01972243.2014.944730. URL: http://www.tandfonline.com/doi/abs/10.1080/01972243.2014.944730 (visited on 05/01/2023).

[50] Adina R. Lemeshow et al. "Searching one or two databases was insufficient for meta-analysis of observational studies". en. In: *Journal of Clinical Epidemiology* 58.9 (Sept. 2005), pp. 867–873. ISSN: 08954356. DOI: 10.1016/j.jclinepi.2005.03.004. URL: https://linkinghub.elsevier.com/retrieve/pii/S0895435605001356 (visited on 03/27/2023).

[51] He Li, Lu Yu, and Wu He. "The Impact of GDPR on Global Technology Development". en. In: *Journal of Global Information Technology Management* 22.1 (Jan. 2019), pp. 1–6. ISSN: 1097-198X, 2333-6846. DOI: 10.1080/1097198X.2019.1569186. URL: https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1569186 (visited on 03/16/2023).

[52] Salvatore T. March and Gerald F. Smith. "Design and natural science research on information technology". en. In: *Decision Support Systems* 15.4 (Dec. 1995), pp. 251–266. ISSN: 01679236. DOI: 10.1016/0167-9236(94)00041-2. URL: https://linkinghub.elsevier.com/retrieve/pii/0167923694000412 (visited on 01/03/2023).

[53] Yod-Samuel Martin and Antonio Kung. "Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering". en. In: *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. London, United Kingdom: IEEE, Apr. 2018, pp. 108–111. ISBN: 978-1-5386-5445-3. DOI: 10.1109/EuroSPW.2018.00021. URL: https://ieeexplore.ieee.org/document/8406568/ (visited on 11/16/2022).

[54] Chavi Mehta. "Amazon hit with record EU data privacy fine". In: *Reuters* (June 2021). URL: https://www.reuters.com/business/retail-consumer/amazon-hit-with-886-million-eu-data-privacy-fine-2021-07-30/ (visited on 08/02/2023).

[55] Michel Muszynski. "A Focus Area Maturity Model for Privacy-by-Design". en. MA thesis. Utrecht: Utrecht University, June 2023.

[56] Michel Muszynski et al. *A Focus Area Maturity Model for Privacy-by-Design*. en. Technical Report. Utrecht, The Netherlands: Utrecht University, June 2023. URL: https://github.com/MichelMuszynski/PbD-maturity-data/tree/main.

[57] Jonathan A. Obar and Anne Oeldorf-Hirsch. "The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services". en. In: *Information, Communication & Society* 23.1 (Jan. 2020), pp. 128–147. ISSN: 1369-118X, 1468-4462. DOI: 10.1080/1369118X.2018.1486870. URL: https://www.tandfonline.com/doi/full/10.1080/1369118X.2018.1486870 (visited on 03/07/2023).

[58] Marie Caroline Oetzel and Sarah Spiekermann. "A systematic methodology for privacy impact assessments: a design science approach". en. In: *European Journal of Information Systems* 23.2 (Mar. 2014), pp. 126–150. ISSN: 0960-085X, 1476-9344. DOI: 10.1057/ejis.2013.18. URL: https://www.tandfonline.com/doi/full/10.1057/ejis.2013.18 (visited on 11/16/2022).

[59] Marie Caroline Oetzel and Sarah Spiekermann. "PRIVACY-BY-DESIGN THROUGH SYSTEMATIC PRIVACY IMPACT ASSESSMENT - A DESIGN SCIENCE APPROACH". en. In: ().

[60] Tope Omitola et al. "User Configurable Privacy Requirements Elicitation in Cyber-Physical Systems". en. In: *Adjunct Proceedings of the 30th ACM Conference on User Modeling, Adaptation and Personalization*. Barcelona Spain: ACM, July 2022, pp. 109–119. ISBN: 978-1-4503-9232-7. DOI: 10.1145/3511047.3537683. URL: https://dl.acm.org/doi/10.1145/3511047.3537683 (visited on 05/01/2023).

[61] Matthew J. Page et al. "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews". en. In: *Systematic Reviews* 10.1 (Dec. 2021), p. 89. ISSN: 2046-4053. DOI: 10.1186/s13643-021-01626-4. URL: https://systematicreviewsjournal.biomedcentral.com/articles/10.1186/s13643-021-01626-4 (visited on 01/19/2023).

[62] Dimitrios Papamartzivanos et al. "A Perfect Match: Converging and Automating Privacy and Security Impact Assessment On-the-Fly". en. In: *Future Internet* 13.2 (Jan. 2021), p. 30. ISSN: 1999-5903. DOI: 10.3390/fi13020030. URL: https://www.mdpi.com/1999-5903/13/2/30 (visited on 05/01/2023).

[63] European Parlement. *DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*. English. Oct. 1995. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN.

[64] Ken Peffers et al. "A Design Science Research Methodology for Information Systems Research". en. In: *Journal of Management Information Systems* 24.3 (Dec. 2007), pp. 45–77. ISSN: 0742-1222, 1557-928X. DOI: 10.2753/MIS0742-1222240302. URL: https://www.tandfonline.com/doi/full/10.2753/MIS0742-1222240302 (visited on 12/30/2022).

[65] Ken Peffers et al., eds. *Design Science Research in Information Systems. Advances in Theory and Practice*. en. Vol. 7286. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012. ISBN: 978-3-642-29862-2 978-3-642-29863-9. DOI: 10.1007/978-3-642-29863-9. URL: http://link.springer.com/10.1007/978-3-642-29863-9 (visited on 01/03/2023).

[66] Insan Laksana Pribadi and Muhammad Suryanegara. "Regulatory recommendations for IoT smart-health care services by using privacy impact assessment (PIA)". en. In: *2017 15th International Conference on Quality in Research (QiR) : International Symposium on Electrical and Computer Engineering*. Nusa Dua: IEEE, July 2017, pp. 491–496. ISBN: 978-1-5090-6397-0. DOI: 10.1109/QIR.2017.8168535. URL: https://ieeexplore.ieee.org/document/8168535/ (visited on 05/01/2023).

[67] Jyri Rajamäki. "Design Science Research Towards Ethical and Privacy-Friendly Maritime Surveillance ICT Systems". en. In: *Digital Transformation, Cyber Security and Resilience of Modern Societies*. Ed. by Todor Tagarev et al. Vol. 84. Series Title: Studies in Big Data. Cham: Springer International Publishing, 2021, pp. 95–115. ISBN: 978-3-030-65721-5 978-3-030-65722-2. DOI: 10.1007/978-3-030-65722-2_7. URL: https://link.springer.com/10.1007/978-3-030-65722-2_7 (visited on 05/01/2023).

[68] Jenni Reuben et al. "Privacy Impact Assessment Template for Provenance". en. In: *2016 11th International Conference on Availability, Reliability and Security (ARES)*. Salzburg, Austria: IEEE, Aug. 2016, pp. 653–660. ISBN: 978-1-5090-0990-9. DOI: 10.1109/ARES.2016.95. URL: http://ieeexplore.ieee.org/document/7784630/ (visited on 05/01/2023).

[69] Antonio Robles-González, Javier Parra-Arnau, and Jordi Forné. "A LINDDUN-Based framework for privacy threat analysis on identification and authentication processes". en. In: *Computers & Security* 94 (July 2020), p. 101755. ISSN: 01674048. DOI: 10.1016/j.cose.2020.101755. URL: https://linkinghub.elsevier.com/retrieve/pii/S0167404820300390 (visited on 05/01/2023).

[70] Ira Rubinstein and Nathan Good. "Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents". en. In: *SSRN Electronic Journal* (2012). ISSN: 1556-5068. DOI: 10.2139/ssrn.2128146. URL: http://www.ssrn.com/abstract=2128146 (visited on 03/01/2023).

[71] Alejandra Ruiz et al. "Modeling ecosystems of reference frameworks for assurance: a case on privacy impact assessment regulation and guidelines". en. In: *Software and Systems Modeling* (Nov. 2022). ISSN: 1619-1366, 1619-1374. DOI: 10.1007/s10270-022-01061-6. URL: https://link.springer.com/10.1007/s10270-022-01061-6 (visited on 05/01/2023).

[72] Per Runeson and Martin Höst. "Guidelines for conducting and reporting case study research in software engineering". en. In: *Empirical Software Engineering* 14.2 (Apr. 2009), pp. 131–164. ISSN: 1382-3256, 1573-7616. DOI: 10.1007/s10664-008-9102-8. URL: http://link.springer.com/10.1007/s10664-008-9102-8 (visited on 06/02/2022).

[73] M Sampson. "Should meta-analysts search Embase in addition to Medline?" en. In: *Journal of Clinical Epidemiology* 56.10 (Oct. 2003), pp. 943–955. ISSN: 08954356. DOI: 10.1016/S0895-4356(03)00110-0. URL: https://linkinghub.elsevier.com/retrieve/pii/S0895435603001100 (visited on 03/27/2023).

[74] Jules Sarrat and Raphael Brun. "DPIA: How to Carry Out One of the Key Principles of Accountability". en. In: *Privacy Technologies and Policy*. Ed. by Manel Medina et al. Vol. 11079. Series Title: Lecture Notes in Computer Science. Cham: Springer International Publishing, 2018, pp. 172–182. ISBN: 978-3-030-02546-5 978-3-030-02547-2. DOI: 10.1007/978-3-030-02547-2_10. URL: http://link.springer.com/10.1007/978-3-030-02547-2_10 (visited on 05/01/2023).

[75] Peter Schaar. "Privacy by Design". en. In: *Identity in the Information Society* 3.2 (Aug. 2010), pp. 267–274. ISSN: 1876-0678. DOI: 10.1007/s12394-010-0055-x. URL: http://link.springer.com/10.1007/s12394-010-0055-x (visited on 06/14/2022).

[76] Sanggyu Shin et al. "Proposal for a Privacy Impact Assessment Manual Conforming to ISO/IEC 29134:2017". en. In: *Computer Information Systems and Industrial Management*. Ed. by Khalid Saeed and Władysław Homenda. Vol. 11127. Series Title: Lecture Notes in Computer Science. Cham: Springer International Publishing, 2018, pp. 486–498. ISBN: 978-3-319-99953-1 978-3-319-99954-8. DOI: 10.1007/978-3-319-99954-8_40. URL: http://link.springer.com/10.1007/978-3-319-99954-8_40 (visited on 05/01/2023).

[77] Laurens Sion, Dimitri Van Landuyt, and Wouter Joosen. "The Never-Ending Story: On the Need for Continuous Privacy Impact Assessment". en. In: *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. Genoa, Italy: IEEE, Sept. 2020, pp. 314–317. ISBN: 978-1-72818-597-2. DOI: 10.1109/EuroSPW51379.2020.00049. URL: https://ieeexplore.ieee.org/document/9229841/ (visited on 11/16/2022).

[78] Sarah Spiekermann. "The challenges of privacy by design". en. In: *Communications of the ACM* 55.7 (July 2012), pp. 38–40. ISSN: 0001-0782, 1557-7317. DOI: 10.1145/2209249.2209263. URL: https://dl.acm.org/doi/10.1145/2209249.2209263 (visited on 06/20/2022).

[79] Charnsak Srisawatsakul, Waransanang Boontarig, and Gerald Quirchmayr. *A Process Model for Data Protection Impact Assessment in Thailand's Healthcare Sector*. en. 2023. DOI: 10.24507/icicel.17.01.81. URL: https://doi.org/10.24507/icicel.17.01.81 (visited on 05/01/2023).

[80] Jaehoon Sun and Sungkwon Lee. "A Study on the Implementation of the Effective Privacy Impact Assessment Management System". en. In: *2013 International Conference on Information Science and Applications (ICISA)*. Suwon, Korea (South): IEEE, June 2013, pp. 1–4. ISBN: 978-1-4799-0604-8 978-1-4799-0602-4. DOI: 10.1109/ICISA.2013.6579420. URL: http://ieeexplore.ieee.org/document/6579420/ (visited on 05/01/2023).

[81] David Tancock, Siani Pearson, and Andrew Charlesworth. "The Emergence of Privacy Impact Assessments". en. In: *HP Laboratories* (2010), p. 35.

