A Focus Area Maturity Model for Privacy-by-Design

Michel Muszynski

4010868

A thesis submitted in fulfilment of
the requirements for the degree of

Master of Science

First Supervisor	: Prof. dr. S. Brinkkemper
Second Supervisor	: Dr. M. Brinkhuis
External Supervisor	: F. van Dijk, MSc

Business Informatics
Department of Information and Computing Sciences
Faculty of Science
Utrecht University

25 June 2023

Utrecht University

Abstract

The privacy-by-design (PbD) paradigm was formulated to embed privacy throughout the entire lifecycle of systems, processing activities, and data. However, existing research describes vagueness, a lack of guidance, and a lack of structure resulting in this field being stuck in high-level principles and guidelines, fostering an environment where organisations are adopting their own interpretation of PbD which leads to inconsistent practices and potentially suboptimal solutions. The aim of this research is twofold: (1) structure the privacy-by-design domain by identifying key factors and formulating greater themes and categories to gain an understanding of the functional composition, and (2) create a concrete guiding artifact for the application of PbD in the form of a focus area maturity model to aid practitioners in closing the gap between principles and real design. This research used design science as the overarching paradigm guiding the creation of the maturity model artifact. A concrete maturity model design method was constructed based on method fragments from existing methods that target maturity models. Two multivocal literature reviews were conducted to find PbD factors which were aggregated through a coding approach and subsequently used for the formulation of maturity model elements that populate the maturity matrix. The validation consisted of a focus group interview and the evaluation consisted of a survey presented to participants who had performed an assessment using the created assessment instrument. The main result of this research is a focus area maturity model for privacy-by-design. The proposed model allows organisations to assess their PbD maturity and it suggests improvement actions for maturity development. The accompanying assessment instrument consists of a web-based tool that provides an automated assessment experience and can generate a shareable maturity report. The overall PbD maturity of organisations who performed an assessment was found to be low with all but one not reaching the first maturity level. Practitioner attitude towards the proposed model was neutral to moderately positive. Additional research should address the limitations of this work by aiming to increase the generalisability of the proposed model for different legal systems and organisation types, and by investigating practitioner attitude on a greater scale.

Keywords: privacy, data protection, privacy-by-design, focus area, capability, maturity model, information systems, design science.

Contents

List of figures

List of tables

1 Introduction

With the increase in awareness and public interest over the past decade, multiple regulatory and legislative efforts have commenced to enact protections and guidelines in the realm of privacy and data protection. Perhaps the best known of these is the General Data Protection Regulation (GDPR) introduced in 2016, which has granted European Union (EU) citizens data and privacy protections in one fell swoop (European Parliament and Council of the European Union, 2016). Despite these protections set by law, concerns are still widely shared. In September 2021, a Eurobarometer survey was conducted among 26,530 EU citizens. The results show that 81% of surveyed citizens feel that digital tools and the internet will be important in their lives by 2030. In that same survey, close to half of the respondents (46%) indicated that they are worried about the use of personal data and information by companies or public administrations (European Commission, 2021).

These worries seem justified when taking an inventory of data breach incidents and data protection violations that have happened in recent years. The Amazon owned livestream platform Twitch suffered a data breach in 2021, exposing the earnings of their top-earning streamers to the public (Reuters, 2021). The breach supposedly happened due to the exploitation of an error in server configuration change. The Canadian branch of furniture retailer IKEA reported in 2022 that personal information of approximately 95,000 customers was found in generic employee searches, this information included names, email addresses, phone numbers, and postal codes (Fox, 2022). In 2021, the Irish Data Protection Commission found WhatsApp in violation of the GDPR for unclear privacy policies and lack of transparency in regard to the utilisation of user data, a total fine of 225 million EUR was issued (Data Protection Commission, 2021). Earlier that same year, the Luxembourg National Commission for Data Protection claimed that Amazon Europe's personal data processing did not comply with EU regulations, leading to a record-high imposed fine of 746 million EUR (Amazon.com, Inc., 2021).

The 2021 IBM data breach report presents the results of a study of 537 real breaches across 17 countries and 17 industries (Ponemon Institute & IBM, 2021). According to this report, the average total cost of a data breach in 2021 was 4.24 million USD, a 10% increase compared to the previous year. Of the total breach cost, 1.52 million (38%) is attributed to loss of business including loss of revenue from disruption or downtime, increased customer turnover, and diminished reputation and goodwill. Breaches and violations can lead to eight- or even nine-digit fines or settlements (CMS, 2022; Federal Trade Commission, 2022), and the news of privacy issues can deter users (Felt et al., 2012), push users to alternatives (Egelman et al., 2013), and it can even impact a company's stock value negatively (Acquisti et al., 2006). These observations indicate that responsible data handling is not only of concern to citizens or consumers but also affects organisations and companies.

1.1 Gap in knowledge

The increase in awareness and efforts from watchdogs and regulatory bodies eventually led to the inception of a new systems design approach, coined *privacy-by-design* (PbD) (Cavoukian, 2009). According to PbD, privacy should be embedded throughout the entire system design process as an essential component, being proactive and allowing to identify and mitigate data protection problems early, as opposed to bolting on solutions afterwards which ends up being time-consuming, expensive, and potentially not effective in addressing privacy concerns (Cavoukian, 2009; Schaar, 2010). In an effort to assert control over this field and comply with regulations, the *Privacy Impact Assessment* (PIA) was developed. A PIA is "a process for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary to avoid or minimise the negative impacts" (Wright, 2012, p. 55).

Current work on privacy-by-design often does not get past high-level principles and guidelines—vague notions that leave practitioners with questions regarding their application in system engineering (Gurses et al., 2011; Rubinstein & Good, 2013). Practices surrounding the application of the PIA suffer similarly from a lack of consistency. In order to address the inevitable changes in a system's design or operation, the PIA should be seen as a continuous process rather than a one-time object (Sion, Landuyt,

et al., 2020). Van Puijenbroek and Hoepman (2017) found that theory and practice are often misaligned. Their research indicates that organisations typically only conduct a privacy assessment once in the early stages of system development and do not supplement the assessment afterwards ever. They additionally found that there is a lack of uniformity regarding guidelines or frameworks for conducting PIAs, having observed multiple different frameworks in use from different sources. Lastly, they also found that the quality of the privacy risk analysis was influenced by the availability of privacy expertise within the organisation.

1.2 Problem statement and objective

These observations indicate that there is a lack of structure in the PbD field and that its practices are inconsistent. At the same time, regulatory compliance is becoming more important and societal pressure is increasing. Practitioners are in need of guidance when applying the privacy-by-design paradigm in real system design projects. The aim of this research is twofold: create an artifact that provides guidance to practitioners that want to apply privacy-by-design, while simultaneously delivering an academic contribution by identifying recommended practices, and formulating capabilities and focus areas for this domain, identifying relationships and creating structure in order to aid in closing the gap between principles and real design.

Work in progress by van Dijk (2022) investigates the gap between PIA theory and practice, and proposes a privacy maturity perspective that can be used to assess the progressive maturity of an organisation in a functional domain. This thesis acknowledges the potential maturity perspective and aims to create a maturity model for the privacy-by-design domain as a guiding artifact for practitioners. Stages of growth models are commonly used in organisational research (Solli-Sæther & Gottschalk, 2010), specifically maturity models exist by the dozens (de Bruin et al., 2005; van Looy et al., 2017). They are an established concept in the information systems (IS) field (Cleven et al., 2012), specifically focus area maturity models are suitable for the development of a functional domain (van Steenbergen et al., 2013).

Based on the identified knowledge gap, the objective of this research is to design a focus area maturity model that structures the privacy-by-design domain and allows organisations to effectively employ privacy-by-design practices in information systems design projects. Using the alternative design problem template of Wieringa (2014), this design problem is defined as follows:

> How to *design a maturity model*
> that satisfies *focus area maturity model components and quality attributes*
> so that *organisations can employ effective privacy-by-design practices*
> in *information systems design projects*.

The requirements for the maturity model consist of adhering to the focus area maturity model components, i.e., all syntactical elements according to the meta-model of van Steenbergen et al. (2013). In addition, the model is evaluated according to several evaluation criteria taken from Prat et al. (2015). These form the basis for the formulation of additional quality attributes that the artifact must adhere to completeness, ease of use, effectiveness, operational feasibility, and usefulness. A similar approach for the evaluation of a focus area maturity model by using criteria from Prat et al. was used by Overeem et al. (2022). The requirements are further specified in more detail in chapter 5.

1.3 Research questions

In order to address the gap in knowledge and accomplish the research objective, the following main research question (MRQ) is formulated:

MRQ: How can organisations assess their privacy-by-design practices through a maturity model approach in order to understand the progression of, and the relationships between, various domain factors?

The main research question can be decomposed into several research questions (RQ):

RQ1: What maturity models exist in the relevant and adjacent domains?

Maturity models are an established concept and multiple different types of these models exist, originating from different fields and domains. Before a new model is created, it is wise to get an overview of existing models which can give insights and provide a base of operation (Becker et al., 2009).

RQ2: What are the relevant factors that influence privacy-by-design?

The first step in populating the maturity model is to gather all relevant factors that can influence privacy-by-design, such as best-practices, principles, or guidelines. These factors provide the basis for the capabilities of the model.

RQ3: What does a privacy-by-design focus area maturity model look like?

a. What focus areas does a privacy-by-design focus area maturity model have?

b. What capabilities does a privacy-by-design focus area maturity model have?

c. What are the dependencies between the capabilities in a privacy-by-design focus area maturity model?

d. What does the accompanying assessment instrument look like?

Once the relevant factors in the domain have been identified, they must be analysed, categorised, aggregated, and prioritised into dimensions suitable to populate the maturity model with. The focus area maturity models consist of focus areas and capabilities, with the levels being determined by the dependencies among the capabilities. The maturity matrix is created by populating all these model components. Additionally, an accompanying assessment instrument must be constructed to facilitate the implementation.

RQ4: How does a privacy-by-design focus area maturity model perform in practice?

Designing a model alone is not enough. Since the purpose of the model is to be applied in practice, a validation with expert practitioners will have to be performed to incorporate experiences from practice, and an evaluation to determine whether the artifact will perform in its natural context as expected.

1.4 Thesis outline

This thesis is structured as follows: chapter 2 provides an outline of the research design including the used methods and rationales. Background on privacy and maturity, as well as related works, are described in chapter 3. Chapter 4 presents the results of two literature reviews: a comparison of existing models (RQ1) and an inventory of influential PbD factors (RQ2). The design of the maturity model and its components, the underlying design decisions, and the traceability with the found practices are outlined in chapter 5 (RQ3). Chapter 6 describes the results of the validation activities (RQ4). Chapter 7 presents the design of the accompanying assessment instrument (RQ3). Chapter 8 describes the results of the evaluation activities (RQ4). Furthermore, the discussion in chapter 9 highlights some results, addresses the validity threats, and outlines the limitations of this research. Lastly, chapter 10 concludes by answering the research questions, describing the main contributions, and presenting opportunities for future work.

2 Research design and methods

This chapter provides an overview of the research design, methods, and instruments including design science, the maturity model design method construction, multivocal literature review, focus group interview, survey, and ethical considerations.

2.1 Design science

Maturity models are artifacts used for evaluation, benchmarking, and analysis of characteristics of effective processes at different stages of development. Design science is the design and investigation of artifacts in context (Wieringa, 2014), this notion makes the design science paradigm seem suitable for the development of maturity models. Apart from suitability, a more pressing observation pushes the development of maturity models into the realm of design science. Wendler (2012) states that maturity models must be developed with scientific rigour and validation in order to increase their scientific nature.

This is in accordance with the design science guidelines of Hevner and Chatterjee (2010). Guideline 3: *Design evaluation* states that an artifact's utility, quality, and efficacy must be demonstrated through evaluation methods. Guideline 5: *Research rigour* states that design science relies upon rigorous methods in both the construction and evaluation of the design artifact. Taking these considerations into account, and observing that other researchers are similarly choosing design science for the creation of maturity models, e.g., van Steenbergen et al. (2010) and Mettler (2011), this research is also employing the design science paradigm for its design.

Figure 1 shows the engineering cycle and the encompassed design cycle of Wieringa's (2014) design science method. The design task in a design science project can be decomposed into three separate activities, namely, problem investigation, treatment design, and treatment validation. The relevant domain must be investigated to gain input for the design of an artifact. The resulting design is validated, providing new input for the investigation in the next iteration. This iterative cycle consisting of investigation, design, and validation forms the core of any design science project and is called the design cycle. The result of the design cycle is a validated treatment which must be used and evaluated in the real world. The transfer of a validated treatment to a real-world setting for evaluation purposes is captured in the treatment implementation and evaluation activities, which, on top of the design cycle, all together form the engineering cycle.

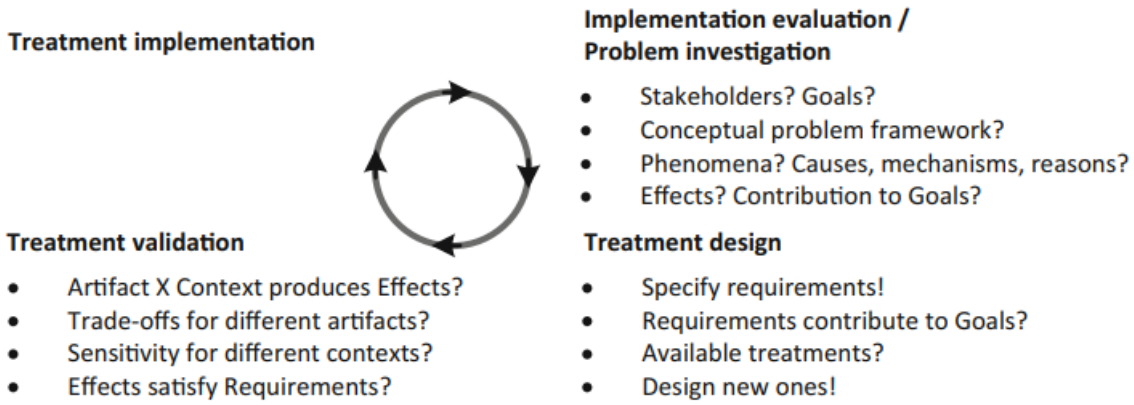

Figure 1: The engineering cycle (Wieringa, 2014).

2.2 Maturity model design method

One of the commonly named criticisms of maturity models is the lack of scientific rigour in the development process. Kohlegger et al. (2009) state that authors of maturity models often build on the models of their predecessors, without critically reviewing the design decisions and underlying assumptions of those models. They come to the conclusion that the nature of maturity models has not

been theorised well in literature, which is a view that is shared by other researchers (de Bruin et al., 2005; McCormack et al., 2009; Pöppelbuß et al., 2011; Solli-Sæther & Gottschalk, 2010).

This observation has led to multiple academic efforts in developing maturity model design methods, often employing and adapting the design science paradigm and its principles. Table 1 shows an overview of five maturity model design methods and the model types which they aim to service. De Bruin et al. (2005) and Becker et al. (2009) present a generic method that does not focus on any particular maturity model type. Others have proposed methods for specific model types: Maier et al. (2012) for maturity grids, van Steenbergen et al. (2010) for focus area maturity models, and Mettler and Rohner (2009) for situational maturity models.

Table 1: Overview of maturity model design methods.

Design method	**Maturity model type**
de Bruin et al. (2005)	Generic
Mettler & Rohner (2009)	Situational
Becker et al. (2009)	Generic
van Steenbergen et al. (2010)	Focus Area
Maier et al. (2012)	Grid

Table 2 provides a comparative overview of the phases of the three relevant maturity model design methods for this research from the overview in Table 1, these being the two generic maturity model methods and the focus area maturity model method. In order to formulate the method for the maturity model development in this research, lightweight situational method engineering is applied. Using the assembly-based approach from van de Weerd and Brinkkemper (2009) in a slimmed-down fashion, relevant method fragments are selected and aggregated into a new method, specific to the needs of this research project. The *method base* from which method fragments are extracted consists of the three methods portrayed in Table 2 as well as Wieringa's (2014) engineering cycle.

Table 2: Comparison of maturity model design method phases.

<table>
<tr><th>de Bruin et al. (2005)</th><th>Becker et al. (2009)</th><th>van Steenbergen et al. (2010)</th></tr>
<tr><td>Scope</td><td>Problem definition</td><td>Scoping</td></tr>
<tr><td rowspan="2">Design</td><td>Comparison with existing maturity models</td><td rowspan="3">Design model</td></tr>
<tr><td>Determination of development strategy</td></tr>
<tr><td rowspan="3">Populate</td><td>Iterative maturity model development</td></tr>
<tr><td>Conception of transfer and evaluation</td></tr>
<tr><td>Implementation of transfer media</td><td>Instrument development</td></tr>
<tr><td>Test</td><td rowspan="3">Evaluation</td><td rowspan="3">Implementation & exploitation</td></tr>
<tr><td>Deploy</td></tr>
<tr><td>Maintain</td></tr>
</table>

Figure 2 shows the Process-Deliverable Diagram (PDD) for the resulting maturity model design method for this research. PDD is a technique used for meta-modelling activities of methods and their resulting artifacts, as described by van de Weerd and Brinkkemper (2009). PDD's combine two diagrams: a process view on the left and a deliverable view on the right. Accompanying the PDD diagram in Appendix A, are the activity table (Table A1) and the concept table (Table A2). The activity table outlines all activities, corresponding subactivities, and the relationship to their generated and consumed deliverables. The concept table outlines all deliverables as concepts with a reference and definition.

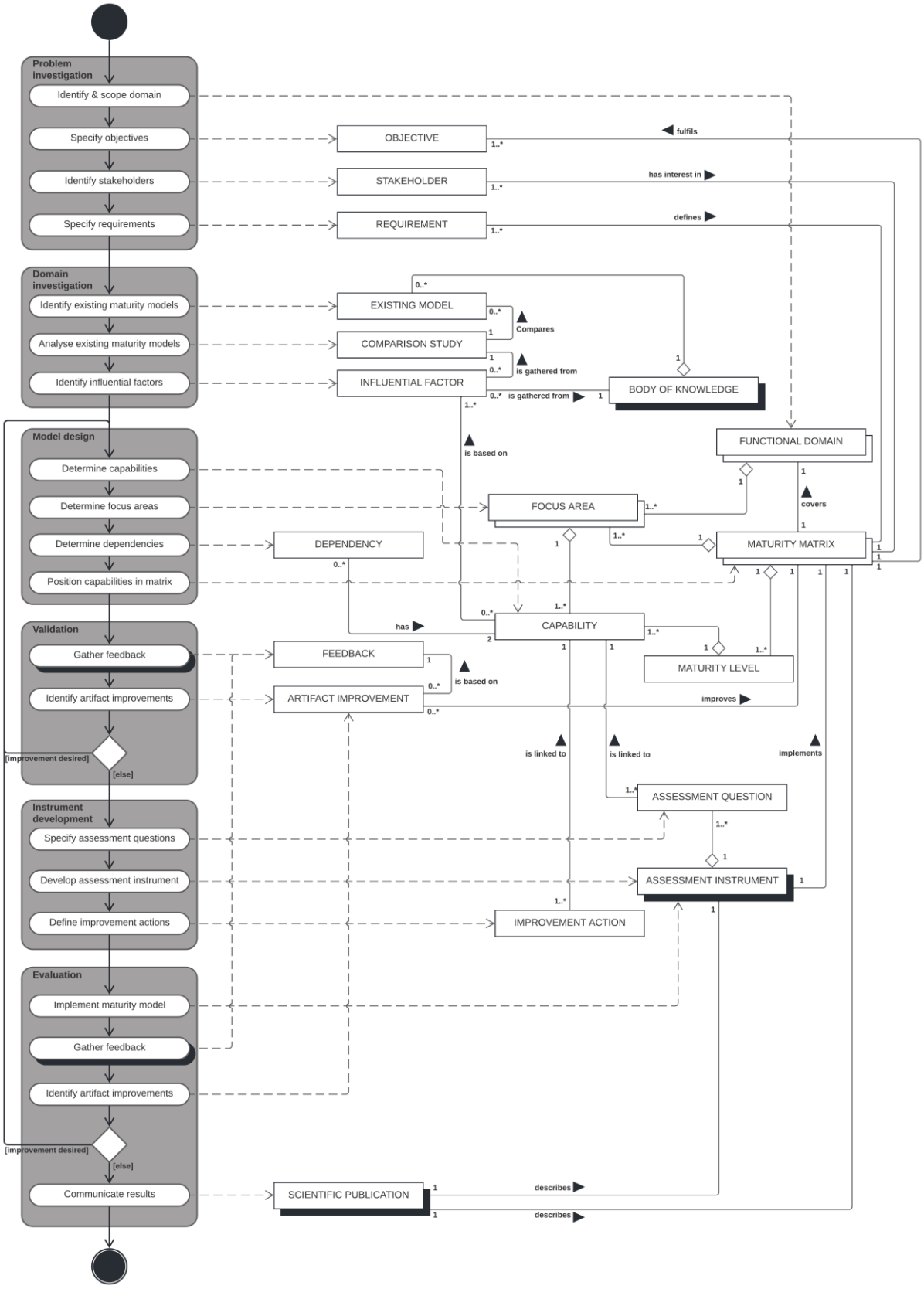

Figure 2: Process-deliverable diagram of the maturity model design method.

2.3 Rationale for method construction

The method fragments, selected from the method base, for the design of the maturity model development method, are based on certain needs. This chapter has already described how the design science paradigm is recommended to use in maturity model development, therefore the method must employ an iterative process with validation/evaluation activities. The model type determines which model components must be developed during the method. In this case, the relevant model type is the focus area maturity model, therefore the method must be tailored to focus area maturity model components. In an effort to determine the content of certain model components, a review of existing work must be performed, therefore the method must contain activities that support this. One of the envisioned contributions of this research is to provide guidance to practitioners. A maturity model must be accompanied by an assessment instrument that allows practitioners to implement the model, therefore the method must suffice in the need for an assessment instrument in conjunction with the maturity model. Lastly, the development of the maturity model, including the results, design decisions, and rationales must be documented extensively to ensure scientific rigour and facilitate extension and evaluation by future researchers, as well as allow practitioners to leverage the benefits that the artifact provides (Hevner et al., 2004).

Table 3 shows the traceability links between the activities and the works they are based on. The *problem investigation* and its subactivities are mostly based on the first phase of Wieringa's (2014) engineering cycle. These are the standard pre-design activities that are relevant to every design science project. The *domain investigation* and its subactivities are the domain review activities intended to analyse existing works. A general investigation of the domain and existing solutions is mentioned by Wieringa (2014). Becker et al. (2009) specifically mention the identification and comparison of existing maturity models in maturity model development. The existing works to be reviewed, are part of the total BODY OF KNOWLEDGE. This concept was added for completeness and represents, in this case, both white and grey literature. The *model design* and its subactivities are adopted from the PDD for focus area maturity model development by van Steenbergen et al. (2010). For this research, the *Determine focus areas* activity and the *Determine capabilities* activity have been swapped. Exploratory domain investigation has shown that it is unstructured and lacks consensus, the decision was made to use a bottom-up approach where domain factors are distilled into capabilities which then are aggregated into focus areas, rather than identifying the focus areas first which would work better in a more mature domain. The *validation* and its subactivities are adopted from Wieringa's (2014) engineering cycle. Wieringa describes how different methods exist for validating artifact designs. Taking this into account with the realisation that different validation methods can be applied in different iterations, the decision was made to model the *Gather feedback* activity as a closed activity. The *Instrument development* and its subactivities are mostly adopted from the PDD by van Steenbergen et al. (2010). The *Specify assessment questions* activity has been derived from the ASSESSMENT QUESTION concept in the meta-model by van Steenbergen et al. (2010, 2013). The Evaluation and its subactivities are mainly adopted from Wieringa's (2014) engineering cycle. Additionally, van Steenbergen et al.'s (2010) PDD contains an *Implement maturity model* activity and *Communicate results* activity which are adopted. The *Improve matrix iteratively* activity from van Steenbergen et al. (2010) has been unfolded into two overlapping loops from the *Validation* and *Evaluation* back to *Model design*. Modelling explicit conditional loops highlights the iterative nature of the development process better and is more in line with Wieringa's (2014) cycles.

Table 3: Method fragment traceability.

Activity	Source
Identify & scope domain	de Bruin et al. (2005); van Steenbergen et al. (2010)
Specify objectives	Wieringa (2014)
Identify stakeholders	Wieringa (2014)
Specify requirements	Wieringa (2014)
Identify existing maturity models	Becker et al. (2009); Wieringa (2014)
Analyse existing maturity models	Becker et al. (2009); Wieringa (2014)
Identify influential factors	de Bruin et al. (2005); Wieringa (2014)
Determine capabilities	van Steenbergen et al. (2010)

Determine focus areas	van Steenbergen et al. (2010)
Determine dependencies	van Steenbergen et al. (2010)
Position capabilities in matrix	van Steenbergen et al. (2010)
Gather feedback (validation)	de Bruin et al. (2005); Wieringa (2014)
Identify artifact improvements (validation)	Wieringa (2014)
Specify assessment questions	de Bruin et al. (2005); van Steenbergen et al. (2010, 2013)
Develop assessment instrument	Becker et al. (2009); de Bruin et al. (2005); van Steenbergen et al. (2010)
Define improvement actions	van Steenbergen et al. (2010)
Implement maturity model	van Steenbergen et al. (2010); Wieringa (2014)
Gather feedback (evaluation)	de Bruin et al. (2005); Wieringa (2014)
Identify artifact improvements (evaluation)	Wieringa (2014)
Communicate results	Becker et al. (2009); van Steenbergen et al. (2010)

2.4 Rationale for model type selection

For the maturity model that is to be developed in this research, the focus area maturity model type is selected. There are several reasons for the selection of this model type. A prevalent criticism of maturity models is that they do not provide adequate guidance in prioritizing and selecting improvement measures (Huang & Han, 2006; Pöppelbuß & Röglinger, 2011). This lack of decision support can be troublesome for managers and executives who have to make decisions in their business process transformation efforts, but, according to Hammer (2007), often struggle to identify a clear starting point. Focus area maturity models address this weakness by also focussing on the development of IS function as opposed to just the measuring part (van Steenbergen et al., 2013). The division of the functional domain into smaller focus areas allows for a finer granularity, which is more suitable for providing a progression path. By using focus areas, different parts of the domain can be assessed independently which facilitates the fact that parts can develop at a different pace and can be in different phases of development, while simultaneously, there exist dependency relationships between the development paths of these parts. This fine-grained approach with explicit dependency relationships provides more guidance in step-by-step IS functions improvement, which makes this maturity model type more appropriate for the step-by-step development of a functional domain (van Steenbergen et al., 2013).

The fact that a focus area maturity model for a functional domain consists of constituting focus areas, helps with the theoretical grounding and addresses the earlier mentioned criticism in regards to the lack of scientific rigour (van Steenbergen et al., 2013). Focus area maturity models do not force a theoretically hard-to-justify set number of maturity levels a priori, as opposed to traditional fixed-level maturity models (e.g., CMM). This open-endedness allows for the full expression of a domain, in as many maturity levels as are required by the identified capabilities and their dependency relationships.

One of the main aims of this research is to provide practitioners with guidance. Therefore, there exists a desire for the artifact to close the gap between theory and practice and provide value not only to academia but also to practitioner experts. A focus area maturity model allows for information representation in a managerial way (e.g., provides a domain overview, easy to use, quick to scan), and provides the envisioned guidance that allows practitioners to prioritise their transformations and develop their capabilities in a functional domain (Spruit & Röling, 2014; van Steenbergen et al., 2013).

2.5 Literature review

In order to answer RQ1 and RQ2, two multivocal literature reviews (MLR) are performed. This type of literature review differs from a structured literature review (SLR) in that it encompasses grey literature, in addition to academic works (Garousi et al., 2019). Examples of grey literature are blogs, whitepapers, videos, or webpages. Garousi et al. (2019) surveyed 24 papers on MLR practices and provide an overview of the MLR process and provide guidelines for its execution. Conducting an MLR commences with a planning phase which defines the motivation and goals. Guideline 3 of their work states that the choice to perform an MLR with grey literature, as opposed to only performing an SLR, should be made

systematically using a well-defined set of criteria or questions. They provide seven binary questions that can be used to determine whether including grey literature might be beneficial, these questions are shown in Table 4. One or more positive responses to these questions suggest the inclusion of grey literature could be beneficial.

The choice to conduct MLRs over traditional SLRs in this research is based on the observation that maturity models are widely used in industry. A simple google search unearths an array of industry-sourced maturity models, guidelines, and frameworks, which can contain information that could be useful in the creation of a privacy-by-design maturity model. This reasoning is corroborated by Mettler et al. (2010) who similarly recognise the importance of looking beyond academia in the field of maturity models. Preliminary review has shown that while there is moderate consensus on ideal outcomes, the quality and volume of evidence are inconsistent or non-existent, hence the twofold response to question two. More formally, the choice to conduct MLRs is substantiated by multiple positive answers to the seven grey literature inclusion questions (Table 4).

Table 4: Questions to decide whether to include grey literature (Garousi et al., 2019).

#	Question	Response
1	Is the subject "complex" and not solvable by considering only the formal literature?	No
2	Is there a lack of volume or quality of evidence, or a lack of consensus of outcome measurement in the formal literature?	Somewhat
3	Is the contextual information important to the subject under study?	No
4	Is it the goal to validate or corroborate scientific outcomes with practical experiences?	No
5	Is it the goal to challenge assumptions or falsify results from practice using academic research or vice versa?	No
6	Would a synthesis of insights and evidence from the industrial and academic community be useful to one or even both communities?	Yes
7	Is there a large volume of practitioner sources indicating high practitioner interest in a topic?	Yes

For the execution of the MLRs, Garousi et al.'s (2019) guidelines and procedure are applied. This procedure was constructed by adapting the typical SLR practices as presented by Kitchenham and Charters (2007) and consists of the following five phases: search process, source selection, study quality assessment, data extraction, and data synthesis. The following paragraphs will elaborate on these phases and their activities.

Search process

The typical search process starts with the formulation of a search string. This is a string with relevant key words that will be used to query search engines. Exploratory literature searches can be employed to iteratively identify a complete set of relevant key words, including synonyms or alternative equivalent phrasings. Once an initial pool of sources has been collected by querying with the search string, *snowballing* (Wohlin, 2014) can be applied to expand the pool of sources. This technique entails following citations either backward or forward to identify additional relevant sources.

SLRs focus on formal literature and thus often query academic databases, e.g., IEEE Xplore, Scopus, or ACM. These databases come with search engines that allow for a variety of filters and search criteria allowing researchers to pin-point the relevant works. Grey literature is not as rigorously structured, both individually and as a whole collection—authors can post a variety of works, in a variety of formats, through a variety of channels. Garousi et al. (2019) synthesised four strategies for grey literature sourcing:

- *General web search engine*: Conventional web search engines such as Google are seen as valid options, and have been used in previous works (Adams et al., 2016; McGrath et al., 2006).

- *Specialised databases and websites*: Various databases exist for grey literature, both general, e.g., opengrey.eu, and field-specific, e.g., osti.gov for energy technology and engineering R&D or eldis.org for global development challenges. Other examples include social question-answer websites, e.g., www.stackoverflow.com, and recurring reports such as annual surveys, e.g., the World Quality Report (Capgemini, 2021) or the annual State of Agile report (Digital.ai, 2021).
- *Contacting individuals directly*: In order to gain certain documents (e.g., unpublished studies), individuals can be contacted directly. This also applies to contacting organisations or sending out general open requests through public channels, e.g., social media (Adams et al., 2016).
- *Reference lists and backlinks*: The typical snowballing technique can be applied to grey literature if a reference list is available. However, reference lists often are not provided. For webpages there exist backlink extraction tools, e.g., www.majestic.com, that can identify which webpages link to a certain webpage.

An important question to answer is when to stop a literature search. In formal literature reviews, a search string will generate a finite number of relevant results, which ends the search. This is referred to as a *data exhaustion* stopping criterion (Garousi et al., 2019). In the context of grey literature searches, this is not as simple since a regular search engine might return an unfeasible number of hits. Garousi et al. (2019) state that different stopping criteria are needed, and formulate three options:

1. Theoretical saturation, i.e., stop the search when no new concepts emerge from the search results.
2. Effort bounded, i.e., only examine the first predefined number of hits.
3. Evidence exhaustion, i.e., extracting all the evidence.

Combinations of these stopping criteria are likewise possible, Garousi and Mäntylä (2016) used an effort-bounded criterion where they only examined the first 100 results but continued searching if the last result revealed relevant findings, combining it with a theoretical saturation criterion.

Source selection

Once the initial pool of sources has been obtained, they must be assessed for relevance. Source selection typically consists of determining selection criteria and the selection process. Inclusion/exclusion criteria are used to select sources that are relevant to answering the research question. Guideline 9 of Garousi et al. (2019) states that quality assessment criteria should be combined with inclusion/exclusion criteria since the used methods or outlet types can already exclude sources depending on the goals and research questions. Excluding sources with certainty early on saves the effort required in time-consuming content analysis. Guideline 10 states that both formal and grey literature should be examined with diligence in a coordinated integrated selection process (Garousi et al., 2019).

Study quality assessment

Quality assessment of sources aims to determine the "quality" of found sources. According to Kitchenham and Charters (2007), there is no agreed-upon definition of *study quality*, however, the Cochrane Handbook (Higgins et al., 2020) and the CRD Guidelines (CRD, 2009) both suggest that quality is related to the extent to which the study minimises bias and maximises internal and external validity. Garousi et al. (2019) present seven criteria with accompanying assessment questions for study quality assessment. Answering the 20 questions for each source allows for the calculation of a normalised score that represents the quality of the respective study. Subsequently, a threshold score can be set, sources scoring above the threshold would be included while sources scoring below it would be excluded. In addition to getting a general idea of the quality of a study, Kitchenham and Charters (2007) mention several specific reasons to perform a quality assessment:

- To gather more detailed inclusion/exclusion criteria.
- To investigate quality differences as a variable.
- To weigh the importance of sources appropriately.

- To aid in interpreting findings.
- To aid in recommending further research.

Data extraction
This phase aims to accurately record the information obtained from the found sources to establish traceability between the source and the extracted information (Garousi et al., 2019; Kitchenham & Charters, 2007). In order to codify the extraction, data extraction forms must be designed. These forms should contain standard information such as the name of the reviewer, date of extraction, title, authors, etc., as well as questions that elicit information which is used to answer the research question for which the review has been conducted (Kitchenham & Charters, 2007). Additionally, Kitchenham and Charters (2007) recommend performing data extraction independently by multiple researchers, comparing results and resolving disagreements until a consensus is reached. Single researchers can employ other techniques, such as letting supervisors perform a data extraction on a sample and comparing the results, or using a test-retest procedure where the researcher selects a random selection of sources and performs a second data extraction to check for consistency.

Data synthesis
Data synthesis refers to the procedure for summarising, integrating, combining, and comparing of the findings from the selected sources (Kitchenham et al., 2015). Depending on the type of data and research questions, an appropriate data synthesis technique must be selected. Numerous synthesis techniques are available, both qualitative and quantitative (Kitchenham et al., 2015). Garousi et al. (2019) distinguish mainly three data types that are common in grey literature:

- *Qualitative and experience-based evidence*: reflections and opinions on topics by practitioners require a qualitative synthesis, e.g., narrative synthesis or cross-case analysis (Kitchenham et al., 2015).
- *Quantitative evidence*: a common form of evidence in grey literature is the questionnaire. Statistical meta-analysis could be used, although the lack of rigour and lack of statistical reporting often make this type of synthesis impossible.
- *Data from particular grey literature databases such as question/answer sites*: certain sources allow for both quantitative and qualitative analysis. Taking StackOverflow as an example, view counts or the number of questions can be used to quantitatively determine the popularity of a topic (Raulamo-Jurvanen et al., 2016). Simultaneously, qualitative analysis (Miles et al., 2014) can be used to qualitatively analyse software engineering problems.

All these aforementioned phases must be instantiated for a particular multivocal literature review and codified in a review protocol, this is a documented plan that describes all the details and steps of the review. Kitchenham and Charters' (2007) SLR protocol contains the review rationale, research questions, search strings, selection criteria, quality assessment checklists, data extraction forms, and synthesis procedure. According to Garousi et al. (2019), taking their MLR guidelines into account allows the adaptation of a regular SLR protocol structure for use in an MLR. Using a pre-defined protocol reduces the risk of researcher bias, and allows scrutiny and evaluation by other researchers providing feedback to potentially improve the protocol (Kitchenham et al., 2015; Kitchenham & Charters, 2007).

2.6 Validation

Validating an artifact means justifying that the effects would positively contribute to stakeholder goals (Wieringa, 2014). The main difficulty of validations is the fact that no real-world implementation is yet available. Validations are performed before implementation, thus there is no interaction with the problem context. According to the design science evaluation framework by Venable et al. (2012), this makes the validation *ex ante artificial*, meaning that it involves an artifact that is not yet instantiated and is placed in an artificial context. In design science research, this difficulty is addressed by using a validation model. This entails creating a design theory of the predicted interaction between the artifact

and its natural context. Examples of models used for validation in software engineering include prototypes and simulations (Wieringa, 2014).

According to (Wieringa, 2014), the simplest way of validating an artifact is by asking experts to give their opinion on it. An artifact can be submitted to a group of experts who will imagine how the artifact will interact with the natural problem context and can give predictions regarding the effects they expect. If the predictions do not satisfy the requirements, a modification of the artifact's design is recommended. Negative opinions can identify matters not thought of by the researcher and are useful to discard bad design decisions early. Eliciting expert opinion can be done through interviews, focus groups, or questionnaires (Wohlin, 2014). The validation for this research makes use of a focus group which has been identified as an appropriate method (Sonnenberg & vom Brocke, 2012; Wieringa, 2014).

Data collection through interviews consists of the researcher asking a series of questions to an expert regarding the artifact in question, this includes the design, context interaction, and effects. Qualitative interviews allow for an in-depth exploration of a field about which the interviewee has extensive knowledge, experience, or insight (Charmaz, 2014). The difference between a regular one-on-one interview and a focus group interview is that a focus group has multiple people participating at the same time, this allows participants to not only interact with the researcher but also with each other in order to have an open discussion. Robson and McCartan (2016) differentiate between three types of interviews:

- *Fully structured*: interview with pre-determined questions in a set order and fixed wording, leaving little room for deviation.
- *Semi-structured*: interview based on a guiding set of questions, probes, and prompts. The questions, wording, and order are flexible and can be adapted in the moment to the flow of the interview. Additionally, there is more room for unplanned follow-up questions and the exploration of unforeseen topics.
- *Unstructured*: interviews with a general topic of interest but largely free-form in execution, not bound by any restrictions. This can be completely informal.

Before a focus group interview can be conducted, it may be beneficial to create an *interview protocol* (Charmaz, 2014; Rubin & Rubin, 2005; Seidman, 2006; Weiss, 1994), sometimes referred to as an *interview guide* (Krueger & Casey, 2015; Roberts, 2020). This protocol is the leading document during the interview and typically contains all the questions and probes. Castillo-Montoya (2016) presents the *Interview Protocol Refinement* (IPR) method that can be used to systematically develop and refine an interview protocol, increasing the reliability and effectiveness of an interview. The IPR aims to create well-vetted interview protocols that allow researchers to obtain robust and detailed interview data, it consists of four phases (Table 5).

Table 5: Interview Protocol Refinement method (Castillo-Montoya, 2016).

Phase		Purpose
Phase 1:	Ensuring interview questions align with the research questions.	To map the interview questions against the research questions in an interview protocol matrix.
Phase 2:	Constructing an inquiry-based conversation.	To Construct an interview protocol with a balance between conversation and inquiry.
Phase 3:	Receiving feedback on interview protocol.	To obtain feedback on the interview protocol.
Phase 4:	Piloting the interview protocol.	To pilot the interview protocol with a limited sample.