[82] Christina Tikkinen-Piri, Anna Rohunen, and Jouni Markkula. "EU General Data Protection Regulation: Changes and implications for personal data collecting companies". en. In: *Computer Law & Security Review* 34.1 (Feb. 2018), pp. 134–153. ISSN: 02673649. DOI: 10.1016/j.clsr.2017.05.015. URL: https://linkinghub.elsevier.com/retrieve/pii/S0267364917301966 (visited on 02/08/2023).

[83] Marco Todde et al. "Methodology and workflow to perform the Data Protection Impact Assessment in healthcare information systems". en. In: *Informatics in Medicine Unlocked* 19 (2020), p. 100361. ISSN: 23529148. DOI: 10.1016/j.imu.2020.100361. URL: https://linkinghub.elsevier.com/retrieve/pii/S2352914820301477 (visited on 05/01/2023).

[84] Ceara Treacy, John Loane, and Fergal McCaffery. "A Developer Driven Framework for Security and Privacy in the Internet of Medical Things". en. In: *Systems, Software and Services Process Improvement*. Ed. by Murat Yilmaz et al. Vol. 1251. Series Title: Communications in Computer and Information Science. Cham: Springer International Publishing, 2020, pp. 107–119. ISBN: 978-3-030-56440-7 978-3-030-56441-4. DOI: 10.1007/978-3-030-56441-4_8.

URL: https://link.springer.com/10.1007/978-3-030-56441-4_8 (visited on 05/01/2023).

[85] European Union. "General data protection regulation." In: (2016). URL: https://gdpr-info.eu/.

[86] Frank Vanclay, James T. Baines, and C. Nicholas Taylor. "Principles for ethical research involving humans: ethical professional practice in impact assessment Part I". en. In: *Impact Assessment and Project Appraisal* 31.4 (Dec. 2013), pp. 243–253. ISSN: 1461-5517, 1471-5465. DOI: 10.1080/14615517.2013.850307. URL: http://www.tandfonline.com/doi/abs/10.1080/14615517.2013.850307 (visited on 02/13/2023).

[87] Konstantina Vemou and Maria Karyda. "Evaluating privacy impact assessment methods: guidelines and best practice". en. In: *Information & Computer Security* 28.1 (Aug. 2019), pp. 35–53. ISSN: 2056-4961, 2056-4961. DOI: 10.1108/ICS-04-2019-0047. URL: https://www.emerald.com/insight/content/doi/10.1108/ICS-04-2019-0047/full/html (visited on 05/01/2023).

[88] Paul Voigt and Axel von dem Bussche. *The EU General Data Protection Regulation (GDPR)*. en. Cham: Springer International Publishing, 2017. ISBN: 978-3-319-57958-0 978-3-319-57959-7. DOI: 10.1007/978-3-319-57959-7. URL: http://link.springer.com/10.1007/978-3-319-57959-7 (visited on 01/31/2023).

[89] Kush Wadhwa and Rowena Rodrigues. "Evaluating privacy impact assessments". en. In: *Innovation: The European Journal of Social Science Research* 26.1-2 (Mar. 2013), pp. 161–180. ISSN: 1351-1610, 1469-8412. DOI: 10.1080/13511610.2013.761748. URL: http://www.tandfonline.com/doi/abs/10.1080/13511610.2013.761748 (visited on 05/01/2023).

[90] Adam Warren et al. "Privacy Impact Assessments: International experience as a basis for UK Guidance". en. In: *Computer Law & Security Review* 24.3 (Jan. 2008), pp. 233–242. ISSN: 02673649. DOI: 10.1016/j.clsr.2008.03.003. URL: https://linkinghub.elsevier.com/retrieve/pii/S0267364908000277 (visited on 05/01/2023).

[91] Inge van de Weerd and Sjaak Brinkkemper. "Meta-Modeling for Situational Analysis and Design Methods". en. In: *Handbook of research on modern systems analysis and design technologies and applications*. IGI Global, 2009, pp. 35–54.

[92] Inge van de Weerd, Sjaak Brinkkemper, and Johan Versendaal. "Incremental method evolution in global software product management: A retrospective case study". en. In: *Information and Software Technology* 52.7 (July 2010), pp. 720–732. ISSN: 09505849. DOI: 10.1016/j.infsof.2010.03.002. URL: https://linkinghub.elsevier.com/retrieve/pii/S095058491000042X (visited on 10/20/2021).

[93] Roy Wendler. "The maturity of maturity model research: A systematic mapping study". en. In: *Information and Software Technology* 54.12 (Dec. 2012), pp. 1317–1339. ISSN: 09505849. DOI: 10.1016/j.infsof.2012.07.007. URL: https://linkinghub.elsevier.com/retrieve/pii/S0950584912001334 (visited on 05/30/2023).

[94] Roel J. Wieringa. *Design Science Methodology for Information Systems and Software Engineering*. en. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014. ISBN: 978-3-662-43838-1 978-3-662-43839-8. DOI: 10.1007/978-3-662-43839-8. URL: http://link.springer.com/10.1007/978-3-662-43839-8 (visited on 03/01/2022).

[95] Claes Wohlin. "Guidelines for snowballing in systematic literature studies and a replication in software engineering". en. In: *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering - EASE '14*. London, England, United Kingdom: ACM Press, 2014, pp. 1–10. ISBN: 978-1-4503-2476-2. DOI: 10.1145/2601248.2601268. URL: http://dl.acm.org/citation.cfm?doid=2601248.2601268 (visited on 05/28/2022).

[96] Claes Wohlin et al. *Experimentation in Software Engineering*. en. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012. ISBN: 978-3-642-29043-5 978-3-642-29044-2. DOI: 10.1007/978-3-642-29044-2. URL: http://link.springer.com/10.1007/978-3-642-29044-2 (visited on 03/01/2022).

[97] D. Wright and M. Friedewald. "Integrating privacy and ethical impact assessments". en. In: *Science and Public Policy* 40.6 (Dec. 2013), pp. 755–766. ISSN: 0302-3427, 1471-5430. DOI: 10.1093/scipol/sct083. URL: https://academic.oup.com/spp/article-lookup/doi/10.1093/scipol/sct083 (visited on 05/01/2023).

[98] David Wright. "Should privacy impact assessments be mandatory?" en. In: *Communications of the ACM* 54.8 (Aug. 2011), pp. 121–131. ISSN: 0001-0782, 1557-7317. DOI: 10.1145/1978542.1978568. URL: https://dl.acm.org/doi/10.1145/1978542.1978568 (visited on 05/01/2023).

[99] David Wright. "The state of the art in privacy impact assessment". en. In: *Computer Law & Security Review* 28.1 (Feb. 2012), pp. 54–61. ISSN: 02673649. DOI: 10.1016/j.clsr.2011.11.007. URL: https://linkinghub.elsevier.com/retrieve/pii/S026736491100183X (visited on 05/01/2023).

[100] David Wright and Paul De Hert, eds. *Privacy Impact Assessment*. en. Dordrecht: Springer Netherlands, 2012. ISBN: 978-94-007-5402-7 978-94-007-2543-0. DOI: 10.1007/978-94-007-2543-0. URL: http://link.springer.com/10.1007/978-94-007-2543-0 (visited on 12/07/2022).

[101] Robert K. Yin. *Case study research and applications: design and methods*. en. Sixth edition. Los Angeles: SAGE, 2018. ISBN: 978-1-5063-3616-9.

[102] S. Yungratog et al. "A Conceptual Framework for Assessing Risks for Data Protection Impact Assessment Process in Maritime Industries". en. In: *2022 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*. Kuala Lumpur, Malaysia: IEEE, Dec. 2022, pp. 1083–1087. ISBN: 978-1-66548-687-3. DOI: 10.1109/IEEM55944.2022.9989595. URL: https://ieeexplore.ieee.org/document/9989595/ (visited on 05/08/2023).

[103] Jan Zibuschka. "Analysis of Automation Potentials in Privacy Impact Assessment Processes". en. In: *Computer Security*. Ed. by Sokratis Katsikas et al. Vol. 11980. Series Title: Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020, pp. 279–286. ISBN: 978-3-030-42047-5 978-3-030-42048-2. DOI: 10.1007/978-3-030-42048-2_18. URL: http://link.springer.com/10.1007/978-3-030-42048-2_18 (visited on 05/01/2023).

A Appendix

A.1 18 Principles for Ethical Social Research [86]

Table 9: 18 Principles for Ethical Social Research

Principle	**Meaning**	**How**
Respect for participants	Respect should be demonstrated in all interactions with participants, including refraining from judging or discrediting them and ensuring that their opinions are accurately recorded and given due consideration during the evaluation process.	Researchers will use the term "participant" and actively listen, empathise, and create a safe environment for open communication during the research process.
Informed consent	Participants' involvement should be voluntary, based on sufficient information and understanding of the research and its potential consequences.	Informed consent will be documented in writing through signed consent forms, detailing the research's purpose, methods, and potential risks.
Specific permission for recordings	If researchers plan to audio record, video record, or photograph a participant, the participant's prior consent is required.	Specific permission for recording will be included in the informed consent for interviews, ensuring participants are aware and agree to be recorded.
Voluntary participation and no coercion	Participation must be voluntary, without coercion or potential harm for non-participation.	Informed consent will clearly state that participation is voluntary and individuals are free to decline or withdraw without consequences.
Right to withdraw	Participants must know they can withdraw from the study at any time and request data removal from the analysis, if possible.	Informed consent will explicitly state the right to withdraw and the process for data removal.
Full disclosure of funding sources	The research's funding sources must be fully disclosed.	The research is not funded; this information will be communicated to participants.

No harm to participants	There must be no negative outcomes resulting from participants' involvement.	Participant anonymity and researcher confidentiality will be maintained to protect participants from any harm.
Avoidance of undue intrusion	Research discussions should be limited to relevant issues, avoiding unnecessary intrusion into participants' lives.	Researchers will maintain a professional tone, focus on research questions, and respect participants' boundaries.
No use of deception	Deception should not be employed in the research process.	This research will be transparent and honest in its methods and objectives.
Presumption and preservation of anonymity	Participants expect anonymity, and researchers must protect it.	Anonymity will be ensured in the consent form and maintained throughout data collection, analysis, and reporting.
Right to check and modify a transcript	Identifiable individuals have the right to review and modify how they are quoted.	Although not applicable to this research, participants would have the opportunity to review quotes if necessary.
Confidentiality of personal matters	Personal information must be kept confidential.	This research aims to include personal perspectives, interpretations, and comments sourced from various interviews/focus groups, documents and emails. However, the utmost care will be taken to ensure that all such data are anonymized. This measure is to guarantee that any opinions, views, or comments included in the study cannot be traced back to an individual, thereby preserving the anonymity and privacy of all individuals involved.

Data protection	Data storage must be secure and protected from unauthorised access.	In this study, we will use SURFdrive, a secure cloud storage service for the Dutch education and research community, to store research data. Access will be limited to myself, Hugo van Vliet, and Friso van Dijk, ensuring data confidentiality. Additionally, my laptop, used for the research, is password-protected for added security, safeguarding the research data from unauthorised access.
Enabling participation	Researchers must include all relevant individuals and groups in their studies.	The study will use inclusive recruitment strategies to ensure diverse perspectives are represented.
Ethical governance	Effective ethical procedures require a system of ethical governance.	Utrecht University has an ethical commission overseeing research practices.
Grievance procedure	Participants should have a means to address concerns or complaints.	Though not applicable to this research, a grievance procedure would be established if needed.
Appropriateness of research methodology	Research procedures must be reliable and valid, respecting participants and adhering to professional ethics.	This research helps to contribute to the structuring of the Privacy Impact Assessment domain, this research is committed to employing rigorous and validated methodologies. The study's design adheres to the highest ethical standards to ensure integrity and accuracy. Moreover, the outcomes of this research will provide support to Friso van Dijk's ongoing PhD project.

A.2 Ethics and Privacy Quick Scan

Ethics and Privacy Quick Scan (version: 5 September 2022)

Section 1. Research projects involving human participants

		Yes	No
P1	Does your project involve human participants? This includes for example use of observation, (online) surveys, interviews, tests, focus groups, and workshops where human participants provide information or data to inform the research. If you are only using existing data sets or publicly available data (e.g. from Twitter, Reddit) without directly recruiting participants, please answer no.	**X**	

If no, continue with Section 2; if yes, fill in the following questions.

Recruitment

		Yes	No
P2	Does your project involve participants younger than 18 years of age?		**X**
P3	Does your project involve participants with learning or communication difficulties of a severity that may impact their ability to provide informed consent?[1]		**X**
P4	Is your project likely to involve participants engaging in illegal activities?		**X**
P5	Does your project involve patients?		**X**
P6	Does your project involve participants belonging to a vulnerable[2] group, other than those listed above?		**X**

If the answer to all of P2-P6 is no, continue with P8.

As you are dealing with vulnerable participants (yes to one (or more) of P2-P6) a fuller ethical review is required. Please add more detail on your participants here:

[1] For informed consent people need to be able to (1) understand information provided relevant to making the consent decision, (2) retain this information long enough to be able to make a decision, (3) weigh the information, (4) communicate the decision.

[2] Vulnerable people include those who are legally incompetent, who may have difficulty giving or withholding consent, or who may suffer highly adverse consequences if their personal data were to become publicly available or from participating. Examples include irregular immigrants, sex workers, dissidents and traumatized people at risk of re-traumatization.

		Yes	No
P7	Do you intend to be alone with a research participant or have to take sole responsibility for the participants at any point during your research activity?		

If P7 is no continue with P8, otherwise:

As you will be alone with or solely responsible for vulnerable participants (yes to P7) a fuller ethical review is required. You may also need a Certificate of Conduct (Dutch: VOG) from the government. Please add more detail here:

		Yes	No
P8	Does your project involve participants with whom you have, or are likely to have, a working or professional relationship: for instance, staff or students of the university, professional colleagues, or clients?	**X**	

If the answer to P8 is yes, please answer P9, otherwise, continue with PC1.

		Yes	No
P9	Is it made clear to potential participants that not participating will in no way impact them (e.g. it will not directly impact their grade in a class)?	**X**	

If the answer to P9 is yes, then continue with PC1, otherwise:

As participants may think that not participating may harm them (yes to P8 and no to P9), participation may no longer be voluntary. Hence, a fuller ethical review is required. Please provide more information here:

Consent Procedures		**Yes**	**No**	**Not applicable**
PC1	Do you have set procedures that you will use for obtaining *informed* consent from all participants, including (where appropriate) parental consent for children or consent from legally authorized representatives? (See suggestions for information sheets and consent forms on the website[3].)	**X**		
PC2	Will you tell participants that their participation is voluntary?	**X**		
PC3	Will you obtain explicit consent for participation?	**X**		
PC4	Will you obtain explicit consent for any sensor readings, eye tracking, photos, audio, and/or video recordings?	**X**		
PC5	Will you tell participants that they may withdraw from the research at any time and for any reason?	**X**		
PC6	Will you give potential participants time to consider participation?	**X**		
PC7	Will you provide participants with an opportunity to ask questions about the research before consenting to take part (e.g. by providing your contact details)?	**X**		

If the answer to PC1-PC7 is yes, then continue with PC8, otherwise:

Given your responses to the informed consent questions (a no on any of PC1-PC7), a fuller ethical review is required. Please provide more information regarding the questions that are causing this here:

		Yes	**No**
PC8	Does your project involve concealment[4] or deliberate misleading of participants?		**X**

[3] uu.nl/en/research/institute-of-information-and-computing-sciences/ethics-and-privacy

[4] This may for example involve concealment of the study aim, of the identity of the researcher, or subliminal messaging during the study.

If the answer to PC8 no, continue with Section 2, otherwise:

 As you plan to use concealment or misleading (yes to PC8), and this may impact participants' rights to informed consent, a fuller ethical review is required. Please provide more information on the concealment/misleading here:

Section 2. Data protection, handling, and storage

The General Data Protection Regulation imposes several obligations for the use of **personal data** (defined as any information relating to an identified or identifiable living person) or including the use of personal data in research.

		Yes	No
D1	Are you gathering or using personal data (defined as any information relating to an identified or identifiable living person[5])?	**X**	

If the answer to D1 is yes, please answer the following questions; otherwise, continue with Section 3.

High-Risk Data

		Yes	No
DR1	Will you process personal data that would jeopardize the physical health or safety of individuals in the event of a personal data breach?		**X**
DR2	Will you combine, compare, or match personal data obtained from multiple sources, in a way that exceeds the reasonable expectations of the people whose data it is?[6]		**X**
DR3	Will you use any personal data of children or vulnerable individuals for marketing, profiling, automated decision-making, or to offer online services to them?		**X**

[5] This includes people's name, postal address, unique ID, IP address, voice, photo, video etc. When a person can be identified by combining multiple data points (e.g. gender + age + job role), this also constitutes personal data. When a person can be identified by a simple search online (e.g. with the content of a tweet) this also constitutes personal data. Note that Survey tool Qualtrics by default collects IP addresses and that the survey needs to be anonymized before distribution to prevent this.

[6] This is about the combined use of data sets that have been gathered for different purposes (so not within one study), making the data more personal or sensitive. For example, combining participant data with religion or ethnic statistics data from the CBS based on zip code.

DR4	Will you profile individuals on a large scale[7]?		**X**
DR5	Will you systematically monitor individuals in a publicly accessible area on a large scale[8] (or use the data of such monitoring)?[9]		**X**
DR6	Will you use special category[10] personal data, criminal offense personal data, or other sensitive personal data[11] on a large scale?		**X**
DR7	Will you determine an individual's access to a product, service, opportunity, or benefit[12] based on an automated decision or special category personal data?		**X**
DR8	Will you systematically and extensively monitor or profile individuals, with significant effects[13] on them?		**X**
DR9	Will you use innovative technology[14] to process sensitive personal data[15]?		**X**

If the answer to DR1-DR9 is no, continue with DM1, otherwise:

As high-risk data processing seems involved (yes to any of DR1-DR9), a fuller privacy assessment is required. Please provide more information on the DR1-DR9 questions with a yes here:

[7] Large scale is for example thousands of people, all visitors to a university website, data obtained over a very large time span
[8] Large scale is for example thousands of people, all visitors to the area, data obtained over a very large time span
[9] This may also include camera surveillance and use of drones
[10] Special category personal data is information about a person's health, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used in identification), sex life or sexual orientation.
[11] Other sensitive personal data includes for instance financial data (from which people's income, capital position or spending patterns can be derived), location data (from which people's movement patterns can be derived), achievement data (e.g. outcome of course work/exams, intelligence test; this excludes performance on tasks in a research study that are unrelated to their study/job), and communication data.
[12] Examples include: access to a mortgage, insurance, credit card, smartphone contract, course or degree programme, job opportunity.
[13] Significant effects are for example impacts on somebody's legal rights, automatic refusal of a credit application, automatic rejection for a job application.
[14] Innovative technology includes e.g. machine learning (including deep learning), neuro measurement (e.g. brain activity), autonomous vehicles, deep fakes, wearables, blockchain, internet of things.
[15] Sensitive personal data includes all data mentioned in DR6.

Data Minimization

		Yes	No
DM1	Will you collect only personal data that is strictly necessary for the research?	**X**	

If you answered yes to DM1 continue with DM4, otherwise:

		Yes	No
DM2	Will you only collect not strictly necessary personal data because it is (1) technically unfeasible not to collect it when collecting necessary data[16], or (2) needed as a source of necessary data[17]?	**X**	
DM3	Will you (1) extract any necessary data as soon as possible from the collected not strictly necessary data and (2) delete the not strictly necessary data immediately after any required extraction?[18]	**X**	
DM4	Will you anonymize the data wherever possible?[19]	**X**	
DM5	Will you pseudonymize the data if you are not able to anonymize it, replacing personal details with an identifier, and keeping the key separate from the data set?	**X**	

If the answer to any of DM2-DM5 is no, see warning below, otherwise continue with DC1.

As you do not seem to minimize data collection (no to any of DM2-DM5), a fuller privacy assessment is required. Please provide more information on the DM2-DM5 questions with a no here:

[16] This may for instance occur when IP data is collected automatically in Qualtrics, and it is unfeasible not to do so as other personal data such as email needs to be collected.
[17] This may, for instance, occur when audio data is captured from which audio features need extracting or a transcript needs to be produced.
[18] This may for instance happen when you collect audio data, extract audio features or transcribe an audio interview as soon as possible, and delete the original audio recording once done.
[19] Possible also means given the research question. So, for example, if you have done interviews and you need to be able to at a later date link them to performance data, it is impossible to anonymize the interviews, and you will need to pseudonymize them. You can then answer yes to DM4 as you are anonymizing where it is possible, and yes to DM5 if indeed you pseudonymize. Note that in such a case you should anonymize once the linking has been done, destroying the key that links the pseudonym to the identity of the participant.

Using Collaborators or Contractors that Process Personal Data Securely

			Yes	No
DC1	Will any organization external to Utrecht University be involved in processing personal data (e.g. for transcription, data analysis, data storage)?			**X**

If the answer to DC1 is yes, please complete DC2 otherwise continue with DI1.

		Yes	No
DC2	Will this involve data that is not anonymized?		

If the answer to DC2 is yes, please complete DC3-DC5, otherwise continue with DI1.

		Yes	No	Not Applicable
DC3	Are they capable of securely[20] handling data?			
DC4	Has been drawn up in a structured and generally agreed manner who is responsible for what concerning data in the collaboration?			
DC5	Is a written contract covering this data processing in place for any organization which is not another university in a joint research project?			

If the answer to any of DC3-DC5 is no, see warning below, otherwise continue with DI1.

As you do not seem to have appropriate processes in place for sharing data with collaborators or contractors (no to any of DC3-DC5), a fuller privacy assessment is required. Please provide more information on the DC3-DC5 questions with a no here:

International Personal Data Transfers

[20] Secure handling includes for example: (1) only sharing data with those who legitimately need to see it, (2) data being securely stored on password-protected employer authorized IT systems (or in the case of non-digital data: in a secure locked location), (3) if portable devices such as USB sticks are used then only encrypted and password protected with data deleted as soon as it is no longer required to be portable, (4) reporting lost or stolen data immediately, (5) deleting or disposing of data as soon as it is no longer required and in a secure manner, (6) not discussing sensitive data in public places, (7) only carrying needed data when working off-site.

		Yes	No
DI1	Will any personal data be transferred to another country (including to research collaborators in a joint project)?		**X**

If the answer to DI1 is yes, please complete DI2, otherwise continue with DF1.

		Yes	No
DI2	Do all countries involved in this have an adequate data protection regime?[21]		

If the answer to DI2 is no, please complete DI3, otherwise continue with DF1.

		Yes	No
DI3	Is a legal agreement in place?		

If the answer to DI2 and DI3 is no, see warning below, otherwise, continue with DF1.

 **As you do not seem to have appropriate safeguards in place for international data transfers (no to DI2 and DI3), a fuller privacy assessment is required.** Please provide more information on intended international data transfers here:

Fair Usage of Personal Data to Recruit Participants

		Yes	No
DF1	Is personal data used to recruit participants?[22]	**X**	

If the answer to DF1 is yes please answer DF2-DF4, otherwise continue with DP1

		Yes	No
DF2	Have potential participants provided this personal data voluntarily to be contacted about the research or is the data publicly available?	**X**	

[21] Countries with an adequate data protection regime include EU countries, Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, Japan, the United Kingdom, and South Korea.

[22] Intended here is the direct use of personal data to target a specific person. If you are using personal data indirectly to address a group of people, for example, sending a message via a *pre-existing* Microsoft Team, Blackboard course, Discord Channel, WhatsApp group, or crowd-sourcing platform, that is fine and will not be regarded as the use of personal data here. If you are asking friends or family members this will also not be regarded as use of personal data here.