An interview protocol brings structure and focus, functioning as a reference for the topics to be addressed (Rubin & Rubin, 2005). The interviewer does not have to worry about remembering questions, probes, or themes, and can focus on the conversational aspect of the interview including the responses given by the interviewee (Charmaz, 2014). Furthermore, the physical protocol acts as a prop, showing a level of preparedness on the researcher's part, and it can even be shared with the research subjects upfront to put them at ease and create transparency (Rubin & Rubin, 2005). Constructing a protocol forces the researcher to think about the order and wording of the questions. These should be relevant to the topic at hand, non-judgmental, and open to capture the interviewee's experiences and

stories (Charmaz, 2014). Questions should be worded in a manner that does not lead, confuse, or otherwise manipulate an interviewee's response (Rubin & Rubin, 2005; Seidman, 2006). Additionally, creating a protocol in preparation for an interview can expose shortcomings or potential problems. Therefore phase 3 of the IPR recommends submitting an interview protocol to an institutional review board, fellow researcher, or supervisor, so that issues can be identified and resolved beforehand, ensuring a smooth sailing interview.

Focus groups work specifically well in exploring feelings, perceptions, and thinking about ideas, products, services, opportunities, or issues (Krueger & Casey, 2015). They can be used in an early research stage to build a foundation for further survey research or they can be used after other research methods to support result interpretation or recommendation formulation for future action or study. Krueger and Casey (2015) recommend a focus group to have five to eight participants, a moderator, and a co-moderator. Additionally, they provide extensive guidance on topics including interview guide creation, participant selection, moderating, and analysis.

2.7 Evaluation

The goal of implementation evaluation is to evaluate an implementation of an artifact by applying it to the original natural problem context (Wieringa, 2014). The researcher is interested in describing and explaining the contribution of the artifact, be it positive or negative, and its effects on stakeholder goals. This classifies implementation evaluation as *ex post naturalistic*, meaning that an instantiation of the artifact is placed in a real, natural, context (Venable et al., 2012). Different methods can be applied for implementation evaluation, e.g., Surveys, case studies, statistical difference-making experiments, ethnography, or phenomenology (Venable et al., 2012; Wieringa, 2014). This research will make use of a survey for the evaluation, which has been identified as a suitable method (Sonnenberg & vom Brocke, 2012; Venable et al., 2012; Wieringa, 2014).

Questionnaires are one of the primary means of gathering data in survey investigations (Wohlin et al., 2012). The questionnaire is applied to a representative sample of a population, after which the findings are analysed for descriptive or explanatory purposes. The conclusions are then generalised from the sample to the original population from which the sample was taken. According to Denscombe (2014), a research survey should do the following things:

- Be designed to collect information which can be used subsequently as data for analysis.
- Consist of a written list of questions.
- Gather information by asking people directly.

Similar to interview design, questionnaire design must take care to avoid vague, ambiguous, compound, leading, duplicate, or offensive questions (Denscombe, 2014). Robson and McCartan (2016, p. 264) provide a checklist for diagnosing problems in question-wording. Questionnaires, especially the self-completion kind, should be minimally complex and come with a low response burden (Denscombe, 2014; Robson & McCartan, 2016). The questions should be limited to the core topics of the research and avoid redundant details or tangentially important matters. They must be brief, to-the-point, and in service of answering the research questions (Robson & McCartan, 2016)—cramming in a high number of open questions risks intimidating respondents which can lower the response rate (Denscombe, 2014).

The questionnaire used in this research is a web questionnaire. This type of questionnaire is administered through a webpage, providing a number of benefits compared to traditional paper questionnaires (Denscombe, 2014). Web questionnaires allow the use of digital advantages such as embedding imagery, video, or audio, as well as aesthetic customization with graphics to make it more enticing. Additionally, using standard form elements like checkboxes allows respondents to fill out a web questionnaire quickly and comfortably from their digital device of choice. The ease of use does not only apply to respondents though, responses typically are automatically collected and presented in a spreadsheet, ensuring timely and accurate data collection.

2.8 Ethical considerations

Whenever human subjects are involved in an empirical research activity, ethical aspects must be taken into consideration (Wohlin et al., 2012). It is paramount that researchers understand research ethics and are able to apply them since they play a role in the management of a research project (Singer & Vinson, 2002) and, in turn, can affect the success of a project (Vinson & Singer, 2008). The sole expectation of scientists to simply behave ethically has been deemed inadequate (Singer & Vinson, 2002). Therefore, efforts have been made in an attempt to standardise ethical behaviour for researchers, in the hope that the number of incidents involving unethical behaviour in research can be reduced (American Psychological Association, 2017; Gotterbarn et al., 1997; World Health Organisation, 2017). Taking the key principles from Vinson and Singer (2008) and combining them with the guidelines by Wohlin et al. (2012), results in a list of ethical topics which should be taken into consideration, these are described next.

Ethical review
Studies involving human subjects can be mandated to be reviewed by an Ethical Review Board (ERB) of the university, government agency, or other centralised institute. An ethical review can be mandatory by law, as is often the case for medical studies involving human subjects. Researchers submit a proposal with a description of the project, details on the subjects and treatments, an outline of how informed consent is obtained, and the relevant ethical considerations regarding confidentiality, data storage, recruitment, benefits, and risks (Vinson & Singer, 2008; Wohlin, 2014). It is the ERB's task to scrutinise any research proposal in order to determine whether it adheres to ethical standards and principals. An ERB's review and approval not only protects research subjects, but also the researcher since unethical practice can lead to a loss of trust, access to data, or funding (Vinson & Singer, 2008). While not every research project demands an ethical review, it is good practice to adhere to ethical research standards nonetheless.

Informed consent
A key tenet of human-oriented studies is that subject participation is voluntary and that subjects have complete and accurate information allowing them to make an informed deliberate decision to participate or not. Vinson and Singer (2008) recommend splitting the informed consent into two separate sheets: a subject information sheet and a subject consent form. The information presented to the subject should entail the background, motivation, and goals of the study, as well as the sampling method, location, subject expectations, and subject benefits. Subjects should be informed that their participation is voluntary and that consent can be withdrawn at any time without adverse consequences. Furthermore, confidentiality provisions and limitations need to be included, in addition to describing how sensitive results will be handled. Informed consent is written for the subjects and should therefore be comprehensible, avoiding jargon or technical terms (Vinson & Singer, 2008).

In this research, human subjects are involved during the validation and evaluation phases. Informed consent forms are part of the interview protocols, questionnaires, and case study protocols.

Confidentiality
The principle of confidentiality refers to the right of a research subject to expect that any information they provide during the research project will remain confidential (Vinson & Singer, 2008). Confidentiality consists of three main aspects (Vinson & Singer, 2008; Wohlin et al., 2012):

- *Data privacy*: restricting access to data through, for example, password protection or encryption.
- *Data anonymity*: Decoupling the identities of subjects from the gathered data.
- *Anonymity of participation*: Keeping consent decisions of subjects secret.

Researchers should conceal and protect the identities of research subjects, be it individuals or organisations. Examination or analysis of the data should not reveal any identities of subjects. This can be achieved by gathering no or minimal identifiable information or by only reporting aggregated data results. The identities of participating subjects should not be shared with colleagues, managers,

professors, clients, competitors, or the public (Vinson & Singer, 2008). Individuals and organisations can suffer negative consequences from having their identities leaked to managers or competitors. Full confidentiality might not always be possible, subjects should be informed of the limitations before they agree to participate.

Sensitive results

Study outcomes can prove to be sensitive to some stakeholders, these could be: managers, professors, organisations, sponsors, or the researchers themselves (Wohlin et al., 2012). For subject sensitivity, confidentiality procedures should be applied, independently of the revealed facts. For sponsor sensitivity, clear statements on the right for independent publication of anonymised results should be included in the informed consent. For researcher sensitivity, the statistical analyses can be performed by peers, independent from the experimenters who may also have designed the treatment. This has the additional benefit of reducing the threat of experimenter expectancies (Wohlin et al., 2012).

Inducement

Researchers should strive for the greatest beneficence for research subjects, meaning maximal benefits and minimal harm. Harm in this context is not limited to physical harm, it includes, among others: stress, disruption, financial harm, the loss of self-esteem or dignity, and tedium (Vinson & Singer, 2008). Participation benefits are typically used as inducements to attract subjects. Gaining knowledge or experience may be inducement enough for a subject to participate. Monetary inducement is possible although care should be taken to keep a balance where the consent to participate is truly voluntary, and not steered by a too large economic or other inducement (Wohlin et al., 2012).

Feedback

Research subjects should be presented with the opportunity to receive information regarding the study and its results. If confidentiality permits it, an individual subject may receive a report on their personal performance during the study, in addition to a general analysis. Sharing feedback on the study results and analysis allows to maintain trust and long-term relationships with the research subjects (Wohlin et al., 2012).

3 Background and related work

This chapter provides background information on the main concepts relevant to this study, these being privacy and maturity. The background concepts regarding privacy and the position of this research therein are explained first, including privacy-by-design and the privacy impact assessment. Second, the workings and goals of maturity models are outlined, including definitions, different model types, and criticisms.

3.1 Privacy

Most people have a sense of what privacy is—they flinch back when they feel that their privacy is being violated. Simultaneously, it is fascinatingly difficult to articulate comprehensively what privacy entails. This elusiveness of the definition of privacy has long been recognised: "nobody seems to have any very clear idea what it is" (Thomson, 1975, p. 1). After more than a century of research spanning multiple spheres of social sciences, providing philosophical, sociological, psychological, and legal perspectives, Solove (2006) concludes that privacy "is in disarray and nobody can articulate what it means" (p. 477). Nonetheless, researchers attempt to bring structure to this domain. Smith et al. (2011) conducted an interdisciplinary review of privacy-related research with a sample of over 400 works. They broadly classify two distinct approaches to defining general privacy: value-based and cognate based.

3.1.1 Definition

Value-based definitions
The value-based definitional approach regards general privacy as a human right that is essential to the moral value system of human society and was historically the first definition of general privacy (Smith et al., 2011). This absolute normative notion of privacy as a right raised questions regarding its emergence, philosophical justification (Schoeman, 1984), and the protection responsibility (Milberg et al., 2000). The debate regarding the status of general privacy as a human right did not only take place on the academic podium but was also relevant in courtroom proceedings. According to Smith et al. (2011), these legal battles exposed two major issues. First, there was a need for a more rigorous definition of general privacy. Second, the role of the state in protecting general privacy became a point of contention.

Two main camps have formed in the discussion of this second issue (Hirsch, 2011; Smith et al., 2011). The first camp views privacy as the right to develop as independent persons, protected by government regulation (Rosen, 2001; Walsh et al., 2017). Opponents of this view see privacy as an economic commodity which is subject to trade-offs and cost-benefit analyses (Smith et al., 2011). They find a call for regulation to be at odds with the economy of the information market (Cohen, 2001) where privacy can be exchanged for perceived benefits (Campbell & Carlson, 2002). This notion is known as *privacy as a commodity* and is, together with *privacy as a right*, part of the value-based definitional approach.

Cognate-based definitions
In 1967 the general privacy concept was expanded with the notion of *state* by Westin, in an effort to provide a more rigorous definition. According to Westin, the four states of privacy are solitude, intimacy, reserve, and anonymity. An individual can transition between these states depending on their personal needs. The choice regarding what state an individual wants to be in and the level of self-revelation that comes with it is seen as critical for self-development and responsible citizenship (Westin, 1967). Weinstein (1971) defined general privacy as a state of "being apart from others" (p. 88). Some years later, Schoeman (1984) describes a definition of general privacy as "a state or condition of limited access to a person" (p. 3).

In addition to *privacy as a state*, the cognate-based definitional approach includes *privacy as control*. These definitions focus on the control of information that is to be disclosed (Belanger et al., 2002; Walsh et al., 2017). Altman (1975) defines general privacy as "the selective control of access to

the self" (p. 24). Altman's and Westin's perspectives were combined by Margulis (1977) who proposed a different definition centred on control: "Privacy, as a whole or in part, represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimise vulnerability" (p. 10). According to Johnson (1974), general privacy is "secondary control in the service of need-satisfying outcome effectance" (p. 91). Other works describe control as a key factor in shaping privacy, rather than general privacy being defined as control, e.g., Laufer & Wolfe (1977) argue that "a situation is not necessarily a [general] privacy situation simply because the individual perceives, experiences, or exercises control" (p. 26), they propose control being a mediating variable within general privacy.

Privacy is a challenging concept to grasp, with debates and discussions still ongoing. It is not the purpose of this thesis to define the greater privacy concepts, nor to take a hard stance on an existing interpretation—that discussion is far greater and beyond the scope of this work. This subsection merely provides some perspectives in order to create enough context to place the main topics of study in.

3.1.2 Pillars of Privacy framework

Privacy is a multidisciplinary field relevant to any discipline involved with processing information from people. Because of this nature, privacy is divided into many smaller communities that each focus on their own paradigms. Examples include data mining (Verykios et al., 2004), consumer privacy (Lanier & Saini, 2008), and health data (Lane & Schur, 2010). This fragmentation results in communities not considering their relationship to the overall privacy research community which makes it harder for researchers to identify the field's foundational theories (van Dijk et al., 2021).

The fragmented nature of the privacy research field motivated van Dijk et al. (2021) to quantitatively investigate the privacy research community by conducting a multi-stage bibliometric network analysis. They collected an initial set of 119,710 records and distilled them into 11 core theories. Van Dijk et al.'s network analysis found that a majority of privacy research is focused on the organisational level. Yet, it seems that it is barely represented in the widely used high-level frameworks for privacy research. Subsequent network analysis notably found that there is no influential central research community regarding organisational privacy knowledge, such as privacy management, despite numerous calls for more organisational research (van Dijk, Gadellaa, et al., 2023). One of the identified theories is the *Privacy-Friendly System Design* (PFSD) framework (Spiekermann & Cranor, 2009) which was the only theoretical contribution at the organisational level of analysis.

To bridge this gap, they propose the *Pillars of Privacy* (PoP) framework, a high-level, multilevel model for information privacy research (Figure 3). The framework consists of two axes. Horizontally, the columns distinguish the three theoretical efforts of privacy research: Privacy Concern, Privacy Calculus, and Behavioural Outcomes. Vertically, the framework identifies four levels of analysis: individual, group, organisational, and societal.

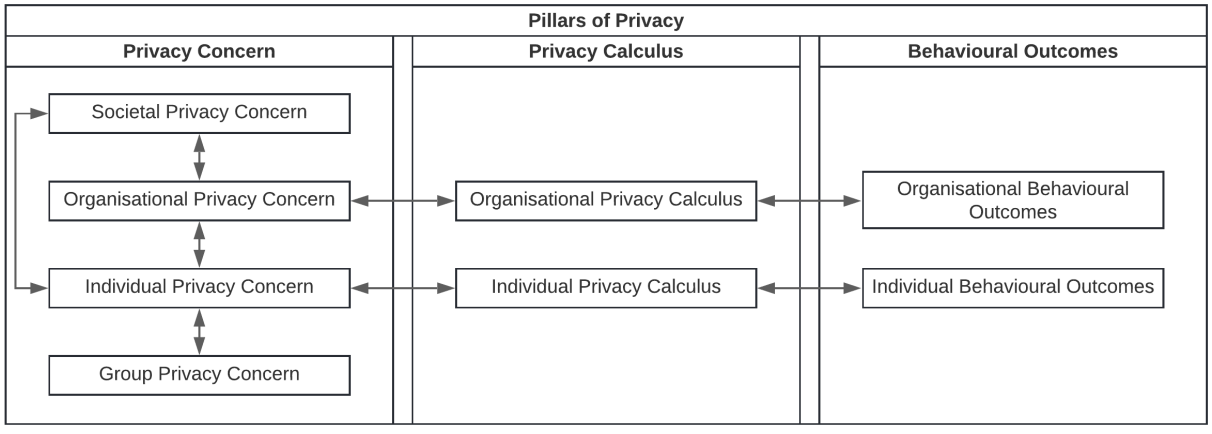

Figure 3: Pillars of Privacy framework (van Dijk et al., 2021).

The Privacy Concerns pillar forms the basis of the PoP framework and is the best-defined, with a theoretical foundation of 8 out of 11 core theories. This pillar represents the subjective fairness views

related to privacy, including beliefs, perceptions, and attitudes (Agarwal et al., 2004; Smith et al., 2011). The four levels of analysis and the relationships between them are derived from the Privacy Concern Multilevel Framework (IPCMF) as proposed by Belanger and Crossler (2011).

The Privacy Calculus pillar encompasses the complex decision-making processes and trade-offs that generate the intent to act. Individual Privacy Calculus is a concept that has been previously established, it is defined as an individual's behaviour and decision-making process regarding the intent to disclose personal information, where potentially competing factors are weighed (Li, 2012). The PoP adds the newly formulated organisational equivalent to this pillar, based on the observation that organisations in a similar fashion must make architectural trade-offs (van Dijk et al., 2021).

Lastly, the Behavioural Outcomes pillar embodies the actual behaviour, this has been identified as a key component in understanding privacy (Norberg et al., 2007). On the individual level of analysis, behavioural outcomes are defined as "the disclosure of personal information to a third party, primarily in the interaction with an organisation or information system" (van Dijk et al., 2021, p. 12). The PoP derives the organisational equivalent, which is incorporated as the Organisational Behavioural Outcomes and represents the privacy-oriented behaviour exhibited by an organisation. This includes built information systems, formulated policies, configurations, and processing activities.

3.1.3 Organisational privacy calculus

This thesis mainly focusses on the organisational level of analysis of the Privacy Calculus pillar of the PoP. Within the Organisational Privacy Calculus, organisations make architectural trade-offs and design decisions. Once options have been weighted and choices have been made, the organisation sets a course to address individual privacy risks, this display of intent is referred to as the *Privacy-oriented Behavioural Intent* (PoBI) which rests at the centre of the Organisational Privacy Calculus (Figure 4).

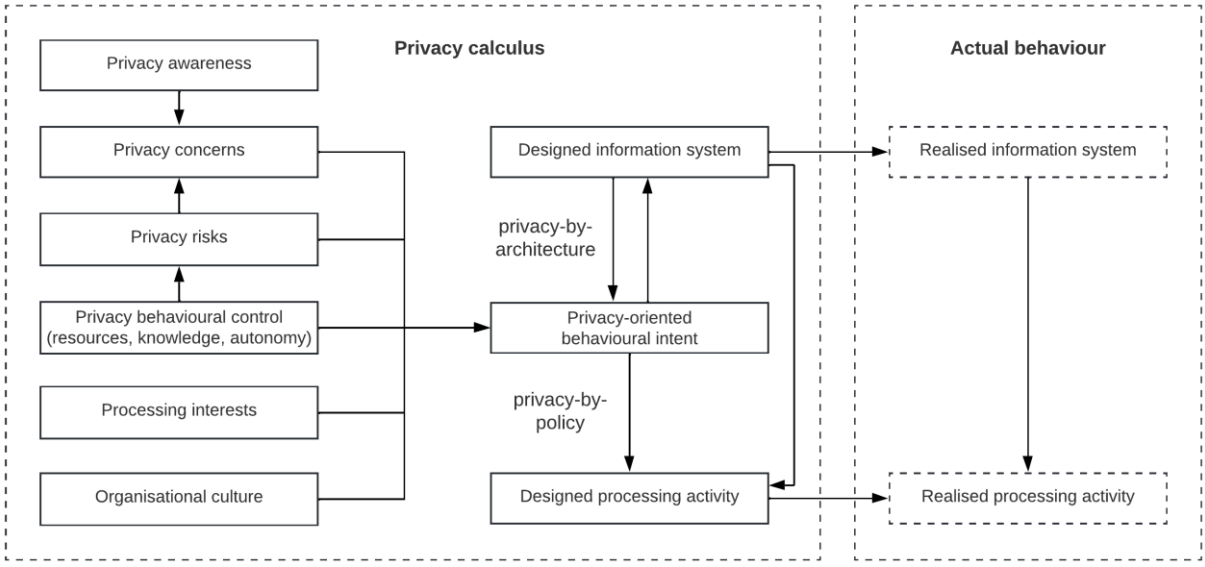

Figure 4: Organisational privacy calculus (van Dijk, van Toledo, et al., 2023).

Antecedents

Van Dijk (2022) identifies six antecedents which influence PoBI: privacy awareness, privacy concerns, privacy risks, privacy behavioural control, processing interests, and organisational culture.

Privacy awareness is defined as the extent to which a practitioner is informed about the designed processing activity, the supporting information system, and the organisational privacy practices (Smith et al., 2011; van Dijk, van Toledo, et al., 2023). It serves an intermediary role between these concepts and privacy concerns (Agarwal et al., 2004; Smith et al., 2011).

Privacy concerns can be both concerns within the organisation for individual privacy (Belanger & Crossler, 2011) and concerns raised by individuals (Spiekermann & Cranor, 2009). Privacy concerns affect the PoBI as they have been shown to influence organisational decision-making (Belanger & Crossler, 2011; Spiekermann & Cranor, 2009).

Privacy risks influence behavioural intent by incentivizing the application of risk mitigation or avoidance measures. In addition, they influence individual privacy concerns (Dinev & Hart, 2006). Privacy risks can be identified through various methods (e.g., Wuyts et al., 2020) during the risk modelling and analysis of the PIA process (Clarke, 2009; Deng et al., 2011).

Privacy behavioural control is the level of control that decision-makers are allowed to have in deciding to address privacy issues appropriately in processing activity design (van Dijk, van Toledo, et al., 2023). Perceived control is a direct influence on behavioural intent, according to the Theory of Planned Behaviour. Privacy behavioural control is influenced by multiple factors, including deadlines, privacy knowledge, autonomy, and budgets (Spiekermann et al., 2019). Van Puijenbroek and Hoepman (2017) found the available privacy expertise in an organisation to influence the quality of the privacy risk analysis and resulting measures, which is expressed as the PoBI in this model.

Processing interests are the intrinsic motivations for an organisation to use personal data in achieving its goal. They are the starting point of the Organisational Privacy Calculus as they determine the desired outcomes of the processing activities (van Dijk, van Toledo, et al., 2023).

Organisational culture refers to the cultural context in which privacy decisions are made. This privacy culture influences the outcome of privacy decisions (Belanger & Crossler, 2011; Culnan & Armstrong, 1999; Warkentin et al., 2011).

Privacy engineering

The PoBI is captured in document form in the PIA, it lists the identified privacy risks and how the organisation intends to address these with mitigating measures. The designed information system and designed processing activity are the actual design outcomes, realised by expressing the PoBI. In order to achieve privacy in systems design, Spiekermann and Cranor (2009) distinguish two privacy engineering approaches: privacy-by-architecture and privacy-by-policy.

Privacy-by-architecture aims through the architectural design of a system to keep the collection of identifiable personal data to a minimum. In the best case, personal data is not collected at all and individuals retain the highest level of anonymity. In practice, there are often (valid) reasons for the collection of personal information. The PoBI influences the designed system through architectural choices, however, this is a bidirectional relationship where the system design can influence the PoBI. In a situation where privacy measures must be implemented in an existing system, the behavioural options might be limited by past design decisions. Additionally, the designed information system can be subject to changes external to the privacy calculus (Bass et al., 2013), changes that do not concern themselves with privacy but can affect privacy as a quality attribute.

Privacy-by-policy uses a "notice and choice" approach to privacy—identifiable information is still collected but individuals are notified of the collection and processing, and can exert some level of control over how their personal information is used. In general, it refers to prescribed behaviours in information processing that are not enforced through system design. Organisations generally prefer the privacy-by-policy approach, even though privacy-by-architecture provides better protection by avoiding risks entirely (Spiekermann & Cranor, 2009; van Puijenbroek & Hoepman, 2017).

Privacy engineering overlaps with the notion of privacy as a quality attribute. In software architecture, quality attributes represent the properties of a system that indicate how well the system satisfies stakeholder needs (Bass et al., 2013). According to Bass et al., a good architecture alone is insufficient to ensure quality, hence the complementing approach of architecture and policy for privacy as a quality attribute. Quality attributes are often subject to trade-offs, e.g., modifiability comes at the expense of time-to-market and security typically comes at the expense of real-time performance. Inevitable trade-offs between privacy and other quality attributes can pose the risk of creating non-compliance in regard to restrictions or measures formulated in the PIA, which is essentially the documented PoBI. The discrepancies between the PIA and the designed system or processing activities are referred to as *privacy gaps* (van Dijk, van Toledo, et al., 2023). The PoBI, therefore, provides no guarantees, behavioural intent and actual behaviour can end up differing—discrepancies between the intent to address privacy risks and the designed systems and activities can occur.

3.1.4 Privacy-by-design

Privacy-by-architecture and privacy-by-policy are not mutually exclusive, organisations typically adopt a hybrid approach where a baseline of architectural enforcement is present, while the remainder of the

identified risks is addressed through policy measures, this decision-making process in the expression of the PoBI is what is captured by *privacy-by-design* (van Dijk, van Toledo, et al., 2023). It is an engineering and strategic management paradigm that commits to selectively and sustainably minimise information systems' privacy risks through proactive technical and governance controls (Spiekermann, 2012). An essential aspect of PbD is that it embeds privacy and data protection throughout the entire life cycle of technologies, systems, data, and activities starting with the early design stages to their deployment, utilisation, and eventual termination or disposal (European Commission, 2010). It is an example of an approach that employs the *by-design* thinking which refers to including certain characteristics, qualities, or features early in the design process and making them inherent within the design, rather than treating them as an afterthought (C. Forsberg et al., 2022), other examples include security-by-design (Cavoukian & Dixon, 2013) or economics-by-design (Abou Jaoude et al., 2021).

Privacy engineering and privacy-by-design are often used interchangeably, yet some authors (e.g., Stallings, 2019; Alshammari and Simpson, 2017) make a distinction where privacy-by-design only refers to the planning and actual design activities while privacy engineering encompasses the development, implementation, and monitoring activities of a system design project. This thesis views privacy engineering as a somewhat deprecated term and uses privacy-by-design to refer to the entire lifecycle of systems, data, and processing activities—employing both privacy-by-architecture and privacy-by-policy where appropriate.

Privacy-by-design was coined by Ann Cavoukian during their tenure as Information and Privacy Commissioner of Ontario. According to Cavoukian (2009), information privacy is being challenged by global competition, increasing system complexity, and rapid innovation. In order to address these challenges, a holistic, integrative design-thinking perspective must be adopted where privacy is an integral organisational priority and is incorporated by default. To this end, Cavoukian (2009) introduces The 7 Foundational Principles of Privacy-by-Design:

1. *Proactive not Reactive; Preventative not Remedial*
   PbD does not wait for privacy risks to materialise, it anticipates and prevents invasive events before they happen. It also does not offer remedies for resolving infractions that have already happened—PbD comes before the fact, not after.

2. *Privacy as the Default*
   No action from an individual must be required to protect their privacy. PbD seeks the automatic protection of personal data, built into the system and active by default.

3. *Privacy Embedded into Design*
   Privacy must not be an afterthought that is bolted on after the fact, it must be embedded into the design and architecture of information systems as well as business practices. Privacy is integral to the system, becoming an essential component of the core functionality.

4. *Full Functionality—Positive-Sum, not Zero-Sum*
   PbD aims to accommodate all legitimate needs and objectives in a positive-sum approach, avoiding unnecessary trade-offs and false dichotomies.

5. *End-to-End Security—Lifecycle Protection*
   PbD seeks an end-to-end, “cradle to grave”, secure lifecycle management of information approach. This entails that PbD is embedded into the system before any data collection takes place and that it extends securely throughout the entire data lifecycle, ensuring strong measures from start to finish, from collection to destruction.

6. *Visibility and Transparency*
   Stakeholders must be assured that business practices and technologies are operating according to specifications and objectives. Operations must be visible and transparent, to both users and providers and are subject to independent verification, adopting a *trust but verify* mindset.

7. *Respect for User Privacy*
   PbD requires all involved parties, be it architects or operators, to keep the best interests of the individual in mind. A user-centric view must be adopted by empowering user-friendly options, using strong privacy defaults, and giving appropriate notices.

Cavoukian (2010) views PbD as an evolution from Privacy Enhancing Technologies (PETs), creating a broader scope that allows the consideration of technology, management functions, business processes, and other organisational activities, embedding privacy at each layer. According to van Lieshout et al. (2011), a holistic approach to PbD is indeed valuable but the actual implementation suffers from difficulties such as legacy systems, lack of economic incentives (London Economics, 2010), and lack of adoption of trust of end-users in PbD. More works identify issues with applying PbD: Gurses et al. (2011) call PbD vague, according to van Rest et al. (2014) PbD is shrouded in opaqueness and distrust, and Ayalon and Toch (2021) question the focus of PbD on compliance with regulation and the lack of attention to the needs and attitudes of users.

Cavoukian (2010) states that PbD does not exist in a vacuum and that the privacy protection toolbox must bring together accountability and transparency, consumer awareness and education, market forces, and regulatory instruments. Van Rest (2014) warns that the lack of regulation pushes PbD towards an individualistic nature where everyone is free to assert their design (process) as "privacy-by-design". Allowing each party to decide for itself what PbD means in their domain puts a heavy burden on society in understanding the differences and therefore inhibits the transparency regarding human rights and the market. The GDPR (European Commission, 2016) prescribes the application of the principles of privacy-by-design and privacy-by-default[1], however, the legislation does not specify what the principles entail, how the principles must be applied, or how risks should be mitigated, this has to be addressed by making PbD more concrete (van Rest et al., 2014).

On the implementation spectrum, PbD could imply the deployment of relatively straightforward technologies like encryption, on the other end, it could imply hard-coding data protection rules in machine code. Koops and Leenes (2014) prefer the former and are critical of the latter. They identify multiple pragmatic problems with hard-coding under, what they call, strong forms of techno-regulation: there is a lack of guidance on what provisions from what legal system need to be taken into account, determining where in the system a legal requirement should be encoded is difficult, determining whether a data processing purpose is explicit and legitimate is difficult, embedding compliance with data protection requirements may require more (meta)data, and many legal requirements are formulated for flexible application making them challenging to implement. They conclude that there are too many complications to be able to implement "hard privacy-by-design" as this will frustrate developers who must translate rules that cannot be simply translated to system design requirements. Instead, they point to privacy design strategies as a promising approach that can support developers.

Hoepman (2014) takes a software architecture approach and defines eight privacy design strategies: minimise, hide, separate, aggregate, inform, control, enforce, and demonstrate. The need for privacy strategies rests on the observation that developers stand empty-handed in the early concept and analysis phases of system development—later phases use design patterns (Al-Slais, 2020) and during implementation privacy enhancing technologies are used. These strategies aim to bridge the gap between the project start and architecture phase. The goal is to support privacy-by-design throughout the full development lifecycle, including the early phases. Hoepman (2022) expands his privacy design strategies in The Little Blue Book, adding tactics for each strategy to make them more concrete.

Several studies have taken a developer-centric view and have investigated how developers handle privacy requirements in their software development activities. Hadar et al. (2018) performed interviews with 27 developers and revealed that organisational culture and policies can play a significant role both positively and negatively in encouraging developers to consider privacy in their work. Overall, the results indicate that software developers are actively discouraged from prioritizing privacy by being expected to adhere to practices and norms set by a negative organisational privacy climate. The importance of a suitable organisational privacy climate is also mentioned by Ayalon et al. (2017).

[1] Strictly speaking the GDPR speaks of data protection by design and data protection by default. Some works describe this distinction (e.g., van Puijenbroek & Hoepman, 2017) though in this thesis they can be treated as synonymous.

Sheth et al. (2014) emphasise the need for organisational guidelines to guide software developers in embedding privacy into software system designs. Ayalon et al. (2017) additionally found that developers tend to reject privacy guidelines that do not follow existing software frameworks. Senarath and Arachchilage (2018) investigated 36 software developers in a software design task related to embedding privacy with the goal of identifying the problems they face. Their results present five main challenges: privacy requirements contradict system requirements, privacy requirements are difficult to relate to privacy techniques, lack of verification criteria and assurance, influence of personal opinion, and a lack of knowledge of privacy practices. Their recommendations reinforce the call for comprehensive guidance.

3.1.5 Privacy impact assessment

The PIA has been mentioned a number of times in this thesis and is described as an instrument in service of the privacy-by-design paradigm, yet it knows a longer history. Clarke (2009) identifies two precursors to the PIA. First, is the *technology assessment*, practised by the Office of Technology Assessment of the US Congress starting in the 1970s. The second is the *impact statement*, one of its earliest applications was in the 1960s by the green movements in the form of an Environmental Impact Statement. Clarke (2009) managed to find a reference to *privacy impact statement* as early as 1984, the more comprehensive *privacy impact assessment* term was formulated mid-1990s.

Nowadays, the PIA is mainly associated with inventorying privacy risks and formulating mitigation measures. Legislators have incorporated the practice in their regulatory efforts and it has been postulated as a way of substantiating the principles of PbD. Under certain circumstances, the GDPR (European Parliament and Council of the European Union, 2016) requires data controllers to perform a PIA[2], it is seen as a key means to integrate privacy measures into the foundations of a system (Oetzel & Spiekermann, 2014) and is seen as a practical method to establish PbD (Ahmadian et al., 2018).

Article 35(1) of the GDPR describes the PIA as "an assessment of the impact of the envisaged processing operations on the protection of personal data". Article 35(7) mentions several mandatory components a PIA must contain:

- A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph one;
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

The legislation does not specify any specific assessment methods. Bisztray and Gruschka (2019) compared three widespread impact assessment methods: LINDDUN (Wuyts & Joosen, 2015), CNIL (Commission Nationale de l'Informatique et des Libertés, 2019), and ISO/IEC 29134 (ISO/IEC, 2017). Their results indicate that CNIL has a good selection of support material and is the best in GDPR compliance, however, it underperforms as a process. LINDDUN misses risk assessment despite its good start, furthermore, it has unintuitive aspects to it. The ISO standard proved to be the best both process-wise and content-wise, but it still has shortcomings. Others have proposed their own PIA methods or processes (Ahmadian et al., 2018; Bieker et al., 2016; Oetzel & Spiekermann, 2014).

Vemou and Karyda (2019) reviewed 9 PIA methods, using 17 criteria. They found that most methods include a threshold analysis, use a report template, require a periodical review, and provision publication to stakeholders. Four out of nine methods do not reference any legal framework, six methods do not incorporate the PIA within information technology/information system development, and only

[2] Strictly speaking the GDPR speaks of data protection impact assessment though in this thesis they can be treated as synonymous.

three methods provide guidance on required skills and PIA team setup. Furthermore, three methods do not require an evaluation or audit and only one method is supported by a (BETA) tool.

Sion et al. (2020) observe that the current state-of-the-art in privacy impact and risk assessment works fairly well for static, design-level assessments, yet it insufficiently captures dynamic risk elements originating from an operational system. They propose the PIA to be applied in a continuous, reactive manner, allowing for steering in a run-time context.

3.2 Maturity models

In order to get a proper understanding of what maturity models are and what they are used for, the concept of *maturity* and *maturity model* must be defined. Wendler (2012) noticed that clear definitions are often avoided in publications of maturity models in favour of descriptions of functioning and purpose. Yet multiple works attempt to define these concepts, hence an appropriate start on this topic is to examine some of their definitions and determine what they entail. In addition, this section will explore the different purposes, types, and criticisms of maturity models.

3.2.1 Definition

There are several definitions for maturity models given in academic publications. Becker et al. (2009) state "A maturity model consists of a sequence of maturity levels for a class of objects. It represents an anticipated, desired, or typical evolution path of these objects shaped as discrete stages. Typically, these objects are organisations or processes" (p. 213). Klimko (2001) puts a similar emphasis on the evolutionary aspect of maturity models, stating that "Maturity modelling is a generic approach which describes the development of an entity over time progressing through levels towards a usually idealistic ultimate state" (p. 269). Pullen (2007) defines a maturity model as "a structured collection of elements that describe the characteristics of effective processes at different stages of development. It also suggests points of demarcation between stages and methods of transitioning from one stage to another" (p. 9). This definition, similar to Becker et al.'s, mentions different stages of development, typically referred to as *maturity levels*, which are a core concept of maturity models.

In regards to maturity, the Merriam-Webster English online dictionary defines *maturity* as "the quality or state of being mature" (Merriam-Webster, 2022d) and defines *mature* as "having completed natural growth and development", "having attained a final or desired state", and "of or relating to a condition of full development" (Merriam-Webster, 2022c). Maturity thus implies an evolutionary progression path from an initial state, to a desired end state, experiencing development and growth in the transition.

In the context of maturity models, Rosemann and de Bruin (2005) see maturity as a measure to evaluate an organisation's capabilities in a certain field. The Merriam-Webster English online dictionary defines *capability* as "the quality or state of being capable" (Merriam-Webster, 2022a) and defines *capable* as "having attributes (such as physical or mental power) required for performance or accomplishment", "having traits conducive to or features permitting something", and "having or showing general efficiency and ability" (Merriam-Webster, 2022b). According to Bharadwaj's (2000) academic definition, a capability is the ability to make use of the available resources in order to achieve certain goals. In the context of maturity models specifically, Wendler (2012) describes capability as "the power or ability in general, whether physical or mental to fulfil specified tasks and goals" (p. 1318). De Bruin et al. (2005) equate capability to competency or level of sophistication of a selected domain.

Aggregating the various definitions and descriptions leads to the understanding that maturity models demarcate several sequential discrete stages, representing an evolutionary development path from an initial state, to a desired end state of accomplishment, with each stage describing an ability to achieve a specifically defined goal. Since the objective of this research is to develop a focus area maturity model, the definitions adopted by this work will be the ones provided by van Steenbergen et al. (2013). They provide a meta-model for focus area maturity models in their work, of which Table 6 provides a partial overview with definitions.

Table 6: Partial overview of meta-model definitions (van Steenbergen et al., 2013).

Concept	Definition
Maturity model	A Maturity Model is an instrument to assess and develop the ability of an organisation to perform within a Functional Domain.
Maturity	Maturity indicates the degree of development.
Maturity Level	A Maturity Level is a well-defined evolutionary plateau within a Functional Domain.
Capability	A Capability is the ability to achieve a predefined goal.
Functional Domain	A Functional Domain is the whole of activities, means, responsibilities and actors involved in the fulfilment of a well-defined function within an organisation.

3.2.2 Purpose

Maturity models can be used in varying ways depending on the purpose, de Bruin et al. (2005) identify three main purposes for maturity models: descriptive, comparative, and prescriptive. Descriptive usage entails assessing the as-is situation within an organisation, it merely provides a snapshot of the current performance without looking at potential improvements that can increase the maturity. Once an as-is maturity assessment has been made within an organisation, it can be compared to as-is assessments of other organisations. This comparative usage allows organisations to benchmark themselves against best-in-class organisations that employ the best-known practices and have reached the highest maturity level. A more mature organisation will typically be on a higher maturity level within the same model. This enables a maturity model's prescriptive use; it shows a progression path of certain levels or stages from an as-is situation towards a potential to-be situation, detailing which capabilities need to be developed to improve the maturity within a specific field or organisational component.

While these purposes can be examined as distinct items, they are together part of an evolutionary maturity model lifecycle (de Bruin et al., 2005). In order to prescribe improvements, descriptive assessments must be made first, and to make valid comparisons, descriptions and prescriptions must be performed on a wider scale. By gaining an extensive understanding of the as-is situation in a domain, a descriptive model can evolve into a prescriptive model. Applying this model to a wider range of organisations allows for the collection of sufficient data to facilitate valid comparisons and make it a comparative model.