DF3	If contact details have been provided by a third party, would participants expect their details to be passed on to the university and to be used in this way?	**X**	
DF4	If contact details have been gathered for a purpose other than research, would participants expect their details to be used in this way?	**X**	

If the answer to DF2-DF4 is yes continue with DP1, otherwise:

 **As there seem to be issues with your use of personal data for recruitment (no to one or more of DF2-DF4), a fuller privacy assessment is required.** Please provide more information on the intended use of personal data for recruitment here:

Participants' data rights and privacy information

		Yes	No	Not Applicable
DP1	Will participants be provided with privacy information? (Recommended is to use as part of the information sheet: For details of our legal basis for using personal data and the rights you have over your data please see the University's privacy information at www.uu.nl/en/organisation/privacy.)	**X**		
DP2	Will participants be aware of what their data is being used for?	**X**		
DP3	Can participants request that their personal data be deleted?[23]	**X**		
DP4	Can participants request that their personal data be rectified (in case it is incorrect)?	**X**		
DP5	Can participants request access to their personal data?	**X**		
DP6	Can participants request that personal data processing is restricted?	**X**		
DP7	Will participants be subjected to automated decision-making based on their personal data with an impact on them beyond the research study to which they consented?		**X**	

[23] This only concerns requests for personal data that you still hold. If you can no longer link the data to a participant due to anonymization, you can no longer delete it. This should be clear to participants in the consent form. If the data is pseudonymized and you cannot access the key but the participant can (for example when the key is a WorkerID from a crowd-sourcing platform), participants should be able to request deletion on the provision of the key.

DP8	Will participants be aware of how long their data is being kept for, who it is being shared with, and any safeguards that apply in case of international sharing?	**X**		
DP9	If data is provided by a third party, are people whose data is in the data set provided with (1) the privacy information and (2) what categories of data you will use?	**X**		

If the answer to DP1-DP6, DP8, DP9 is yes and DP7 is no, continue with DE1, otherwise:

As there seem to be issues with the data rights of your participants or the provision of privacy information (no to one or more of DP1-DP6, DP8, DP9, or yes to DP7), a fuller privacy assessment is required. Please provide more detail regarding data rights and/or privacy information here:

Using data you have not gathered directly from participants

		Yes	No
DE1	Will you use any personal data[24] that you have not gathered directly from participants (such as data from an existing data set, data gathered by a third party, data scraped from the internet)?		**X**

If the answer to DE1 is no please continue with DS1.

		Yes	No
DE2	Will you use an existing dataset in your research?		

If the answer to DE2 is yes please answer DE3-DE5, otherwise, continue with DE6.

		Yes	No
DE3	Do you have permission to do so from the owners of the dataset?		
DE4	Have the people whose data is in the data set consented to their data being used by other researchers and/or for purposes other than that for which that data set was gathered?		
DE5	Are there any contractual conditions attached to working with or storing the data from DE2?		

[24] Defined as any data related to an identified or identifiable living person. This includes people's name, postal address, unique ID, IP address, voice, photo, video etc. When a person can be identified by combining multiple data points (e.g. gender + age + job role), this also constitutes personal data.

		Yes	No
DE6	Does your project require access to personal data about participants from other parties (e.g., teachers, employers), databanks, or files[25]?		

If the answer to DE6 is yes please answer DE7-DE8, otherwise, continue with DE9.

		Yes	No
DE7	Do you have a process in place to gain informed consent from these participants?		
DE8	Are there any contractual conditions attached to working with or storing the data from DE5?		

		Yes	No
DE9	Does the project involve collecting personal data from websites or social media (e.g., Facebook, Twitter, Reddit)?		

 **As there may be issues with the use of existing data (no to DE3, DE4, DE7 or yes to DE9), a fuller privacy assessment is required.** Please provide more detail regarding the use of existing data here:

Secure data storage

		Yes	No
DS1	Will any data be stored (temporarily or permanently) anywhere other than on password-protected University authorized computers or servers?[26]	**X**	

If the answer to DS1 is yes, please answer DS2, otherwise, continue with DS4.

[25] For example, do you get a student's grade from the teacher, in addition to data gathered directly in your study or data in an existing research data set?

[26] OneDrive business, Qualtrics, Microsoft Forms are ok. Do not use Google Drive/Sheets/Docs/Forms, Dropbox, OneDrive personal. See https://tools.uu.nl/tooladvisor/ for tools that are safe/not safe to use. Bachelor and master students are authorized to use a password-protected personal computer, as long as that computer is not shared with other people.

		Yes	No
DS2	Does this only involve data stored temporarily during a session with participants (e.g. data stored on a video/audio recorder/sensing device), which is immediately transferred (directly or with the use of an encrypted and password-protected data-carrier (such as a USB stick)) to a password-protected University authorized computer or server, and deleted from the data capture and data-carrier device immediately after transfer?		**X**

If the answer to DS2 is yes, continue with DS4, otherwise answer DS3.

		Yes	No
DS3	Does this only involve data stored with a collaborator or contractor?	**X**	
DS4	Excluding (1) any international data transfers mentioned above and (2) any sharing of data with collaborators and contractors, will any personal data be stored, collected, or accessed from outside the EU[27]?		**X**

If the answer to DS2 and DS3 is no, or the answer to DS4 is yes, see the warning below, otherwise continue with Section 3.

As there may be issues with secure data storage (no to DS2 and DS3, or yes to DS4), a fuller privacy assessment is required. Please provide more detail regarding data storage here:

[27] This may happen, for instance, when data is collected and stored on a Utrecht University laptop whilst abroad.

Section 3: Research that may cause harm

Research may harm participants, researchers, the university, or society. This includes when technology has dual-use, and you investigate an innocent use, but your results could be used by others in a harmful way. If you are unsure regarding possible harm to the university or society, please discuss your concerns with the Research Support Office.

		Yes	No
H1	Does your project give rise to a realistic risk to the national security of any country?[28]		**X**
H2	Does your project give rise to a realistic risk of aiding human rights abuses in any country?[29]		**x**
H3	Does your project (and its data) give rise to a realistic risk of damaging the University's reputation? (E.g., bad press coverage, public protest.)		**X**
H4	Does your project (and in particular its data) give rise to an increased risk of attack (cyber- or otherwise) against the University? (E.g., from pressure groups.)		**X**
H5	Is the data likely to contain material that is indecent, offensive, defamatory, threatening, discriminatory, or extremist?		**X**
H6	Does your project give rise to a realistic risk of harm to the researchers?[30]		**X**
H7	Is there a realistic risk of any participant experiencing physical or psychological harm or discomfort?[31]		**X**
H8	Is there a realistic risk of any participant experiencing a detriment to their interests as a result of participation?		**X**
H9	Is there a realistic risk of other types of negative externalities?[32]		**X**

[28] For example, research that can be used for autonomous armed vehicles/drones/robots, research on automated detection of objects, research on AI-enhanced forgery of video/audio data.

[29] For example, research on natural language/video/audio processing for automated identification of people's identity, sentiments, or opinions.

[30] For example, research that involves potentially violent participants such as criminals, research in likely unsafe locations such as war zones, research on an emotionally highly challenging topic, research in which the researcher is alone with a not previously known participant in the participant's home.

[31] For example, research that involves strenuous physical activity, research that stresses participants, research on an emotionally challenging topic.

[32] A negative externality is a harm produced to a third party, society in general, or the environment. For instance, intended or unintended negative ethical (e.g. bad governance or management practices), social (e.g. consumerism, inequality) or environmental effects (e.g. large CO_2 footprint or e-waste production) of your project.

If the answer to H1-H9 is no continue with Section 4, otherwise:

As you replied yes to one (or more) of H1-H9, a fuller ethical review is required. Please provide more detail here on the potential harm, and how you will minimize risk and impact:

Section 4: Conflicts of interest

		Yes	No
C1	Is there any potential conflict of interest (e.g. between research funder and researchers or participants and researchers) that may potentially affect the research outcome or the dissemination of research findings?		**X**
C2	Is there a direct hierarchical relationship between researchers and participants?		**X**

If the answer to C1-C2 is yes, continue with Section 5, otherwise:

As you replied yes to C1 or C2, a fuller ethical review is required. Please provide more information regarding possible conflicts of interest and how you mitigate them here:

Section 5: Your information

This last section collects data about you and your project so that we can register that you completed the Ethics and Privacy Quick Scan, sent you (and your supervisor) the summary of what you filled out, and follow up where a fuller ethics review and/or privacy assessment is needed. For details of our legal basis for using personal data and the rights you have over your data please see the University's privacy information. Please see the guidance on the ICS Ethics and Privacy website on what happens on submission.

Z0. Which is your main department?

X Information and Computing Science
○ Freudenthal Institute
○ Other, namely:

Z1. Your full name: Hugo van Vliet

Z2. Your email address: h.s.vanvliet@students.uu.nl

Z3. In what context will you conduct this research?

- ○ 1. As a student on a course with course coordinator:
- ○ 2. As a student for my bachelor thesis, supervised by:
- X 3. As a student for my master thesis, supervised by: Matthieu Brinkhuis
- ○ 4. As a PhD student, supervised by:
- ○ 5. As an independent researcher (e.g. research fellow, assistant/associate/full professor)

In case the answer to Z3 is 2:

Z4. Bachelor programme for which you are doing the thesis:

- ○ Artificial Intelligence (Kunstmatige Intelligentie)
- ○ Computing Science (Informatica)
- ○ Information Science (Informatiekunde)
- ○ Other:

In case the answer to Z3 is 3:

Z5. Master programme for which you are doing the thesis:

- ○ Applied Data Science
- ○ Artificial Intelligence
- X Business Informatics
- ○ Computing Science
- ○ Data Science
- ○ Game and Media Technology
- ○ Human-Computer Interaction
- ○ Other:

In case the answer to Z3 is 1, 2, 3, or 4:

Z6. Email of the course coordinator or supervisor (so that we can inform them that you filled this out and provide them with a summary): m.j.s.brinkhuis@uu.nl

In case the answer to Z3 is 2 or 3:

Z7. Email of the moderator (as provided by the coordinator of your thesis project):

g.wagenaar@uu.nl

Z8. Title of the research project/study for which you filled out this Quick Scan:

Maturity of project privacy management

Z9. Summary of what you intend to investigate and how you will investigate this (200 words max):

"PIA is a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme." (Clark, 2009) Therefore, there is a need to make the PIA more of a process, as opposed to the current situation in which multiple documents are delivered, compiled, and referred to as the PIA. Making a PIA is a very complicated procedure, and there is little research on its application in practise. When conducting a PIA, it is necessary to consider "Privacy-by-Design" (Oetzel & Spiekermann, 2012). "Privacy by Design" anticipates and prevents events that violate privacy before they occur (Cavoukian, 2009). However, it is not well documented how a PIA should be formatted and which elements are required for a well-written PIA. Consequently, the PIA is not a one-time compliance review at the completion of a project, but rather a continuing procedure. However not every part of the PIA needs to be changed every time the PIA is updated. This would be too expensive, require too many man-hours, and be unnecessary given that certain aspects of the PIA have not changed. The following primary research question is proposed in order address this problem and to structure the research domain: How should a maturity PIA be designed for privacy project management?