3.2.3 Model versus method

March and Smith (1995) differentiate four different design science products, with Hevner and Chatterjee (2010) adding a fifth:

- Constructs (vocabulary and symbols)
- Models (abstractions and representations)
- Methods (algorithms and practices)
- Instantiations (implemented and prototype systems)
- Better design theories

A descriptive artifact portrays a description of a current situation. This aligns best with the definition of a model. March & Smith (1995) state that "A model can be viewed simply as a description, that is, as a representation of how things are" (p. 256). According to Mylopoulos (1992), models represent a description of "some aspects of the physical or social world around us for the purpose of understanding and communication" (p. 51).

A prescriptive artifact, on the other hand, tells you what to do. It provides guidance in a procedure or steps and hence fits the definition of a method. March and Smith (1995) state that "A method is a set of steps (an algorithm or guideline) used to perform a task" (p. 257). According to Brinkkemper (1996), methods are used "to perform a systems development project, based on a specific way of thinking, consisting of directions and rules, structured in a systematic way in development activities with corresponding development products" (p. 275).

Mettler (2011) observes that maturity models exhibit characteristics from both models and methods. The descriptive purpose allows for state descriptions in a model fashion (what), while the prescriptive purpose outlines improvement steps in a method fashion (how). The designation maturity *model* might therefore not be completely accurate, insofar that Mettler positions maturity models, as an artifact, somewhere in between models and methods.

3.2.4 Type

The foundations of maturity models were built in the 1930s when Shewart (1931) started working on process improvement through quality control. While his work is incomparable to maturity models as they are known today, his principles of statistical quality control provided a base for extension and adaptation by numerous researchers in the years after. Yet it was not until 1979 that Crosby introduced his so-called *quality management maturity grid* (QMMG) which was the first model to introduce consecutive stages that build on each other, similar to many of today's maturity models. Fraser et al. (2002) propose a typology which divides maturity models into three basic types: maturity grids, CMM-like models, and Likert-like questionnaires. Since 2002 research in maturity models has continued and has provided new insights, therefore this list is supplemented with situational maturity models and focus area maturity models.

Maturity grids: The aforementioned QMMG (Figure 5) is an example of a maturity grid. It consists of a matrix structure outlining the maturity levels as columns, versus the measurement categories as rows. The cells contain textual descriptions for each category-level pair detailing the characteristics of performance. The number of levels is equal for all categories, although the number can be fairly arbitrary (Fraser et al., 2002). The QMMG consists of a 6 × 5 matrix, describing 5 maturity levels for all 6 categories. Other examples of maturity grids include a technical innovation audit tool (Chiesa et al., 1996), an assessment tool for environmentally conscious design (Moultrie et al., 2016), and a maturity grid for sustainability reporting (Isaksson & Cöster, 2018).

CMM-like models: The Capability Maturity Model was first introduced in 1993 by Paulk et al., it describes itself as a software process maturity framework that provides an evolutionary path from ad hoc, chaotic processes to mature, disciplined software processes. CMM differs from maturity grids in that it uses a cumulative set of key process areas (KPAs) in a staged representation (Fraser et al., 2002). CMM is a fixed-level model typically consisting of five levels denoting maturity from an initial level, to an optimised level. As the level of maturity increases, all KPAs respective to a level must be performed, leading to one maturity level in the range of 1–5. Figure 6 contains a data science assessment model and is an example of a CMM-based maturity model. In this example, the creators chose to add a level 0 as a base starting stage. In 2006 a successor model was released named the Capability Maturity Model Integration (CMMI). CMM(I) models are widely used nowadays and provide the base for many maturity models (Hansen et al., 2004; Wendler, 2012), in a variety of domains. Examples include e-learning (Marshall & Mitchell, 2002), educational project management (Demir & Kocabaş, 2010), blockchain adoption (H. Wang et al., 2016), and artificial intelligence (Alsheiabni et al., 2019).

Likert-like questionnaires: A questionnaire using Likert scales to measure the level of performance can be used as a rudimentary maturity model (Fraser et al., 2002). The "questions" in these questionnaires are statements of (best) practice. The respondent, who is performing the assessment, is tasked with rating the relative performance of the organisation for each of the practices on a scale from 1 to n. Likert-like questionnaires are similar to maturity grid approaches where only the top-level categories are rated. In the case where the rating scale is binary (i.e., $n = 2$), the questionnaire functions like an ordinary checklist where each performance assessment per practice can be interpreted as "not adhering" or "fully adhering". Mettler (2010) positions Likert-like questionnaires as hybrids between CMM-like models and maturity grids. Examples of a Likert-like questionnaire approach include knowledge sharing and firm capability (Lin, 2007), organisational self-assessment of knowledge management (Kulkarni & St. Louis, 2003), and the *open source usability maturity model* (OS-UMM) (Raza et al., 2012). The OS-UMM contains 11 practices related to usability in open-source projects, which must be rated on a 5-point scale ranging from "1. not-fulfilled" to "4. fulfilled", with 0 being a "not-applicable" score.

QUALITY MANAGEMENT MATURITY GRID					
Measurement Categories	*Stage I: Uncertainty*	*Stage II: Awakening*	*Stage III: Enlightenment*	*Stage IV: Wisdom*	*Stage V: Certainty*
Management understanding and attitude	No comprehension of quality as a management tool. Tend to blame quality department for "quality problems."	Recognising that quality management may be of value but not willing to provide money or time to make it all happen.	While going through quality improvement programme learn more about quality management; becoming supportive and helpful.	Participating. Understand absolutes of quality management. Recognise their personal role in continuing emphasis.	Consider quality management as an essential part of company system.
Quality organisation status	Quality is hidden in manufacturing or engineering departments. Inspection probably not part of organisation. Emphasis on appraisal and sorting.	A stronger quality leader is appointed but main emphasis is still on appraisal and moving the product. Still part of manufacturing or other.	Quality department reports to top management, all appraisal is incorporated and manager has role in management of company.	Quality manager is an officer of company; effective status reporting and preventive action. Involved with customer affairs and special assignments.	Quality manager on board of directors. Prevention is main concern. Quality is a thought leader.
Problem handling	Problems are fought as they occur; no resolution; inadequate definition; lots of yelling and accusations.	Teams are set up to attack major problems. Long-range solutions are not solicited.	Corrective action communication established. Problems are faced openly and resolved in an orderly way.	Problems are identified early in their development. All functions are open to suggestion and improvement.	Except in the most unusual cases, problems are prevented.
Cost of quality as % of sales	Reported: Unknown Actual: 20%	Reported: 3% Actual: 18%	Reported: 8% Actual: 12%	Reported: 6.5% Actual: 8%	Reported: 2.5% Actual: 2.5%
Quality improvement actions	No organised activities. No understanding of such activities.	Trying obvious "motivational" short-range efforts.	Implementation of a multi-step programme (e.g., Crosby's 14-step) with thorough understanding and establishment of each step.	Continuing the multi-step programme and starting other pro-active / preventive product quality initiatives.	Quality improvement is a normal and continued activity.
Summary of company quality posture	"We don't know why we have problems with quality".	"Is it absolutely necessary to always have problems with quality?"	"Through management commitment and quality improvement we are identifying and resolving our problems."	"Defect prevention is a routine part of our operation."	"We know why we do not have problems with quality."

Figure 5: Quality management maturity grid (Crosby, 1979).

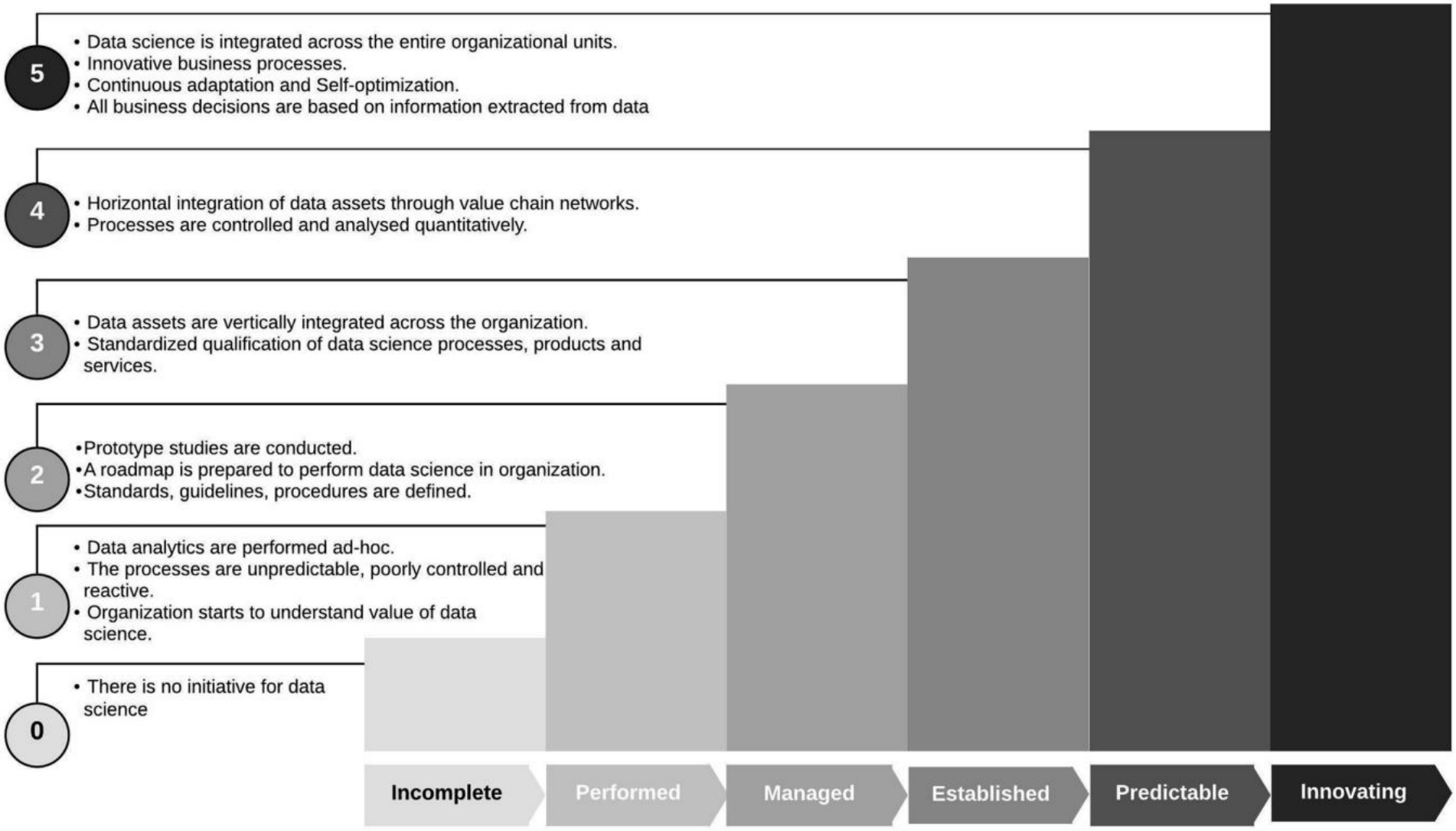

Figure 6: Data science capability maturity model (Gökalp et al., 2021).

Focus area models: Focus area maturity models consist of a number of focus areas; these are coherently defined subsets of the respective functional domain (van Steenbergen et al., 2013). For each focus area, a number of capabilities are defined and the dependencies between the capabilities are determined. In contrast to CMM-like models, focus area models are non-fixed-level models. The number of levels is not set a-priori and depends on the number of focus areas, capabilities, and the dependencies between the capabilities. Additionally, focus areas are not restricted to the same number of capabilities. Figure 7 shows an example of the enterprise architecture management (EAM) domain, it shows the focus areas as rows with several capabilities ranging from two to four, each represented by a letter. The columns portray the maturity levels which are derived from the dependency relationships between the capabilities. Capabilities in each level are dependent on the capabilities of the previous levels. The idea is to develop all the capabilities associated with a level before moving to the capabilities of the next level. Each focus area has its own maturity level denoted by the shaded cells, allowing for better identification of areas that need improvement. Examples of this model type include the software ecosystem governance maturity model (SEG-*M²*) (S. Jansen, 2020), ISFAM: The Information Security Focus Area Maturity Model (Spruit & Röling, 2014), and a focus area maturity model for IT Carve-out projects (Pflügler et al., 2015).

Maturity Level **Focus Area**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
Development of architecture		A			B			C						
Use of architecture			A			B				C				
Alignment with business		A				B				C				
Alignment with the development process			A				B		C					
Alignment with operations					A			B			C			
Relationship to the as-is state					A				B					
Roles and responsibilities				A		B					C			
Coordination of developments							A			B				
Monitoring				A		B		C		D				
Quality management								A		B			C	
Maintenance of the architectural process							A		B		C			
Maintenance of the architectural deliverables					A			B					C	
Commitment and motivation		A					B		C					
Architectural roles and training				A		B			C			D		
Use of an architectural method				A						B				C
Consultation			A		B				C					
Architectural tools							A				B			C
Budgeting and planning				A							B		C	

Figure 7: EAM focus area maturity model (van Steenbergen et al., 2010).

Situational models: The effectiveness of a maturity model application can be influenced by the compatibility between the model and the organisation. The maturity model could be too restrictive, as was the case in a study done by Hayes and Zubrow (1995) who found that 73% of assessed organisations were stuck in CMM-level 1 because they could not meet the prescribed requirements. Another example of an incompatibility is a demographic mismatch. CMM was designed for larger companies which might make the prescribed improvement activities too costly or bring along too much bureaucratic overhead for smaller organisations. Similar to the field of method engineering, where situational methods are common and play a vital role in the artifact development process (Brinkkemper, 1996; Karlsson & Ågerfalk, 2004), situational maturity models allow organisations to add situativity parameters to a maturity model in order to tailor the assessment to best fit their organisation (Mettler & Rohner, 2009). An example of a situational maturity model can be found in the IT governance (ITG) domain. Smits and Van Hillegersberg (2015) observed that ITG is situational which implies a one-size-fits-all approach may not be suitable, hence they opted to create a situational maturity model for ITG.

For additional examples of maturity models, a number of works provide aggregated overviews. Pöppelbuß et al. (2011) conducted an extensive literature review and analysis, taking a look at maturity model research from both an academic perspective as well as a practitioner's perspective. Wendler conducted a systematic mapping study in 2012, detailing different aspects of maturity model research and providing numerous examples. Proença and Borbinha (2016) analysed 22 maturity models in terms of structure, assessment, and support. Lastly, Sanchez-Puchol and Pastor-Collado (2017) present a comparative review of 16 focus area maturity models.

3.2.5 Criticism

While maturity models enjoy widespread usage in the information systems field, they are not without criticism. Becker et al. (2009) critique the similarity of many maturity model applications, suggesting a certain arbitrariness exists. Röglinger et al. (2012) question whether the large amount of maturity model work also translates into high quality. They conducted a review of business process management maturity models and found that prescriptive design principles were hardly met. This aligns with Pfeffer and Sutton (1999) who argue the existence of a knowledge-doing gap. The purpose of these models is to identify gaps which can be addressed with improvement actions, yet often there is no guidance on how to do this.

Many maturity models focus on a limited amount of specific dimensions, e.g., CMM looks mainly at processes and has therefore been critiqued for overemphasizing this one dimension and disregarding people's capabilities (Bach, 1994). Multiple works point out that in general, more dimensions are relevant when performing a specific function, e.g., people and objects, (Mettler & Rohner, 2009; Niazi et al., 2005). Hammer (2007) even argues that for sustained business performance, enterprise-wide capabilities such as leadership, expertise, and culture are needed. Thus, these models oversimplify reality and do not provide a complete assessment (de Bruin et al., 2005; King & Kraemer, 1984). Additionally, Mettler (2011) states that maturity models frequently are based on practices and factors of projects that resulted in favourable results in specific organisations or sectors. Taking these observations into account, there is no guarantee that complying with a maturity model will lead to success, and can potentially lead to a false sense of certainty among decision-makers (Mettler, 2011). Normann Andersen et al. (2020) counter this sentiment by arguing that maturity models should not be treated as providers of a single absolute truth, instead, they should be seen as useful instruments, aiding practitioners in comprehending and dealing with complex tasks, subject to iterative incremental development and improvement.

Maturity models have been described as step-by-step recipes (McCormack et al., 2009) that oversimplify the real domain and are insufficiently empirically validated (de Bruin et al., 2005; McCormack et al., 2009). Some of the critiques, regarding the lack of theoretical foundation and the lack of scientific rigour in the design process, have already been described in chapter 2. The lack of general scientific rigour in maturity models, including their foundation, design, and validation, is one of the key points of criticism and has been pointed out by a myriad of other works (Becker et al., 2009; Biberoglu & Haddad, 2002; Kohlegger et al., 2009; Mettler & Rohner, 2009; Pöppelbuß et al., 2011; Rosemann & de Bruin, 2005; Solli-Sæther & Gottschalk, 2010).

Other criticism points out that the increased focus on improvement activity formalisation and the inevitable accompanying bureaucracy can inhibit innovation in people as they do not consider other options (Herbsleb & Goldenson, 1996). In a similar fashion, Teo and King (1997) state that maturity models do not take alternative options into account and tend to ignore potential paths that are equally viable or advantageous.

4 Domain investigation

The domain investigation consists of two multivocal literature reviews. The first literature review identifies existing maturity models in the privacy domain and relevant adjacent domains. These models are compared and analysed in order to get an understanding of what solutions already exist and to provide a base of operation for the maturity model that is to be designed. The second literature review investigates the influential factors in the privacy-by-design domain. These factors are analysed and aggregated into a set of candidate capabilities and/or focus areas which will be the starting point for populating the maturity matrix. Both reviews are conducted in accordance with a literature review protocol following the steps, principles, and guidelines (see section 2.5) of Kitchenham and Charters (2007) and Garousi et al. (2019).

4.1 Multivocal literature review 1: Existing maturity models

The first multivocal literature review (MLR 1) aims to inventory existing maturity models. The found models are analysed and compared in order to gain an understanding of existing solutions and to form a basis for the new model that is to be created. This is a multivocal literature review meaning that both academic and grey works are considered. While the review of academic works is straightforward, using well-established methods, finding and reviewing works from grey literature sources comes with certain difficulties. The review is performed according to the method described in chapter 2, this includes adherence to a review protocol which describes the entire process and ensures replicability. The review protocol for this review can be found in Appendix B.

4.1.1 Source selection and quality assessment

The search, screening, and assessment steps of this review are summarised in an adapted PRISMA flow diagram (Page et al., 2021) which is shown in Figure 8. Following the search process described in the review protocol, the search returned 300 records in total. The SCOPUS database is the big hitter with a contribution of 124 records, the other databases returned a number of records in the range of 10–20. The Google search, as expected, returned many millions of hits and thus only the first 100 results were considered. Duplication removal resulted in 71 records being excluded, most of these duplicate records originated from the databases.

During the first screening stage, a total of 165 records were excluded. Not introducing a new artifact was the reason which led to the exclusion of the majority of the records in this stage, for both the database results (29 records) as well as the Google search results (46 records). Examples of these works include: descriptions of models introduced in other works, commercial offers for maturity assessments, and works merely describing or presenting opinions regarding maturity. Other major reasons for exclusion were: introducing a new artifact that is not intended for maturity or capability assessment (18 records) and maturity models addressing an irrelevant domain (70 records). Examples of these irrelevant domains include green IT maturity, digital asset management maturity, global business service organisation maturity, tax management maturity, digital marketing maturity, and virtual team performance maturity.

Seven works were unavailable for retrieval to be used in the full-text screening. From the 57 retrieved works, 28 were excluded in the second stage with most works originating from a database (24 works). Similar to the first screening stage, from the total of 28 exclusions, the major reasons for exclusion were: addressing an irrelevant domain (13 works) and not introducing a new artifact (9 works).

Apart from the works found as a result of searching databases and Google search with a search string, works obtained through other means were added. These other means include snowballing, adding previously identified works, and adding works pointed out by other researchers. A total of 21 additional works were obtained through other means, 4 were unavailable for retrieval, and 9 works were excluded during full-text screening.

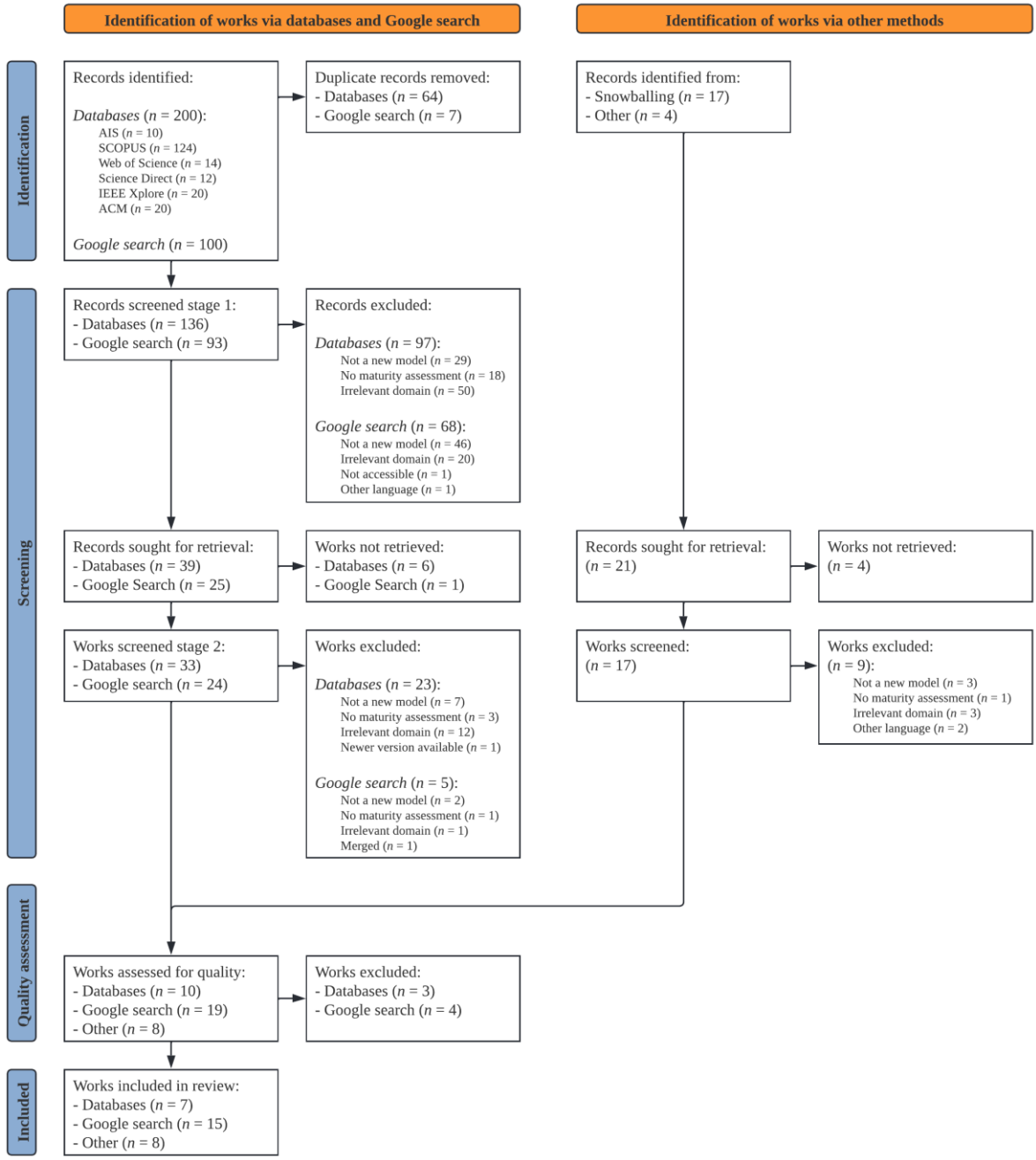

Figure 8: Flow diagram for MLR 1.

Seven works were excluded for quality reasons during the quality assessment phase, four of these were works originating from the Google search. These works were excluded mainly for only presenting a table or figure, lacking description or elaboration, and for unclarity or vagueness. This resulted in a total of 30 works which were included in the review, 7 from databases, 15 from Google search, and 8 obtained through other means, all the works included are listed in Appendix F.

4.1.2 Descriptive statistics

The 30 included works are plotted in a bar diagram (Figure 9) denoting the year of their publication, making a distinction between academic works and grey works. What is notable is that academic interest seems to be non-existent before 2016, while some grey works were getting published in the years before. The start of academic publishing in 2016 and the following peak in 2017 can be explained by the fact that the GDPR was introduced in 2016, which sparked interest as well as the necessity to investigate

these domains. Remarkably, academic publishing decreased after 2017 almost as fast as it initially increased.

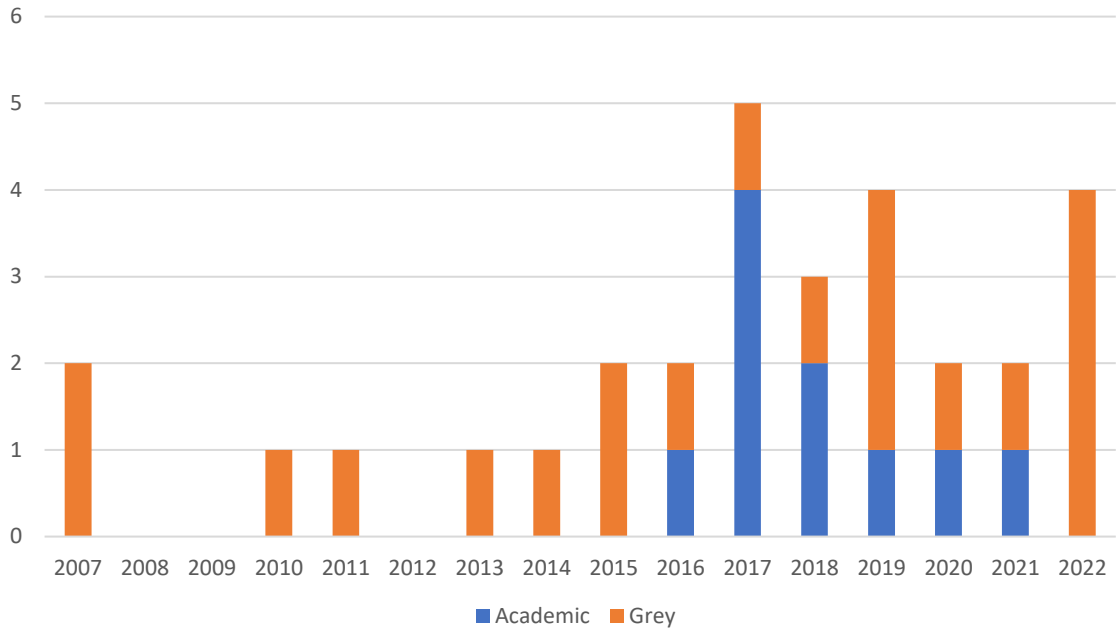

Figure 9: MLR 1 distribution of works between academic and grey literature per year.

The search string for this review featured the privacy, data protection, and data governance domains. Privacy and data protection are the main domains this thesis is interested in, with data governance being an adjacent domain that still might provide some useful insight. Figure 10 shows the distribution of works that address the privacy/data protection (main) domain and works that address other (adjacent) domains, with the distinction between academic works and grey works.

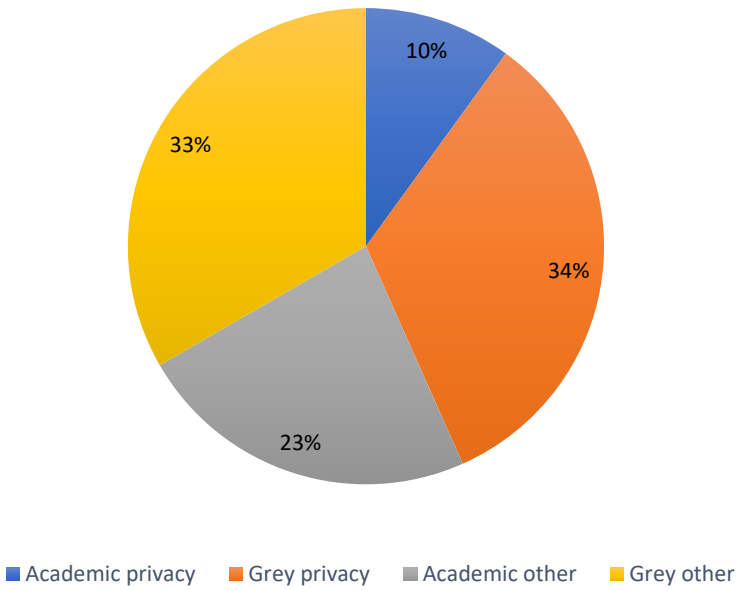

Figure 10: Privacy and other domains distribution between academic and grey literature.

The academic works represent 33% of all included works with the remaining 67% being grey works. Looking at the domains, privacy/data protection is addressed by 44% of the works, meaning a majority of the included works do not address the main domain of interest. The grey literature outnumbers the academic literature in the privacy/data protection domain as well as the collection of other domains. The academic works that address the main domain form the smallest group with only 10% (3 works). This result indicates that academically there does not seem to be much interest in maturity research for the privacy/data protection domain, additionally, it could be an indicator of low maturity of the privacy/data protection domain as a whole, further enforcing the relevance and need for research in the development of not only a privacy-by-design maturity model, but also a general privacy management, organisation, programme, or governance maturity model.

4.1.3 Data synthesis: maturity models

The purpose of the data synthesis is to analyse the contents of the works included in the review. For this review, the review protocol contains a data extraction form (Table B6) for the extraction of certain general maturity model components and properties, a number of these properties are presented in a comparative overview in Table 7. Data governance is by far the most addressed domain within this set of maturity models, other domains include data management, information management, privacy, and legal compliance for both EU and US. Most models contain five maturity levels, which is not surprising since the CMM(I) is also the most used reference model. Additionally, while some models do not explicitly state that they are based on a particular reference model, it is not far-fetched to hypothesise that they were in fact inspired by one. The privacy maturity framework from the New Zealand government (2014), for example, does not mention CMM at all, yet they both have five levels and share multiple level labels.

There are notable exceptions though. Labadie and Legner (2019) present a capability model for data management in EU-GDPR, this model consists of an overview of six main capabilities with between two and four subcapabilities per main capability. Strictly speaking, it is not a maturity model as it does not equate the capabilities to any development plateau. The model contains capabilities but has no levels and it does not guide users in maturity development or measurement. Merkus et al. (2021) worked on a data governance maturity model but they stopped after formulating dimensions and capabilities, essentially only presenting a list of capabilities. Their work did not include any maturity levels, a matrix, or an assessment instrument, only mentioning it as potential future work. Lastly, van Lieshout & Hoepman (2015) present in their book, what they call, a privacy road web (Figure 11). This model consists of a radar chart portrayed as a layered circle, with seven dimensions pointing outwards. The centre of the circle represents the current situation with maturity increasing the further an organisation expands to the outer layers. The dimensions each include steps that an organisation must go through in order to be privacy-respecting. While the book states that the level of maturity increases, the greater the distance from the centre, it is not explicit about what constitutes a level in this model. An obvious interpretation is having each graphical layer be a maturity level, although this would mean that some dimensions have multiple steps in the same level and no steps in other levels. A different option would be to see each step as a level within its dimension, leading to dimension-specific levels rather than one overall maturity level. This interpretation would somewhat resemble the way focus area maturity models are structured. For lack of elaboration, the best guess this thesis makes is that the model employs two to four maturity levels.

The attributes vary wildly in number, name, and structure. Some of the names used include categories, criteria, activities, elements, principles, dimensions, and capabilities. Having high-level attributes that contain multiple subattributes is observed to be a common practice. Table 7 only shows the number of attributes on the highest level, yet there are significant discrepancies in the number of attributes and the used abstraction levels. Looking at some examples, the information management maturity model by Proenca et al. (2016) contains only three dimensions: management, processes, and infrastructure. Combined with 5 maturity levels, this model consists of 15 dimension-level combinations with each a set of capabilities. The Intel Privacy Office (2013) privacy maturity model also uses a structure of 5 levels but has 12 categories, leading to 60 category-level combinations with each a set of capabilities. The Data Management Capability Assessment Model (DCAM) by the EDM Council (2021) seems to be the most extensive model in this review, containing 38 capabilities and 136 subcapabilities. This work includes a scoring guideline that prescribes assessors to score the capabilities (and/or

Table 7: Data extraction comparison for MLR 1.

Source	Origin	Scope	# of levels	# of attributes	Definition of maturity	Assessment instrument	Validation/ evaluation	Reference model	Tool support
Garcia et al. (2018)	Academia	Personal data protection	5	22	Yes	Self-assessment questionnaire	Multiple case study	CMM	Evaluation tool
Carretero et al. (2017)	Academia	Data management	6	21	Yes	Third-party interview questionnaire	Case study	ISO/IEC 33000	-
Rivera et al. (2017)	Academia	Data governance	5	25	No	Assessment matrix	Multiple case study	CMMI	-
Cheng et al. (2017)	Academia	Cloud data governance	5	23	No	Self-assessment & third-party assessment	-	CMMI	-
Al-Ruithe & Benkhelifa (2017)	Academia	Cloud data governance	5	10	Yes	Maturity matrix	-	-	-
Yaqiong et al. (2020)	Academia	Data privacy	5	12	No	Maturity matrix	Interviews, survey, Delphi study	Intel & CMM	-
Labadie & Legner (2019)	Academia	GDPR Compliance	-	6	No	-	Focus groups	-	-
Proenca et al. (2016)	Academia	Information governance	5	3	No	Self-assessment questionnaire	Pilots	CMMI	-
Merkus et al. (2021)	Academia	Data governance	-	11	No	-	-	-	-
Marchildon et al. (2019)	Academia	Data governance	5	11	Yes	Self-assessment questionnaire	Multiple case study	CMMI	-
Office of management & enterprise services (2020)	Industry	Data governance	5	6	No	Score card, Questionnaire	-	Stanford & IBM	-
AICPA/CICA (2011)	Industry	Privacy	5	10	No	Self-assessment	-	CMM	-
Merkus (2015)	Academia	Data governance	5	8	Yes	Assessment matrix scoring	Interviews	-	-
Boswell & Courtright (2022)	Industry	Data governance	4	4	No	-	-	-	-

New Zealand Government (2014)	Government	Privacy	5	9	No	Excel calculator	-	-	Excel sheet
Compliance, Governance and Oversight Council (CGOC) (2019)	Industry	Information governance	4	6	No	Score card	-	-	-
The MITRE Corporation (2019)	Industry	Privacy programme	5	7	Yes	Self-assessment questionnaire	-	CMMI	-
State of Oregon (2022)	Government	Data governance	5	6	No	Gap analysis	-	-	Excel sheet
Fort Privacy (2022)	Industry	GDPR Compliance	5	10	No	-	Case study	AICPA/ CICA	-
Qi (2016)	Academia	Privacy maturity	3	7	No	Self-assessment questionnaire	Multiple case study	-	-
Association of Corporate Counsel (2019)	Industry	U.S. Privacy laws	5	10	No	-	-	-	-
Secure Controls Framework (2022)	Industry	Security & Privacy	6	11	No	-	-	SSE-CMM	-
DataFlux Corporation (2007)	Industry	Data governance	4	4	No	-	-	-	-
Centrum informatie-beveiliging en privacybescherming (2017)	Industry/ government	Privacy	5	13	Yes	Self-assessment Excel questionnaire	-	CMMI & ISOMM	Excel sheet
IBM (2007)	Industry/ academia	Data governance	5	11	No	Self-assessment questionnaire	-	CMM	-
CMMI Institute (2019)	Industry	Data management	5	6	No	Third-party assessment	-	CMM	-
EDM Council (2021)	Industry	Data management	6	38	No	Self-assessment questionnaire	-	-	-
Chen (2010)	Industry	Data governance	4	38	No	Self-assessment	Market research	-	-
van Lieshout & Hoepman (2015)	Industry	Privacy	2–4	7	No	-	-	-	-

Intel Privacy Office (2013)	Industry	Privacy	5	12	No	Assessment process	-	AICPA/ CICA	-

subcapabilities) in the range 1–6, each number corresponding to a defining description. While these scores can be interpreted as maturity levels, the structure of this model is somewhat different in that each capability must be assessed separately and gets its own score. The model describes itself as a capability assessment model and is strictly speaking not a conventional maturity model.

Looking at the abstraction level of the models, some provide more concrete guidance than others. The thesis by Qi (2016) provides low-level concrete activities such as: "Notify personal identifiable information principals about mandatory collection of personal identifiable information" and "Specify the tracking technologies that have been used for personal identifiable information collection" (p. 35). On the other side of the spectrum, the data governance maturity model by Rivera et al. (2017) consists of domains which are split into criteria that must be assessed against five maturity levels. These criteria include: "Organisational culture", "Data planning", "Scope of metadata", and "Data analysis" (p. 211). These examples illustrate the differences in abstraction levels between maturity models. The usefulness of some of the models is questionable as they seem to operate on a subdomain level rather than specifying concrete capabilities per (sub)domain.

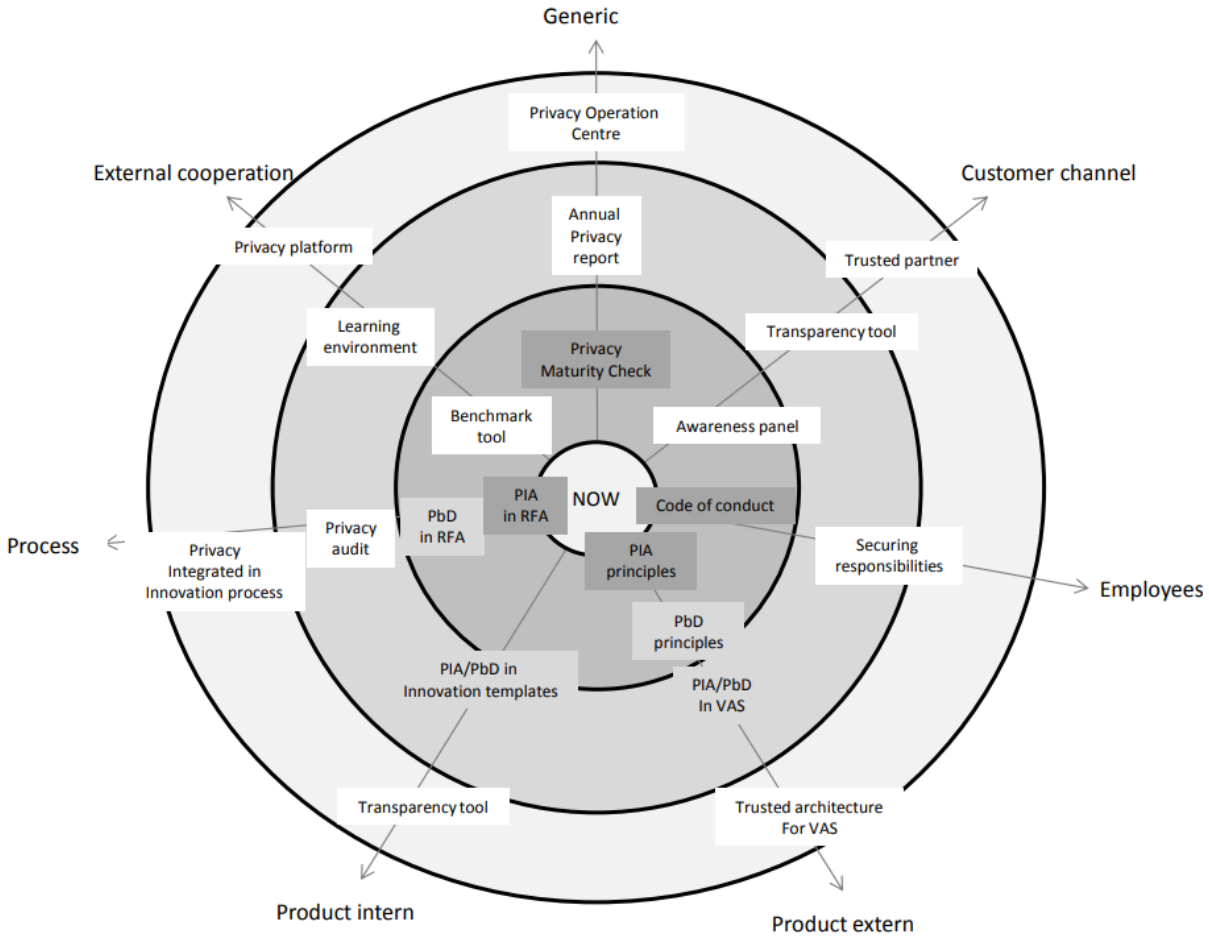

Figure 11: The privacy road web (van Lieshout & Hoepman, 2015).