In case the answer to Z3 is 2 or 3:

		Yes	**No**	**Not Applicable**
Z10.	In case you encountered warnings in the survey, does your supervisor already have ethical approval for a research line that fully covers your project?		**X**	

In case the answer to Z9 is yes:

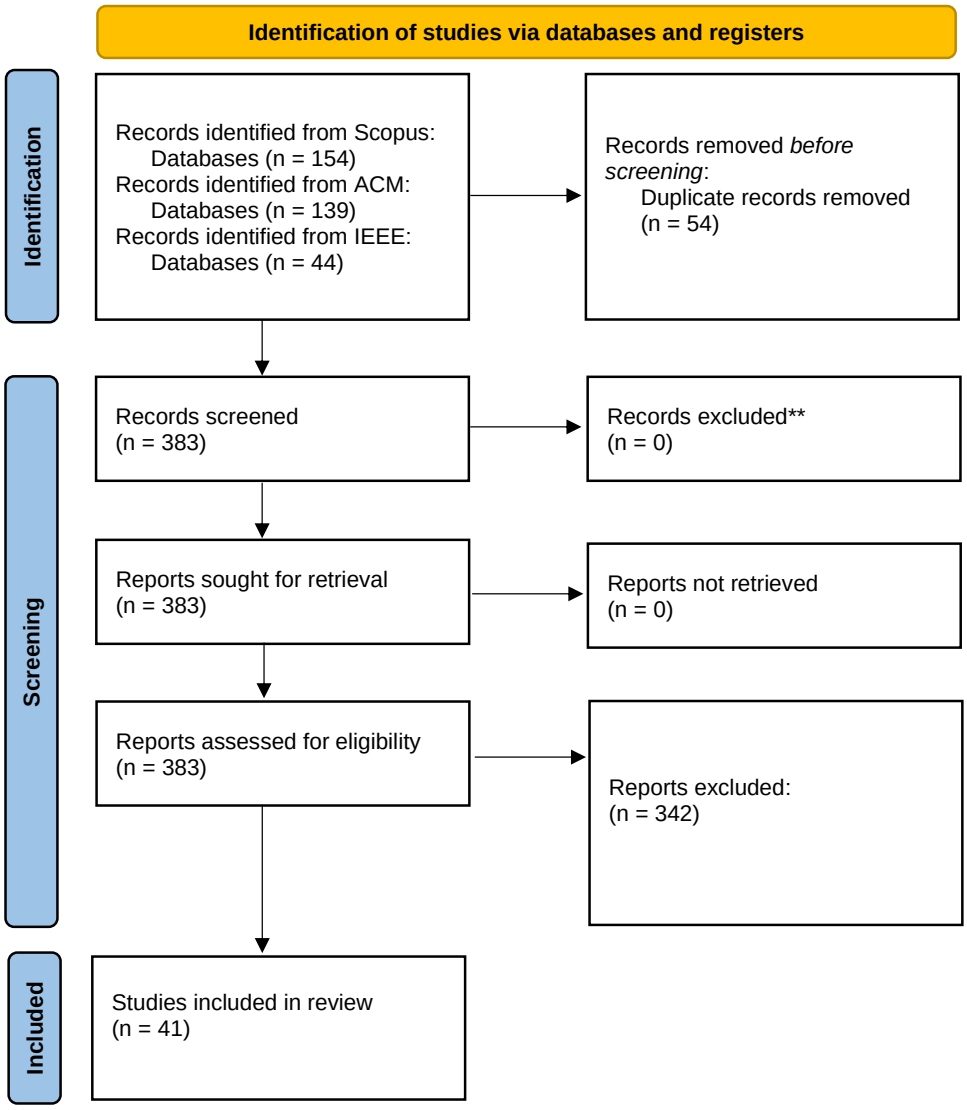
Z10. Provide details on the ethical approval (e.g. ethical approval number):

A.3 Old PIA codes with their updated new codes

Table 10: Old PIA process codes with their updated new codes

Old code	**New code**
Project description	Describing the project
	Identify stakeholders
	Map assets
	Map data flows
	Map data
	List applicable laws
	List applicable policies
	Map business processes.
Risk assessment	Identify threat
	Determine likelihood
	Determine Impact
	Determine risk
Risk measures	Current controls
	New controls
	Cost-benefit analysis
	Risk management plan

A.4 PRISMA flow diagram


Identification of studies via databases and registers
Identification
Records identified from Scopus:
Databases (n = 154)
Records identified from ACM:
Databases (n = 139)
Records identified from IEEE:
Databases (n = 44)
Records removed *before screening*:
Duplicate records removed
(n = 54)
Screening
Records screened
(n = 383)
Records excluded**
(n = 0)
Reports sought for retrieval
(n = 383)
Reports not retrieved
(n = 0)
Reports assessed for eligibility
(n = 383)
Reports excluded:
(n = 342)
Included
Studies included in review
(n = 41)

A.5 Activity & concept table of the activity pre-PIA

Table 11: PDD activity table of **pre-PIA** and its associated sub-activities with description

Activity	**Sub-Activity**	**Description**
Pre-PIA	Describe the project	The initial step in conducting a PIA involves providing a concise overview of the project, defining its scope, and identifying the personal data the actor will use. This information is documented in the artefact titled PROJECT BRIEF.
	Describe the purpose of the project	In the preceding activity, the project's WHAT is outlined. Within this activity, the writer must clarify the WHY behind their chosen WHAT. This information is captured in the artefact named PROJECT BRIEF.
	Execute threshold analysis	The controller must determine if the processing is likely to pose a significant risk to the rights and freedoms of individuals as per Art. 35 (1) GDPR. Beyond the guidelines on processing activities in Art. 35 (3) GDPR, regulatory bodies have created lists of processing activities meeting the appropriate criteria (as per Art. 35 (4) and Art. 68 GDPR). Furthermore, the standards set by the Article 29 European Data Protection Board have be taken into account.
	Inform DPO of PIA	When the threshold is executed, the DPO must be notified about the outcome of the THRESHOLD ANALYSIS and is required to give their approval.

Table 12: PDD Concept table with the concepts, description and reference(s) of the activity **pre-PIA**

Concept	Description

PROJECT BRIEF	The PROJECT BRIEF serves as an document that outlines various aspects of a project. It is composed of multiple key components that provide a short understanding of what the project aims to achieve. Project Description: This section provides an overview of the project, explaining its objectives and what it aims to accomplish. It serves as an introductory guide to what the project is all about [3, 4, 8, 14, 53, 26, 38, 41, 45, 49, 59, 62, 66, 67, 71, 74, 83, 89, 103]. Project Scope: This part delineates the boundaries of the project, specifying what is included and what is excluded [44, 71, 76]. Personal Data Purpose: This segment clarifies why personal data is being collected in the course of the project. Whether it is for customer engagement, research, or other objectives, this section outlines the reasons for gathering such information [53, 37, 44, 41]. Legal Basis: This component is critical for ensuring that the project complies with legal requirements, especially in the context of data protection laws. It identifies the legal grounds that justify the collection and processing of personal data, be it consent, a contractual obligation, or other legitimate reasons [38, 49, 62, 67, 74, 87].
THRESHOLD ANALYSIS	The THRESHOLD ANALYSIS takes the PROJECT BRIEF as its starting point. In this stage, the PROJECT BRIEF undergoes examination to decide whether a PIA (PIA) is necessary. The factors influencing this decision include various attributes that help determine whether to proceed with a PIA. The final result is a decision on whether to carry out a PIA. The concluding activity involves obtaining approval from the Data Protection Officer (DPO), confirming the decision. [3, 8, 34, 4, 15, 14, 36, 41, 42, 45, 49, 66, 68, 71, 76, 80, 87, 90, 100, 97, 99, 103]

A.6 Activity & concept table of the activity PIA-preparation

Table 13: PDD activity table of **PIA Preparation** and its associated sub-activities with description

Activity	**Sub-Activity**	**Description**
PIA Preparation	Identify PIA team	The first sub-activity in the activity *PIA preparation* is to identify a PIA team. The concept where the information of the team is stored is PIA TEAM
	Prepare PIA plan	In the sub-activity *PIA Preparation*, a plan for carrying out the PIA is formulated. The associated concept for this is the PIA PLAN.
	Advice from Data subject	The DATA PROTECTION REQUIREMENTS are defined together with data subjects who are provided information about policies, procedures, controls, and tools that allow them to determine how personal data is used and whether policies are being properly enforced.
	Advice from ethical experts	Advice from ethical experts is gained regarding the DATA PROTECTION REQUIREMENTS for sensitive personal data.
	Define Data protection requirements	Defining privacy requirements entails establishing clear objectives and benchmarks related to the protection of personal data within a system. The processing principles are documented, applied in a structured and methodical manner, and are periodically evaluated. It considers legal, technical, security, and privacy requirements and documents how these will be implemented. Stakeholders are extensively involved in the formulation of privacy goals and the identification of privacy requirements. The associated document for this is the DATA PROTECTION REQUIREMENTS.
	Review PIA plan	In this step the PIA PLAN is reviewed. In case of approval the process will go to the next sub-activity. Otherwise the PIA PLAN has to be revised.
	Identify organisations	In this sub-activity, it is imperative to delineate and list all organisations who might be involved by the processing of personal data. The corresponding artefact is ORGANISATION.
	List applicable laws	The sub-activity refers to a systematic enumeration of all relevant legal statutes, regulations, and directives that pertain to a specific context or activity. This list is crucial in ensuring that actions or projects are conducted within the boundaries of established legal frameworks, helping entities to maintain compliance and avoid potential legal ramifications. The corresponding artefact is LAWS.

	List applicable policies	The sub activity entails a structured compilation of all pertinent policies, guidelines, and best practices that relate to a specific context or operation. Such a list aids in aligning actions or initiatives with established organisational or regulatory standards, ensuring consistency, compliance, and governance. It is also essential to consider Article 40 of the GDPR in this context. The corresponding artefact is POLICIES.

Table 14: PDD Concept table with the concepts, description and reference(s) of the activity **PIA Preparation**

Concept	**Description**
PIA TEAM	The PIA TEAM is a group of individuals assembled to conduct and oversee the PIA process. Each team member is selected based on specific criteria and brings unique skills and expertise. [5, 14, 34, 49, 68, 71, 80, 87, 89, 90, 100, 97, 99, 103]. The composition of the PIA Team includes several key details about each member: Name of the Person: Knowing the names of the team members establishes accountability and facilitates communication among the group. This is the basic identifier for each individual involved. Role within the Organisation: This information describes the official position or job title each member holds within the organisation. Understanding their roles provides context for their responsibilities and authority within the PIA process and the organisation at large. Competence: This refers to the skills, qualifications, and expertise each team member possesses. Competence is crucial because it ensures that each individual is well-suited to perform the tasks required in the PIA process. Responsibility in the PIA: This section outlines which parts of the PIA each team member is responsible for. Whether it's data collection, legal review, or risk assessment, this attribute helps allocate tasks and manage the workflow efficiently.

PIA PLAN	The PIA PLAN is a document formulated by the PIA TEAM. It serves as the roadmap for conducting the PIA, outlining various essential components that guide the entire process [34, 49, 71, 76, 80, 90, 100, 97, 99]. The key elements that constitute the PIA PLAN are: PIA Scope: This section provides a detailed description of what the PIA will cover, including the types of personal data to be processed, the systems involved, and the specific issues or risks that need to be addressed. This is a more elaborated version of the project scope of the PROJECT BRIEF. [44, 71, 76, 14, 87, 98, 103] PIA Budget: This part outlines the resources allocated for conducting the PIA. It may include estimates for staff time, external consultants, technology resources, and other expenses. A well-defined budget ensures that the PIA process is feasible and sustainable [14, 49, 100, 97, 99]. PIA Timetable: This component presents the timeline for completing the PIA, specifying milestones, deadlines, and any dependencies between tasks. Having a structured timetable allows for better planning and ensures that the assessment is completed in a timely manner [49, 76, 87, 90, 97, 99]. Approval Process: This segment describes the steps and criteria for obtaining approval at various stages of the PIA. The approval process ensures that the PIA meets organisational and legal standards [87]. Stakeholder Consultation Plan: This part outlines the strategy for engaging with stakeholders, such as employees, customers, or regulatory bodies, who have an interest in the project or may be affected by its outcomes. It may include methods for gathering feedback, timelines for consultations, and mechanisms for incorporating stakeholder input into the PIA [76].