Out of the 30 works, only 7 contained an explicit definition of *maturity*. Unsurprisingly, most of the works with a definition come from academic origins. However, when looking at all academic works, fewer than half (5 out of 13) contain a definition for maturity. This can be an indicator of a lack of scientific rigour which is a common criticism of maturity models, as mentioned in chapter 3. There is some nuance in the matter since some works do define *maturity model* or describe its function and/or purpose which allows the reader to deduce what maturity is, yet often a clear explicit definition of *maturity* is not included.

Another factor that is related to scientific rigour is the validation/evaluation. Once again, academic works provide most of the found validation/evaluation efforts. Case studies were found to be the most

used method, other methods include interviews, focus groups, pilots, and a Delphi study. Works originating from industry rarely mention any validation/evaluation efforts. In regards to tool support, the works included in the review barely mention any. Only Garcia et al. (2018) describe the development of an evaluation tool, their tool contains questions per domain and topic that allow an assessor to assign a value between one and five. The tool was sent to contacts at organisations included in a case study for self-assessment. Additionally, the State of Oregon (2022), the New Zealand Government (2014), and the Centrum Informatiebeveiliging en Privacybescherming (CIP) (2017) provide an Excel spreadsheet for partial automation. The first allows an assessor to identify gaps and provides suggested actions. The second allows an assessor to calculate the maturity using a score-based approach. The last provides a questionnaire that calculates the maturity level and provides improvement suggestions.

It must be noted that the data extraction is based solely on the contents of the works included in the review. It is possible that evaluations took place at a later point in time, similarly, tools may have been developed since the original release of the models.

4.1.4 Data synthesis: privacy-by-design factors

It has been mentioned already that the literature search for this review includes data governance as an adjacent domain, since it is not a main domain there is a risk that works that address this adjacent domain, while formally adhering to inclusion criteria, are not relevant for the concept under investigation. In this case, privacy-by-design is the main concept under investigation thus the following paragraphs in this subsection will mainly discuss works that contained relevant and useful factors. For this data extraction, relevant domain factors can be capabilities, recommendations, guidelines, principles, or any other type of construct that indicates practices related to PbD. A total of 620 factors have been found and extracted. Of the 30 included works, 16 provided relevant PbD factors. The works with at least one relevant factor are shown in the overview of Figure 12. Eight works mention privacy or data protection by design, these works shall be described in more detail in the following paragraphs.

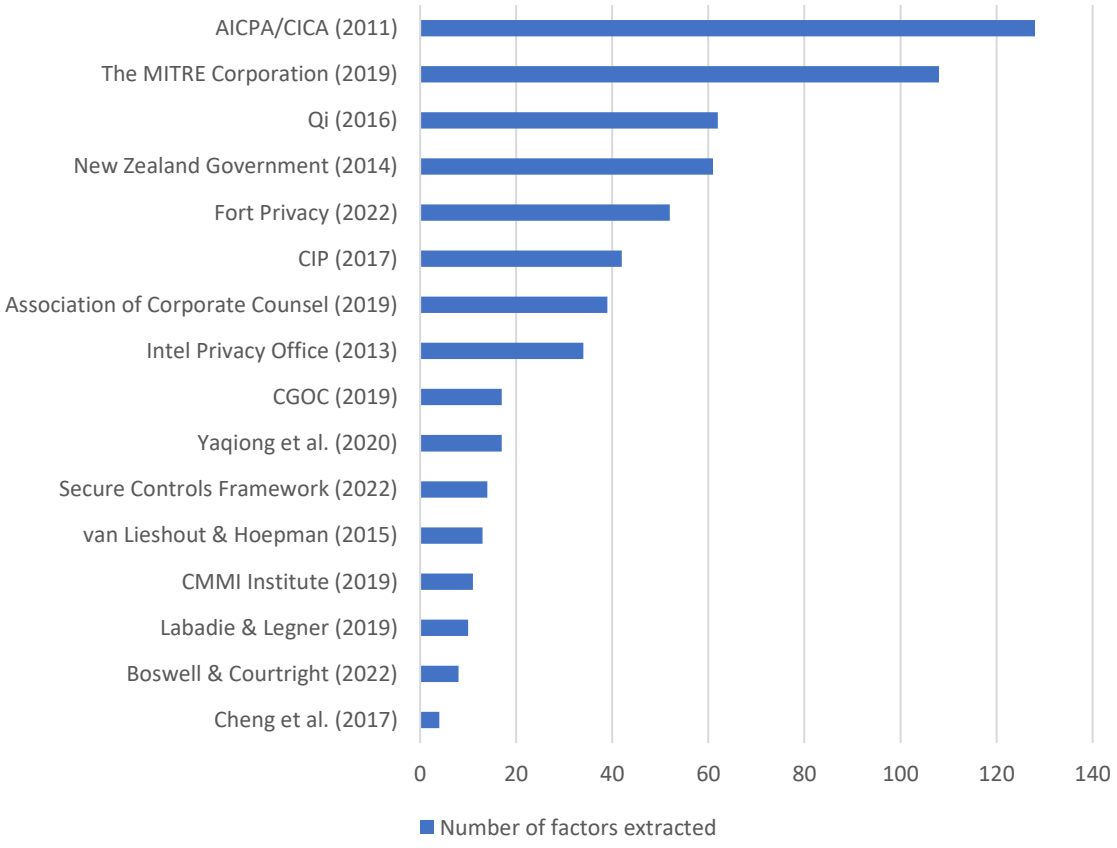

Figure 12: MLR 1 number of factors extracted per work, works with zero factors are excluded.

Labadie and Legner (2019) investigated data protection regulations from a data management perspective. They formulated a capability model with capabilities split into two groups: system capabilities and organisational capabilities. Even though this work only mentions PbD in passing, the system capabilities group is interesting for PbD since it is aimed at information systems development. These capabilities include *identify data objects*, *pseudonymise data*, and *enforce consent-based processing*. All 10 system capabilities are extracted.

Yaqiong et al. (2020) present a data privacy maturity model which they developed by investigating a digital transformation enterprise during COVID-19. Their five-level maturity model explicitly mentions PbD in the *information protection behavior* dimension. This dimension includes the privacy risk assessment, identification and classification of personal data, residual risk management, and documenting and sharing PbD best practices. Eight capabilities are extracted from this dimension. Additionally, the dimension *data privacy awareness* discusses awareness and training capabilities. The lack of privacy knowledge among developers and the lack of awareness among executives have been mentioned as challenges in chapter 3, thus an additional four capabilities are extracted from this dimension. Lastly, the dimension *privacy protection technology generation difference* prescribes the use of security technology, setting up a technical team, implementing comprehensive data privacy technical governance, and continuous monitoring, optimizing, and upgrading. An additional five capabilities are extracted from this dimension.

The information governance process maturity model by the Compliance, Governance and Oversight Council (CGOC) (2019) is an extensive maturity model that encompasses legal, records information management, IT, privacy and security, and business. The *privacy and data protection obligation* dimension is the only dimension that mentions PbD, capabilities include tracking privacy requirements, keeping a catalogue of privacy laws and policies, including privacy controls on any system, and continuous monitoring and updating of privacy obligations. A total of six capabilities are extracted from this dimension. The *data quality & data lineage* dimension addresses data accuracy which is relevant to PbD as this is seen as a key aspect (Stallings, 2019), four capabilities are extracted: fully automated data quality management processes with complete audit trails, master data map is fully integrated and ubiquitous, data management processes can collect and move data to a repository for cleansing, and advanced analytics used to predict the use and misuse of data. A different dimension which is of interest in this model is the *disposal & decommissioning* dimension. This dimension is relevant since PbD addresses the entire lifecycle of a system, including data disposal and application decommissioning at end-of-life. Four capabilities are extracted from this dimension: IT responding to decommission requests, automatic data deletion, proactive identification of low-value systems, and routine disposal. Lastly, the *audit* dimension provides general capabilities related to verification, testing, and auditing of all other dimensions. Three capabilities are extracted from this dimension.

The next relevant model is The Fort Privacy GDPR Compliance Framework by Fort Privacy (2022). This is another 5-level maturity model consisting of 10 GDPR compliance dimensions. From the *governance* dimension, two capabilities related to roles and responsibilities that demonstrate data protection compliance commitment are extracted. The next dimension that provides relevant capabilities is the *accountability* dimension. Accountability is an integral part of PbD as part of the *visibility and transparency* principle of Cavoukian's (2009) foundational PbD principles. Seven capabilities are extracted related to data protection policy and procedure implementation, keeping an inventory of all data processing activities, keeping a risk register as part of risk management, and auditing data processing activities. Staying with the *visibility and transparency* principle, the *transparency* dimension concerns itself with user notices. Four capabilities are extracted, these address data processing notices, notice updates as part of change management, and website compliance including cookies. The legal basis management dimension provides capabilities related to the legal basis for processing personal data. This is highly relevant for PbD since the GDPR (article 35(7)) prescribes that a PIA must describe the processing operations with the underlying purposes, legitimate interests, necessity, and proportionality. The four extracted capabilities from this dimension address: legal basis for processing, consent management, and contract management. The next dimension of interest is the *data subjects rights (DSR) management* dimension. Cavoukian's (2009) last principle, *respect for user privacy*, entails key aspects such as: consent, accuracy, and access (Stallings, 2019). These aspects are codified in the GDPR (European Commission, 2016) as rights, examples include right of access (article 15), right to rectification (article 16), and right to erasure (article 17). Eight capabilities that enable data subject rights

have been extracted from this dimension. The sixth dimension of this model is the *data transfer management* dimension. Three capabilities regarding documenting processing agreements are extracted from this dimension. The *data management* dimension focusses on enabling the principles of purpose limitation, data minimalization, accuracy, and storage limitation. These principles are associated with privacy-by-default which is a foundational principle of privacy-by-design (Cavoukian, 2009). Eight capabilities are extracted from this dimension. While security is a separate domain from privacy, their tight coupling is evident. End-to-end security is a foundational principle of PbD (Cavoukian, 2009), thus four capabilities are extracted from the *security* dimension, related to system security procedures and network security processes. The last dimension under investigation in this model is perhaps the most insightful, being the only one that includes capabilities that explicitly mention data protection by design. The *change management* dimension contains capabilities related to change management policies and procedures, data protection impact assessments, and data protection by design and by default. Eight capabilities are extracted from this dimension.

The Centrum informatiebeveiliging and privacybescherming (CIP) [Centre for information security and privacy protection] is a Dutch semi-public organisation that provides several privacy and data protection knowledge-sharing products like documents, podcasts, and workshops. One of these products is a privacy maturity model (2017), consisting of 5 levels and 13 dimensions. The *privacy governance* dimension provides two capabilities for extraction related to formalizing and documenting privacy policies. The *risk management, privacy by design and the PIA* dimension prescribes the application of PbD, the execution of PIAs, and the use of risk management. Six capabilities are extracted from this dimension. The *data processing purpose limitation* dimension addresses the purpose and lawfulness of processing activities, three capabilities are extracted. Purpose limitation (article 5(1)(b)) and lawfulness of processing (article 6) are key principles outlined in the GDPR (European Commission, 2016). The *processing activities register* dimension provides capabilities for the setup and operation of a register detailing all personal data processing activities, four capabilities are extracted. The *quality management* dimension concerns itself with guarding the accuracy of personal data and enabling rights including rectification and erasure, four capabilities are extracted from this dimension. These rights, among others, are described in Chapter 3 of the GDPR (European Commission, 2016). The *personal data processing security* dimension provides capabilities regarding information security, five capabilities are extracted. The *data subject notice for personal data collection* dimension focusses on formalizing the decision-making and processes surrounding providing notice to data subjects in regard to data processing activities. Four capabilities are extracted from this dimension. Article 5(1)(e) of the GDPR (European Commission, 2016) outlines the principle of *storage limitation* which restricts the storage of personal data beyond the duration required for the defined purpose. The *personal data storage* dimension of the maturity model prescribes capabilities that ensure the formulation and enforcement of data storage limits, six capabilities are extracted. The *audit* dimension provides capabilities related to integrating audits into existing processes in order to perform a check on the lawfulness processing activities, five capabilities are extracted. The last dimension of interest from this model is the *data access* dimension which focusses on formalizing the facilitation of data subject rights, specifically the right of access as described in article 15 of the GDPR (European Commission, 2016). Three capabilities are extracted from this dimension. All extracted factors from this model have been translated from Dutch to English by a Dutch native speaker.

The earlier mentioned privacy road web (Figure 11) from van Lieshout and Hoepman (2015) is another maturity model that explicitly mentions PbD. The first dimension of interest is the *customer channel* dimension. This dimension examines the role of the customer, two capabilities are extracted: organizing customer panels to obtain customer feedback on privacy policies and introducing transparency tools like privacy dashboards which allow customers to control their data. The next dimension that provides relevant factors is the *employees* dimension, describing capabilities related to promoting privacy awareness. The three extracted capabilities are: formulating data processing responsibilities, developing awareness tools, and using privacy champions for awareness. The *product extern* dimension is the main dimension concerned with PbD. Five capabilities are extracted related to PbD strategy, PIA, and architectural embedding which is a promising development in the PbD domain, as described in chapter 3. The *product intern* dimension is straightforward in that it prescribes that the PbD principles and processes that are used in external products, should also be applied to internal products, this is the only capability that is extracted. The last dimension of this model that provides

factors is the *process* dimension. This dimension aims to promote privacy-aware processes by embedding privacy in initial system requests and organizing privacy audits for all activities that handle privacy requirements. Two capabilities are extracted.

The privacy office of the American semiconductor chip manufacturer Intel has developed a privacy maturity model (2013) to assess, measure, and improve the privacy profile of a standalone subsidiary after acquisition. The model features 12 dimensions that provide capabilities over 5 levels. While the model is created in the context of an organisational acquisition, the capabilities can be adapted to any organisation, the wording of some extracted capabilities is changed to reflect this. The first dimension is the *privacy policies* dimension which provides four capabilities related to formalizing privacy policies. From the *accountability* dimension, two capabilities are extracted: assigning roles and responsibilities and addressing local data protection requirements. The *identification and classification* dimension describes how personal data should be inventoried and categorised, three capabilities are extracted. Four capabilities are extracted from the *notice and use* dimension. This dimension focusses on the provision of notices, consent, data use reviews, and monitoring. The *training* dimension provides three relevant capabilities: employees who process personal information receive privacy training, the organisation has a comprehensive privacy training programme and monitors employee participation, and the organisation updates the training programme when regulatory changes happen. The next dimension is the only dimension that discusses PbD explicitly. The *privacy by design (PbD)* dimension provides capabilities related to documenting risk assessment processes, documenting a PbD process including training and controls, and cooperating with industry peers to document PbD methods and best practices. Three capabilities are extracted from this dimension. The *third-party transfer* dimension looks at managing consent and implementing procedures for sharing personal data with third parties, two capabilities are extracted. The *access and accuracy* dimension revolves around data subjects exercising their rights related to access and rectification, five capabilities are extracted. Four capabilities are extracted from the *retention and disposal* dimension which prescribes capabilities for the retention and disposal of personal data including management, monitoring, and enforcement of retention periods and disposal methods as well as updating policies reflecting regulatory change. The last relevant dimension of this model is the *security* dimension which provides three capabilities for extraction related to referencing related security policies in privacy policies, employee awareness of security policies, and improving and monitoring violations of security policies.

The last of the eight models that mention PbD is a privacy maturity model introduced in the Master thesis by Qi (2016). The unique aspect of this maturity model is that it aims to be applicable to assess privacy-by-design best practices, thus it is the closest to a true privacy-by-design maturity model out of all the models included in this review. The model consists of seven privacy principles with accompanying activities. The first principle *lawfulness & consent* contains activities regarding data processing notifications, consent obtainment and withdrawal, and defining lawful purposes for data processing, 13 factors are extracted from this dimension. Four factors from the *data minimization* dimension are extracted, revolving around minimising data collection activities in accordance with their purpose. The next dimension is *individual rights & data quality*, this dimension includes activities like: collect personal data directly from data subjects whenever possible, allow data subjects to amend, correct, and remove their personal data, and check regularly the accuracy, completeness, up-to-date, adequacy and relevance of personal data. Ten factors are extracted from this dimension. The *purpose binding & limitation* dimension focusses on defining, documenting, and evaluating the purpose of data processing activities. Eight factors are extracted, including identify and document the purposes for conducting activities involving personal data, periodically evaluate the alignment between personal data and its purpose, and retain personal data for a limited time span only as needed or as required by law. Nine factors are extracted from the *transparency & openness* dimension. This dimension describes activities that enhance transparent and accessible communication with data subjects regarding their rights and choices. The next dimension is the *information security* dimension which provides six factors for extraction. The main focus of this dimension is handling threats, privacy requirements, and security risks, examples of activities include: conduct attack surface analysis and privacy threat modelling, validate and verify the system's alignment with the privacy requirements, and design and implement adequate privacy-enhancing technologies (PETs). The last relevant dimension is the *accountability & compliance* dimension which contains activities for dealing with breaches, sharing personal data, auditing, and privacy responsibilities. This dimension provides 12 factors for extraction.

Factor aggregation

A coding approach is used for the initial analysis of the factors, this is a qualitative technique commonly used in grounded theory (Corbin & Strauss, 2015). The usage of this technique here is merely for the data analysis, there is no further intent to apply the grounded theory method or adhere to its principles. This type of application of grounded theory techniques for data analysis is described by Matavire and Brown (2013). The coding technique entails scanning the qualitative data and keeping track of recurring terms or concepts to create a first grouping of similar data items in order to identify themes or categories. It gives insight into what concepts privacy-by-design consists of and allows for the identification of categories of factors and even greater themes which can be used as a precursor for the focus areas of the maturity model. Because the reviewed artifacts are of a similar type and address similar domains, there exists quite some overlap and duplication within the initial set of extracted factors. Therefore, similar factors have been consolidated during the coding process, resulting in a slimmed-down collection of 401 factors from the initial collection of 620 factors. The full collection of the consolidated privacy-by-design factors resulting from this review can be found in Appendix C.

Figure 13 shows the high-level abstract themes resulting from the factor coding, the themes are accompanied by a number in brackets which denotes the underlying number of factors that the theme encompasses. The theme with the most encompassing factors is *data processing*, it contains many factors related to data subject rights and GDPR processing principles which indicates that there is an emphasis on the legal side of privacy. Nonetheless, *privacy-by-design* is the second largest theme with 54 underlying factors.

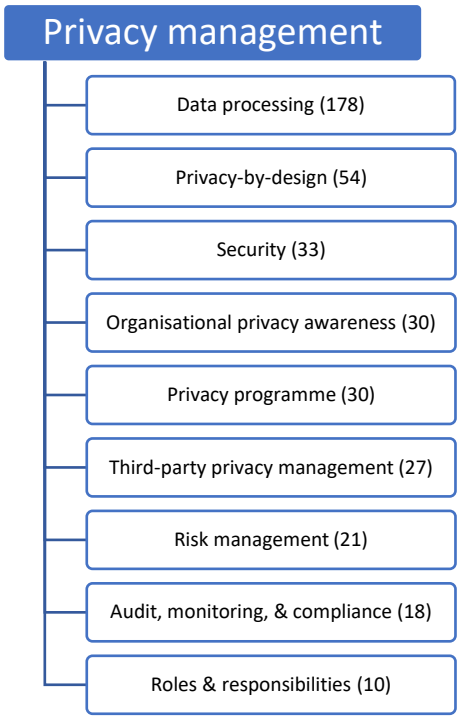

Figure 13: MLR 1 abstract factor themes with factor quantity.

Figure 14 shows the full results of the factor coding. The diagram shows the factor categories and encompassing themes, elements that are accompanied by a number in brackets are low-level categories that encompass factors with the number indicating the number of factors. The outer elements are more concrete with elements closer to the centre being more abstract—right in the centre, *privacy management* is the most abstract overarching theme that encompasses all other categories and thus all factors. As stated before, the MLR that generated the factors for this diagram has a broader scope of comparing maturity models in the privacy/data protection domain, instead of just focussing on privacy-by-design. Because of this, privacy-by-design is not the all-encompassing theme.

The first notable observation is that multiple categories are formed that naturally align with the principles relating to the processing of personal data (e.g., data minimisation, accuracy, or purpose limitation) and the rights of the data subject (e.g., data access, data rectification, or data erasure) as described in the GDPR (European Commission, 2016). This is not unexpected since multiple of the analysed works come from European origins and specifically target the GDPR or are placed in its context. *Data subject rights* and *data processing principles* seem to be addressed elaborately, containing respectively 76 factors and 64 factors. Their overarching *data processing* grouping encompasses a total of 178 factors which makes this theme by far the biggest underneath the all-encompassing *privacy management* (Figure 13).

The *privacy-by-design* theme encompasses categories including DPIA, technology, requirements, controls, PbD activities, and system design & development. Most of the 54 PbD factors are capabilities that do not mention PbD explicitly. Nonetheless, these factors are grouped under PbD based on the PbD foundational principles by Cavoukian (2009), the information privacy lifecycle by Stallings (2019) and the GDPR (European Commission, 2016). The factors that do mention PbD are mostly high-level capabilities that state that a PbD strategy must be formulated and that PbD principles must be applied and documented.

The *third-party privacy management* category consists of 27 factors related to sharing personal data with third parties. This includes obtaining additional consent, disclosure of policies, providing notices, PIA execution, and auditing. Additionally, there are factors related to (processing) agreements, more specifically, there is a subgrouping of factors related to *service-level agreements.*

The inclusion of a *security* category can potentially raise some eyebrows since privacy and security are described as different fields of expertise (Belanger et al., 2002). Nonetheless, their intertwined relationship is hard to deny, after all the fifth foundational principle of PbD calls for end-to-end security and full lifecycle protection (Cavoukian, 2009). The *incident & breach response* subcategory is just as relevant to privacy as it is to security. Personal data breaches that result in risks for natural persons must be reported to the supervisory authority (article 33) and the data subject in question must be informed (article 34) according to the GDPR (European Commission, 2016).

The *organisational privacy awareness*, *privacy programme*, and *audit, monitoring, & compliance* categories encompass factors that are not directly associated with PbD but can still have an influence in the greater context. Factors in these categories include having clear roles & responsibilities through ownership and a clear privacy programme, increasing privacy-related knowledge and awareness of the employees by providing (training) materials, formulating competency requirements, and employing awareness tools. Additionally, there are factors related to fostering a privacy culture and a privacy mindset through open discussions, employee accountability, and rules of behaviour. Some of these factors are in line with the already mentioned influential factors in section 3.1 related to the implementation difficulties of PbD principles, including the lack of knowledge and an unsuitable organisational privacy climate. On top of that, the earlier introduced organisational privacy calculus (Figure 4) by van Dijk (2022) identifies privacy awareness, privacy behavioural control, and organisational culture as influential antecedents of privacy behaviour.

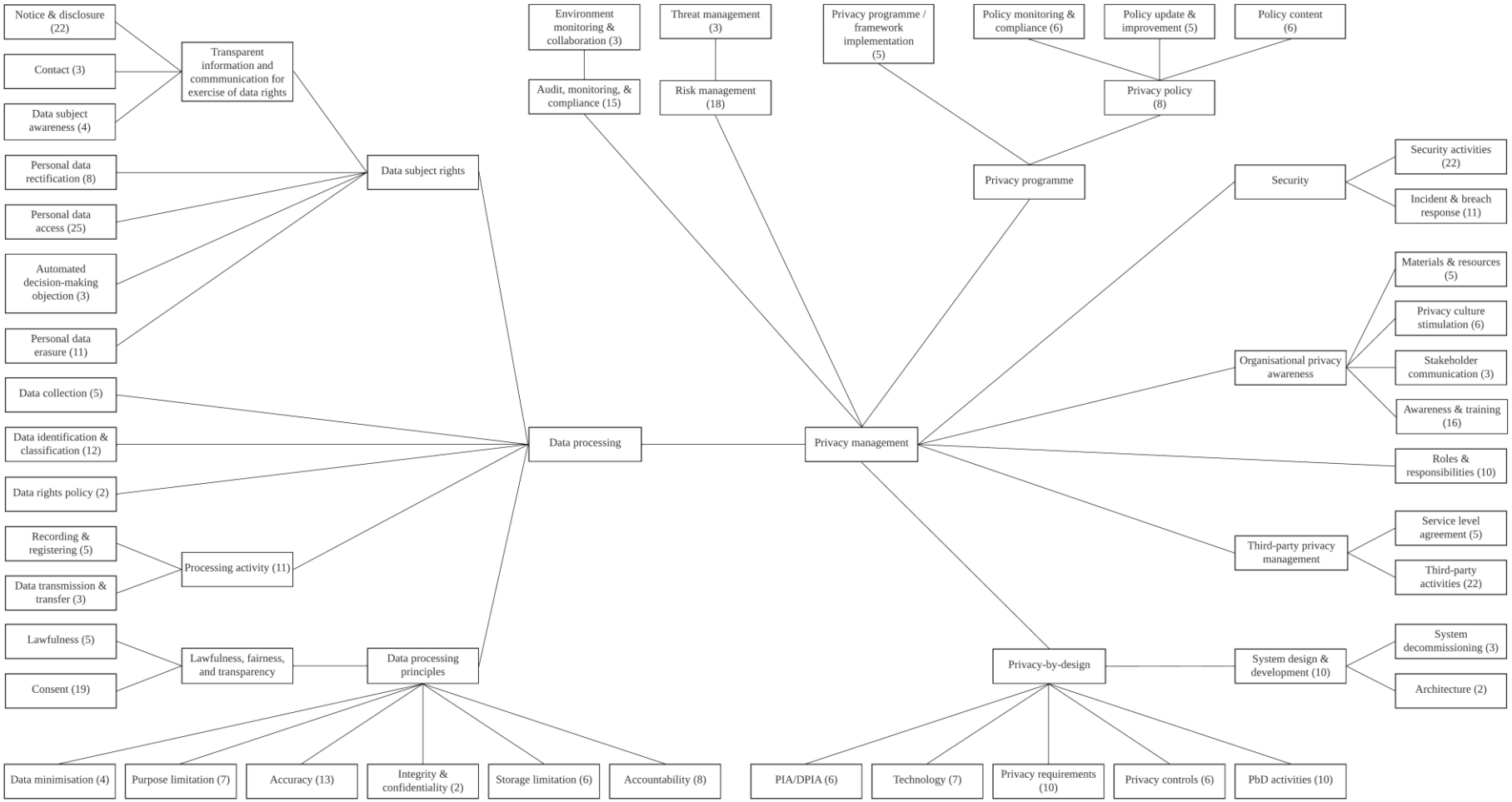

Figure 14: MLR 1 factor aggregation overview.

4.2 Multivocal literature review 2: Privacy-by-design factors

The second multivocal literature review (MLR 2) aims to inventory factors specific to privacy-by-design. There are no restrictions on the artifact type or application domain. Similar to MLR 1, this is a multivocal literature review that considers both academic and grey works, using the same methods and process as the first review. The review protocol for this review can be found in Appendix D.

4.2.1 Source selection and quality assessment

The search, screening, and assessment steps of this review are summarised in an adapted PRISMA flow diagram (Page et al., 2021) which is shown in Figure 15. Following the search process described in the review protocol, the search returned 645 records in total. Web of Science and IEEE Xplore returned the most results with respectively 184 and 181 records. Similar to MLR1, the Google search was limited to the first 100 results. Duplication removal resulted in 103 records being excluded, most of these duplicate records originated from the databases.

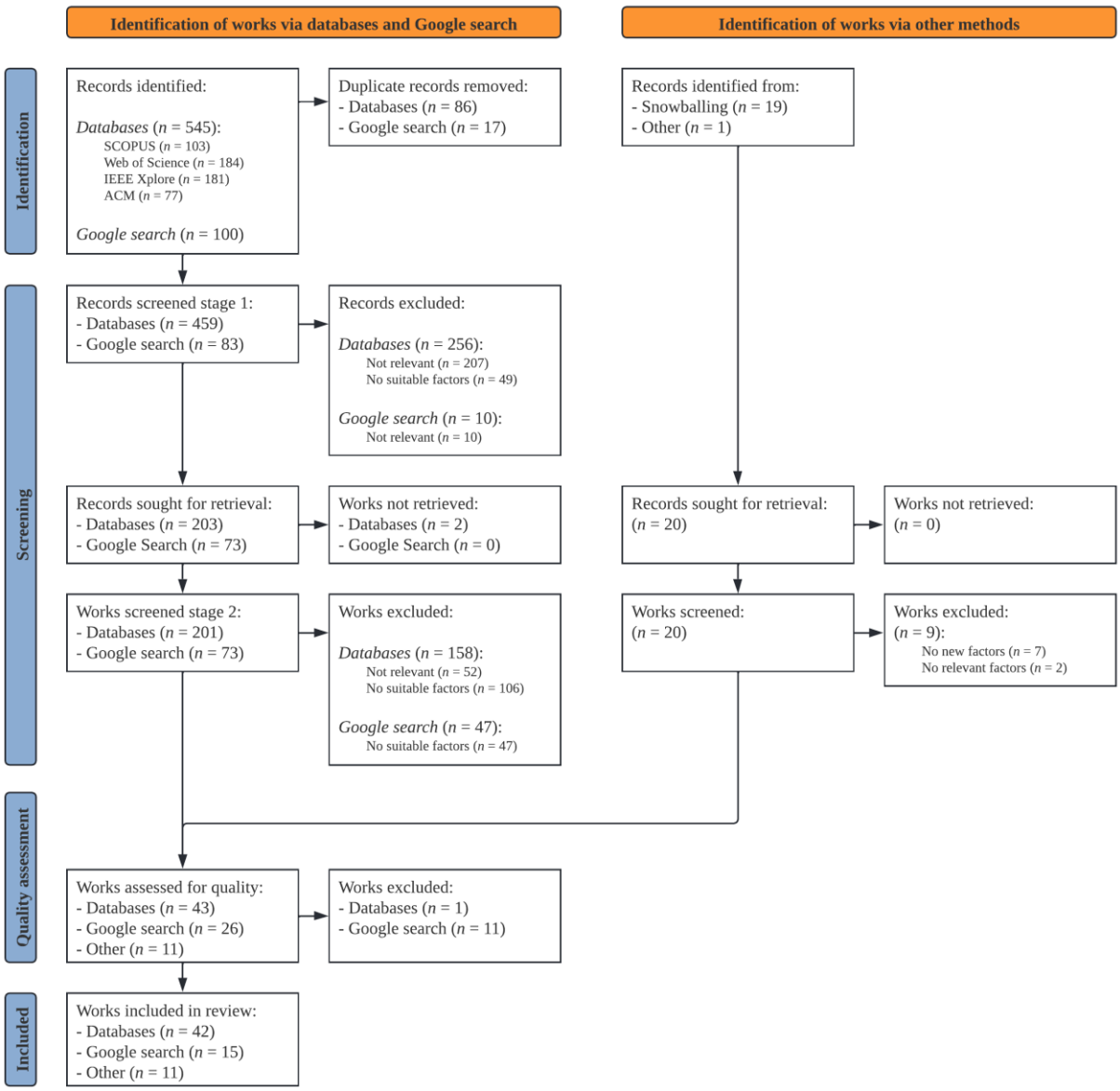

Figure 15: Flow diagram for MLR 2.

During the first screening stage, a total of 266 records were excluded. Of these, 217 records were excluded for not being relevant, which was the most common reason for exclusion during this stage.

Examples of topics addressed by excluded works include Automated text similarities identification between GDPR and other works, digitally sustainable information systems, JPEG scrambling as a privacy protection tool, and embedding cryptographic engineering into secure software. The other reason for exclusion is that the work did not contain relevant factors (49 records), these works do discuss privacy-by-design but introduce concrete technical solutions or only address domain-specific applications in domains such as smart grids, IoT, blockchain, or facial recognition.

Two works were unavailable for retrieval to be used in the full-text screening. From the 274 retrieved works, 205 were excluded in the second stage with the majority of works originating from a database (158 works). In this stage, 52 works were excluded for not being relevant and 153 works were excluded for not containing relevant factors.

Apart from the works found as a result of searching databases and Google search with a search string, works obtained through other means were added. These other means include snowballing, adding previously identified works, and adding works pointed out by other researchers. A total of 20 additional works were obtained through other means, all works were available for retrieval, 9 of these works were excluded during full-text screening.

During the quality assessment phase, 12 works were excluded for quality reasons, 11 of these were works originating from the Google search. These works were excluded mainly for being 3rd tier grey literature sources (Garousi et al., 2019) with authors whose expertise could not be established. This resulted in a total of 68 works which were included in the review, 42 from databases, 15 from Google search, and 11 obtained through other means, all the works included are listed in Appendix F.

4.2.2 Descriptive statistics

The 68 included works are plotted in a bar diagram (Figure 16) denoting the year of their publication, making a distinction between academic works and grey works. Similar to MLR 1, the years leading up to 2017 were pretty calm regarding the number of works published, the notable outlier in 2011 being an exception. This spike could potentially be explained by a resolution of the International Conference of Data Protection and Privacy Commissioners on the adoption of privacy-by-design which passed end of 2010. This resolution has been described as a landmark resolution (Cavoukian, 2011), whether this is the true explanation for the higher number of publications in the year after cannot be verified though. The same trend as is visible in MLR 1, is also visible in MLR 2 where the number of works published increases since 2017, possibly associated with the introduction of the GDPR in 2016. Unlike MLR 1, the number of publications did not immediately decline after 2017 for MLR 2.

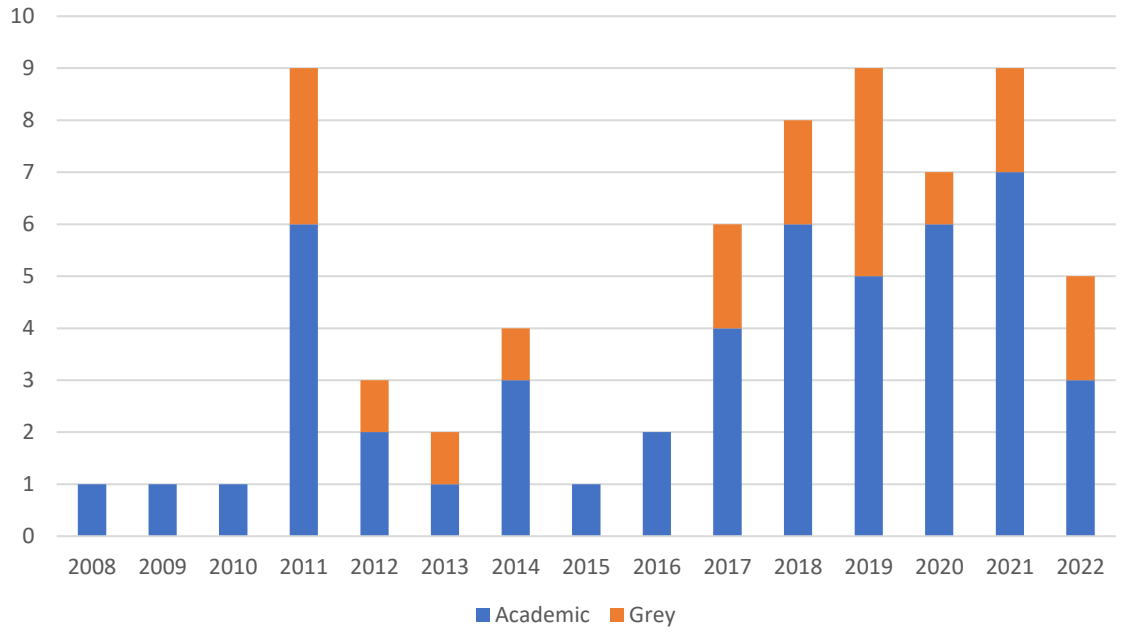

Figure 16: MLR 2 distribution of works between academic and grey literature per year.

Most of the works included in the review are of academic origin, Figure 17 shows the distribution between the origin of the works: 71% academic (48 works) and 29% grey literature (20 works). Academic works being the dominant group in MLR 2 contrasts the results of MLR 1 where 67% of included works (20 works) are grey literature. Comparing the absolute number of works between both MLRs; the number of included grey literature works is nearly equal between both MLRs, while the number of academic works is almost five times greater in MLR 2. This could indicate that academia favours privacy-by-design as a research domain over privacy/data governance maturity models, which is intuitively not a surprising observation since MLR 1 addresses a specific artifact (maturity model) as opposed to a whole domain (privacy-by-design) in MLR 2.

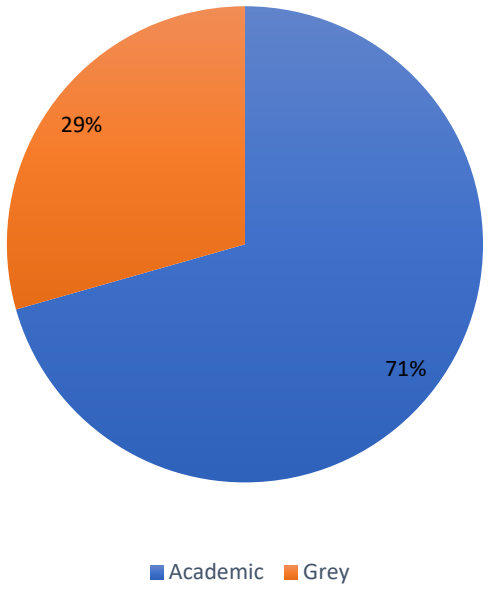

Figure 17: Distribution between academic and grey literature.

4.2.3 Data synthesis: privacy-by-design factors

A total of 713 factors have been found and extracted. Of the 68 included works, 64 provided relevant PbD factors. The works with at least one relevant factor are shown in the overview in Figure 18. The rest of this subsection describes some notable observations and findings.

Some works discuss privacy-by-design in the context of a specific domain. Healthcare is one of the domains that is addressed by multiple works. Hospitals and other medical care providers naturally process large amounts of personal data, including sensitive health-related data which must be handled with care. Semantha et al. (2020) conducted a systematic literature review on privacy-by-design in the healthcare sector. They examine the PbD principles, detail data breach issues, and present PbD frameworks, all in the context of the healthcare sector. Bincoletto (2019) and Semantha et al. (2021) investigate electronic health and patient records. Respectively, providing a model with measures and providing a conceptual framework for a patient record management system. Kalloniatis et al. (2021) incorporate privacy-by-design in body sensor networks for medical applications. They propose a privacy and data protection framework that outlines the appropriate steps to undertake the proper technical, organisational, and procedural measures. The framework supports PbD principles, GDPR requirements, and requirements validation during the DPIA.