DATA PROTECTION REQUIREMENTS	DATA PROTECTION REQUIREMENTS is a concept that outlines the various standards and conditions that must be met to ensure the proper handling and protection of personal data. This document serves as a guide for understanding and implementing data protection measures [3, 34, 14, 53, 26, 38, 44, 47, 59, 68, 84, 87, 102]. Here are the key components that make up DATA PROTECTION REQUIREMENTS: Processing Principles: This section lays out the fundamental principles that guide how personal data should be processed. These might include concepts like data minimisation, purpose limitation, and transparency. Understanding these principles is essential for ensuring that data handling practices are ethical and compliant with relevant laws. Legal Requirements: This portion specifies the legal obligations that must be adhered to, such as those outlined by data protection laws like GDPR, CCPA, or any other local regulations. It provides a legal framework within which the data processing activities must occur, covering aspects like consent, data subject rights, and data transfers. Technical Requirements: This segment details the technical specifications needed to protect personal data. This could include information on data encryption, secure data storage, and safe data transfer protocols. Security Requirements: Here, the document outlines the security measures that must be in place to safeguard personal data. This may involve physical security controls, access restrictions, and the use of security software. The section aims to ensure that data remains confidential and intact. Privacy Requirements: This part focuses on measures that protect the privacy of individuals whose data is being processed. It can cover topics like anonymization techniques, data masking, and PbD principles. The goal is to minimise the exposure of sensitive personal information. Description of These Elements: Each of the above components should be accompanied by detailed descriptions that explain their relevance, application, and methods for implementation. These descriptions serve as explanatory notes, helping stakeholders understand the rationale and procedures behind each requirement.

organisations	organisations serves as a record of all entities involved in the data processing activities. It is an essential tool for identifying the various stakeholders and understanding their respective roles and responsibilities [5, 14, 53, 26, 34, 38, 44, 42, 49, 62, 66, 68, 71, 76, 80, 87, 89, 90, 98, 100, 97, 99, 103, 41]. Here are the primary components that make up the organisations: Name: This is the official name of the entity involved in data processing. It serves as the primary identifier and is critical for establishing formal relationships and accountability. Role: Each organisation's role is clearly defined, whether it acts as a Data Processor, Data Controller, or any other role defined under data protection laws. This classification is crucial for understanding legal obligations and responsibilities in data handling and protection. organisation: This segment identifies what kind of entity each organisation is. Whether it's a private company, governmental body, non-profit organisation, etc. Understanding the type of organisation helps set the context for its involvement and may influence its regulatory obligations. Description: This section provides a brief overview of each organisation, explaining its core activities, area of expertise, and relevance to the data processing tasks at hand. This information offers additional context and can be particularly helpful when multiple organisations with varied backgrounds and specialties are involved.
LAWS	LAWS serves as a critical repository of legal texts and regulations that have a direct impact on data processing activities. It goes beyond merely listing the laws to provide a nuanced understanding of how specific articles or clauses affect the organisation's data processing [5, 14, 53, 34, 36, 79, 103]. Here are the key components of the LAWS: Law Itself: This section provides the full text or references to the specific laws, articles, or regulations that are relevant to data processing. These could range from international frameworks like the GDPR to national or even local laws. The inclusion of the legal text ensures that the exact wording is readily available for interpretation and compliance. Impact on Processing Activities: This is arguably the most crucial part of the document, as it delves into how each law, article, or clause specifically impacts data processing within the organisation.

POLICIES	POLICIES is a resource that outlines the organisation's guidelines and protocols concerning data processing activities. It doesn't just enumerate the policies; it also delves into the significant impact that each policy has on the processing of data [4, 5, 34, 79, 87]. Here are the main components of POLICIES: Policy Itself: This section contains the actual text of each policy, outlining what is expected, allowed, or prohibited when it comes to data processing. These guidelines serve as the governing principles that staff and other stakeholders must adhere to. Impact on Processing Activities: This is a critical part of the document, detailing how each individual policy affects the organisation's data processing activities.

A.7 Activity & concept table of the activity View creation

Table 15: PDD activity table of **View Creation** and its associated sub-activities with description

Activity	**Sub-Activity**	**Description**
View creation	Mapping personal data	The initial sub-activity involves identifying and mapping the personal data that is or will be utilised. The corresponding artefact is PERSONAL DATA REGISTER.
	Mapping personal dataflows	The following sub-activity is mapping personal data flows. This refers to the act of recording, examining, and illustrating how personal data moves within and between systems, networks, organisations, and various entities. The corresponding artefact is DATAFLOW DIAGRAM.
	Mapping software and hardware	Mapping software and hardware is a step in which one identifies and documents all the software applications and hardware components in a system or network. The corresponding artefact is PERSONAL ASSETS.
	Mapping business process	Business Process Mapping (BPM) serves as a visual tool to capture, document, and analyse the flow of activities within an organisation The corresponding artefact is BUSINESS PROCESS DIAGRAM.
	List actors	Mapping actors refers to the process of identifying, documenting, and visualising all the key players or stakeholders involved in the process of personal data. The corresponding artefact is ACTORS.

Table 16: PDD Concept table with the concepts, description and reference(s) of the activity **View Creation**

Concept	Description

PERSONAL DATA REGISTER	PERSONAL DATA REGISTER serves as a centralised inventory of all personal data held or processed by the organisation. It's not merely a list but a structured database that provides details about the types and categories of personal data in possession. The register aims to enhance transparency and accountability, ensuring that data is managed responsibly [4, 14, 26, 34, 38, 42, 41, 62, 76, 80, 100, 103]. The key components of the PERSONAL DATA REGISTER are: Data Type: For each entry in the list, the data type is specified. This could range from simple types like text and numbers to more complex types like images or geolocation data. Understanding the data type is crucial for applying the correct data handling and security measures. Data Category: This part identifies the category to which each type of personal data belongs. Categories could include sensitive data, identification data, health data, etc. Categorising the data helps in understanding its sensitivity level and the kind of protection it requires.
DATAFLOW DIAGRAM	DATAFLOW DIAGRAM (DFD) is a graphical representation that illustrates how data moves through an information system, including its processes and storage points. It's a critical tool for understanding, analysing, and optimising data-related activities [4, 5, 14, 26, 34, 42, 41, 49, 60, 62, 66, 79, 80, 87, 89, 98, 100, 103]. Here are the key elements that make up DATAFLOW DIAGRAM: External Entities: These are the sources or destinations outside the system that interact with it. This could be users, third-party services, or other systems. Identifying external entities helps in understanding the system's boundaries and the data exchange points that may need extra security measures. Processes: These are the operations or tasks within the system that process the data. Processes can range from simple actions like data retrieval to complex algorithms for data analysis. Understanding processes is essential for knowing how data is manipulated, transformed, or consumed within the system. Data Stores: These are the repositories where data is held temporarily or permanently within the system. This could be databases, flat files, or even in-memory storage. Knowing what data is stored where is critical for assessing storage security and data access controls. Data Flows: These are the paths that data takes as it moves from one part of the system to another. Data flows can be simple, like a one-way transmission, or complex, involving multiple stops for processing and storage. Mapping out data flows allows for a better understanding of how data travels and where it may be exposed to risks. Trust Boundaries: These delineate zones within the DFD where different levels of trust are required. Trust boundaries might separate external entities from internal processes or data stores, or they might exist between different internal components that have varying levels of security. Identifying these boundaries is crucial for implementing appropriate security controls and access permissions.

ASSETS	ASSETS is a inventory that catalogues all the software and hardware resources owned or used by an organisation. [1, 5, 26, 34, 44, 62, 71, 102].
BUSINESS PROCESS DIAGRAM	BUSINESS PROCESS DIAGRAM is a visual tool used to map out the different elements and interactions in a business process. It serves as both an analytical and a communication tool, helping stakeholders to understand, optimise, and streamline workflows [62, 76, 98]. Here are the key elements that make up a BUSINESS FLOW DIAGRAM [35]: Flow Objects: Activities: These are the core actions or tasks that occur within the process. Understanding activities is essential for grasping what work is done at each stage of the process. Events: These represent specific triggers or outcomes that initiate, modify, or complete a process. They provide context for how and when a process starts, changes, or ends. Gateways: These serve as decision-making points within the process. They control the flow of activities based on certain conditions, helping to model various scenarios and outcomes. Connecting Objects: Sequence Flows: These arrows or lines indicate the order of activities and the direction of the process flow. They are crucial for understanding the linear progression or hierarchy of tasks. Message Flows: These show interactions between different entities, which could be individuals, departments, or external partners. Message Flows help to visualise how information or materials are exchanged within the process. Associations: These are connectors that link additional information or artefacts to flow objects. They add context and detail to activities, events, or gateways. Swim Lanes: Pools: These are broader categories that represent the major participants involved in a process. Pools help to organise the process at a high level and indicate who or what is responsible for a set of activities. Lanes: These are subdivisions within pools and represent specific roles, departments, or other smaller units. Lanes help to further allocate responsibilities and indicate who does what within the larger process. artefacts: Data Objects: These symbols indicate what data is required, produced, or used at various points in the process. They are essential for understanding the data dependencies within the process. Annotations: These are textual notes or comments added to clarify specific points or elements within the diagram. Annotations provide extra information that helps in understanding the process better. Groups: These are visual containers that do not affect the flow but are used to highlight or group together a set of related activities or flow objects for easier understanding or analysis.

ACTORS	In the context of systems design, business processes, or project management, the ACTORS serves as an directory that profiles the different participants involved. These could be individuals, teams, departments, or even external entities like customers, third-party vendors or attackers. By detailing the actors' names, roles, responsibilities, and interactions, the document helps clarify who does what, how they contribute, and how they interact within the system or process [5, 62, 76, 98, 100, 97, 99]. Here are the key elements of ACTORS: Name: This is the official name or designation for the actor, serving as the primary label for tracking and referencing. It could be a person's name, a team's title, or an external organisation's name. Roles: This outlines the specific roles that the actor plays within the system or process. Roles define what kind of activities, decisions, or interactions the actor is involved in. Responsibilities: This section details the specific tasks or duties that fall under the actor's purview. Knowing this helps allocate work and define the scope of involvement. Interactions: This part identifies the other actors or system components that this actor interacts with. It helps map the network of relationships and dependencies.

PERSONAL DATA LIFECYCLE	PERSONAL DATA LIFECYCLE is an essential tool for understanding how personal data is managed throughout its entire lifecycle within an organisation. From data creation and collection to processing, storage, and ultimately deletion, this document outlines the various activities involved, the types of personal data, and the roles responsible for each stage. This view is for ensuring compliance with data protection laws and maintaining data integrity and security [56, 55]. Here are the key elements of the PERSONAL DATA LIFECYCLE [5]: Activities: This refers to the various stages or activities that personal data goes through within an organisation. Starting with its initial creation or collection, the data may be processed for specific purposes like analytics or customer service. It is then securely stored, and at times, transmitted to other systems or third-party entities. Finally, the data reaches a stage where it is either deleted or archived for long-term retention. Understanding these activities helps the organisation to manage data responsibly and efficiently. Personal Data: This aspect identifies the kinds of data that are being managed. It's not just about knowing that the organisation has data, but what kind of data it is. Are we dealing with simple identifiers like names and email addresses, or more sensitive categories like financial or health records? This granularity aids in applying the appropriate security measures and compliance checks for each type of data. Lifecycle Roles: This component outlines the different responsibilities attached to managing personal data at each stage of its lifecycle. For example, a "Data Creator" could be responsible for initially gathering the data. This role then passes the baton to a "Data Processor" who manipulates and uses the data. A "Data Custodian" ensures the data's secure storage, and a "Data Consumer" might access it for analysis or other activities. Finally, a "Data Archivist" or "Deleter" takes charge of the data's long-term storage or secure deletion.
COLLECTION OF VIEWS	COLLECTION OF VIEWS serves as a repository for various perspectives that have been generated, offering a centralized storage space for diverse viewpoints.

A.8 Activity & concept table of the activity Assessment

Table 17: PDD activity table of **Assessment** and its associated sub-activities with description

Activity	**Sub-Activity**	**Description**
Assessments	Extract actors from ACTORS list	Retrieve specific individuals or entities from the "ACTORS" list.
	Extract use cases from COLLECTION OF VIEWS list	From the perspectives gathered, a use case can be developed and subsequently integrated into the USE CASE MODEL.
	Assess necessity	By establishing operational ties with the USE CASE, it is inferred that data processing adheres to legal standards when the actor embodies the role of a data processor or controller. This alignment ensures that processing is driven by a clear and legitimate purpose.
	Assess proportionality	The connections with the USE CASE implies that data processing remains within legal bounds, especially when the actor functions as a data processor or controller, ensuring that the processing is proportionate to its intended purpose.
	Demonstrate compliance to legal body	By correlating actions with the USE CASE, it's evident that the data processing is in line with legal requirements. This is especially true when the actor in the use case demonstrates their role as a data processor or controller, showcasing compliance with specific regulations.
	Describe use case	This refers to detailing a specific scenario or situation in which a system or service interacts with users or other systems.

Table 18: PDD Concept table with the concepts, description and reference(s) of the activity **Assessment**

Concept	Description
ACTOR	ACTOR is extracted from the COLLECTION OF VIEWS, which contains the list with ACTORS [5, 62, 76, 98, 100, 97, 99]
USE CASE	A USE CASE is how a user interacts with a system to accomplish a specific goal. USE CASE are often used to capture functional requirements and to outline the intended behaviour of a system. How the system behaves can be extracted from the COLLECTION OF VIEWS. Essentially, USE CASE serve as a guide for what a system will do, without detailing how it will do it.