A different reoccurring domain is the Internet of Things (IoT) domain, this encompasses systems in the form of a network of physical objects enabled with networking, computing, or sensing capabilities which facilitate the collection and transfer of data. Perera et al. (2016) have observed the lack of privacy protection features in IoT applications and middleware platforms which they attribute to the absence of systematic methods for privacy design that can guide the IoT development process. In order to address this, they introduce a framework for assessing the privacy capabilities of IoT applications and they

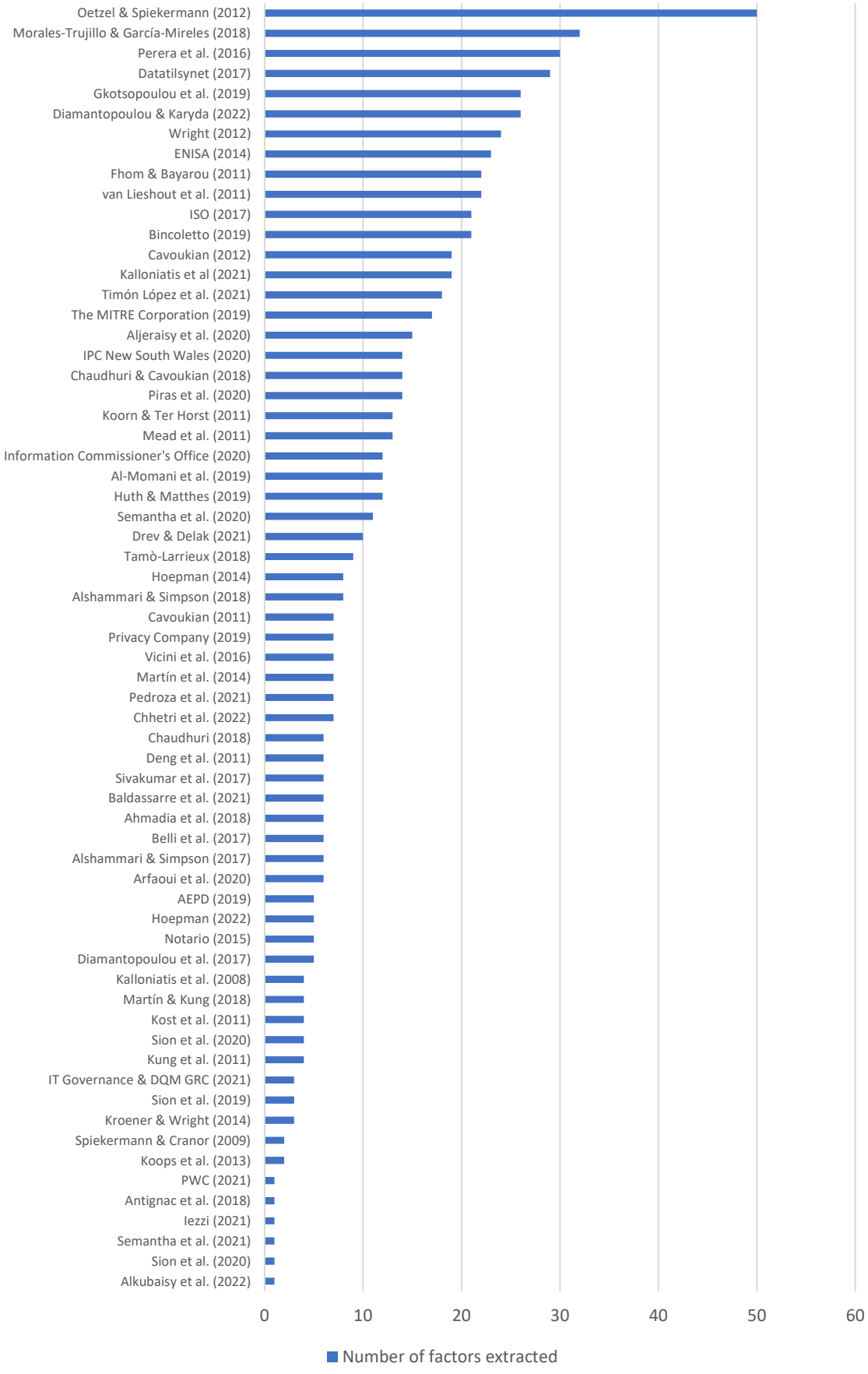

Figure 18: MLR 2 number of factors extracted per work, works with zero factors are excluded.

provide an extensive set of guidelines. Chaudhuri (2018) proposes a six-step approach for privacy-by-design in IoT. Chaudhuri & Cavoukian (2018) introduce the Proactive and Preventive Privacy (3P) framework for IoT privacy-by-design. This framework consists of an eight-phase cycle that envisions baking privacy measures into IoT device architectures and smart service design with user-centricity and transparency. Aljeraisy et al. (2020) enumerate through privacy and data protection laws and distil 15 key principles and 13 individuals' rights. Additionally, they analysed the principles and rights against PbD elements (principles, strategies, and guidelines) within different PbD schemes. Finally, they present multiple use cases with examples of privacy pattern application in IoT scenarios.

In line with the IoT domain, Gkotsopoulou et al. (2019) investigate the translation of data protection by design recommendations into technical solutions for cybersecurity systems within smart home environments. Fhom & Bayarou (2011) contribute towards a privacy engineering approach for smart grid systems. Their privacy-aware design method includes privacy-aware engineering flow and design guidelines and privacy-preserving countermeasures. The last notable domain is discussed by Koops et al. (2013) who investigate the collection, analysis, and use of data from open sources for intelligence purposes. While the open-source intelligence (OSINT) domain is not an obvious typical application domain of privacy-by-design, the authors of the paper observe that OSINT by state authorities poses challenges for intellectual-property enforcement and privacy protection. They argue for the application of technically-enforced legal compliance through revocable privacy and a policy enforcement language.

This multivocal literature review resulted in the identification of multiple works originating from data protection authorities. The website of the Information Commissioner's Office (ICO) (2022), which is the data protection authority of the United Kingdom, elaborates on the application of data protection by design by outlining UK GDPR principles, involved parties, PbD principles, motivations, and goals. They provide a checklist and link to resources for further reading. The Information and privacy commission New South Wales (2020) is the data protection authority of the Australian state New South Wales. They provide a fact sheet detailing the key PbD principles, bullet points that describe how a PbD approach can be embedded in an organisation, and it mentions PIAs and PETs. Some of the mentioned embedding strategies include considering whether a PIA is needed when starting a new project or making changes to an existing project, adopting a 'plain language' policy for public documents, and ensuring that personal information is automatically protected without individuals having to take any specific action.

The Datatilsynet (2017) is the Norwegian data protection authority, their website provides extensive guidelines regarding software development with data protection by design. They present a continuous process consisting of seven activities: training, requirements, design, coding, testing, release, and maintenance. Each activity is elaborated upon and accompanied by a comprehensive checklist of relevant elements. For training, it specifies what training should be provided, who should receive it, when it should be given, why it should be carried out, and it provides examples of how it should be carried out. For requirements, it specifies prerequisites for setting the requirements, details different types of requirements, and discusses the DPIA. For design, it specifies data-oriented design requirements and process-oriented design requirements, it discusses threat modelling and attack surface analysis, and it gives examples of tools. For coding, it specifies tools and frameworks, code analysis and review, and secure coding motivation. For testing, it specifies requirements validation, security testing, and attack surface review. For release, it specifies how to create an incident response plan, how to conduct a security review, why to set release management, and it specifies approval and archiving. Lastly, for operation, it specifies how to handle breaches, maintenance activities, and why requirements should be imposed.

The last work of a data protection authority that will be discussed is a privacy-by-design guide from the Spanish data protection authority (AEPD) (La Agencia Española de Protección de Datos, 2019). This work puts more emphasis on the engineering portion of privacy-by-design. It describes a chronological sequence of reusable design abstractions that are applied in decreasing levels of abstraction: privacy design strategies, privacy design tactics, privacy design patterns, and privacy-enhancing technologies. *Privacy-enhancing technologies* have been an established concept within the privacy domain, the *design patterns* concept is adopted from software architecture where it represents a commonly recurring structure. Hoepman (2014) introduced *privacy strategies* in order to bridge the gap between the project start and the architecture phase, later expanding his strategies with corresponding *tactics* in The Little Blue Book (Hoepman, 2022). The use of strategies, tactics, patterns, and PETs is

referenced or used in many works in this domain, e.g., Aljeraisy et al. (2020), Alshammari and Simpson (2018), European Network and Information Security Agency (ENISA) (2014), and Semantha et al. (2021) just in this review. The AEPD guide additionally provides a privacy engineering method which is shown in Figure 19, resembling the classical V-model (K. Forsberg & Mooz, 1991). Strategies and tactics are applied during concept formulation and requirements engineering, patterns are applied during system architecture and system design, and PETs are applied during system design and development.

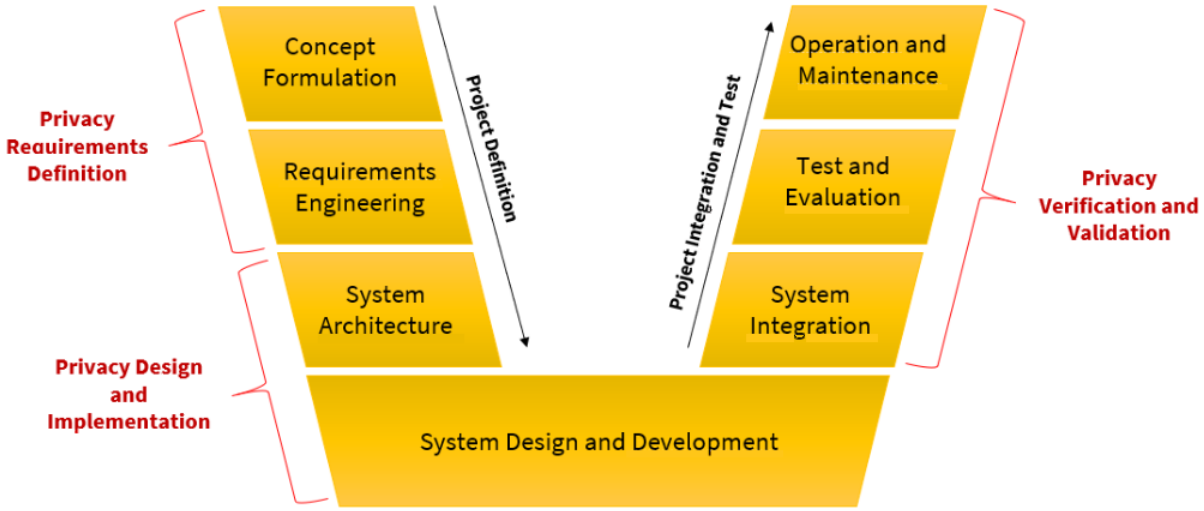

Figure 19: Privacy engineering method (La Agencia Española de Protección de Datos, 2019).

Al-Momani et al. (2019) present their own vision of the V-model by adapting it to a privacy-aware V-model. They took the classical V-model stages and embedded privacy considerations to create privacy-enhanced model stages. On top of that, they added two new stages: privacy analysis and privacy-enhanced architecture (PEAR). The privacy analysis stage is entirely privacy-centric and entails eliciting privacy threats and formulating countermeasures to formulate privacy requirements, it also includes performing a PIA. The PEAR stage can be subdivided into a privacy-preserving high-level and low-level design. Both stages integrate the privacy requirements into the design resulting in a privacy-enhanced architecture that meets privacy and business requirements.

Morales-Trujillo and Garcia-Mireles (2018) took a different approach in connecting software development and privacy-by-design, they took ISO standard 29110 (ISO/IEC, 2011), which specifies software engineering lifecycle profiles for small entities, and extended it by integrating PbD goals. They added 14 new tasks, examples include defining privacy policy together with customers, auditing software for privacy, and creating a role/functionality matrix. Additionally, they added six new work products, examples include privacy goals, privacy scenarios, and a sensitive data dictionary. Lastly, a new role was also formulated: a PbD manager. The explicit formulation of a new PbD-specific role is noteworthy since few works were found to do this or even discuss PbD-related roles at all. The competencies of the role are defined as: “[having] experience in data governance, familiarity with privacy protection techniques and knowledge of data privacy laws” (Morales-Trujillo & Garcia-Mireles, 2018, p. 60). They state that the role can be part of the responsibilities of a chief data officer.

The work from which the most factors have been extracted is the paper by Oetzel and Spiekermann (2014) which presents a systematic method for privacy impact assessments. They present a seven-step method which starts with characterising the system and ends with creating a PIA report. The method prescribes the formulation of privacy principles which are decomposed into actionable privacy targets. Subsequently, privacy threats are formulated for each privacy target. Finally, the privacy threats are matched with controls that eliminate or mitigate the threat. This provides full traceability, justifying the selected controls. According to the two authors, existing PIA approaches lack easy applicability, are insufficiently structured, are imprecise, and are lengthy. They argue that employing their method allows organisations to achieve privacy-by-design. Other works that discuss the PIA/DPIA extensively are Wright (2012), ISO/IEC (2017), Timón López et al. (2021), Ahmadian et al. (2018), and Sion et al. (2020).

Factor aggregation

The extracted factors in MLR 2 are analysed in the same manner as MLR 1 using a coding approach to identify categories or themes. The first step is to identify and consolidate duplicate factors. The review has resulted in the identification of 713 factors which have been consolidated during the coding process into 446 factors. The full collection of the consolidated privacy-by-design factors resulting from this review can be found in Appendix E.

Figure 20 shows the high-level abstract themes resulting from the factor coding, the themes are accompanied by a number in brackets which denotes the underlying number of factors that the theme encompasses. Unsurprisingly, *privacy-by-design* is the theme that encompasses the most factors. While the *data processing* theme is not as big as it is in MLR 1, it still provides a sizeable contribution as the second biggest theme with 98 factors. Other common themes between both MLRs include *security*, *organisational privacy awareness*, *roles & responsibilities*, *audit, monitoring, & compliance*, and *third-party management*.

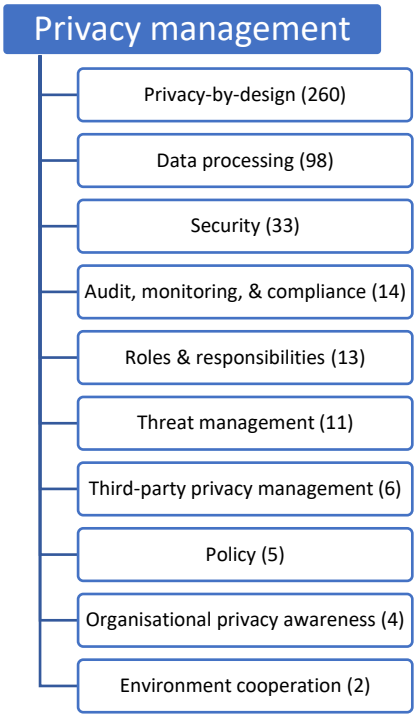

Figure 20: MLR 2 abstract factor themes with factor quantity.

Figure 21 shows the full results of the factor coding. The diagram shows the factor categories and encompassing themes, elements that are accompanied by a number in brackets are low-level categories that encompass factors with the number indicating the number of factors. The outer elements are more concrete with elements closer to the centre being more abstract—right in the centre, *privacy management* is the most abstract overarching theme that encompasses all other categories and thus all factors.

Compared to MLR 1, similar themes and categories are present including *data subject rights*, *data processing principles*, *privacy-by-design*, and *security*. The bulk of the factors in this MLR are concentrated in the lower right quadrant. This stands in contrast to MLR 1 (Figure 14) where the left half of the diagram contains the most factors. There is a clear emphasis on factors related to *PIA/DPIA* (104 factors) and *system design & development* (59 factors). About half of the factors (54) in the *PIA/DPIA* category pertain to elements that should be included in a PIA with 16 factors describing the content of a PIA report.

Other big hitters include *requirements* (40 factors), *security* (33), *technology* (20), *system development* (20), and *architecture* (15). There is a clear distinction in perspective between the factors of both MLRs. MLR 1 provides a legal perspective with prominence for data subject rights and GDPR

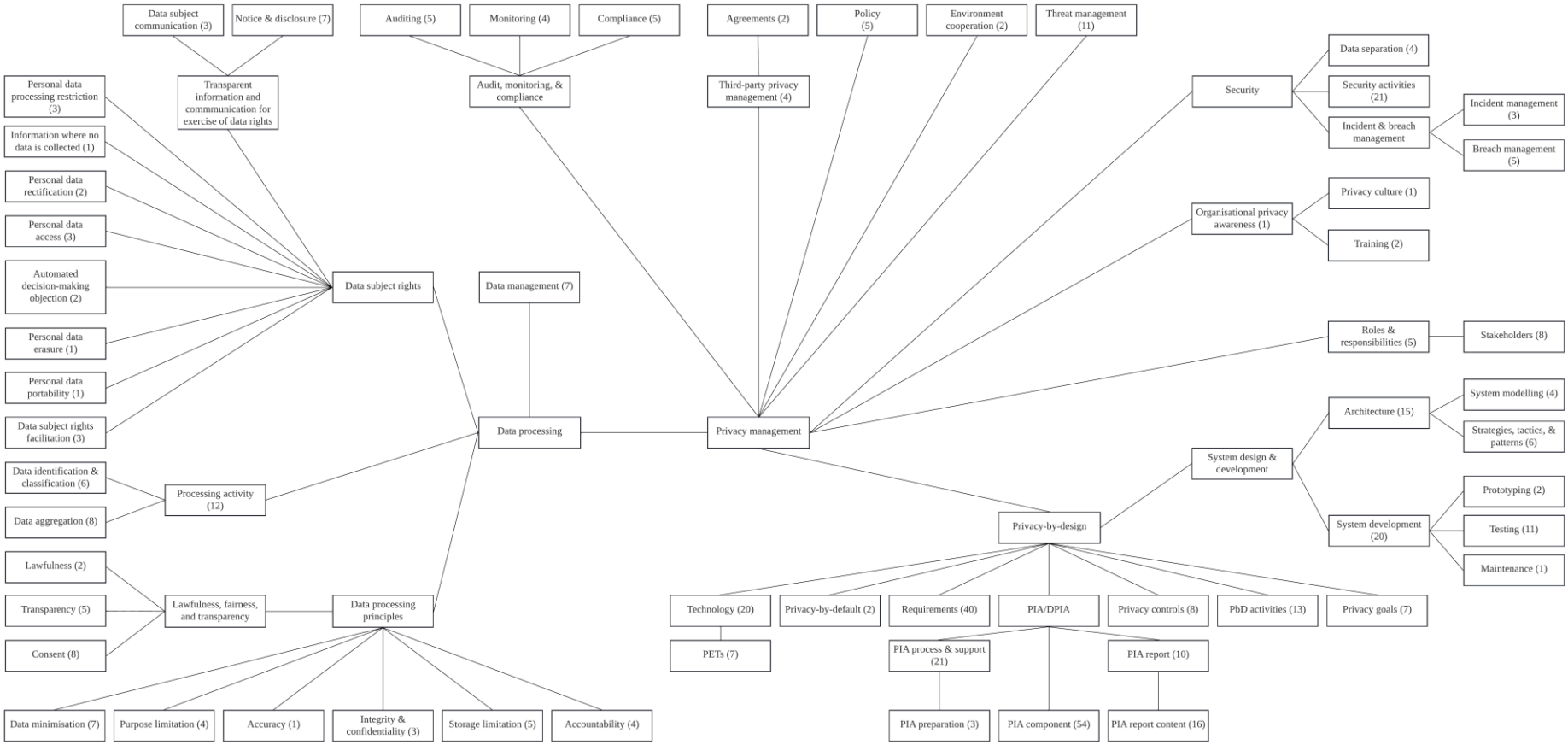

Figure 21: MLR 2 factor aggregation overview.

processing principles, as opposed to MLR 2 which takes a system-centric view focussing on development and lifecycle embedding. Considering the nature of both reviews, i.e., the artifact types and search strings, this observation is expected. Additionally, MLR 2 provides fewer factors than MLR 1 for awareness, culture, training, privacy programme, and policy-related categories.

The factor aggregation overviews of both MLRs (Figure 14 and Figure 21) have been constructed by grouping concepts into natural categories, using source literature, and employing a 'best fit' approach. Numerous factors can arguably be placed in different categories and not look out of place. These diagrams should therefore not be interpreted as complete, comprehensive conceptual models of privacy, privacy management, or privacy-by-design—they were never intended to fulfil that purpose. Their purpose is to gain an idea of what kind of concepts and categories of concepts are relevant to the domain under investigation, to get the lie of the land and provide suggestions for the formulation of focus areas for the maturity model.

5 Maturity model design

This chapter describes the design and construction process of the privacy-by-design focus area maturity model. This includes the conversion of factors into focus areas and capabilities, determining and modelling dependency relationships between capabilities, documenting design decisions and assumptions, and maintaining traceability.

5.1 Design process

This section describes the design process of converting the PbD factors, that were identified in the previous chapter, into a PbD focus area maturity model. Figure 22 shows the 3 phases with a total of 10 activities modelled using the PDD notation (van de Weerd & Brinkkemper, 2009). This process can be interpreted as a more elaborate look at the model design phase of the method PDD in Figure 2.

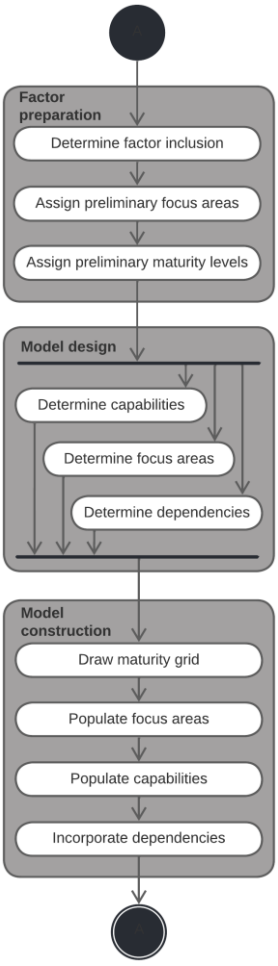

Figure 22: Process for converting domain factors into a maturity model.

After identifying the relevant domain factors resulting from the two literature reviews, all factors are aggregated into one list. The first activity of the *factor preparation* phase is to iterate through this list of factors and determine whether the factor contains suitable content that could be relevant for the formulation of a capability in the PbD domain. Factors that are deemed suitable are included for further processing, other factors are discarded. The next two steps include assigning a preliminary focus area and assigning a preliminary maturity level to each included factor. This creates a general grouping of factors and gives insight into the potential maturity development within each focus area.

The following phase, *model design*, entails creating the design by determining the capabilities, (final) focus areas, and dependency relationships. These three activities are modelled as concurrent activities in Figure 22 since they are tightly coupled. Changing the wording of a capability could result in a necessary change in the dependency relationships of that capability, similarly creating a new focus area would mean that new capabilities are created or moved from other focus areas. In practice, these three groups of model elements go hand-in-hand in their formulation.

Once all model elements are known, the model can be constructed in the *model construction* phase. The basic framework of a focus area maturity model is a grid that must be drawn first, with the maturity levels denoted on the horizontal axis. Subsequently, the grid is populated with all focus areas on the vertical axis and all capabilities in the grid cells representing the appropriate focus area-maturity level combinations. The last step is to incorporate dependency relationships between capabilities into the model by shifting each capability to a higher maturity level than the maturity level of the capability it is depending on.

5.2 Requirements

Section 3.2 presents the functions and properties of maturity models in short, including focus area maturity models. While that description suffices to gain a basic understanding, in order to ensure scientific rigour, a more extensive elaboration is necessary for the creation of a maturity model of this type. This section presents a more formal view of focus area maturity models, formulating structural requirements as well as quality attributes.

5.2.1 Meta-model

A partial overview of the meta-model for focus area maturity models from van Steenbergen et al. (2013) is shown in Figure 23, this has also been incorporated into the PDD for this research (Figure 2). According to the meta-model, a focus area maturity model consists of five concepts: a maturity matrix, focus areas, maturity levels, capabilities, and dependency relationships. A focus area maturity model addresses a functional domain which can be represented as the set FD of domain elements (e.g., actors and activities). The set of focus areas that constitute a particular domain can be defined as FA with each focus area being a subset of FD. The partitioning of FD into a number of focus areas can be expressed as $FD \; \dot{\bigcup}_{FA \in I} \; FA$. The set of all focus areas related to FD are denoted by I and the union operator with the dot denotes a disjoint union, meaning that there are no common elements between the different focus areas. The meta-model dictates that a focus area maturity model must have at least one focus area. The other axis of the maturity matrix consists of the maturity levels L, these are defined as a finite totally ordered set $(L, \leq_L)$ of levels. A focus area maturity model must have at least one maturity level. In order to define the maturity matrix, the Cartesian product of both axes, i.e., focus areas and maturity levels, is used: $I \times L$. Since not every focus area needs to have the same number of levels, this Cartesian product will typically be too big. The maturity matrix is thus defined as $C \subseteq I \times L$ where C denotes a subset of capabilities with the pairs $(FA, l) \in C$ corresponding to the cells in the matrix that contain a capability.

A focus area must contain at least one capability and a maturity level must likewise contain at least one capability. Empty focus areas, empty maturity levels, or an empty maturity matrix have no raison d'être and thus cannot exist according to the meta-model. Dependency relationships on the other hand are not strictly necessary, a dense maturity matrix with all capabilities in direct consecutive sequence would constitute a valid focus area maturity model. For a more in-depth mathematical formalisation of focus area maturity models this thesis refers to the appendix of van Steenbergen et al. (2013).

A graphical representation of the generic layout of a focus area maturity model is shown in Figure 24, adapted from Sanchez-Puchol and Pastor-Collado (2017). The vertical axis denotes the set of focus areas $(fa_1, \ldots, fa_n)$, the horizontal axis denotes the set of maturity levels $(l_1, \ldots, l_n)$, consisting of a consecutive ascending numerical sequence of integers starting with level 0. Within the maturity matrix, each focus area is associated with a set of capabilities $(a_1, \ldots, n_n)$, consisting of a consecutive ascending alphabetical sequence of letters starting with 'A'. Dependencies within the matrix between capabilities are ensured by positioning a capability y in a maturity level higher than capability x, if x must precede y, or in other words y depends on x. An example of a dependency in Figure 24 could be capability b_1 depending on capability b_2.

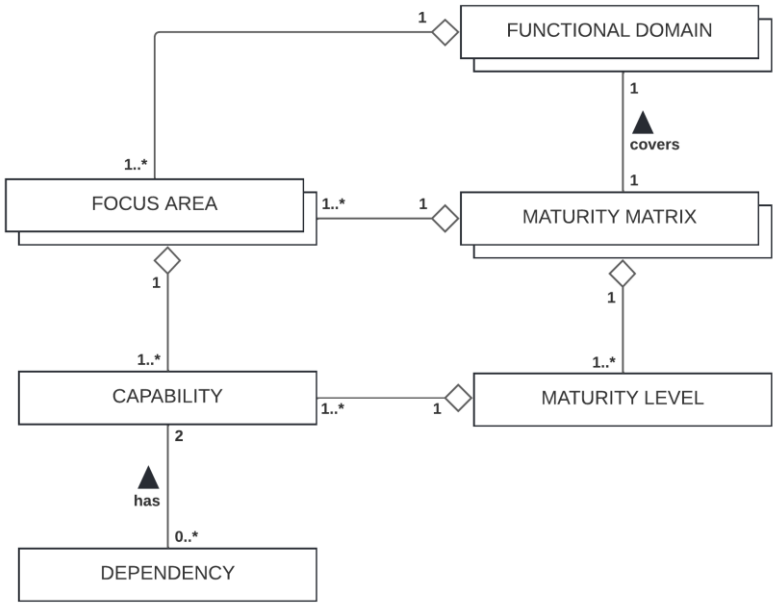

Figure 23: Focus area maturity model meta-model (van Steenbergen et al., 2013).

	l_1	l_2	l_3	…	l_n
fa_1	a_1		b_1		
fa_2	a_2	b_2	c_2		
fa_3		a_3	b_3		
…					
fa_n	a_n	b_n	c_n		n_n

Figure 24: Generic focus area maturity model layout (Sanchez-Puchol & Pastor-Collado, 2017).

5.2.2 Quality attributes

Ensuring the created model contains all necessary structural components and adheres to the cardinalities set by the meta-model is captured by the *completeness* quality attribute. Four more quality attributes are formulated as evaluation criteria (Table 8): *ease of use*, *effectiveness*, *operational feasibility*, and *usefulness*. These criteria are chosen from the evaluation criteria taxonomy for information artifact evaluation as presented by Prat et al. (2015). The four evaluation criteria selected here have been previously used to evaluate a focus area maturity model for API-management by Overeem et al. (2022)

Table 8: Quality attributes used as evaluation criteria.

Quality attributes	Description
Completeness	The degree to which the structure of the artifact contains all necessary elements and relationships between elements.
Ease of use	The degree to which the use of the artifact by individuals is free of effort.
Effectiveness	The degree to which the artifact achieves its goal in a real situation.
Operational feasibility	The degree to which management, employees, and other stakeholders, will support the proposed artifact, operate it, and integrate it into their daily practice.
Usefulness	The degree to which the artifact positively impacts the task performance of individuals.

5.3 The model

5.3.1 Factor preparation

The first step of the model creation process is to determine which factors are to be included for further processing. Table 9 provides an overview of the number of remaining factors after each processing phase per MLR. All 847 factors were assessed by the author together with a colleague researcher who is also a practitioner expert in the privacy domain in order to achieve a consensus on the inclusion, focus area classification, and maturity allocation of each factor. The reductive criteria for the factors used during the inclusion assessment are:

1. Fitness within the scope of privacy-by-design.
2. Significance of contribution compared to previously included factors.
3. Suitability of abstraction level for a maturity model.

Factors that are too concrete might not be suitable for a general maturity development path and factors that are too abstract risk being perceived as vague or too open to interpretation. A total of 476 factors were discarded in this phase. Appendix G provides an overview of all 371 initially included factors and their final model inclusion status.

Table 9: Number of remaining factors after each processing phase.

Phase	Number of factors		
	MLR 1	MLR 2	Total
Initial	401	446	847
Included	148	223	371
Capability formulation	97	160	257

5.3.2 Design of focus areas and capabilities

The included factors were assigned a preliminary focus area based on identified commonalities and by using the factor aggregation overviews from Figure 14 and Figure 21 as suggestions. Figure 25 shows the handwritten first formulation of the focus areas. In addition, the included factors were assigned a preliminary maturity level based on the content of each factor as well as comparisons between factors.

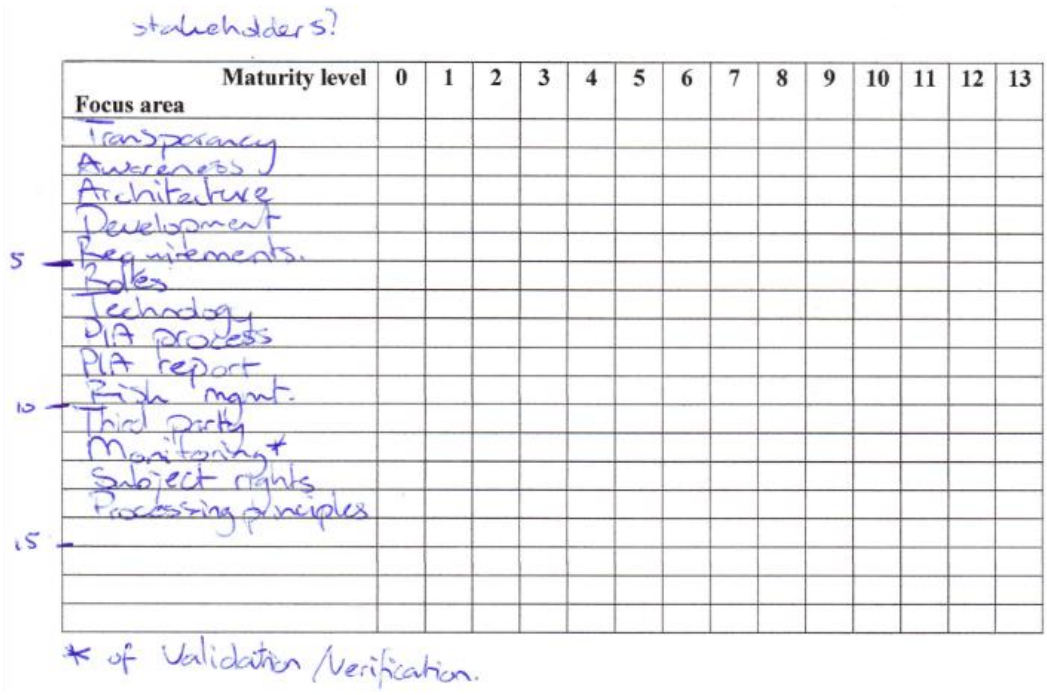

Figure 25: Model version 0.1 with the first formulation of focus areas.

The preliminary focus area groupings provide a viable start to select relevant factors and aggregate them into capabilities for a particular focus area. In general, a best-fit approach was employed keeping the previously mentioned three criteria in mind. In some cases, factors could almost literally be copied and combined. In others, capabilities had to be written from scratch. Examples of reasons for this include the factors being only partially relevant, the factors mentioning concrete elements that need to be generalised, or the factors having inconsistent wording or terminology usage. Other considerations in capability formulation include making sure the newly formed capabilities are clear, not too long, and form a coherent whole with other capabilities. This includes ensuring that a focus area has a sensible maturity progression path where higher maturity capabilities build upon lower maturity capabilities. The formulation of capabilities and focus areas took multiple passes of moving elements around, tweaking, and refining. The full list of included and excluded factors with focus area grouping and maturity level can be found in Appendix G.

Of the 371 included factors, 257 factors were selected to formulate 59 capabilities spread over 14 focus areas. The distribution of capabilities over the focus areas is displayed in Figure 26. Most focus areas encompass four capabilities, *third-party management* and *awareness* are quantitively the smallest focus areas with three capabilities each. *Development*, *technology*, and *monitoring* have each five capabilities while the *PIA process* focus area is quantitively the largest with six capabilities.

		Maturity level													
#	**Focus area**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
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										
14	Monitoring		A	B	C	D	E								
15															
16															
17															

Figure 26: Model version 0.2 with focus areas and capabilities.

The rest of this subsection shall briefly discuss each of the 14 focus areas, including the assumptions about the starting state (level 0) and the general maturity development. A full overview of the complete definitions of all capabilities per focus area can be found in Appendix H, this appendix additionally includes the traceability of the factors that form the basis for the formulation of each capability.

Requirements

The requirements focus area deals with explicitly formulating privacy requirements so that there is a clear and traceable translation from a need to design. Level zero is defined as: Privacy requirements are not explicitly formulated. The maturity development includes formulating privacy requirements, validating privacy requirements, involving stakeholders, and gaining advice from ethical experts.

Architecture
The architecture focus area is concerned with formalising the incorporation of privacy requirements into the design of a system. Level zero is defined as: Privacy is not explicitly considered in the software architecture. The maturity development includes creating a privacy viewpoint in the architecture documentation, modelling data flows, verifying models, using privacy strategies, tactics, design patterns and PETs, and keeping a centralised catalogue for patterns and PETs.

Development
The development focus area entails the actual building of the system and the implementation of privacy measures. Level zero is defined as: Privacy is not explicitly addressed during development. The maturity development includes ensuring that the system meets the privacy requirements, integrating privacy in the methods and activities of the development lifecycle, applying PbD within change management, and establishing a catalogue of privacy design patterns.

Technology
The technology focus area contains capabilities related to the management and application of technological measures, PETs, and privacy-by-architecture. Level zero is defined as: Privacy enhancing technologies are not explicitly implemented. The maturity development includes applying encryption, implementing privacy design patterns through PETs, assessing selected technologies, enforcing privacy policies through technical design, and implementing revocable privacy.

PIA process
The PIA process focus area deals with activities related to the management and execution of the privacy impact assessment. Level zero is defined as: A PIA is a one-time process and product. Unlike most other focus areas, basic knowledge of the PIA is assumed, i.e., knowing what a PIA is and that it must be performed. The maturity development includes updating the PIA whenever the project changes, conducting a preliminary threshold analysis, decoupling the process from the report, holding a senior executive accountable for the quality, and subjecting the PIA process to continuous review and improvement efforts.

PIA report
The PIA report focus area is concerned with the report that is used to communicate about the PIA process. Level zero is defined as: The PIA report is tightly coupled with the PIA process. There is one report for all audiences. The maturity development includes reviewing the report, storing PIA reports in a centralised registry, submitting the report for audit, and generating different PIA reports for different purposes or audiences.

Risk management
The risk management focus area entails integrating privacy risks into an organisational risk management programme. Level zero is defined as: Privacy is not integrated into the organisation's risk management programme. The maturity development includes employing a privacy risk analysis framework, keeping an inventory of privacy risks, implementing documented policies to monitor and optimise privacy risk management, and using predictive analytics to automatically identify data risks.

Processing principles
The processing principles focus area contains capabilities related to the application of the GDPR processing principles which guide data processing activities. Level zero is defined as: Data processing principles are not actively applied. The maturity development includes applying the principles to all processing activities, periodically evaluating the application of the principles, using a dashboard to provide an overview of the lawfulness of processing activities, and proactive managing of compliance with the processing principles.

Subject rights
The subject rights focus area deals with facilitating the rights of data subjects. Level zero is defined as: Data subject rights are not actively facilitated through design. The maturity development includes recording and documenting requests for the exercise of data subject rights, facilitating data rights through technical mechanisms, having a dashboard that provides insight into data access requests, and employing user-driven control of personal data.

Transparency
The transparency focus area is concerned with informing data subjects about processing activities and handling consent. Level zero is defined as: A privacy notice exists on a public website and data subjects are referred to it. The maturity development includes conducting privacy policy revision meetings, obtaining consent for additional processing, defining the privacy policy with data subjects, and publishing PIAs.

Third-party management
The third-party management focus area entails the interaction and management of third parties in the data processing chain. Level zero is defined as: Data processing agreements are established on an individual basis. The maturity development includes conducting a privacy risk assessment for third parties, using exception reports to record unacceptable activities by third parties, and making privacy level agreements as part of a service level agreement.

Roles
The roles focus area contains capabilities related to the formulation and formalisation of roles and responsibilities related to privacy activities. Level zero is defined as: Privacy-related roles are not formally defined for the entirety of the PbD process. The maturity development includes identifying stakeholders of privacy activities, appointing a chief privacy officer, assigning a technical privacy officer to support operational privacy-by-design activities, and appointing a privacy committee.

Awareness
The awareness focus area deals with stimulating privacy awareness among people who are involved in applying privacy-by-design. Level zero is defined as: Privacy awareness is not actively stimulated. The maturity development includes training different target groups, obtaining management commitment for PbD application, and learning from and contributing to the available body of knowledge.

Monitoring
The monitoring focus area is concerned with monitoring, validating, and improving privacy activities. Level zero is defined as: Privacy-related activities are not structurally monitored or validated. The maturity development includes having an assurance process in place to support compliance with regulation, logging events during all processing activities, having management continuously monitor policy compliance, performing periodic reviews and audits on processing activities, and having systematic and independent audit examinations.

5.3.3 Dependency relationships
A focus area maturity model contains two types of capability dependency relationships: *intra*-focus area dependencies and *inter*-focus area dependencies. The intra-focus area dependencies are the dependencies between capabilities of the same focus area, i.e., within a focus area. Figure 26 provides a clear overview of these dependencies. Taking the first two capabilities as an example: for each focus area, capability A always precedes capability B, in other words, capability B depends on capability A. Extending this dependency logic to all capabilities within each of the 14 focus areas leads to the identification of 45 intra-focus area dependency relationships, which can be found in Appendix I.

Using graph theory (Cormen et al., 2022), a focus area maturity model can be modelled as a directed graph $G = (V, E)$ where V is the set of vertices (capabilities) and E is the set of directed edges (dependency relationships). Dependency relationships are denoted using the tuple notation for graph

edges: (u, v) where vertex u has an outgoing directed edge to vertex v. In the context of this research, the notation is to be interpreted as: capability u precedes capability v, or v depends on u. While the intra-focus area dependencies are often not mentioned in other works because they are implicit and expected, it is necessary to be aware of their existence as dependency relationships for the analysis that is to follow in this subsection.