NECESSITY	The concept of NECESSITY in use cases revolves around the operationalization of goals. When a goal is linked directly to a use case, it implies that the associated data processing is essential for achieving that goal [8, 26, 34, 41, 45, 67].
PROPORTIONALITY	PROPORTIONALITY here refers to the extent of data processing in relation to the role of the actor in the use case. If the actor serves as a data processor or controller, the level of data processing is considered to be proportionate to the objectives [8, 26, 34, 41, 45, 67].
COMPLIANCE	COMPLIANCE in this context pertains to adhering to legal and organisational standards for data processing. When the actor in a use case is identified as a data processor or controller, it indicates that the data processing activities are likely to be in compliance with relevant regulations [67, 89, 97, 99].
DESCRIPTION	DESCRIPTION serves to elaborate on the implications of each aspect, offering a fuller understanding of their significance.
USE CASE MODEL	USE CASE MODEL is a graphical representation that showcases how ACTORS interact with a system to achieve specific goals or objectives. It helps in defining the different roles that users play while interacting with the system and the actions they perform to achieve particular goals.

A.9 Activity & concept table of the activity Risk assessment

Table 19: PDD activity table of **Risk Assessment** and its associated sub-activities with description

Activity	**Sub-Activity**	**Description**
Risk assessment	Map threats	Identifying and documenting potential risks or vulnerabilities in a system or process. The corresponding concept is THREATS
	Determine likelihood	This sub-activity revolves about identifying the likelihood of a threat occurring. The corresponding concept is LIKELIHOOD.
	Determine impact	This sub-activity assesses the potential consequences should a particular threat materialise. The corresponding concept is IMPACT.
	Determine risk	The risk is likelihood x impact. The corresponding concept is RISK.
	Prioritise risk	The risk are sorted on priority. The corresponding concept is PRIORITY.

Table 20: PDD Concept table with the concepts, description and reference(s) of the activity **Risk Assessment**

Concept	Description
LIKELIHOOD	The concept LIKELIHOOD plays an important role in risk assessment, particularly when evaluating the potential threats associated with data processing. It quantifies the probability that a specific threat will actually materialise, offering valuable insights for prioritising risk mitigation efforts [34, 38, 59, 1, 3, 5, 53, 34, 36, 38, 47, 59, 62, 71, 76, 79, 83, 87, 102].
IMPACT	The concept IMPACT is a cornerstone in understanding the ramifications of potential threats related to data processing. IMPACT indicates the severity of the consequences should that threat materialise [1, 3, 5, 53, 34, 36, 38, 47, 59, 62, 71, 76, 79, 83, 87, 102].
RISK	The concept of RISK serves as a critical metric that combines both IMPACT and LIKELIHOOD to assess the overall threat level. Essentially, risk quantifies the potential damage a threat could cause, weighed against the probability of that threat actually occurring. This holistic measure aids organisations in prioritising their risk mitigation and management strategies [3, 5, 53, 34, 36, 38, 47, 59, 62, 71, 76, 79, 83, 87, 89, 102].
PRIORITY	PRIORITY functions as a mechanism to categorise and sequence threats based on their corresponding RISK levels. Essentially, it's a structured approach to spotlight the most pressing threats that require immediate attention, thus enabling efficient resource allocation and timely intervention [69].

THREATS	Identifying and elaborating on the THREATS is a crucial aspect of managing the security and integrity of a data ecosystem. This involves not only pinpointing potential vulnerabilities but also understanding their implications and the risk they pose to both data and operations [3, 5, 14, 53, 34, 36, 38, 44, 42, 41, 45, 47, 49, 59, 60, 62, 66, 68, 69, 71, 76, 79, 80, 83, 84, 87, 89, 90, 98, 100, 97, 99, 103, 102].
LIST OF THREATS	LIST OF THREATS serves as a repository that enumerates all identified THREATS and associates them with their corresponding PRIORITY RISK levels.

A.10 Activity & concept table of the activity Risk measures

Table 21: PDD activity table of **Risk Measures** and its associated sub-activities with description

Activity	**Sub-Activity**	**Description**
Risk measures	Identify current controls	Determine and document the existing measures in place to protect privacy and data. The concept that encapsulate this is CURRENT CONTROLS.
	Identify new controls	Determine and document the new measures in place to protect privacy and data. Privacy controls are methodically assessed using metrics. The corresponding concept is NEW CONTROLS.
	Execute Cost-Benefit Analysis	Conduct an assessment to weigh the financial and non-financial advantages against the costs and potential risks of a decision or project. The corresponding concept is COST-BENEFIT ANALYSIS.
	Prioritise controls	Rank the protective measures based on their importance and effectiveness in addressing potential risks and vulnerabilities. The concept that encapsulate this is PRIORITY.
	Create plan for risk management	Develop a structured approach address potential risks and vulnerabilities to ensure data protection and compliance. The concept that encapsulate this is RISK MANAGEMENT PLAN.
	Identify threats with residual risk	Pinpoint and document threats that still pose potential risks even after implementing current controls. The corresponding concept is RESIDUAL RISK.
	Identify threats with high residual risk	Highlight and document threats that, even after current controls are applied, continue to pose a significant potential risk. The corresponding concept is RESIDUAL HIGH RISK.
	Consult authorities	If threats continue to pose a high residual risk even after introducing new controls, it's necessary to consult the relevant authorities. The concept that encapsulate this is RESIDUAL HIGH RISK.

Table 22: PDD Concept table with the concepts, description and reference(s) of the activity **Risk Measures**

Concept	Description
CURRENT CONTROLS	CURRENT CONTROLS serves as an archive that catalogues all the existing security measures, protocols, and safeguards in place within an organisation [1, 3, 8, 14, 53, 26, 34, 36, 38, 44, 42, 41, 45, 47, 49, 59, 60, 62, 67, 68, 69, 76, 79, 83, 84, 87, 90, 98, 100, 97, 99, 102, 103].

NEW CONTROLS	NEW CONTROLS serves as a tailored strategy for risk mitigation within an organisation. This ensures that every threat pinpointed through risk assessment is paired with relevant technical or non-technical controls to neutralise or minimise its impact and likelihood [1, 3, 8, 14, 53, 26, 34, 36, 38, 44, 42, 41, 45, 47, 49, 59, 60, 62, 67, 68, 69, 76, 79, 83, 84, 87, 90, 98, 100, 97, 99, 102, 103].
COST-BENEFIT ANALYSIS	COST-BENEFIT ANALYSIS is a methodical strategy employed in the process of decision-making to evaluate the overall anticipated expenses in comparison to the overall anticipated benefits of one or more courses of action, with the aim of selecting the optimal or most financially advantageous alternative. The objective of this study is to assess the efficacy of several options and ascertain which option offers the greatest advantage at the lowest expense. [66, 87, 102].
PRIORITY	PRIORITY serves as a method to order and classify controls using a COST-BENEFIT ANALYSIS. Essentially, it's a systematic way to highlight the most impactful CONTROLS that need urgent attention, allowing for effective resource distribution and prompt action [1, 62, 74, 83, 87].
PRIVACY CONTROL SELECTION	The PRIVACY CONTROL SELECTION serves as a comprehensive record, detailing how the CONTROLS are proportioned and balanced. This documentation ensures that there's a clear understanding of the distribution and emphasis of each control in relation to privacy measures [56].
RISK MANAGEMENT PLAN	The RISK MANAGEMENT PLAN is a detailed implementation strategy that pinpoints the specific CONTROLS set to be rolled out, accompanied by a clear timeline. This plan not only identifies the necessary controls but also ensures that they are introduced in a timely and systematic manner to effectively mitigate potential risks [38, 45, 74, 76, 80, 87, 90, 47].
RESIDUAL RISK	RESIDUAL RISK records the risks that persist even after the proposed mitigation efforts. It offers an in-depth description of these remaining risks and categorises them based on their urgency and importance, ensuring that stakeholders are aware of the potential challenges and can address them effectively [79, 38, 47, 59, 68, 71, 79, 83, 102].
RESIDUAL HIGH RISK	RESIDUAL HIGH RISK captures the risks that remain even after attempted mitigation. It provides a thorough description of these lingering high risks and explains the reasons why such high-level risks are unavoidable. This comprehensive account ensures that stakeholders are not only informed about the persisting threats but also understand the underlying factors that make them inevitable [79, 14, 34, 38, 47, 83, 87].

A.11 Activity & concept table of the activity Report

Table 23: PDD activity table of **Report** and its associated sub-activities with description

Activity	Sub-Activity	Description
Report	Create PIA report	This activity is to get all the artefacts and put them in one report namely PIA REPORT.
	Review PIA report	This involves a thorough examination and evaluation of the PIA (PIA) report to ensure accuracy, completeness, and compliance with privacy standards and regulations before finalisation or implementation.
	Consult DPO	Consult DPO is the process of seeking advice or guidance from the Data Protection Officer (DPO).
	Audit by third party	Audit by Third Party is the independent examination of an organisation's processes, systems, or financial statements by an external entity. This external review ensures that the organisation's operations align with established standards, regulations, or contractual agreements. Third-party audits provide an unbiased perspective, enhancing trust and credibility, and identifying areas of improvement or non-compliance that may not be evident to internal stakeholders.
	Publish third party audit summary	Publish Third Party Audit Summary acts as publicly releasing a condensed version of the findings from an external audit. This summary provides stakeholders, including the public, with a transparent overview of the audit results, highlighting key findings, areas of compliance, and potential areas for improvement. Publishing such a summary fosters trust, demonstrates accountability, and showcases an organisation's commitment to transparency and adherence to established standards or regulations.
	Get PIA approval	This refers to the process of seeking and obtaining formal authorisation or endorsement for the PIA (PIA) report, ensuring that the identified risks and mitigation strategies are acknowledged and accepted by the relevant authorities or stakeholders. Appoint a central entity responsible for privacy related issues such as a privacy committee. A senior executive is held accountable for the quality and adequacy of a PIA .

	Create Public PIA report	Develop a version of the PIA (PIA) report intended for public disclosure, ensuring transparency while possibly omitting sensitive or confidential information to maintain security and privacy standards. A mechanism is implemented for publishing PIA reports to the general public whenever significant changes are made to processing activities. Different PIA reports can exist per PIA process, these reports are adapted to their intended audience in both content and form.

Table 24: PDD Concept table with the concepts, description and reference(s) of the activity **Report**

Concept	Description
PIA REPORT	The PIA REPORT is the main artefact which contains PIA PLAN, DATA PROTECTION REQUIREMENTS, COLLECTION OF VIEWS, USE CASE MODEL, LIST OF THREATS, LIST OF CONTROLS, PRIVACY CONTROL SELECTION, RISK MANAGEMENT PLAN, RESIDUAL RISK and RESIDUAL HIGH RISK [3, 4, 14, 45, 49, 68, 67, 71, 76, 79, 80, 83, 87, 89, 90, 102, 103].
AUDIT REPORT	AUDIT REPORT is a formal document that presents the findings of an audit conducted by an independent body or auditor. The primary purpose of the report is to provide an objective assessment of the subject matter's compliance with specific criteria, be it financial statements, internal controls, processes, or any other aspect [90, 49, 87, 56].
AUDIT SUMMARY	An AUDIT SUMMARY is a condensed version of the full audit report, designed to provide stakeholders with a quick and comprehensive overview of the audit's most significant findings, conclusions, and recommendations. When some information in the full report is classified or confidential, the audit summary becomes even more critical. It ensures that stakeholders get the necessary insights without revealing sensitive details [90, 49, 87].
SIGNED PIA REPORT	SIGNED PIA REPORT refers to PIA REPORT that has undergone scrutiny and received formal approval [36, 45, 49, 71, 56]
CUSTOM PIA REPORT	CUSTOM PIA REPORT refers to a PIA REPORT that is tailored or customised for a specific stakeholders. Instead of employing a generic, one-size-fits-all approach, a custom PIA takes into consideration the unique attributes, requirements, and nuances of a particular scenario or environment [3, 14, 49, 76, 79, 87, 89, 100, 97, 99, 102, 103, 56].