The inter-focus area dependencies are the dependencies between the capabilities of two different focus areas. Identifying these relationships is not as straightforward. In this research, two heuristics were used to somewhat structure the identification of this type of dependency: intra-level assessment and concept linking.

The first heuristic, coined *intra-level assessment*, entails assessing the capabilities within a maturity level to determine whether dependencies exist among them. For example, capability 1A and 2A start both in level 1 (Figure 26), since a privacy architecture would need privacy requirements, dependency relationship $(1A, 2A)$ was identified and all capabilities of the architecture focus area were shifted one level higher. In this research, manually adapting the model in real-time by shifting capabilities to higher maturity levels as dependencies were identified worked well. Applying this heuristic in an iterative cyclical manner until no new relationships are identified seems to be a viable approach with the state of the focus area maturity model as depicted in Figure 26 proving to be an excellent starting point for the application of this heuristic.

Additionally, the second heuristic, coined *concept linking*, was used to identify dependencies by looking at which capabilities address the same concepts. For example, capability 1A prescribes the elicitation of privacy legal requirements while capability 14A prescribes the demonstration of compliance with regulation, thus a conceptual link regarding regulation exists between these two capabilities. Upon closer inspection, it was decided that this link formed the basis for the dependency relationship $(1A, 14A)$. Table 10 shows all identified inter-focus area dependencies with motivation.

Table 10: Inter-focus area dependencies.

Dependency	Motivation
$(1A, 2A)$	Privacy requirements must be formulated before a privacy architecture can be created.
$(1A, 11A)$	Privacy requirements must be formulated before risks related to third parties can be identified.
$(1A, 5A)$	Privacy requirements must be formulated before a PIA can document how they are implemented.
$(1A, 14A)$	Privacy legal requirements must be formulated before compliance with regulation can be demonstrated.
$(1B, 2C)$	Elicited privacy requirements must be validated before the privacy architecture models that are based on those requirements are verified for completeness and soundness.
$(1B, 14A)$	A set of validated privacy requirements are necessary before an assurance process can be put in place to demonstrate compliance.
$(2A, 1B)$	A privacy architecture must map the privacy requirements onto the project architecture before the privacy requirements can be validated for technical soundness and implementation viability.
$(2B, 7B)$	Data flows must be modelled as part of the privacy architecture before privacy threats can be linked to them.
$(2C, 3D)$	Privacy tactics must be translated to privacy patterns before a centralised privacy pattern catalogue can be established.
$(2C, 4B)$	Privacy tactics must be translated to privacy patterns before PETs can be developed based on those privacy patterns.
$(2D, 4E)$	An exhaustive, sound, and complete privacy architecture must be in place before revocable privacy can be implemented.
$(2D, 5F)$	An established mature privacy architecture must be in place before privacy-by-architecture can be prioritised.

$(3A, 1B)$	Privacy requirements must be incorporated in low-level design before the adherence of the system to the requirements can be validated.
$(3B, 8C)$	Operational behaviour related to lawfulness must be checked against applicable policies and procedures before reporting on the lawfulness of processing activities in a dashboard.
$(3D, 2D)$	A catalogue of reusable privacy patterns must be established before it can be structurally implemented in the privacy architecture.
$(3D, 4C)$	A catalogue of reusable privacy patterns must be established before PETs and their relevant patterns can be catalogued.
$(4B, 9B)$	PETs must be selected and implemented before data subject rights can be facilitated through technical mechanisms.
$(4D, 3E)$	Privacy enforcement must be embedded in the technical design before privacy policies can be automatically enforced.
$(4D, 9D)$	Privacy enforcement must be embedded in the technical design before consent can be automatically updated in processing systems whenever a change occurs.
$(5A, 7A)$	The PIA process must be formalised before it can be integrated within risk management.
$(5C, 3C)$	The PIA process must be formalised and applied throughout the project's lifecycle before integration within change management can happen.
$(5C, 10C)$	The PIA process must be formalised and applied throughout the project's lifecycle before data subjects can be informed extensively about the procedures and policies.
$(5C, 13C)$	The PIA process must be formalised and applied throughout the project's lifecycle before relevant insights can be contributed to a body of knowledge.
$(5D, 6C)$	The PIA process and report must be decoupled before independent reporting cycles can be established.
$(5E, 7D)$	Risks must be modelled continuously before automated risk identification can be effective.
$(6B, 5D)$	A centralised PIA report registry must be established before the PIA process can reference these reports centrally.
$(6B, 10C)$	A centralised PIA report registry must be established before data subjects can be informed extensively about the procedures and policies.
$(6B, 10D)$	A centralised PIA report registry must be established before summaries of PIAs are published.
$(6C, 10D)$	PIA reports must be audited before PIA audit results can be published.
$(7A, 11B)$	A formally defined risk management framework must be established before third-party safeguards can be assessed.
$(7B, 8C)$	An inventory of privacy risks must be established before the lawfulness of processing activities can be reported in a dashboard.
$(7B, 10C)$	An inventory of privacy risks and a control implementation plan must be established before data subjects can be informed extensively about the procedures and policies.
$(7B, 12D)$	An inventory of privacy risks must be established before a privacy committee can do its work effectively.
$(7B, 13C)$	An inventory of privacy risks must be established before relevant insights can be contributed to a body of knowledge.
$(7C, 5E)$	Documented policies and procedures for privacy risk management must be established before continuous risk identification can be implemented.
$(7C, 6C)$	A privacy risk management improvement feedback loop must be established before third-party audits are performed.
$(8B, 14C)$	The GDPR processing principles must be implemented before the monitoring of processing policies, regulations, and procedures makes sense.
$(9D, 4E)$	Consent items that are automatically updated through all systems must be implemented before revocable privacy is possible.

$(11B, 13C)$	Third-party management must be formalised before relevant insights can be contributed to a body of knowledge.
$(12A, 1C)$	Stakeholders must be identified before they can be involved in privacy requirements elicitation.
$(12A, 13A)$	Stakeholders must be identified before targeted awareness activities can be applied.
$(12B, 5C)$	The roles and responsibilities of stakeholders must be defined before PIA process responsibilities can be assigned.
$(12B, 5E)$	The accountability of stakeholders must be defined before it can be enforced.
$(12B, 6A)$	Roles and responsibilities must be codified for who reviews a PIA report before reviewing PIA reports.
$(12B, 11B)$	Roles and responsibilities must be formulated for safeguard determining procedures before these procedures can be performed.
$(12B, 13B)$	Roles and responsibilities must be formulated before executive support and resources can be effectively provided.
$(12B, 14B)$	Roles and responsibilities must be formulated before performance can be regularly reported to management.
$(14A, 7C)$	Audits and periodic reviews must be performed before feedback can be used to improve risk management processes.
$(14B, 11C)$	A monitoring programme must be established before third parties can be monitored.
$(14C, 8D)$	Continuous monitoring must be implemented before process improvement can be managed proactively.

Combining the intra-focus area dependencies of Appendix I with the inter-focus area dependencies of Table 10 and incorporating them into the model results in the new model as depicted in Figure 27. Using the set of dependency relationships, the entire maturity model can be modelled as a directed graph—a visual representation of this is shown in Figure 28. This figure depicts all 59 capabilities as vertices and a total of 95 dependency relationships as directed edges (45 intra-focus area dependencies plus 50 inter-focus area dependencies).

		Maturity level													
#	**Focus area**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
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								
14	Monitoring					A	B	C	D	E					
15															
16															
17															

Figure 27: Model version 0.3 with all dependencies.

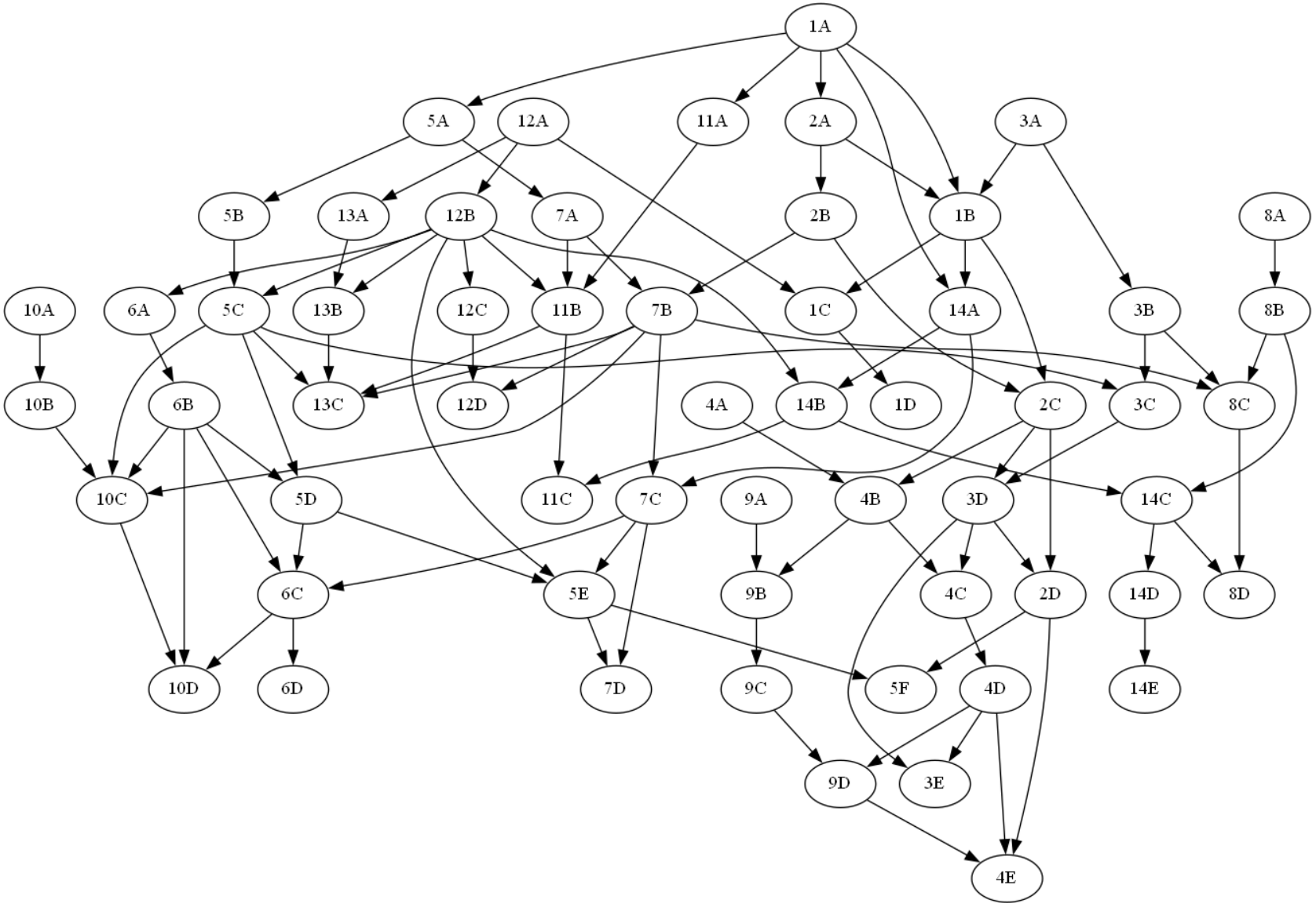

Figure 28: The dependencies modelled as a directed acyclic graph.

Modelling the dependencies as a graph allows for the application of several useful graph operations. The first thing that can be done, is to ascertain whether the graph contains a dependency cycle. In the context of focus area maturity models, the existence of a dependency cycle would create a paradoxical situation where the maturity development path has no start and no end. This would mean that the maturity model is incorrect, unsound, and unusable. Determining whether a graph has a dependency cycle can typically be done through a *topological sort* algorithm (Cormen et al., 2022). In this case, an additional step is taken by not only calculating a topological sort but also stratifying the vertices into *topological generations*. A topological generation is a collection of vertices whose ancestors are guaranteed to be in a previous generation and whose descendants are guaranteed to be in a following generation. The vertices are placed in a generation using a minimal approach, meaning that they are placed in the earliest possible generation while still respecting the ancestor/descendant constraints (NetworkX, 2022). The topological generations are calculated using the code provided in Appendix J, the result of running that code is shown below:

```
 1. ['1A', '3A', '4A', '8A', '9A', '10A', '12A']
 2. ['2A', '11A', '5A', '3B', '8B', '10B', '12B', '13A']
 3. ['2B', '1B', '5B', '7A', '12C', '6A', '13B']
 4. ['1C', '2C', '14A', '5C', '7B', '11B', '6B']
 5. ['1D', '4B', '14B', '3C', '7C', '8C', '12D', '13C', '5D', '10C']
 6. ['9B', '14C', '11C', '3D', '5E', '6C']
 7. ['9C', '14D', '8D', '2D', '4C', '7D', '6D', '10D']
 8. ['14E', '5F', '4D']
 9. ['9D', '3E']
10. ['4E']
```

Since the calculation was successful in generating topological generations, without error, the input graph must be acyclic. Finding a topological sorting or the topological generations is not possible if a cycle is present in a graph, this means that the graph in question is a directed acyclic graph (DAG)—free of paradoxical dependency cycles (Cormen et al., 2022). The result of the topological generations calculation has a familiar structure. Each of the 10 lines represents a generation. Looking back at Figure 27, it is clear that each generation corresponds to a maturity level. Calculating the topological generations algorithmically verifies that the manual approach in this research was applied correctly. Additionally, this seems to be a viable and low-effort manner of algorithmically generating the maturity matrix once the dependency relationships have been identified.

The second useful thing that can be done with the graph structure is analysing the distribution of dependency relationships by calculating the *in-degree* and *out-degree* of each capability. The in-degree property of a node denotes the number of edges pointing to the node, i.e., the number of capabilities that the capability in question is depending on. The out-degree property of a node denotes the number of edges pointing out from the node, i.e., the number of capabilities that are depending on the capability in question. Table 11 provides a descending overview of the 10 nodes with the largest numbers for in-degree, out-degree, and total degree (in plus out). Additionally, the node degrees are represented in Figure 28 through the number of incoming and outgoing arrows.

Capability 10C (transparency) and 13C (awareness) have the highest in-degree, both depending on four other capabilities. Since Table 11 includes the intra-focus area dependencies, both these capabilities depend on three capabilities from a different focus area. Capability 10C depends on capabilities from PIA process, PIA report, and risk management. Capability 13C depends on capabilities from PIA process, risk management, and third-party management. Having a capability with a high in-degree could be indicative of it being a complex capability that requires multiple different pre-established components. Capability 10C entails involving data subjects in the formulation of the privacy policy as well as providing extensive information regarding policies and procedures. This capability relies on having a formalised PIA process, a PIA report registry, a complete overview of privacy risks, and a control implementation plan—after all, you cannot inform data subjects extensively of what you do not know yourself. The capabilities with the highest in-degree are mostly C's and higher, with only two B's. A higher in-degree thus suggests a higher level of maturity.

Table 11: Overview of the 10 capabilities with the largest degree per category.

In		Out		Total	
Capability	**Degree**	**Capability**	**Degree**	**Capability**	**Degree**
10C	4	12B	7	12B	8
13C	4	1A	5	7B	7
1B	3	7B	5	1B	6
4E	3	5c	4	5C	6
5E	3	6B	4	1A	5
6C	3	1B	3	2C	5
8C	3	2C	3	3D	5
10D	3	3D	3	5E	5
11B	3	4D	3	6C	5
1C	2	7C	3	7C	5

Having a higher out-degree for a capability indicates that this capability is a pre-requisite for many other capabilities, which can be interpreted as it being a key capability of the maturity model that opens the developmental door for many other capabilities. Capability 12B is the capability with the highest out-degree, having six inter-focus area dependencies with five different focus areas: PIA process, PIA report, Third-party management, awareness, and monitoring. It is also the capability with the highest total degree, making it a *nexus capability* that is the most connected within the model. Intuitively, it is unsurprising that capability 12B is a key capability since it entails formalising stakeholder roles and responsibilities. This would be necessary before any structured processes that involve stakeholders can be implemented such as: determining who reviews a PIA report (6A), reporting about performance to the responsible manager (14B), or holding senior executives accountable for the quality of PIAs (5E).

Other capabilities with higher out-degrees include 1A and 7B. Capability 1A entails specifying privacy requirements and eliciting privacy-related business and legal requirements. This is needed before a privacy architecture can be created (2A), requirements implementation can be documented in the PIA (5A), a third-party risk assessment can be performed (11A), and before legal compliance can be demonstrated (14A). Capability 7B entails keeping a documented inventory of privacy risks and producing a control implementation plan with a feasibility analysis. This capability is required before automatic retention flagging and lawfulness-dashboarding can be implemented (8C), data subjects can be informed extensively (10C), a central entity responsible for privacy issues can be appointed (12D), and before the organisation can contribute to the body of knowledge (13C).

Aggregating the in-degrees and out-degrees per focus area, results in the degrees of each focus area. Table 12 displays the degrees per focus area per category in descending order with the side note that only the inter-focus area dependencies are considered here. The PIA process focus area has the (joint) highest in-degree, one of the higher out-degrees, and the (joint) highest total degree. It depends on five capabilities from four different focus areas, simultaneously six capabilities from five different focus areas depend on the PIA process. The risk management focus area has the joint highest total dependencies with the PIA process focus area. Seven capabilities from seven different focus areas depend on risk management, while risk management depends on four capabilities from three different focus areas. This implies that the PIA process and risk management focus areas are the most connected focus areas and represent the proverbial backbone of the model. Especially for PIA process, this observation aligns with its intuitive importance; PIA process is quantitively the largest focus area with six capabilities and represents a continuous process that commences early in the application of privacy-by-design and potentially lasts throughout its entire lifecycle. An additional noteworthy observation is that the transparency and awareness focus areas have an out-degree of zero, this means that no capabilities from different focus areas depend on capabilities from these two focus areas.

Table 12: Overview of the focus areas with the degrees per category.

In		Out		Total	
Focus area	**Degree**	**Focus area**	**Degree**	**Focus area**	**Degree**
PIA process	5	Roles	8	PIA process	11
Technology	5	Risk management	7	Risk management	11
Transparency	5	Requirements	6	Roles	9
Awareness	5	Architecture	6	Requirements	9
Risk management	4	PIA process	6	Architecture	9
Third-party management	4	Development	4	Technology	8
Monitoring	4	PIA report	4	Development	7
Requirements	3	Technology	3	PIA report	7
Architecture	3	Monitoring	3	Monitoring	7
Development	3	Subject rights	1	Transparency	5
PIA report	3	Processing principles	1	Third-party management	5
Processing principles	3	Third-party management	1	Awareness	5
Subject rights	2	Transparency	0	Processing principles	4
Roles	1	Awareness	0	Subject rights	3

5.3.4 Model overview and analysis

The focus area maturity model meta-model (Figure 23) prescribes that no empty focus areas or maturity levels are allowed, thus the model as depicted in Figure 27 must be cleaned up. Culling the empty focus areas and maturity levels results in the model as depicted in Figure 29, which is the end result of the design phase.

		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					
14	Monitoring					A	B	C	D	E		

Figure 29: The result of the design phase: version 1.0 of the PbD focus area maturity model.

This model has at least one maturity level, it has at least one focus area, each focus area has at least one capability, and each maturity level has at least one capability, thus this model adheres to the meta-model and satisfies the completeness quality attribute as formulated in Table 8. Yet, there is an exception: maturity level zero proves to be an anomaly. The cardinalities of the meta-model prescribe that a maturity level must have at least one capability. One can thus claim that strictly speaking, a level zero with no capabilities cannot exist in the model. On the other hand, the argument can be made that

level zero is no true maturity development level. It signifies the begin state of the organisation that does not adhere to a level one capability, thus level zero cannot contain a capability since it expresses the situation before the first capability. On top of that, including a capability-less level zero seems to be an established practice, e.g., Overeem et al. (2022) and Spruit & Röling (2014) include it. Even the authors of the meta-model present a maturity model which includes an empty level zero (Figure 7). Pragmatically, adding a level zero serves the purpose of allowing an assessor to indicate that a focus area was assessed (by colouring the level zero cell) but that it did not reach maturity level one. Taking all these considerations into account, this thesis adheres to the established practice and retains the inclusion of a capability-less level zero maturity level.

The final model consists of 14 focus areas, encompassing 59 capabilities, which are divided over 10 maturity levels, based on 95 dependency relationships. Figure 30 provides an overview of the distribution of capabilities per maturity level. The capabilities are reasonably evenly distributed across the maturity levels up to level seven, after which it declines steeply. This could be explained by the lack of knowledge on what high maturity really looks like in this domain thus few works describe high maturity factors, as opposed to the early levels whose factors enjoy broader and deeper elaboration in source works. Level 10 has the least capabilities, having only 1, while level 5 has the most with 10 capabilities. Completing level 4 encompasses completing the first 29 capabilities, meaning that subsequently completing one level 5 capability would put an organisation past the halfway point, capability-wise. Completing level 5 equals completing 66% of the capabilities.

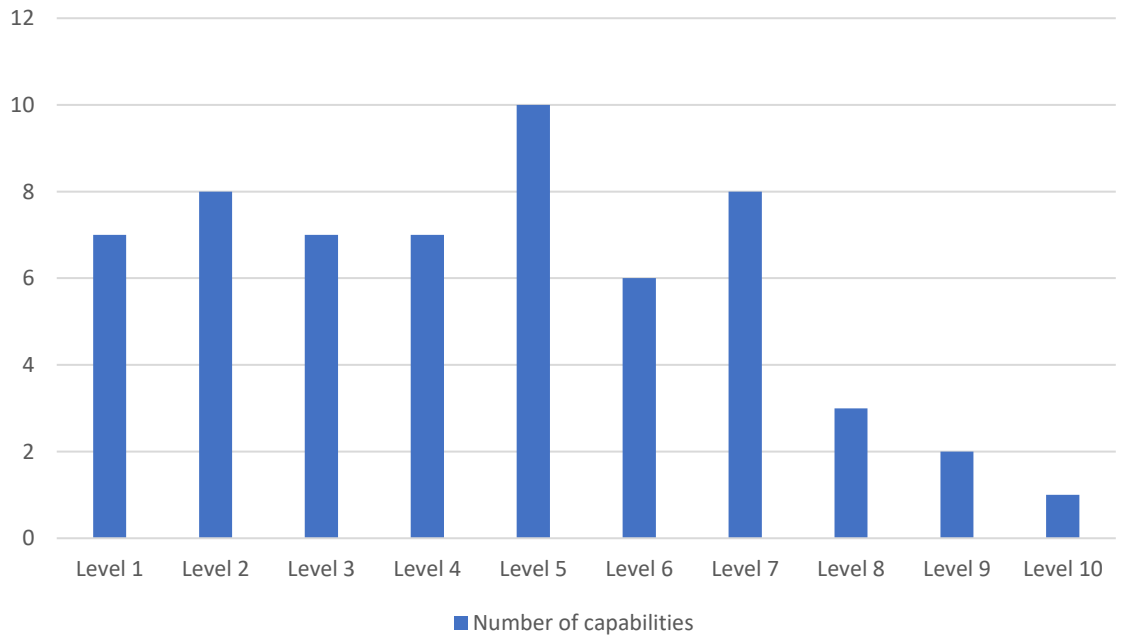

Figure 30: Distribution of capabilities per maturity level.

A total of 257 factors were selected to formulate 59 capabilities, leading to an arithmetic average of about 4 factors per capability. The number of factors forming a capability ranges from 1 (13A, 3E, 6C, 6D, 1D, 4E) to 14 (2A). A sidenote must be made here: one factor does not have to equal one source work since multiple works can mention the same factor, duplicate factors have been aggregated in an earlier phase. From a focus area perspective, each focus area is supported by an arithmetic average of about 18 factors. Table 13 provides an overview of the exact number of factors per focus area, including the distribution among both MLRs. Out of the 14 focus areas, 10 are supported by more factors from MLR 2 than MLR 1. *Processing principles*, *subject rights*, *third-party management*, and *monitoring* are the only focus areas with more MLR 1 factors than MLR 2 factors. In general, it is not surprising that MLR 2 contributes more factors since that MLR focusses on privacy-by-design specifically, as opposed to MLR 1 focussing on general privacy and data governance maturity.

PIA report and *awareness* have the least underlying factors, while *PIA process* and *architecture* have the most.

Table 13: Number of factors per focus area with MLR distribution.

Focus area	MLR 1	MLR 2	Total
Requirements	1	14	15
Architecture	3	24	27
Development	9	13	22
Technology	2	13	15
PIA process	10	23	33
PIA report	0	7	7
Risk management	9	12	21
Processing principles	14	9	23
Subject rights	13	9	22
Transparency	8	9	17
Third-party management	10	4	14
Roles	3	10	13
Awareness	2	4	6
Monitoring	13	9	22

Table 14 goes a step further and shows the distribution of the origin type of all factors for each focus area, split over both MLRs. The table makes a distinction between factors that originate from academic-only works, grey-only works, and factors that originate from both. The first notable observation is that most focus areas are mainly based on grey factors looking at MLR 1, as opposed to MLR 2 where the majority of focus areas are mainly based on academic factors. MLR 1 providing mainly factors from grey literature is expected since 319 of the 401 consolidated factors originate from grey-only works. Similarly, for MLR 2 it is not surprising that most of the used factors originate from academia since 312 of the 446 consolidated factors originate from academic-only works.

Table 14: Distribution of factor origin per focus area split on MLR.

Focus area	MLR 1			MLR 2		
	Academic	Grey	Both	Academic	Grey	Both
Requirements	0	0	1	11	2	1
Architecture	0	3	0	17	5	2
Development	1	8	0	8	4	1
Technology	2	0	0	8	3	2
PIA process	0	9	1	14	4	5
PIA report	0	0	0	4	2	1
Risk management	3	6	0	11	1	0
Processing principles	2	11	1	5	2	2
Subject rights	3	9	1	5	2	2
Transparency	1	7	0	2	6	1
Third-party management	0	10	0	3	1	0
Roles	1	1	1	7	2	1
Awareness	0	2	0	1	3	0
Monitoring	0	12	1	5	2	2
Total	13	78	6	101	39	20

Looking at the total contribution of academic-only works, the a*rchitecture* focus area is academically the best supported with 17 factors while *awareness* is academically the least supported with only 1 factor. The monitoring focus area is the focus area with the most factors originating from grey-only works with 14 factors, *requirements* and *PIA report* have the least with only 2 factors. The

PIA process focus area is supported by the most factors that originate from both academia and grey literature: six factors. Examining the difference, *transparency* has the biggest gap (10) between academic-only factors and grey-only factors (3 and 13 respectively). Other focus areas with a large imbalance include *requirements* (11 and 2), *architecture* (17 and 8), and *monitoring* (5 and 14). The *PIA process* focus area is the most balanced with 14 academic-only factors and 13 grey-only factors.

The proportion of academic-only works and grey-only works turns out to be fairly balanced with a total of 117 factors (46%) originating from grey-only works and a total of 114 factors (44%) originating from academic-only works, a total of 26 factors (10%) are based in both academia and grey literature. This distribution aligns with the distribution of considered factors: 372 academic-only (44%), 408 grey-only (48%), and 67 factors rooted in both (8%).

5.3.5 Design decisions

This subsection elaborates on the main design decisions, assumptions, and considerations related to the model design, including focus area formulation, scoping, start state assumptions, and model application assumptions.

Design decision 1: Excluded *Policy* focus area

During the formulation of the focus areas, two more potential focus areas were considered based on the accumulated factors. The first is a *policy* focus area concerned with capabilities related to a privacy-by-design policy. The number of relevant factors related to policy is limited and most factors do not go deeper past formulating a policy and updating a policy. Considering the other focus areas that are already identified, policy seems to be an odd one out where the formulation of, and adherence to, a privacy-by-design policy intuitively feels valuable, yet the inclusion of a policy focus area does not seem to fit the model. The substantiation of a policy focus area with the identified factors is somewhat unsatisfying while simultaneously policy factors do not naturally fit in any other focus area either, therefore the decision was made to not include a policy focus area and exclude the relevant factors.

Design decision 2: Excluded *Asset inventory* focus area

The other focus area that was considered is the *asset inventory* focus area. Multiple factors were identified related to identifying, documenting, and keeping an inventory of various assets, examples include data records, processing systems, categories of data subjects, data assets that can be affected by breaches, or existing technical and organisational data protection measures. Since 12 factors of this nature were identified, the inclusion of this focus area was considered. After further examination and discussions, some of the factors were deemed basic or almost implicit and not suitable as maturity development capabilities. In the end, the decision was made to not include an asset inventory focus area as the perceived added value of such a focus area was deemed lacking.

Design decision 3: Excluded factors related to culture

The next focus area of interest is the *awareness* focus area. The point of contention regarding awareness is whether it is part of privacy-by-design specifically, or whether it should be addressed on a higher level of abstraction, e.g., in a privacy management maturity model. General privacy awareness was deemed to be out of scope after discussions, yet the role of awareness in privacy-by-design is seen as important thus the decision was made to include an awareness focus area but have it focus mainly on specific privacy-by-design awareness stimulating activities. Concordantly, identified factors related to creating a privacy culture were excluded since culture was regarded as out-of-scope, creating a combined *culture & awareness* focus area was considered.

Design decisions 4: Excluded factors related to the content of a PIA report

In the formulation of the *PIA report* focus area, numerous factors were discarded that specified what components a PIA report should contain. Examples of these components include system boundaries, chosen privacy controls, person who approved the PIA, system purpose, or involved stakeholders. The underlying motivation for this is that these are elements that would be suitable for a PIA report template artifact, not so much a maturity development artifact. Additionally, many different PIA report templates exist depending on legal jurisdiction or market, e.g., Centrum Informatiebeveiliging en Privacybescherming (CIP) (2019), iapp (2020), or Information Commissioner's Office (ICO) (2018). It

is not the purpose of this thesis to contribute to that body of knowledge. The PIA report focus area is limited to how the report is used, reviewed, updated, and who is responsible for it, not so much what it contains.

Design decision 5: Decoupled the PIA process from the PIA report
Another conscious design decision that was made relates to both the *PIA report* and *PIA process* focus areas. Factor 162 prescribes that a PIA report should be understandable for technical and non-technical experts, combined with factor 349 that prescribes publishing the PIA report or summary thereof, indicates that the PIA report should be a dynamic artifact that adapts its content to its audience (Appendix F). A similar structure is employed in software architecture where different views and viewpoints portray the same system under development in a fashion that is tailored to the expectations and expertise of the intended stakeholder audience (Bass et al., 2013). The researchers agreed that a comparable mechanism is appropriate where the PIA, as a model, is separated from its presentation artifact. This allows for the PIA process to continue independently and that at any point in time different, specific, reports (or other artifacts) can be generated for a particular purpose and/or audience—introducing what might be coined as *PIA views*. The decision was therefore made to include the decoupling of the process and the report of the PIA as part of capability 5D of the PIA process focus area.

Design decision 6: Excluded factors related to GDPR requirements
The last major design decision that must be elaborated upon, relates to the assumption of the start-state of the organisation that wants to apply this maturity model and the relation of the model with legal compliance. Many initially found factors prescribe basic activities which are legally required by the GDPR. This raises the question of what the relationship between privacy-by-design maturity and legal compliance is. The researchers came to the consensus that the goal of this privacy-by-design maturity model is to develop PbD practices, not to assess compliance with the law. It is a model for maturity assessment, not compliance assessment. Furthermore, including legal compliance in the model suggests that an organisation, in the worst case, starts in a state of complete non-compliance. It does not seem appropriate or obvious for an organisation in such a state to start developing its privacy-by-design practices in-depth through a maturity model. The decision was therefore made to leave factors prescribing GDPR requirements mostly out of the model. A notable exception is capability 8A of the *processing principles* focus area that prescribes the application of the GDPR processing principles as outlined in article 5 of the GDPR (European Commission, 2016). This capability is included to bridge the gap between not applying the principles (level zero) and formalising the application of the principles (8B). The model thus assumes that an organisation already has some basics related to privacy management in order (see 5.3.2 for additional level zero assumptions), before it starts with dedicated privacy-by-design practices development.

6 Validation

This chapter describes the validation step of this research project which was performed through the application of a focus group interview. The sections of this chapter discuss the focus group choice motivation, the process, the results with analysis, and the implementation of changes to the model.

6.1 Motivation

There are multiple methods for validation and evaluation in design science, Sonnenberg and vom Brocke (2012) provide an overview of four different evaluation activities with input, output, criteria, and corresponding methods. Wieringa (2014) states that asking expert practitioners about their opinion is the easiest way of validating a design science artifact. The desired validation activity for this case can therefore be characterised as: take the PbD maturity model as input, generate expert opinions, and provide a validated model as output. This general outline fits the third design science evaluation activity of Sonnenberg and vom Brocke (2012). It takes an instance of an artifact as input and provides a validated artifact instance in an artificial setting, the recommended methods for this activity are prototype demonstration, prototype experiment, system experiment, benchmarking, survey, expert interview, and focus group.

Considering the preference for expert opinion, a survey, expert interview, or focus group are the main methods of interest. Taking into account the complexity of the artifact and the design decisions, there was a need for in-depth qualitative feedback which is better suited to be elicited from an expert interview or focus group, rather than a survey. While a series of expert interviews would also have resulted in useful feedback, the decision was made to go with a focus group validation. The added benefit of a focus group is that participants do not only interact with the moderator but also with each other. Considering that privacy-by-design is rather multidisciplinary, combining legal, social, and technical dimensions, having a group with diverse backgrounds and vocations interact with each other has the potential for it to become more than the sum of its parts and can generate unique and useful insights (Krueger & Casey, 2015). The PbD maturity model depicts an extensive development journey which traverses through various domains, organisational layers, and stakeholder groups. Using a focus group allows for scrutiny from multiple perspectives which has the intended effect of creating a validated artifact that is broadly supported and which considers interactions between or across different domains.

6.2 Validation Process

This section describes the validation process of the privacy-by-design focus area maturity model by using a focus group interview. Figure 31 shows the 3 phases and 10 activities modelled using the PDD notation (van de Weerd & Brinkkemper, 2009). This process can be interpreted as a more elaborate look at the model validation phase of the method PDD in Figure 2.

Organising a focus group starts with the preparation, the first step is to define its purpose. Defining what the expected results are is important to ensure that the focus group does not miss its mark, that useful data is gathered, and to prevent disappointment.

Whenever human subjects are involved in a study, matters related to ethics must be considered, as has been mentioned before in section 2.8. A focus group interview is no different and participants must be informed of the study's risks and rewards, about participation being voluntary, about confidentiality, and ensured that they can stop participating at any time (Krueger & Casey, 2015). Additionally, participants must provide explicit consent to record their decision to participate and allow the researcher to use the results as research data. Creating informed consent documentation must thus be done before candidates can be invited.

Similar to regular expert interviews, it is recommended to create an interview guide or protocol to guide the focus group session (Krueger & Casey, 2015). This protocol describes the general flow of the focus group, contains all questions, additional probes, and reminders for the moderator such as ensuring that consent forms are collected and that recordings are turned on.

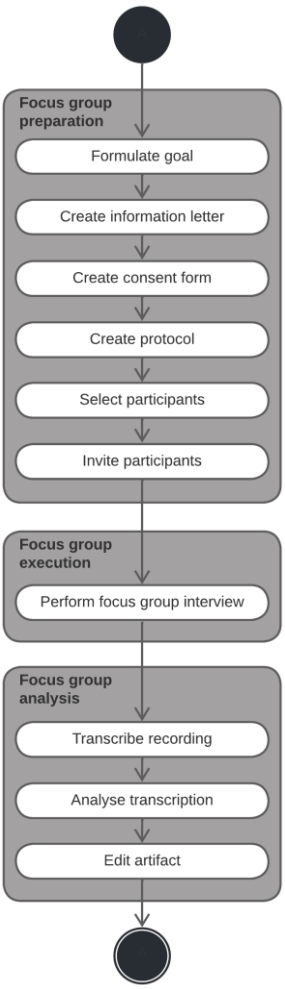

Figure 31: Process for validating the PbD maturity model.

It is recommended to not plan a focus group with more than 10 participants because a group this big becomes difficult to control and it limits contribution opportunity for each participant, the ideal range seems to be 5 to 8 participants (Eliot & associates, 2005; Krueger & Casey, 2015). The next step is to determine what types of people could provide the information that is desired. The composition of a focus group should be carefully considered, not all demographic combinations are suitable depending on the purpose (Krueger & Casey, 2015). Once the participant profile has been established, suitable candidates must be recruited. Krueger and Casey (2015) outline several recruitment strategies, examples include using existing lists of people that fit the profile, using a neutral party to nominate candidates from their network, snowball sampling (ask selected candidates for nominations), piggybacking focus groups (add a focus group to another event or meeting and use those participants), recruiting people related to the same organisation, or using a screening and selection service which are commonly used in commercial market research firms.

Once participants have been selected, they can be invited and the focus group interview can be performed. Eliot & associates (2005) and Krueger and Casey (2015) provide numerous recommendations and tips for conducting and moderating a focus group. Examples include employing active listening, clarifying concepts when participants misinterpret, facilitating differing points of view, and using pauses and probes appropriately.

Recording a focus group session allows the moderators to focus on asking questions and listening rather than taking notes. Afterwards, during the analysis phase, the recording can be transcribed and the transcript can be analysed through a coding approach to elicit the desired feedback. Once the feedback has been documented, it can be incorporated. For this research, incorporating the feedback entails adapting the maturity model which can include adding/removing focus areas, capabilities, or dependency relationships, additionally reformulating focus areas or capabilities is also possible.

6.3 Design and execution

The purpose of this focus group is to validate the PbD focus area maturity model. This includes getting feedback from expert practitioners on the inclusion/exclusion of model components, their relevance to PbD, the maturity development path, and getting feedback on the major design decisions.

The informed consent for this focus group consists of two parts: an information letter and a consent form, both can be found in Appendix K (in Dutch) and are based on a template provided by Utrecht University[3]. The information letter describes the overall research project and the purpose of the focus group validation therein. It informs potential participants of the inducements, costs, and risks, it emphasises the voluntary nature of participation, it explains how the collected data will be handled and processed, it states that the session will be recorded, it details the participant's rights including the ability to quit at any time, and it provides contact information for questions or complaints. The consent form ensures that the participant has been informed sufficiently, has had the ability to ask questions, is participating voluntarily, is aware that they will be recorded, and is aware of how their data will be used.

In order to create conditions for a fruitful discussion, a semi-structured interview approach was selected. This allows the researchers to have questions which guide the group along certain topics, yet retain enough flexibility to explore other topics that organically arise. The questions and general flow of the focus group session are described in a focus group protocol which was designed based on the recommendations from Eliot & associates (2005) and Krueger and Casey (2015), it can be found in Appendix L (in Dutch). The questions elicit general feedback on the set of focus areas. This includes determining whether the model is complete or missing focus areas, as well as suggesting the inclusion of focus areas which were considered during the design stage but were not included (policy and asset inventory). Other questions examine the first level of the model and examine some focus areas in detail.

A nomination strategy was employed to generate a list of potential candidates, combined with an organisational recruiting strategy by using the organisational network of a colleague researcher who is also an expert practitioner in this domain. The initial list contained 12 potential candidates, more than recommended to offset denials and cancellations. A variation of occupations and roles were selected to ensure a multi-perspective examination of privacy-by-design. All candidates were approached with an invitation through e-mail, seven responded positively and indicated wanting to participate, two participants had to cancel last-minute, leaving five participants and two moderators. All five participants work for government organisations in The Netherlands, the group composition is shown in Table 15.

Table 15: Overview of the focus group participants.

Number	Function	Experience in current function
Participant 1	Security/privacy officer	2.5 years
Participant 2	Data scientist	3.5 years
Participant 3	Data protection officer	4 years
Participant 4	Product owner	4 years
Participant 5	Security architect	5 years

The focus group session was conducted and recorded. Afterwards, a transcript was produced where names of organisations and individuals were redacted. Additionally, some sensitive information regarding the operation of an organisation was redacted. The transcript was cleaned by removing filler words that did not add anything meaningful to the topic of interest. The analysis of the transcript is discussed in the next section.

6.4 Synthesis

The transcript of the focus group interview was analysed through a coding approach (Corbin & Strauss, 2015), this resulted in the identification of several topics which will be outlined in this section. Quotes

[3] https://fetc-gw.wp.hum.uu.nl/voorbeelddocumenten-voor-studenten-geen-fetc-gw-toetsing/

in this subsection from focus group participants have been translated from Dutch to English by a Dutch native speaker.

The first topic of interest is a potential *policy* focus area. Including a policy focus area was considered but in the end, the decision was made not to include it (see subsection 5.3.5). This omission was noticed by the participants who initially indicated that they expected policy to be mentioned. Participant 5 said:

> You would want to determine per organisation whether a privacy-by-design policy has been approved already or if a policy is in use. …I am thinking out loud so I do not know for sure if it even should be included, but it is my first thought.

Participant 1 referred to other maturity models on this matter "So in other [maturity models]: ISOM, CMMI, policy is often required". Upon further examination and asking whether there is a desire for more explicit integration of policy in the maturity model, some of the difficulties with adding a policy focus area became clear. Participant 2 stated:

> Yes, although I do not know what kind of degrees [of maturity] it has. Then it ends up being: do you have a policy or not? That is how it feels. Do you have a general policy where all these elements [focus areas] are addressed? … I understand that it is possible to formulate degrees [of maturity] for these focus areas, but I find it more difficult to do that for policy. Perhaps that is why it is problematic.

An idea of how a policy focus area could be approached was brought up by participant 5:

> If you have formulated a specific privacy-by-design policy, which includes certain statements, you could use that to make more targeted statements. …You can then perhaps formulate policy on policy. So, you have a general encompassing privacy-by-design policy for organisation 1 which includes certain privacy principles. You can then, for example, make targeted statements regarding certain products or services provided by organisation 1—deduct additional policy, specific to particular products or services.

A different perspective on the matter was provided by participant 1:

> Or you have policy and the question becomes: is the organisation adhering to the policy? You can have a formulated policy but how do you translate that …into practice? Is it abided by within the organisation? That could be a kind of degree [of maturity].

The researchers pointed out that checking for adherence would perhaps be more suitable for the monitoring focus area which is already included. Additionally, some of the motivations regarding excluding policy were shared, the suggestion was made that the difficulty with adding a policy focus area is perhaps tied to the level of abstraction—adding a policy focus area to a privacy management maturity model would be an easy decision. Participants 1, 2, and 5 understood the difficulty of adding a policy focus area and agreed with the decision to exclude it since the group was not able to formulate a

meaningful maturity development path for it and since policy elements are somewhat contained in already existing focus areas.

A different focus area that was also the subject of discussion was the *awareness* focus area. Participant 3 stated that they expect awareness to be addressed earlier "they need to realise that it involves personal data. If you are not aware of that, I believe you will blunder in regards to this whole principle. So, awareness should be addressed earlier in my opinion". Participant 2 and 5 agreed with this, participant 4 said, "I expect awareness [in level one], it starts with that". The first capability of awareness is part of maturity level two and prescribes targeted training for specific stakeholder groups, participant 5 wondered whether the transition from level zero to the first capability is not too big: "I wonder, the step from zero to A, is that indeed a logical step or is that a very big step?". A suggestion was made to add an additional capability in the awareness focus area at level one maturity. Targeting specific groups with training is not what the lowest level of awareness maturity should be, according to participant 2 and participant 3. Adding a general awareness of privacy-by-design capability at level one was supported, participant 3 said:

> What I often see going wrong is that people do not even know what personal data is, they have doubts regarding that, let alone having them actually conduct a PIA. …If you do not even have that [basic knowledge], then you will not do the rest either in my opinion. The starting point is so crucial. So, I believe you cannot do without [a level one awareness capability].

An additional change regarding the awareness focus area that was proposed, is moving the part of capability B that prescribes executive support to the newly suggested level one maturity capability. Participant 1 said, "that [management commitment] comes first, in my opinion. That forms the basis for any commitment at all within the organisation". Participant 2 somewhat disagreed with this and stated "I think that you can already have an idea and do things based on the principles which you have gained in other places or your studies before management says that it is important". Participant 5 added:

> Privacy-by-design can be developed on the work floor by people who have enough knowledge and vision and who do not wait for a manager to initiate something. Insofar you can [start without management]. But sooner or later at a higher level of maturity, you will want to involve management and make them act. …If you want to enact changes then you must have commitment on the executive level. Else you will never get it [privacy-by-design] accepted within the organisation.

The third topic of discussion relates to the first capability of the *technology* focus area, this capability prescribes the usage of encryption at rest and in transit. Participant 2 commented, "I find that 'personal data is encrypted in transit and at rest' quite good if that is already level one. I would do that one later". A distinction between encryption at rest and encryption in transit was made in regard to their maturity. The focus group pointed out that encryption at rest is a rather high-level measure which most companies do not employ, participant 1 concluded that encryption at rest could not be a level one capability because barely any company would get past level zero. Encryption in transit should be at a lower maturity level than encryption at rest, in the opinion of participant 2. Participant 5 suggested something different for level one: "I was thinking about access control. The way you enter the system, user-ID, password. That you get access to specific data, I would take that as level one". This comment triggered participant 4 to propose role-based access as a level one capability in the technology focus area, ensuring separation of responsibilities through an authorisation matrix. The discussion was pivoted by participant 3 by questioning whether the mentioned measures are not just requirements rather than capabilities, they said:

> Should it not say that there has been some sort of an assessment? A security assessment. Because once again, it is giving substance to something which has not been ascertained yet. …You cannot implement a default measure for data protection. That is my objection. I think you should have performed at least a security assessment or a risk assessment. It could be the PIA or a security assessment or whatever, which maps out what needs to be done for the proposed initiative.

Participant 2 wondered what focus area would contain this security assessment and asked whether it is part of *monitoring*. Participant 5 did not see it as monitoring and indicated that a security assessment is the same thing as a risk analysis while participant 4 stated that the suggestion of participant 3 should be part of the PIA.

The fourth topic that led to some discussion is the omission of most legal requirements from the model and the assumption that an organisation should first focus on compliance before starting to develop privacy-by-design in-depth. Participant 2 and participant 5 were initially puzzled by this decision. Participant 3 commented:

> It depends, because even if your organisation is not compliant with GDPR you can still choose to develop that through the initiative at hand. I sometimes get a DPIA which makes me question whether the rights of data subjects are facilitated correctly. I question them about it and then they reply 'Thanks for letting us know, we will fix it'. You can interpret it as a trigger to become more mature within the organisation. If your assumption is that you should already have it [compliance], then I believe that to be a weird assumption, I cannot imagine it.

Additionally, the example of a start-up company starting from scratch was provided by participant 3, they questioned whether it could apply privacy-by-design. The researchers elaborated upon the design decision and explained that it is not obvious for an organisation to develop their PbD practices before building some foundational structures. Participant 2 said:

> But I think that you can develop those basics, that is column A, fairly quickly without being completely GDPR compliant. I think they [compliance and maturity development] can intertwine. There are companies and other organisations that are not compliant with GDPR and get fined for that, but perhaps they do have a privacy-by-design policy. I do not see a hard distinction and do not believe you need to be absolutely compliant before you can start with this [PbD maturity development]. I think that it can happen simultaneously.

Further discussion led to the consideration of the maturity model goal. The group came to the consensus that the goal of the model is not to measure compliance but to develop PbD capabilities. With that in mind, participant 2, participant 5, and participant 3 stated that they did not expect the model to encompass legal requirements so that it can be used to measure compliance. On this matter, participant 2 commented:

> No, I do not expect that. I think that is a whole different story. You will get a ruckus about how to interpret the GDPR and indeed what you just said, it [necessity to apply PbD] is mentioned somewhere [in the GDPR]. Somewhere it tells you to apply privacy-by-design and that is it, you are now compliant. I find the degrees of maturity like they are presented here, something you can grow towards, something that has an evolution, while GDPR compliance is either yes or no.

Another interesting discussion topic was the privacy-by-design lifecycle, more specifically the start point and end point. Participant 3 was adamant about starting PbD as early as possible:

> The choice is: do we use personal data or not? Do we want to process that? That is a by-design choice. You have done nothing yet with security and nothing yet with third parties. Do we even want that? That is where it starts for me. If you determine that you do not want to do this [process personal data], then this whole idea is not relevant anymore. …I believe also that it starts as early as possible. You can choose whether to process personal data and which data. Why do we need this data? You are already somewhat applying the principles before you can start the processing. So in my definition of privacy-by-design, it begins really early in the design starting with the idea—we want an application, why do we actually want an application? It starts with this [question].

Participant 1 added:

> It really starts with the PPM-procedure [project portfolio management], so determining what it is you really want to purchase or what project you want to start. The PIA process happens much later, you already have identified whether the PIA is really necessary and whether sensitive personal data is in play. You have a need which is formalised in the PPM-procedure. The pre-scan [PIA threshold analysis] is performed also within the PPM-procedure and then the PIA is performed and the tool is purchased based on the requirements which are partially elicited from the PIA.

Participant 1 and participant 3 agreed that privacy-by-designs starts with formulating the needs that the project is going to satisfy and asking whether personal data are going to be processed and whether that processing is the right solution to satisfy the formulated needs. Both participants also gave examples indicating that discussing privacy in this early phase can be difficult for non-privacy roles within an organisation. Participant 1 said:

> You can set it up in a way that a security or privacy officer is part of formulating the needs. I know for example that at organisation 2 there is an intake form to specify the

> needs accurately. It has certain requirements. My colleagues find it quite difficult to determine whether a PIA is necessary. They cannot fill out that form on their own so you could propose that our PPM-process or project management ensures that a security or privacy officer joins in to provide input and help decision-making around privacy-by-design.

Regarding the end of privacy-by-design, the group asked the researchers what their definition of PbD is and when the process ends. This thesis has already stated that the definition used is: the embedding of privacy concerns in the lifecycle of data, systems, and processing activities. This implies that PbD ends when the processing activity ends, the data is deleted, and the system is taken offline. The participants did not object to this definition, participant 3 stated "PIA is a living document that progresses with the initiative which happens continuously, until you decide to quit entirely with the processing activity. That is indeed true, that is how it really ends, once it is gone".

The last major subject is the decoupling of the PIA process and PIA report as well as adapting PIA reports to a stakeholder audience. The group struggled with envisioning how this would work in practice, participant 3 stated:

> I think that I am not yet understanding the decoupling. I believe that separating your PIA would mean that you are distilling and summarising and then you target management—this is a management PIA and this one is a work PIA? I am not feeling it, I wonder is it still a PIA then? If you are going to dissect and rehash it and make a management version, I wonder if it then still should have the status of a PIA.

Connecting the publishing of a PIA report to organisational maturity was difficult for participant 1. Similarly, participant 3 thought that it should not be tied to maturity and provided an example of a company that might have secret technology which it does not want to leak to competitors. It would not be of the highest maturity if it purposefully chooses not to share its PIA report. Those companies should still publish essential documents in the opinion of participant 5, although they were doubtful if the PIA is one of them. The researchers pointed out that redacting or editing the PIA is a possibility as just publishing everything without thought would not constitute high maturity either. Participant 5 agreed with this statement, sadly there was not enough time left to continue discussing this matter.

The last two paragraphs of this section highlight some smaller observations and comments from the focus group session. The relationship between privacy and security came up where participant 3 immediately linked privacy-by-design to security-by-design. This tight coupling was supported by participant 1, who stated that there is a dependency and that neglecting security can also affect privacy measures. Participant 4 and participant 5 added the sidenote that the intertwined relationship between privacy-by-design and security-by-design only exists in the context of personal data protection—a system regulating water infrastructure has nothing to do with personal data or privacy protection, yet one would still want to have their security measures in order for such a system.

A question was asked about the inclusion of storage limitation and information management by participant 3. Storage limitation is encompassed by the *processing principles* focus area and information management or data governance is out of scope. Related to the topic of not addressing compliance explicitly, participant 1 asked whether a different maturity model should be used prior to the proposed model in question. The researchers recommend building the privacy fundamentals before applying the privacy-by-design maturity model, (partially) applying a different model first, such as a privacy management model (e.g., Centrum informatiebeveiliging en privacybescherming, 2017), could be a structured way of tackling this challenge for an organisation that is still in its infancy. No other missing focus areas were identified by the group and the current 14 were deemed sufficient.

The focus group lasted two hours which is not nearly enough to examine a complex model which contains as many elements as this one, performing additional validations is certainly something that should be considered for future work.

6.5 Model revision

This section outlines the changes made to the model based on the synthesis from the focus group data which has been described in the previous section. A new version of the model is presented which is the final result of this validation. The synthesis has led to the identification of eight changes which are shown in Table 16. Three focus areas have been affected by the changes, these are further discussed in detail.

Table 16: Maturity model changes resulting from the focus group.

Type of change	Description
Capability reformulation	In technology A the mention of encryption at rest is removed and purpose-based access is added.
Capability reformulation	In processing principles A the GDPR specificity is removed from the processing principles.
Capability reformulation	In processing principles B the GDPR specificity is removed from the processing principles.
Capability reformulation	In processing principles D the GDPR specificity is removed from the processing principles.
Capability maturity change	Awareness A is relabelled to awareness B.
Capability maturity change	Awareness B is relabelled to awareness C.
Capability maturity change	Awareness C is relabelled to awareness D.
Capability addition	A new capability A is added to awareness which includes general PbD awareness and management support.

The first focus area that has been changed is the *technology* focus area (Table 17). In the opinion of the focus group participants, encryption at rest and encryption in transit are not part of the same maturity level. Additionally, comments were made about encryption as a whole being a specific measure instead of a capability. This thesis agrees with encryption at rest not being something ubiquitous and it indeed is more of a specific requirement than a general capability as few organisations would have the need for it. The parts of technology A that mention encryption at rest have therefore been removed from the model. Concerning encryption in transit, this thesis argues that encryption in transit is a basic and standard measure nowadays which can be applied by requesting a digital certificate. There are current initiatives that provide this service freely, automatically, and securely (e.g., Let's Encrypt, 2023). Thus, encryption in transit has been retained in capability A of the technology focus area. A different suggestion that the participants made is the inclusion of role-based access. This thesis agrees with the suggestion of limiting data access, yet role-based access has been slightly modified into purpose-based access to be more aligned with the processing principles. The purpose limitation principle states that data can only be collected for the specified purposes and cannot be processed further for non-specified purposes, the main limitation for data access is thus the motivation rather than the person. Lastly, a security assessment was suggested by a participant. This suggestion is disregarded as security has generally been treated as out-of-scope, moreover (elements of) such an assessment could be part of the PIA.

Table 17: Technology focus area capability reformulations.

Capability	Version	Description
A	Previous	Personal data is encrypted in transit and at rest.
	New	Purpose-based access is used to limit access to personal data so that it can only be accessed for legitimate processing activities. Personal data is encrypted in transit.

The next focus area that has been modified is the *processing principles* focus area (Table 18). This focus area prescribes the application and facilitation of the GDPR processing principles—one of the rare inclusions of legal requirements. The discussion regarding the purpose of the model and the inclusion of legal requirements so that it can be used to measure compliance resulted in a consensus that the participants do not expect the model to include them and to be used for compliance assessment. This conclusion sparked the change to remove any explicit prescription of the GDPR principles and to replace them with 'a set of processing principles'. The affected capabilities are A, B, and D. Capability A still provides the GDPR processing principles as a suggestion, but apart from that it is formulated neutrally to increase the generalisability of the model into other geographical regions and jurisdictions.

Table 18: Processing principles focus area capability reformulations.

Capability	Version	Description
A	Previous	The GDPR processing principles (lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability) are applied to all processing activities.
	New	A set of standard processing principles are applied to all processing activities (e.g., GDPR processing principles).
B	Previous	The GDPR processing principles are documented, applied in a structured and methodical manner, and periodically evaluated.
	New	The processing principles are documented, applied in a structured and methodical manner, and periodically evaluated.
D	Previous	Compliance with the GDPR processing principles is proactively managed to deliver deliberate process optimisation. Issues of non-compliance are identified and remedial action is taken to ensure compliance in a timely fashion. Automated controls prevent the deletion of personal data that would violate legal retention requirements.
	New	Compliance with the processing principles is proactively managed to deliver deliberate process optimisation. Issues of non-compliance are identified and remedial action is taken to ensure compliance in a timely fashion. Automated controls prevent the deletion of personal data that would violate legal retention requirements.

The last focus area that has been edited is the *awareness* focus area (Table 19). The focus group indicated that the step from level zero to A in awareness is too big and that they expected an entry-level awareness capability that indicates that the organisation has a basic understanding of privacy-by-design. Additionally, participants agreed that management support is vital in achieving organisational change and that it should be included in a lower maturity level. These suggestions have been incorporated by adding a new capability in the awareness focus area at maturity level one of the model. Since the first capability of awareness was part of maturity level two, none of the capabilities needed to be repositioned in the model. The original three capabilities have shifted up one maturity level within the focus area, in other words, A has become B, B has become C, and C has become D. The new capability A has been added at level one and prescribes the organisation to possess an understanding of the basic principles of privacy-by-design as well as having management supporting the application of privacy-by-design.

Table 19: Awareness focus area capability reformulations.

Capability	Version	Description
A	Previous	Different target groups involved in privacy-by-design are identified and receive training for raising awareness as well as transmitting knowledge relevant to their specialisation.
	New	The organisation is aware of the basic principles of privacy-by-design and management is committed to applying them.

B	Previous	Management is committed to applying privacy-by-design and provides resources, such as manuals, guides, and handbooks, to support consistent implementation of privacy policies, procedures, and standards, as required and appropriate.
	New	Different target groups involved in privacy-by-design are identified and receive training for raising awareness as well as transmitting knowledge relevant to their specialisation.
C	Previous	The organisation participates in learning from and contributing to the available body of knowledge amassed by the privacy community. Staff and management are comfortable identifying areas for improving privacy practices and discuss/raise these freely and proactively.
	New	Resources are provided, such as manuals, guides, and handbooks, to support consistent implementation of privacy policies, procedures, and standards, as required and appropriate.
D	Previous	-
	New	The organisation participates in learning from and contributing to the available body of knowledge amassed by the privacy community. Staff and management are comfortable identifying areas for improving privacy practices and discuss/raise these freely and proactively.

Incorporating these changes into the maturity model results in the model as depicted in Figure 32, the only noticeable change being awareness now starting at maturity level one and it having four capabilities instead of three. Adding a new capability, especially a level one capability, raises the question of whether new dependency relationships come into existence. The nature of the new awareness capability makes it somewhat of a prerequisite for most capabilities, yet these are not specific hard dependencies. Developing privacy-by-design capabilities with intent is not possible without having a basic understanding of what PbD entails. Similarly, a start can be made without management support but if organisation-wide changes are to be implemented then management support becomes indispensable. Since awareness A is a level one capability, it is already required to be implemented before any capability from higher maturity levels. The decision was therefore made to not explicitly formulate dependency relationships between awareness A and a multitude of other capabilities. This thesis does recognise the importance of this capability and recommends it to be implemented early.

		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		

Figure 32: Model version 1.1 with focus group feedback incorporated.

7 Assessment instrument design

A maturity model is operationalised by an assessment instrument which allows an assessor to perform an assessment to ascertain the maturity level of an organisation. This chapter describes the creation of an assessment instrument for version 1.0 of the privacy-by-design focus area maturity model (Figure 32).

7.1 Assessment questions

Maturity model assessment instruments typically consist of a questionnaire which ascertains whether capabilities are implemented or not, an example of such a questionnaire is included in the work by Marchildon et al. (2018). The capabilities of the focus area maturity model for privacy-by-design can be assessed by the assessment instrument through a number of assessment questions. Since some capabilities prescribe multiple practices, all 60 capabilities were decomposed into a more granular collection of a total of 186 atomic practices. Having 60 capabilities amounts to an arithmetic average of 3.1 practices per capability and 13.29 practices per focus area. The *PIA process* focus area is quantitatively by far the biggest with 29 practices, *roles* and *awareness* are quantitatively the smallest with both having 7 practices.

Initially, the intent was to convert all 186 practices into assessment questions, where a positive answer for all practices constituting a capability, would indicate the development of said capability. After discussions, the decision was made not to use the practices as assessment questions since having 186 questions was deemed as too many, having a potentially intimidating effect on assessors. One of the goals of this research is to create an artifact that can be applied in practice and help practitioners, this is thus mostly a pragmatic consideration where a trade-off must be made with scientific rigour as measuring each practice separately could provide unique insight into practice development in organisations as well as preventing the usage of complex compound capabilities which can cause confusion during the assessment process.

The decision was therefore made to use the short list of 60 capabilities for the assessment rather than the long list of 186 practices. The assessment consists of essentially only one question which asks the assessor to indicate for each capability whether the organisation applies it, has it developed, or has it implemented. The capabilities are presented per level, starting with level one, in ascending order. Only if all capabilities from the same level are answered with *yes* has the organisation reached that maturity level. During this study, the author has had several conversations with expert practitioners who indicated that they experience the incorrect application of maturity models in practice at times. Situations were described where maturity levels were reported higher than they were in reality. This could potentially be explained by a lack of knowledge or experience regarding maturity models. It is essential to remember that maturity models consist of maturity plateaus, there are no in-between levels. While informally someone might state that the organisation is at maturity level two and a half, meaning it has fully achieved level two and some capabilities of level three, strictly speaking, a maturity model does not recognise this and according to the model, the organisation is still at level two. An inexperienced maturity assessor might make the mistake to try to round up and report a level three maturity, providing an inaccurate maturity view of the organisation.

Assessment questions typically have a binary yes/no answer possibility. In order to dissuade assessors from ‘rounding up’ to a yes-answer when they don’t know the answer or when the accurate answer is ‘somewhat’ or ‘partially’, the design decision was made to add two additional answer options. The full answer options for each capability are: {no, somewhat, yes, unknown}. Under the hood, only a confident *yes* for each question will constitute maturity level achievement. The goal of this design decision is to guide an assessor to a more conservative assessment where a yes-answer is only elicited if the assessor is truly confident that the capability is fully developed. After all, an accurate maturity result depends on the accuracy of the answers that the maturity assessor provides. This somewhat mitigates the risks introduced by using complex capabilities, rather than atomic practices.

7.2 Tool support

This section describes how the assessment instrument is implemented in a tool for automatic application and results generation. It includes the motivation for the tool support as well as a description of the design and features.

7.2.1 Motivation

The results of MLR 1 (section 4.1) indicate that tool support for maturity models in the privacy domain is scarce, only 1 out of 30 models was found to have tool support with three other models being supported by Excel sheets. One of the goals of this research is to create a model that can be applied by practitioners in the field. Tool support would contribute significantly to reaching this goal as there are multiple automation opportunities in performing a maturity assessment and generating the results.

As mentioned before, performing an assessment consists of answering assessment questions. This is no different than completing a questionnaire which nowadays is often performed digitally, enjoying all benefits of modern technology. Additionally, tool support allows for the exertion of control over the assessment results, both in content and form. This allows for dynamic on-the-fly generation of a presentation artifact containing the maturity results in an informative and aesthetically pleasant format, providing increased utility and attractiveness over a standard spreadsheet approach.

The purpose of the tool is to provide practitioners with a burdenless experience in performing a privacy-by-design maturity assessment by automating the process as much as possible, removing hurdles for a smooth experience, and presenting relevant results—ultimately striving to decrease the barrier of entry and increase adoption.

7.2.2 Design

For this research, the tool support consists of a web application. This allows any user to access the assessment instrument from anywhere in the world, at any time, to perform an assessment without the need to install additional software. The entire source code for this application can be found in Appendix M. The web application can be accessed at:

https://www.privacymaturity.org/

The application is modest in size, containing a main index page, two informational pages, and the pages relevant to the assessment. The main index page contains a section that describes the benefits of focus area maturity models, a section that shortly describes the model and links to the model page, a section that shortly describes the research and links to the research page, a section with a promotional video, and a frequently asked questions section. The model page provides an overview of the model alike to its depiction in Figure 32. Hovering over the letters that denote the capabilities will show a popover with a description of what the capability entails. In addition to that, all capabilities are listed per focus area in an accordion dropdown below the model for easy reference. The research page provides a short summary of the research context, including the goal, other relevant ongoing research projects, and an explanation of the main topics of study.

The web pages mentioned so far mainly serve an embellishing role. The lion's share of the provided value comes from the implementation of the assessment instrument. Once an assessment has been initiated, each page of the assessment represents a maturity level with all capabilities related to that level. For each capability, the assessor must indicate whether the capability is implemented by choosing the appropriate radio button related to one of the four answer options. Only one answer per capability can be chosen. Figure 33 shows a screenshot of what the page looks like for level 3 of the maturity assessment. Level numbers are not shown to avoid socially desired answer patterns.

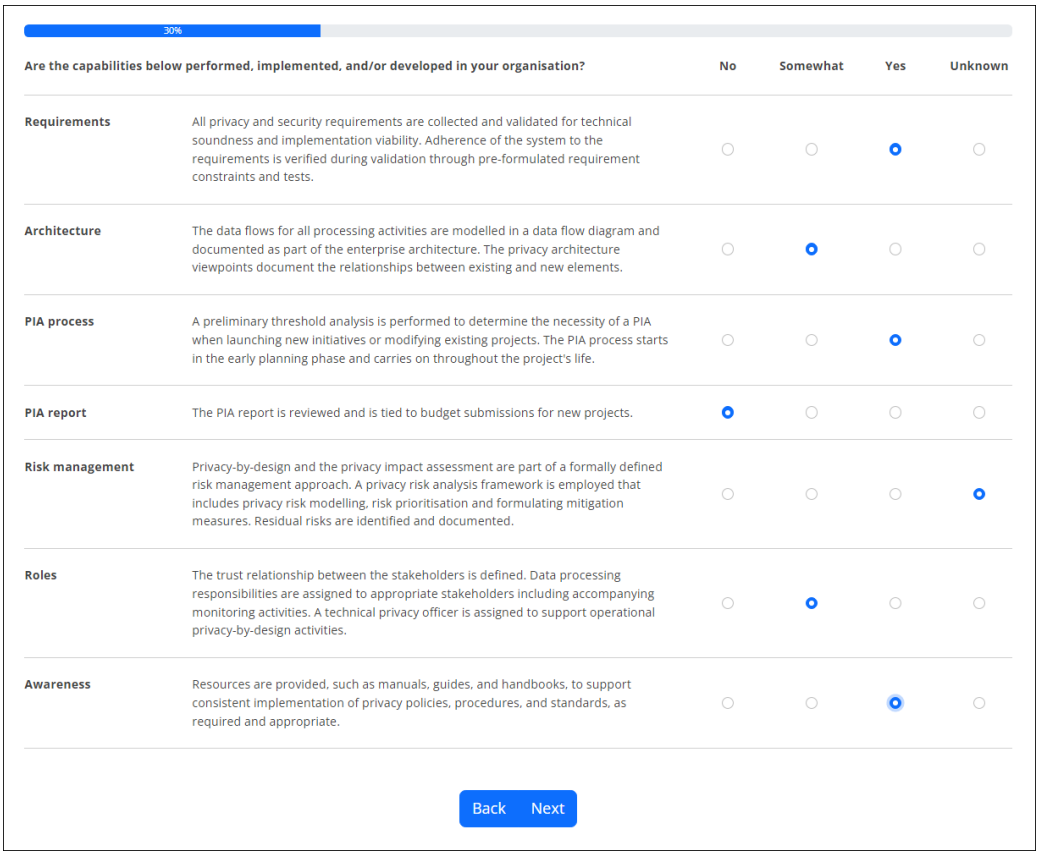

Figure 33: Screenshot of the level 3 maturity assessment page.

The maturity model contains some high-maturity practices which few organisations are expected to have implemented. The expected maturity level of organisations is thus not high. In the context of the assessment instrument, if at least one capability of a level is answered by a non-yes answer, the overall maturity can effectively be established without completing the rest of the assessment. Considering this observation in addition to the low maturity expectation, a shortcut was added to the tool that allows assessors to skip to the results as soon as the overall maturity can be established. Using this option answers all remaining questions as 'unknown' and prevents the burden of having to complete all 60 capabilities when the maturity result is known early on. If an assessor is interested in a more granular result that includes the maturity of each focus area, then they can choose not to skip and continue with the full assessment. Once an answer option has been provided for all capabilities, across all levels, the application generates a maturity report.

7.2.3 Maturity result presentation artifact

The results of the maturity assessment can be presented in various ways. The maturity presentation artifact of this application, the so-called *maturity report*, consists of two major components: the visualisation of the maturity and the improvement actions.

The standard way of displaying the results of a maturity assessment for a focus area maturity model is to colour the maturity matrix. For each focus area, the cells in the matrix are coloured according to the maturity established from the given answers during the assessment. Figure 34 shows an example of the visualisation of the maturity results: the rows are coloured up to the first capability that is not implemented, or are coloured fully in case all capabilities of that row are implemented. The overall maturity level can be deduced by identifying the numerically last column that is fully coloured, in this example the overall privacy-by-design maturity is therefore level 3.

The second component of the maturity report consists of the improvement actions. These are the activities that the organisation will have to perform in order to reach the next maturity level. While the 186 practices that are mentioned in section 7.1 were found to be not suitable as assessment questions, they are useful for the formulation of improvement actions. Revisiting the example of Figure 34,

capability C of *PIA process* and capability B of *PIA report* must be implemented for the organisation to reach the next maturity level (level 4). The maturity report contains an overview of the capabilities that must be implemented to reach the next level. Each of these capabilities contains a breakdown of the constituting practices which are presented as improvement actions, this provides practitioners with concrete bite-sized steps towards higher maturity. Figure 35 provides an example of the improvement actions that correspond to the maturity example of Figure 34. The maturity report generated by the tool can be downloaded as a PDF-file for future reference, Appendix N contains a full example of a downloaded maturity report.

		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		

Figure 34: Example of the diagram displaying the results of a PbD maturity assessment.

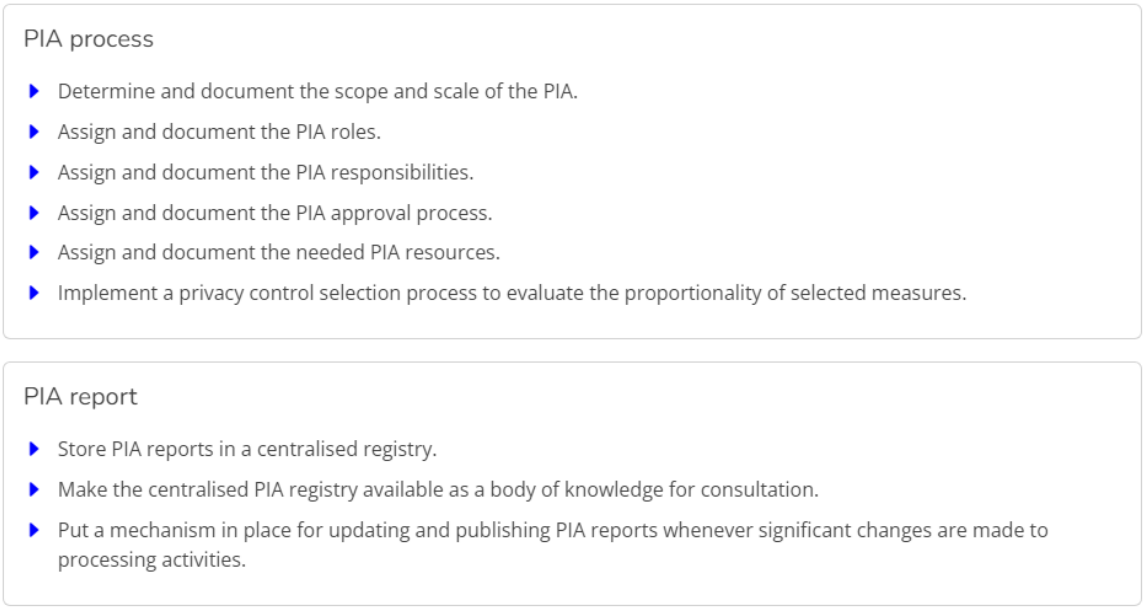

Figure 35: Example of improvement actions for two capabilities.

7.2.4 Tool architecture

The tool is a Python 3.9 web application built using the Flask[4] micro web framework (version 2.0.0) for the back-end, the Bootstrap[5] toolkit (version 4.0.0) for the front-end, and a MySQL database for storage. Figure 36 provides an overview of the high-level components and communications including the used frameworks. Users communicate with the web application by visiting the webpages, these use HTML and CSS for the structure and visualisation, the assessment and evaluation questionnaires contain JavaScript code supporting the presentation of the questions as well as functionalities such as detecting when the maturity can be determined, allowing the assessor to skip the rest of the questionnaire.

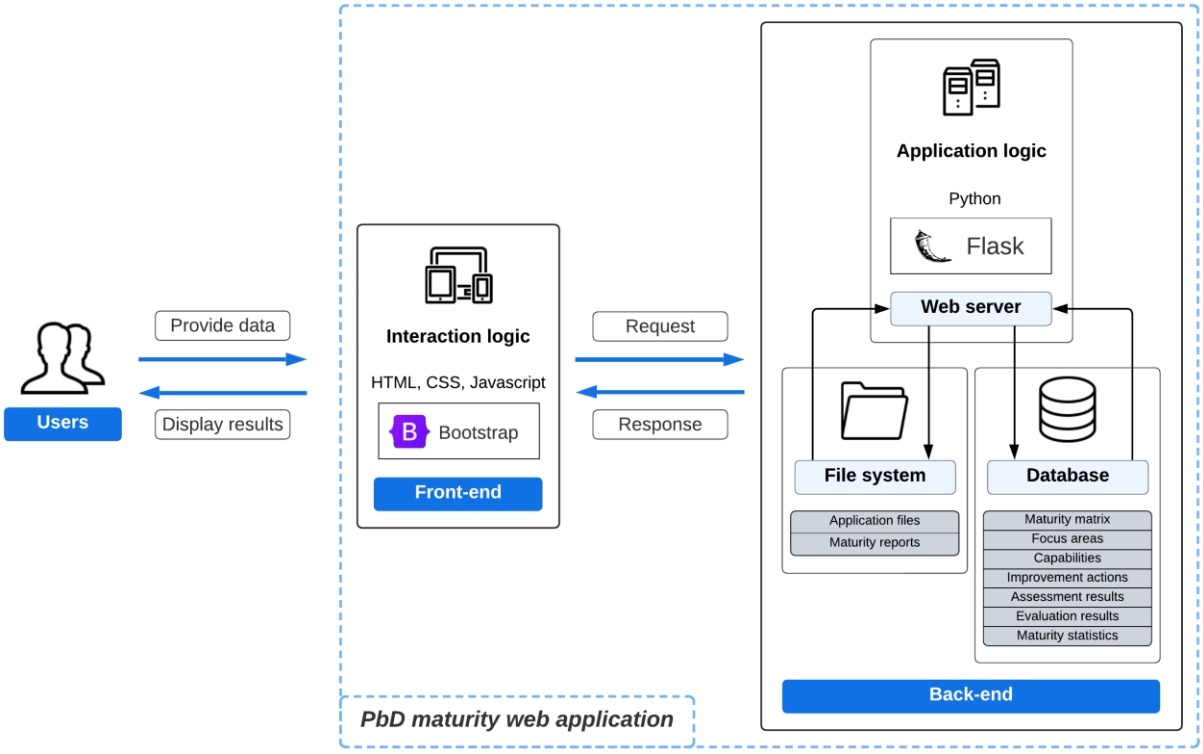

Figure 36: High-level overview of the application architecture including used frameworks.

The back-end consists of a web server for the application logic and uses a file system and database for storage. The file system contains the application files and the generated maturity reports. The database stores the model elements, including the maturity matrix, focus areas, capabilities, and improvement actions, as well as the answers to the assessments and evaluations, and the resulting maturity statistics. The application logic is handled through Flask using Python code. Flask allows webpages to route to certain endpoints which handle the appropriate processing logic for HTTP methods. Figure 37 provides an overview of all endpoints, including URL-routing, return value, and client communication. The `app.route()` decorator maps the URL to a specific function that handles the logic for that URL. Most of the webpages do not require additional processing thus only have a `GET` request associated with them which returns the relevant HTML file. The endpoints that do contain processing logic, gain input data from the user through `POST` requests.

Figure 38 shows all endpoints that contain data processing logic and the interactions between them, the client, the database, and the file system. The majority of the logic is associated with the assessment and evaluation questionnaires. A user that desires to perform an assessment is directed to the *assessment introduction* page which provides general information about the assessment. Additionally, it contains an informed consent notice and it requests the user to specify whether they want to participate in the

[4] https://flask.palletsprojects.com/
[5] https://getbootstrap.com/

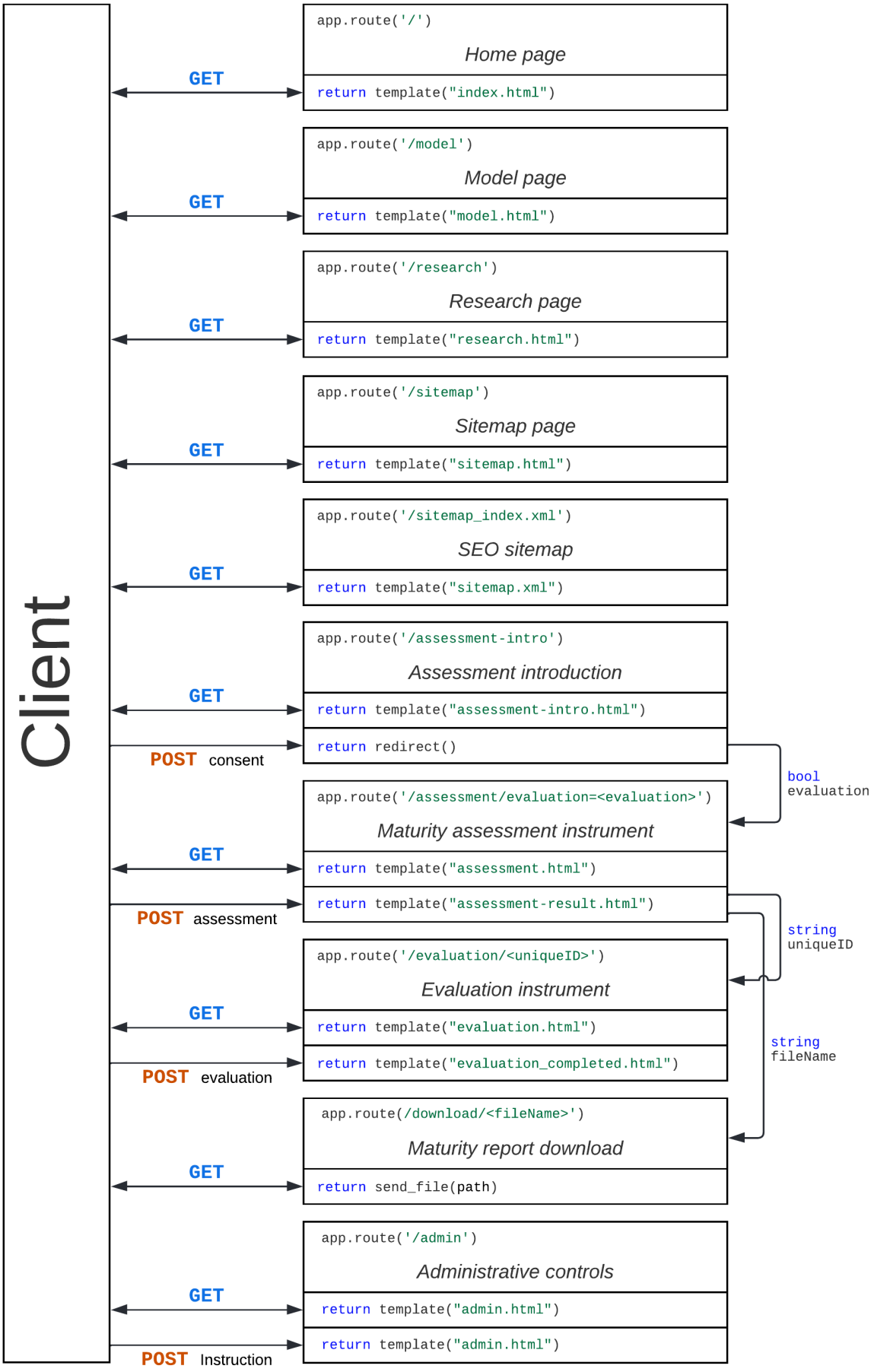

Figure 37: Overview of application endpoint routing and HTTP communication.

evaluation after performing an assessment. The consent choice is registered as a Boolean value and returned to the webserver which redirects the user to the *maturity assessment instrument* page. Upon completing the assessment questionnaire, the forms containing the answers are submitted to the web server for further processing. The application logic corresponding to this endpoint handles the formatting of the results, saving the assessment results to the database, creating a model object based on the answers, and generating a maturity report which is saved in the file system. The filename of the maturity report is passed on to the appropriate *maturity report download* endpoint which can retrieve the file from the file system and send the file to the user if they decide to download their maturity report.