A.12 Interview information letter

Universiteit Utrecht

INFORMATIEBRIEF over deelname aan:

Interview voor validatie van het Privacy Impact Assessment PDD

Onderzoekstitel: Designing a Privacy Impact Assessment Process Deliverable Diagram

1. Inleiding

Beste heer, mevrouw,

Wij vragen u vriendelijk om mee te doen aan een wetenschappelijk onderzoek. U ontvangt deze brief omdat u kennis en/of ervaring uit de praktijk heeft die relevant zijn voor het onderzoeksonderwerp. Om mee te doen aan dit onderzoek is uw schriftelijke toestemming nodig. Het doel van deze brief is om u te informeren over de inhoud van het onderzoek en wat meedoen voor u betekent zodat u een weloverwogen besluit kunt nemen. Meedoen is geheel vrijwillig. Lees de informatie in deze brief rustig door en vraag de onderzoeker om uitleg als u meer informatie nodig heeft of vragen heeft.

2. Wat is de achtergrond en het doel van het onderzoek?

In de context van een steeds meer data-gedreven wereld, is het essentieel om het concept van 'Privacy by Design' verder te verkennen en te integreren in onze technologieën en systemen. Dit geldt in het bijzonder voor het beoordelingsproces van privacyrisico's, zoals uitgevoerd tijdens de Privacy Impact Assessment (PIA). Er is een duidelijke noodzaak om diepgaander onderzoek te doen naar de variabelen en factoren op procesniveau die bijdragen aan de effectiviteit en het succes van een PIA, over de verschillende volwassenheidsniveaus van een organisatie. Dergelijk onderzoek kan licht werpen op de mechanismen die de doeltreffendheid van een PIA kunnen verbeteren en kan mogelijk leiden tot verbeterde praktijken en richtlijnen op dit gebied.

3. Door wie wordt het onderzoek uitgevoerd?

Het onderzoek is een masterthesisproject uitgevoerd door een Business Informatics masterstudent van de Universiteit Utrecht. Het project wordt begeleid door een PhD kandidaat van de Universiteit Utrecht die werkzaam is bij [redacted]. Het onderzoek wordt uitgevoerd bij [redacted], onderdeel van het ministerie van Binnenlandse Zaken en koninkrijksrelaties van de Rijksoverheid.

4. Hoe wordt het onderzoek uitgevoerd?

Uw deelname aan het onderzoek is specifiek voor een interview als onderdeel van de validatiefase. De gehele sessie neemt ongeveer 1 tot 1:30 uur tijd in beslag. Gedurende de sessie wordt een versie van het Privacy Impact Assessment Process Deliverable Diagram getoond en toegelicht. Er wordt van u gevraagd om uw gedachten en meningen te delen en om feedback te geven op het model. Er zijn verder geen kosten en vergoedingen aan uw deelname in dit onderzoek verbonden. Er zijn geen fysieke, juridische of economische risico’s verbonden aan uw deelname.

5. Wat gebeurt er met uw gegevens?

De audio van het interview wordt opgenomen. Er zal een transcriptie gemaakt worden die daarna geanalyseerd wordt op relevante inhoud. De ruwe gegevens, zoals de directe opname en transcriptie,

worden alleen gebruikt voor de analyse van de uitkomsten van het interview. Deze gegevens worden niet gepubliceerd of op andere manier met derden gedeeld. De audio opnames worden permanent vernietigd nadat deze zijn getranscribeerd. De anonieme transcripties worden bewaard voor tien jaar, in lijn met het beleidskader onderzoeksdata van de Universiteit Utrecht.

De inhoudelijk relevante gegevens zoals meningen, uitspraken, visies en/of gedachten worden verwerkt als validatie uitkomsten en worden gebruikt voor verdere ontwikkeling van het Privacy Impact Assesment Process Deliverable Diagram. Deze uitkomsten worden als onderdeel van het onderzoek gepresenteerd in werken zoals een thesis, wetenschappelijke artikelen en/of presentaties. Deze werken kunnen worden gepubliceerd. Uw naam zal nooit in een werk genoemd worden en geen enkel tekstdeel zal persoonlijk herleidbaar zijn. De verwerkte gegevens worden in geanonimiseerde en/of geaggregeerde vorm gepresenteerd. Het is hierbij mogelijk dat functietitels, functie ervaring, type organisatie en/of betreffende markt genoemd worden.

U geeft toestemming voor gebruik van uw gegevens voor dit onderzoek. Daarnaast geeft u toestemming voor het hergebruik van de geanonimiseerde resultaten voor het beantwoorden van onderzoeksvragen in eventuele vervolgonderzoeken. De geluidsopnamen worden niet hergebruikt of gedeeld.

6. Wat zijn uw rechten?

Deelname is vrijwillig. Uw gegevens mogen alleen voor het onderzoek verzameld worden als u hier toestemming voor geeft. Als u toch besluit niet mee te doen, hoeft u verder niets te doen. U hoeft niets te tekenen. U hoeft ook niet te zeggen waarom u niet wilt meedoen. Als u wel meedoet, kunt u zich altijd bedenken en op ieder gewenst moment stoppen — ook tijdens het onderzoek. En ook nadat u heeft meegedaan kunt u uw toestemming nog intrekken. Als u daarvoor kiest, hoeft de verwerking van uw gegevens tot dat moment overigens niet te worden teruggedraaid. De onderzoeksgegevens die wij op dat moment nog van u hebben, zullen worden gewist. Het afzien van deelname of het vroegtijdig stoppen heeft geen nadelige gevolgen voor u.

7. Klachten

Heeft u een klacht of een vraag over de verwerking van persoonsgegevens, dan kunt u terecht bij de functionaris voor gegevensbescherming van de Universiteit Utrecht (privacy@uu.nl). Deze kan u ook helpen bij het uitoefenen van de rechten die u onder de AVG heeft. Verder wijzen we u erop dat u het recht heeft om een klacht in te dienen bij de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

8. Meer informatie over dit onderzoek?

Als u na het lezen van deze informatie verdere vragen heeft, kunt u contact opnemen met:

Uitvoerend onderzoeker	Hugo van Vliet	h.s.vanvliet@students.uu.nl
Onderzoeker	F. van Dijk, MSc	f.w.vandijk@uu.nl

9. Bijlagen:

- Toestemmingsverklaring

A.13 Interview declaration of consent

Universiteit Utrecht

TOESTEMMINGSVERKLARING voor deelname aan:

Focusgroep voor validatie van het Privacy Impact Assessment PDD

Onderzoekstitel: Designing a Privacy Impact Assessment Process Deliverable Diagram

Ik bevestig:

- dat ik via de informatiebrief naar tevredenheid over het onderzoek ben ingelicht;
- dat ik in de gelegenheid ben gesteld om vragen over het onderzoek te stellen en dat mijn eventuele vragen naar tevredenheid zijn beantwoord;
- dat ik gelegenheid heb gehad om grondig over deelname aan het onderzoek na te denken;
- dat ik uit vrije wil deelneem.

Ik stem ermee in dat:

- de verzamelde gegevens voor wetenschappelijke doelen worden verkregen en bewaard zoals in de informatiebrief vermeld staat;
- de verzamelde, geanonimiseerde onderzoeksgegevens door wetenschappers kunnen worden gedeeld en/of worden hergebruikt om eventueel andere onderzoeksvragen mee te beantwoorden;
- er voor wetenschappelijke doeleinden geluidsopnamen worden gemaakt.

Ik begrijp dat:

- ik het recht heb om mijn toestemming voor het gebruik van data in te trekken, zoals vermeld staat in de informatiebrief.

Naam deelnemer: _____

Handtekening: _____ Datum, plaats: ___ / ___ / ____, _____

In te vullen door de uitvoerend onderzoeker:

Ik verklaar dat ik bovengenoemde deelnemer heb uitgelegd wat deelname aan het onderzoek inhoudt.

Naam: _____

Handtekening: _____

Datum: ___ / ___ / _____

A.14 Interview invitation

Beste [naam],

Graag nodigen wij u uit om deel te nemen aan een interview als onderdeel van een onderzoek naar het Privacy Impact Assessment Proces. De Universiteit Utrecht doet onderzoek in samenwerking met [redacted] naar het Privacy Impact Assessment Proces en de bijhorende Deliverables en hoe deze zich tot elkaar verhouden, met als doel het creëren van een nieuw Privacy Impact Assessment Proces. Dit model kan praktijkbeoefenaars gidsen welke proces stappen en bijhorende documentatie moet worden ondernomen om tot een volwaardig Privacy Impact Assessment te komen.

Hoewel Privacy Impact Assessments (PIAs) een cruciale rol spelen in privacybescherming, is de exacte definitie en praktische uitvoering van een PIA vaak onduidelijk. Zowel in de wetenschappelijke literatuur als in de wettelijke context blijft het ongewis welke stappen een organisatie dient te nemen voor de effectieve implementatie van een PIA.

Er is een literatuurstudie uitgevoerd om helderheid te verkrijgen over de aanbevolen processtappen en noodzakelijke Deliverables voor een PIA. Gebaseerd op de inzichten die uit deze studie naar voren zijn gekomen, hebben we een voorlopige versie van het PIA proces ontwikkeld. Dit proces dient ter ondersteuning van organisaties in hun streven naar effectieve privacybescherming.

Momenteel bevindt ons onderzoek zich in de validatiefase. Deze fase is cruciaal om te waarborgen dat het model het beoogde effect daadwerkelijk bereikt. Een belangrijke stap in deze validatie is het organiseren van een focusgroep met praktijkexperts. Uw bijdrage als deelnemer zou bestaan uit het geven van feedback op het voorgestelde model. Daarnaast zal uw kennis en ervaring bijdragen aan de vormgeving van het traject naar volwassenheid en verdere ontwikkeling van het model.

Indien u interesse heeft om deel te nemen aan deze sessie, vernemen wij dit graag van u. De deelnemende experts zullen op een later tijdstip een informatieve brief ontvangen met meer details over het onderzoek en pratische informatie over het interview. Deze brief zal tevens een toestemmingsverklaring voor het gebruik van de onderzoeksdata bevatten.

Het interview vindt plaats op [datum], [tijd], bij [redacted]

Met vriendelijke groet,

Hugo van Vliet
Friso van Dijk

A.15 Interview protocol

Universiteit Utrecht

Interview protocol

The interviews were carried out in the Dutch language, consequently, the interview protocol adhered to this linguistic medium.

Introductie - 5 minuten

• *Introductie van onderzoek*

Voor het schrijven van mijn thesis heb ik een process deliverable diagram gemaakt. In dit geval gaat het onderzoek over de Privacy Impact Assessment. Dit onderzoek zal duidelijk maken welke process stappen er nodig zijn om een privacy impact assessment te doorlopen op verschillende volwassenheids niveaus.

Een "volwassenheidsniveau" (ook wel bekend als een "maturity level" in het Engels) verwijst naar het niveau van ontwikkeling, bekwaamheid, of vooruitgang van een bepaald proces, systeem of organisatie op een specifiek domein of gebied. Volwassenheidsniveaus worden vaak gebruikt om de effectiviteit, efficiëntie en volwassenheid van bedrijfsprocessen te meten en te benchmarken.

• *Doel interview*

Het doel van dit interview is om het ontwikkelde model te valideren en bij te stellen door gebruik te maken van de kennis en inbreng van experts.

• *Toestemming geven*

Voor we dieper op de inhoud ingaan, heb ik jullie toestemming vereist om alle informatie die uit deze validatie voortkomt te gebruiken als onderzoeksgegevens voor de verdere ontwikkeling van het model. Jullie hebben een informatiebrief en een toestemmingsverklaring ontvangen. Hebben jullie de gelegenheid gehad deze documenten door te nemen? Zijn er vragen hieromtrent?

Het staat jullie volledig vrij om deel te nemen; op elk gewenst moment kun je besluiten om te stoppen, dat is geen enkel probleem.

De audio van deze sessie word opgenomen. Bent u hiervan op de hoogte en gaat u hiermee akkoord? Deze audio-opname wordt enkel gebruikt om een transcriptie te maken en zal daarna verwijderd worden. De transcriptie en de onderzoeksdata zullen niet naar individuele personen te herleiden zijn.

[Laat toestemmingsverklaringen tekenen]

[Recording starten]

Interviewee - 5 minuten

• Wat is uw rol binnen de overheid?

• In hoeverre heeft u ervaring opgedaan met projecten waarvoor een PIA moest worden uitgevoerd?