The Boolean value denoting the consent determines whether the user will get an evaluation prompt on their results screen. In the case where the evaluation is to be performed, the user is redirected to the evaluation instrument endpoint which contains the evaluation questionnaire. Upon completion, the forms with the answers are submitted to the web server which formats the results and saves them to the database. A universally unique identifier is generated for each user and is passed around so it can be included in the database record for both the assessment result and evaluation result, allowing these to be linked for future analysis.

The last endpoint containing processing logic is the *administrative controls* endpoint. This corresponds to a shielded administration page which regular users do not interact with. This page allows the administrator to update the maturity model elements in the database by reading the CSV-files that contain the relevant data from the file system and saving it to the database, overwriting the current data.

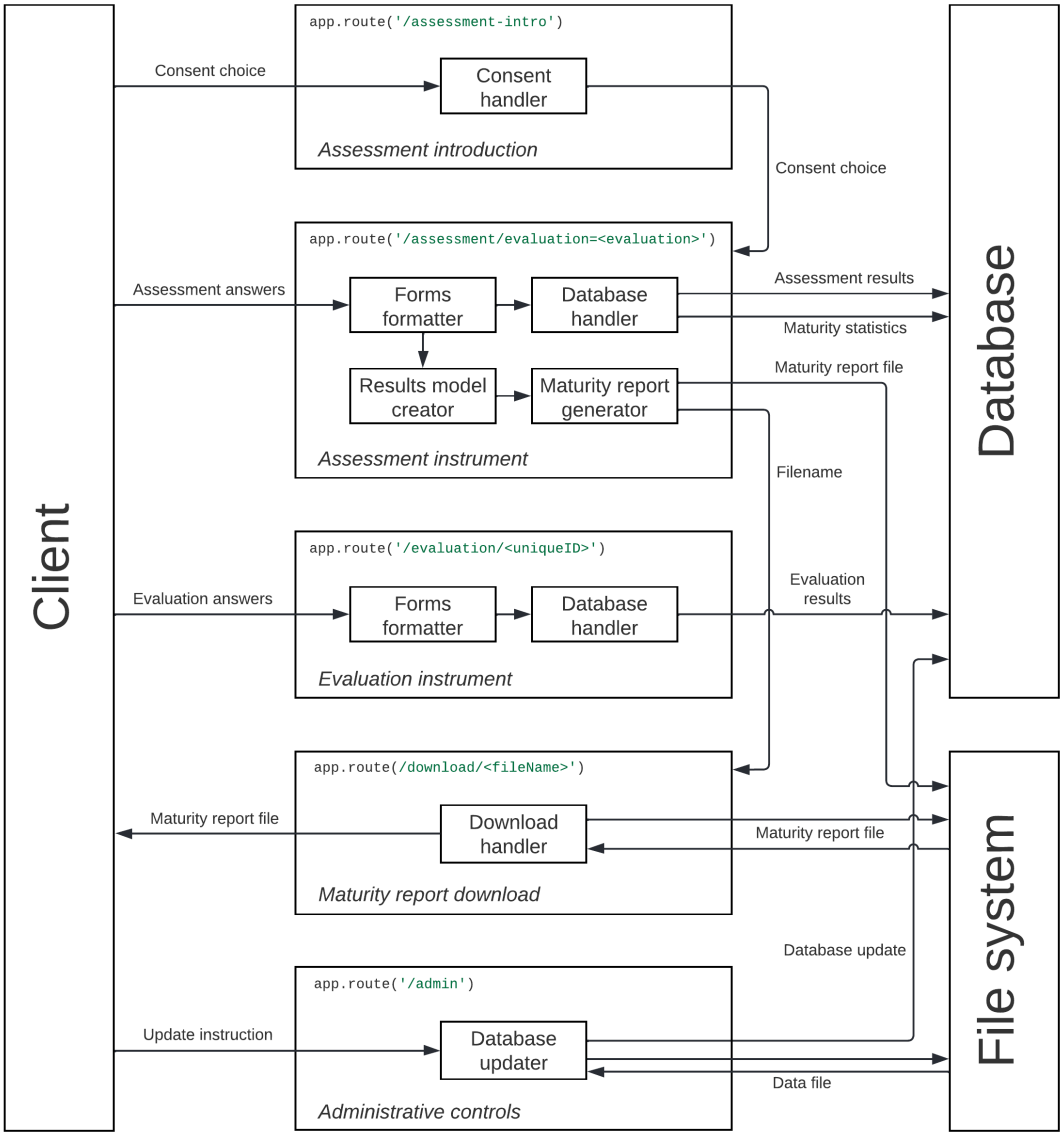

Figure 38: Logical model describing the application logic per endpoint.

8 Evaluation

This chapter describes the evaluation step of this research project which was performed through the application of a questionnaire. The sections of this chapter discuss the survey choice motivation, the questionnaire design, a pilot test, and an analysis of the results.

8.1 Motivation

The desired evaluation activity for this research can be characterised as: take the validated PbD maturity model as input, generate expert opinions after model use, and provide an evaluated model as output. Using the overview of validation/evaluation activities from Sonnenberg and vom Brocke (2012) once more, this evaluation corresponds to evaluation activity four. It takes an instance of an artifact as input and provides an evaluated artifact instance in a natural setting, the recommended methods for this activity are case study, field experiment, survey, expert interview, and focus group.

Considering that the validation in this research consists of a small-scale focus group, there is a need to introduce the artifact under investigation to a broader audience. Therefore, the decision was made to make use of the survey method through a questionnaire. Questionnaires are convenient instruments to collect quantitative data for specific evaluation criteria. Using a digital questionnaire allows for the easy introduction of the model to practitioners from different organisations, different countries, and different legal systems, which increases the external validity of the results and can provide useful feedback from new perspectives.

Additionally, the maturity assessment itself consists of a questionnaire, using an evaluative questionnaire on top of that allows for seamless integration of the evaluation activity into the assessment instrument. This reduces the burden for evaluation participants who do not have to perform the assessment and then switch to a different application for the evaluation.

8.2 Evaluation design

According to Patten (2017), the first step in conducting questionnaire research is to specify the objectives of the research. In this case, the questionnaire is used for the evaluation of an artifact. The objective is thus to evaluate the privacy-by-design focus area maturity model by practitioners, who have performed an assessment, in terms of a number of evaluation criteria. The evaluation criteria used for this questionnaire are selected from the taxonomy of evaluation methods for information systems artifacts as presented by Prat et al. (2015). Table 20 shows the criteria with their original definition as well as the adapted form that is used in this research. A similar design has been used by Overeem et al. (2022) for the evaluation of a focus area maturity model for API management.

Table 20: Evaluation criteria selected from Prat et al. (2015) and adapted for this research.

Evaluation criterion	Definition
Effectiveness	**Prat et al.:** the degree to which the artifact achieves its goal in a real situation.
	This research: the degree to which a privacy professional can achieve privacy-by-design maturity assessment and development by using the privacy-by-design focus area maturity model.
Operational feasibility	**Prat et al.:** the degree to which management, employees, and other stakeholders, will support the proposed artifact, operate it, and integrate it into their daily practice.
	This research: the degree to which privacy professionals will support, integrate, and make use of the privacy-by-design focus area maturity model in their privacy-by-design maturity assessment and development practices.

Usefulness	**Prat et al.:** the degree to which the artifact positively impacts the task performance of individuals.
	This research: the degree to which the privacy-by-design focus area maturity model positively impacts privacy professionals in assessing and developing maturity.
Ease of use	**Prat et al.:** the degree to which the use of the artifact by individuals is free of effort.
	This research: the degree of difficulty for privacy professionals to use the privacy-by-design focus area maturity model in assessing and developing maturity.
Structural completeness	**Prat et al.:** the degree to which the structure of the artifact contains all necessary elements and relationships between elements.
	This research: the degree to which the privacy-by-design focus area maturity model is complete; all relevant and required focus areas, capabilities, and dependencies are included.

The questionnaire asks practitioners to indicate how they feel about the maturity model in relation to the criteria listed, the intent is thus to measure practitioner attitude. A common way of measuring attitude is through Likert-type items (Patten, 2017). In order to facilitate this, the adapted definitions from Table 20 are reformulated into declarative statements. The full set of statements is presented in Table 21, the questionnaire asks participants to indicate to what degree they agree with each statement on a five-point scale ranging from *strongly disagree* to *strongly agree*. The evaluation questionnaire presents these statements in an order that alternates the evaluation criteria and contains three negatively formulated statements, following the guidelines of Patten (2017) to mitigate the *halo effect* and mitigate individuals having an *acquiescence* response set.

Table 21: Evaluation statements for each evaluation criterion.

#	Evaluation criterion	Statement
1	Effectiveness	I am able to assess the privacy-by-design maturity by using the privacy-by-design focus area maturity model.
2	Effectiveness	I am able to formulate a development path by using the privacy-by-design focus area maturity model.
3	Operational feasibility	The privacy-by-design focus area maturity model is likely to be supported, used, and integrated by privacy professionals in their privacy-by-design maturity assessment practices.
4	Operational feasibility	The privacy-by-design focus area maturity model is likely to be supported, used, and integrated by privacy professionals in their privacy-by-design maturity development practices.
5	Usefulness	The privacy-by-design focus area maturity model positively impacts my ability to perform a privacy-by-design maturity assessment.
6	Usefulness	The privacy-by-design focus area maturity model positively impacts my ability to formulate a privacy-by-design development path.
7	Ease of use	I find it easy to assess the privacy-by-design maturity by using the privacy-by-design focus area maturity model.
8	Ease of use	I find it easy to formulate a privacy-by-design maturity development path by using the privacy-by-design focus area maturity model.
9	Structural completeness	The privacy-by-design focus area maturity model contains all required focus areas.
10	Structural completeness	The privacy-by-design focus area maturity model contains all required capabilities.

Besides the 10 evaluation questions mentioned above, the evaluation contains 3 demographic questions asking for the country that the organisation is located in, the size of the organisation in terms of the number of employees, and an indication of the importance of privacy and data protection within the organisation expressed as a five-point Likert scale. This information is collected to gain insight into differences in both the maturity results and the evaluation results between different demographics. The last component of the evaluation questions consists of two optional questions which allow participants to provide qualitative feedback on positive and negative aspects of the model and the assessment.

8.3 Assessment instrument integration

The assessment instrument and the evaluation instrument used in this research are both questionnaires. This coincidence creates the opportunity for the integration of both instruments into a single experience (Figure 39), providing a convenient, quick, and seamless process for an evaluation participant. To achieve this integration the web application requires expansion.

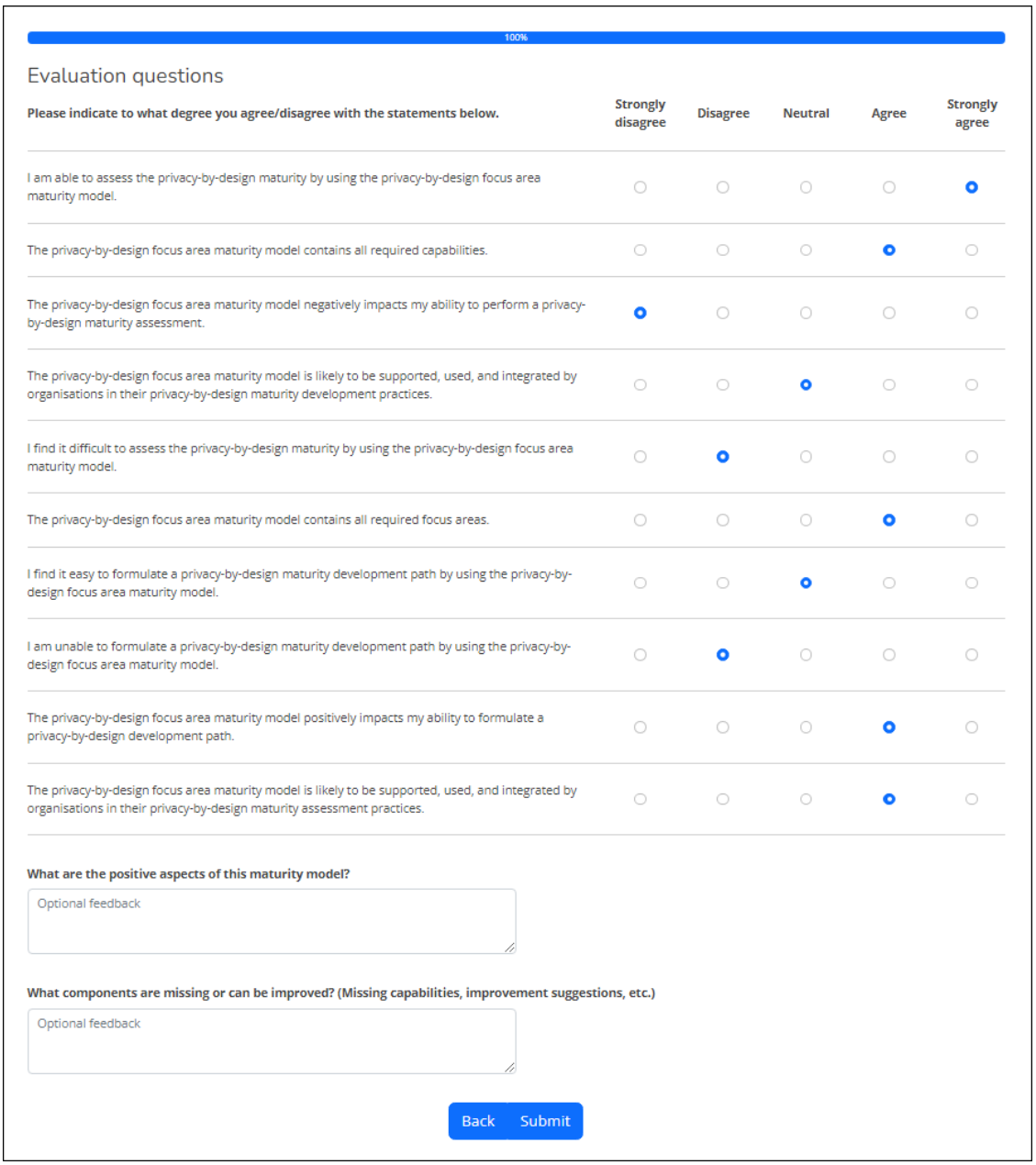

Figure 39: The evaluation questions pertaining to the evaluation criteria.

The first change consists of adding an assessment introduction page. This page allows an assessor to choose whether they want to participate in the study. It includes an informed consent notice (Appendix O) similar to the one used in the validation, describing the overall research project and the purpose of the evaluation. It informs potential participants of the inducements, costs, and risks, it emphasises the voluntary nature of participation, it explains how the collected data will be handled and processed, it details the participant's rights including the ability to quit at any time, and it provides contact information for questions or complaints. The consent form ensures that the participant has been informed sufficiently before participating. Participation must be confirmed by selecting the appropriate radio button, not consenting to participate will still allow a user to perform an assessment without evaluation.

Once the user starts the assessment, they will be presented with the assessment questionnaire which consists of the maturity assessment questions. Upon completion of the assessment, the user is provided with the maturity report which shows the assessment results. If the user has indicated to participate in the study, the user will be prompted to start the evaluation. The evaluation questionnaire will open in a new tab allowing the user to reference their maturity results while completing the evaluation. The first page of the evaluation consists of the demographic questions, while the second page contains the 10 evaluation questions that measure the selected criteria as well as optional text areas for positive and negative feedback.

8.4 Pilot

A pilot test was conducted with a limited number of test subjects to run the evaluation to ensure participants will not encounter issues during the full rollout. Six expert practitioners were requested to perform the evaluation, of which four did. No major problems regarding the evaluation process were reported. Positive feedback included consistent language usage, clear explanation, and the results providing a solid foundation for a multi-year strategy. Other observations stated that the model is quite strict and that it is rather disappointing that answering 'somewhat' to a capability is represented in the results as non-development. This portrays the organisation in a rather negative light and inhibits the usability of the maturity report when passed on to management or the board. An example was provided where a capability can be basically developed, but not yet adopted throughout the entire organisation. The assessment question that asks to what degree this capability is developed should strictly speaking be answered with 'somewhat'. In doing this, the resulting maturity report would imply that no development at all has taken place, even though the organisation might be hard at work in finalising the development of the capability in question. The feedback presented a demand for the visualisation of capabilities that are not achieved, yet are being worked on.

8.4.1 Artifact revision

Following the pilot test, the provided feedback was analysed and converted into revision actions. The main suggestion for a revision came from the desire to visualise capabilities that are partially developed. To implement this suggestion, the maturity results on the web application and the downloadable maturity report would have to be expanded. Full capability development is denoted in the matrix with a full colouring of the respective cell. The decision was made to add a partial colouring for capabilities that are partially developed, an example of this new visualisation is shown in Figure 40. The partial colouring is limited to sequentially consecutive partially developed capabilities. A similar decision was made for the visualisation of fully developed capabilities: isolated hanging capabilities are not visualised, be it fully developed or partially developed. The intent of this decision is to keep the model as intuitive as possible in visualising the maturity level and capability development, and avoiding the introduction of unnecessary complexity.

Naturally, visualising the development of disconnected capabilities can be explored in future work, using colour differentiation between connected and disconnected capabilities might add additional information regarding the capability development without adding too much potential for confusion. This can be a component of a broader investigation into the design of a maturity presentation artifact. While the initial intention of this study was to generate a maturity report which can serve as input for a more comprehensive reporting document which will be presented to a board or management, the feedback

generated by the pilot test indicates this might be a naive thought—what can happen is that practitioners will perform a self-assessment and ship the generated PDF-file as-is to their management. This changes the design perspective of the generated maturity report which might have to be adapted through future research to be able to fulfil the demands of the role of a standalone management report.

		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		

Figure 40: Example of the revised results with partial capability development visualisation.

8.5 Synthesis

Subsequent to the pilot test, a full evaluation was rolled out. An invitation to participate in this study was spread through the network of colleague researchers and posted on public platforms such as LinkedIn and Reddit. This subsection describes the results of the full evaluation in terms of the assessment questions and evaluation questions of the survey.

8.5.1 Maturity assessments

The data collection started in the spring of 2023 and lasted for about six weeks. During this period, 25 assessments were performed including the pilot test. Two assessments were discarded during the data cleaning. Considering they answered all 60 questions in just over 2 minutes, it is likely that these respondents were testing the assessment instrument rather than performing a legitimate maturity assessment. The results of the remaining set of 23 assessments are discussed in the remainder of this subsection.

Looking at the overall PbD maturity, 22 assessments resulted in maturity level 0, meaning that these organisations have not implemented all capabilities of level 1. A single assessment resulted in maturity level 1. These results indicate that the overall PbD maturity is low. A more granular overview of the maturity per focus area is presented in Table 22. The first notable observation is that the minimum levels are not zero for each focus area, this could indicate that those early capabilities are implemented more often. In this case, this is a misleading conclusion because of the way the maturity levels before the first capability are registered. Not all focus areas have their first capability in level one, the *risk management*

focus area, for example, does not have its first capability till level three. This results in the minimum level for *risk management* always being level two since the first two levels are accomplished by default. In this case, the minimum values in Table 22, therefore, represent the state with no capability development at all for each focus area. This should also be considered when examining the mean values. The *monitoring* focus area has one of the highest mean values but in reality, it is barely over the minimum value.

Table 22: Descriptive statistics for maturity level per focus area (N=23).

#	Focus area	Minimum	Maximum	Mode	Mean	Std. Deviation
1	Requirements	0	10	0	1,57	2,253
2	Architecture	1	3	1	1,35	0,714
3	Development	0	5	0	0,70	1,608
4	Technology	0	6	0	1,65	2,145
5	PIA process	1	10	1	2,87	3,065
6	PIA report	2	10	2	3,52	2,810
7	Risk management	2	10	2	2,65	1,824
8	Processing principles	0	6	0	1,26	1,936
9	Subject rights	0	8	5	2,96	2,722
10	Transparency	0	4	0	0,65	1,152
11	Third-party management	1	10	1	2,70	3,140
12	Roles	0	10	0	1,87	3,362
13	Awareness	0	10	0	1,26	2,816
14	Monitoring	3	5	3	3,17	0,576

The maximum values show more variation compared to the minimum values. The results show that some organisations have achieved level 10 maturity for particular focus areas. Considering the low overall maturity, this indicates that the capability development is somewhat dispersed—some organisations have simultaneously highly developed focus areas and underdeveloped focus areas. Additionally, a low maximum value could imply that those focus areas are tougher to develop or have a lower priority. *Architecture*, *transparency*, *development*, and *monitoring* have lower reached maximum levels.

Comparing the minimum to the mode shows that the minimum level is simultaneously the most observed level for all but the *subject rights* focus area, further signifying the low PbD maturity. The higher mean and mode of *subject rights* show that the first capability of this focus area (9A) is one of the most implemented capabilities. This is corroborated by Figure 41 which shows the answer distribution per capability with the 10 levels demarcated by black lines. Capability 1A and 9A are the most implemented capabilities, these are both level 1 capabilities. Unsurprisingly, the capability development drops off as the capability maturity increases, especially from level 6 onwards where some capabilities are not fully implemented by any of the organisations that performed an assessment. The partial implementation of capabilities also decreases similarly, although not nearly as sharply as the full implementation.

Regarding the ‘unknown’ answers, there is a noticeable observation where this answer follows a somewhat staggered pattern with a similar value within each maturity level. This can be explained by the skip functionality which was previously described in subsection 7.2.2. If an assessor chooses to skip then the remaining questions shall be automatically answered as ‘unknown’. Naturally, the number of unknowns increases as maturity increases. Nonetheless, there is still some variation. Capability 3D, 2D, 4C, and 14D are the capabilities that assessors were the most unsure of (N=13). The first three entail formulating privacy patterns, translating patterns to PETs, and structuring the relevant processes. The last of the four is related to the periodic reviews and audits of processing activities. Considering three of the four capabilities are related to system design (*architecture*, *development*, and *technology*), it could imply that the expertise or familiarity with technical topics of some assessors is limited.

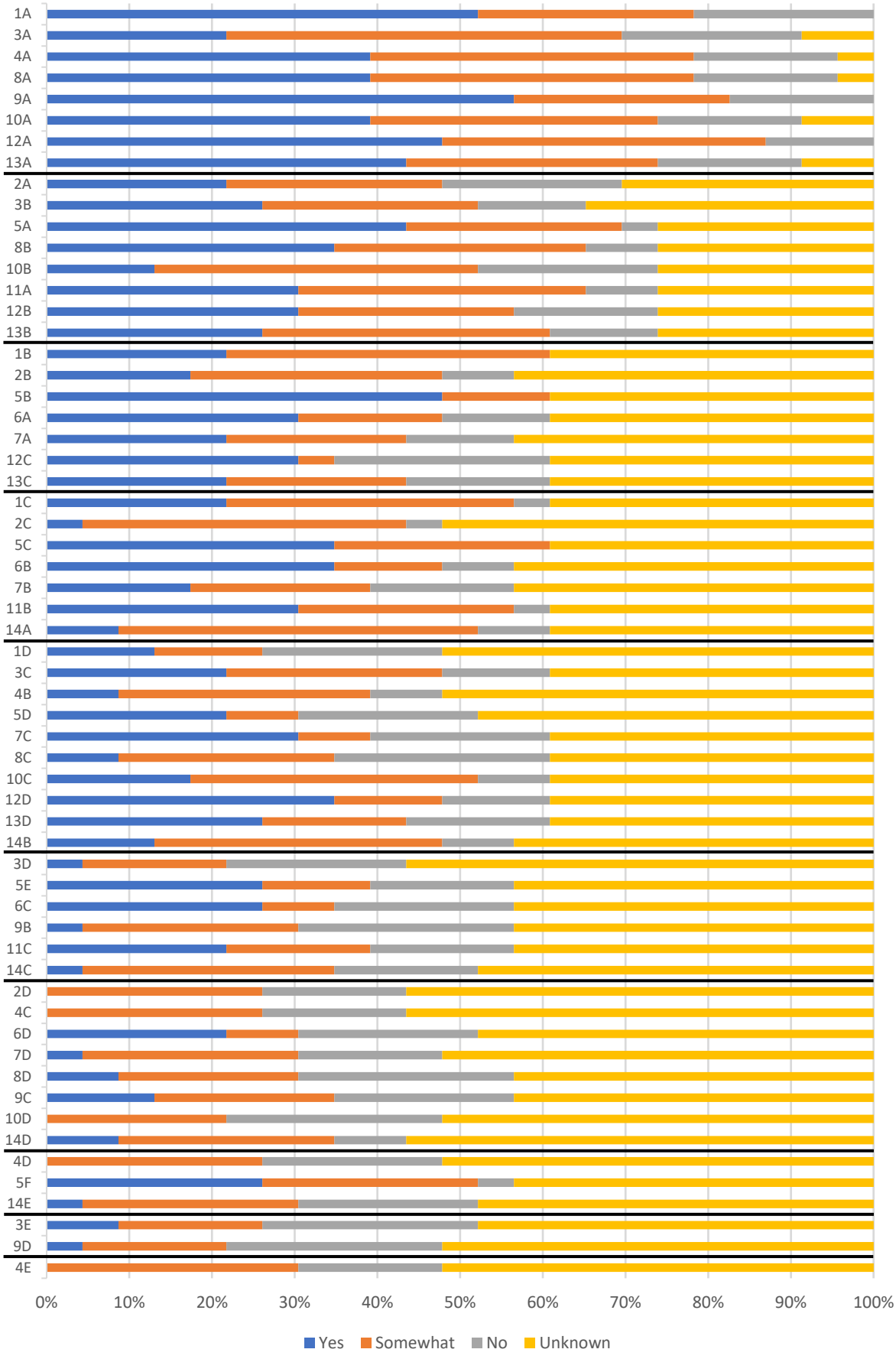

Figure 41: Distribution of assessment answers per capability with level demarcations (N=23).

Capability *roles* C, *processing principles* C, *subject rights* B, *processing principles* D, *transparency* D, *development* E, and *subject rights* D were most often marked as not implemented at all. Most of these are medium to high-level maturity, with the exception of *roles* C which is a level 3 capability and thus could be an early bottleneck. This capability prescribes the definition of trust relationships between stakeholders, assigning processing responsibilities, and assigning a technical privacy officer. A different remarkable capability is *development* A in level 1 which has the lowest value for full implementation and the highest value for no implementation within this level. This capability entails incorporating privacy requirements in low-level design and using acceptance testing to ensure these requirements are met. It seems to be an early maturity bottleneck compared to the other capabilities in level 1.

A different variable that was also tracked is the time taken to perform the assessment (Table 23). A distinction is made between assessments that used the skip functionality and assessments that did not, as this evidently influences the time it takes to perform an assessment. Assessments with a skip took just over a minute on average. Taking into account the low maturity, most of these assessments were skipped after the first level. The time taken is more dispersed for assessments where all questions were answered as evidenced by the higher standard deviation, with an average approaching 28 minutes. In general, the time taken to perform an assessment can be influenced by the manner in which the assessment has been performed, for example, one person versus a panel discussion. Additionally, the expertise and organisational knowledge of the assessor can play a role.

Table 23: Descriptive statistics for time taken to perform the maturity assessment (hh:mm:ss).

	N	Minimum	Maximum	Mean	Std. Deviation
With skip	9	0:00:15	0:03:38	0:01:08	0:01:05
Without skip	14	0:05:52	1:16:16	0:27:47	0:19:18
Total	23	0:00:15	1:16:16	0:17:22	0:19:56

8.5.2 Model evaluations

In addition to performing a maturity assessment, the assessment instrument allows users to participate in the evaluation by indicating to what degree they agree with 10 statements on a five-point Likert scale. The five evaluation criteria have been previously detailed in section 8.2. The results of these evaluations are described in Table 24 with the statement numbers corresponding to the numbers in Table 21. The statements in the assessment instrument were presented in the order: {1, 10, 5, 4, 7, 9, 8, 2, 6, 3}, statements 5, 7, and 2 were formulated negatively and had their scores recoded.

Table 24: Descriptive statistics for evaluation results per statement (N=4).

Criterion	Statement	Minimum	Maximum	Mean	Std. Deviation
Effectiveness	1	4	5	4,25	0,500
	2	3	4	3,75	0,500
Operational feasibility	3	2	4	3,25	0,957
	4	3	4	3,50	0,577
Usefulness	5	3	5	4,00	0,816
	6	3	4	3,75	0,500
Ease of use	7	2	5	3,00	1,414
	8	3	4	3,75	0,500
Structural completeness	9	3	4	3,50	0,577
	10	3	4	3,75	0,500

Participants were asked to indicate how important privacy and data protection issues are to their organisation. From very low (1) to very high (5), the results show a mean value of 4,25 which indicates that privacy and data protection are indeed seen as important issues. All participants represent organisations in The Netherlands with 500+ employees, except one organisation which has 251–500 employees. Taking a closer look at Table 24, a generally neutral to moderately positive attitude can be observed for the evaluation criteria. *Effectiveness* and *usefulness* are the highest-scoring criteria. Remarkably, statement seven of the *ease of use* criterion has the lowest scoring mean and the highest

scoring standard deviation. Opinions seem to differ on how difficult it is to assess PbD maturity using the proposed model and assessment instrument. Alternatively, since this is one of the statements that was formulated negatively, participant misinterpretation may have generated outlier values which have influenced the results negatively.

One participant commented on the capability granularity, describing how some topics are implemented while others are not and suggested splitting capabilities up, possibly needing more levels. The practice versus capability granularity battle has somewhat been discussed in section 7.1 in the context of the assessment instrument. Currently, the model contains 60 capabilities that indeed consist of multiple practices each. Compared to other focus area maturity models (e.g., Spruit and Röling, 2014; van Steenbergen et al., 2010), this thesis argues that 60 is a reasonable number. Nonetheless, some capabilities might contain too many practices. Future work could investigate if and how capabilities must be split. A different participant remarked that the model currently is generic for all stakeholders and suggests creating specific user groups that only contain what is respectively necessary and relevant. Essentially, suggesting a situational maturity model with the relevant stakeholder as the pivoting variable. Considering the great variety of stakeholders involved in PbD, investigating this option in the future could prove beneficial.

Only 4 assessors out of the 20 who performed an assessment decided to participate in the evaluation. This small sample size makes it difficult to generalise these results and attribute weight to them. A greater number of evaluations is needed to gain a more comprehensive view of practitioner attitude regarding the maturity model and its merit. A greater variety in geographical location and organisational size would additionally be beneficial.

9 Discussion

This section highlights some of the findings, presents some examples, and discusses some relevant implications. Additionally, the limitations and threats to the validity of the study are described, including mitigation measures.

9.1 Examples, findings, and implications

9.1.1 Strategies, tactics, patterns, and technologies

The results of MLR 2 which are described in subsection 4.2.3, briefly touch upon reusable design elements. This concept consists of a design system of reusable elements for embedding privacy in system design, layered into four different abstraction levels: *privacy design strategies*, *privacy design tactics*, *privacy design patterns*, and *privacy-enhancing technologies*. The notion of reusable design patterns as an abstraction for implementation technologies is a well-engrained concept in software development (Bass et al., 2013). Various collections of privacy design patterns exist, such as the libraries provided by privacypatterns.org (2023) and Stanford Legal Design Lab (2022).

The privacy design patterns can be implemented through concrete technologies, commonly referred to as privacy enhancing technologies (PETs). Hoepman (2014) observed that while the implementation stage of a software development project is supported by patterns and technologies providing standardised reusable solutions, there is a shortage of practical guidance for the protection of privacy in the early phases. Patterns are often used for the purpose of solving a particular implementation problem and are typically not considered early in the development cycle, thus the developer stands empty-handed at the start of a project. Hoepman bridges this gap by introducing two additional abstraction layers: strategies and tactics.

Strategies are more suitable for use in the concept development and analysis phase of the development cycle because they do not force particular structures on the system. They guide the initial design and allow us to think about system requirements and how these can be realised in a privacy-friendly manner early on. A *privacy design strategy* is a design strategy that has the goal to achieve a certain degree of privacy protection. Hoepman (2022) introduces eight privacy design strategies: *minimise*, *separate*, *abstract*, *hide*, *inform*, *control*, *enforce*, and *demonstrate* (Figure 42). The first four strategies are data-oriented and focus on processing data in a privacy-friendly manner. The second four strategies are process-oriented and focus on the processes related to responsible personal data handling.

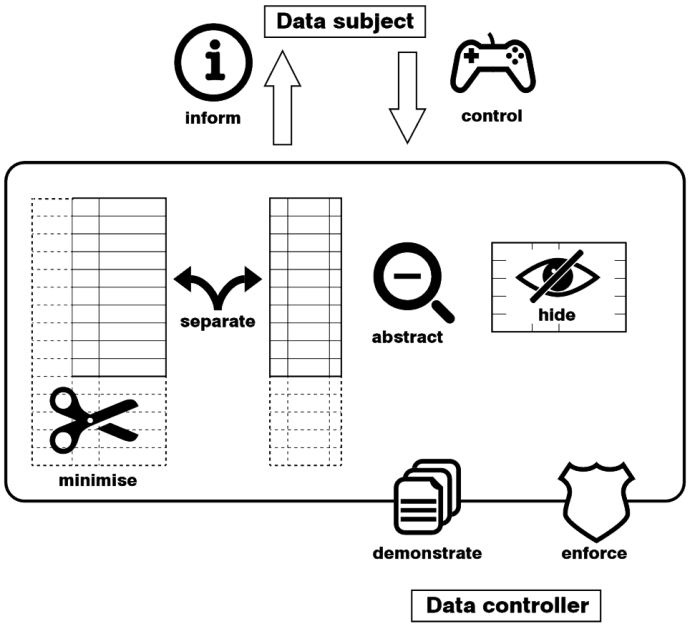

Figure 42: Visualisation of the eight privacy design strategies (Hoepman, 2022).

Each strategy is accompanied by several *tactics* (Figure 43), these are different ways in which the overarching strategy can be concretised. It is unfortunate that a semantic discrepancy has come into existence where a tactic is more abstract than a pattern in the privacy-by-design domain, while a pattern is more abstract than a tactic in the software architecture domain. The use of these terms, therefore, requires careful consideration and specification of the domain in question, especially since privacy-by-design and software architecture are closely related. In this thesis, unless specified differently, the design system of Hoepman is used, thus *tactic* refers to the second highest abstraction level.

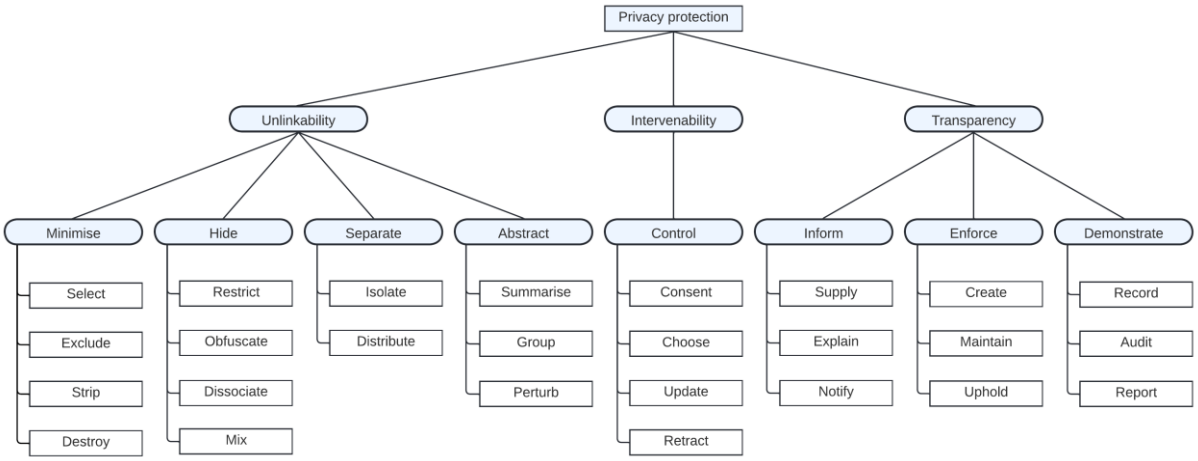

Figure 43: Privacy strategies and tactics from the diagram of Alshammari and Simpson (2018).

Hoepman's design system is found throughout several works, some of which have been included in MLR 2 and are described in subsection 4.2.3, including documentation from a European data protection authority. Looking at the privacy-by-design maturity model that this thesis proposes, elements from this same design system can be found spread over several different focus areas and capabilities, mainly concentrating on system development. For example, capability *architecture A* prescribes the translation of privacy design strategies to tactics, capability *technology B* prescribes the selection, development, and usage of PETs to implement privacy design patterns, and capability *development D* prescribes the establishment of a catalogue of privacy patterns with code excerpts.

9.1.2 Method and lifecycle integration

Capability B of the *development* focus area of the privacy-by-design maturity model prescribes the integration of privacy and data protection activities in the methods and workflows of the software development lifecycle (Appendix H). According to Diamantopoulou and Karyda (2022), designing and implementing systems with respect to privacy requires privacy requirements to be integrated into the typical engineering activities. Section 4.2.3 has briefly described some frameworks with privacy embedding that were found in MLR 2, this subsection expands on this with additional thoughts and examples.

One of the core ideas of privacy-by-design is to address privacy concerns throughout the entire system lifecycle. Hoepman's (2022) work adheres to this idea by integrating the reusable design elements into the system lifecycle—linking strategies, tactics, patterns, and technologies to the appropriate lifecycle phases. The early phases, ideation and definition, are supported by privacy design strategies (and further specified through tactics). Privacy design patterns are applied during the design phase and privacy-enhancing technologies are implemented during development. This integrated system lifecycle guides practitioners in addressing privacy concerns in a structured manner, from the conceptual inception of a system to its technological implementation. It forces practitioners to make fundamental high-level design decisions explicit and enables them to make conscious choices regarding privacy protection that are well-motivated.

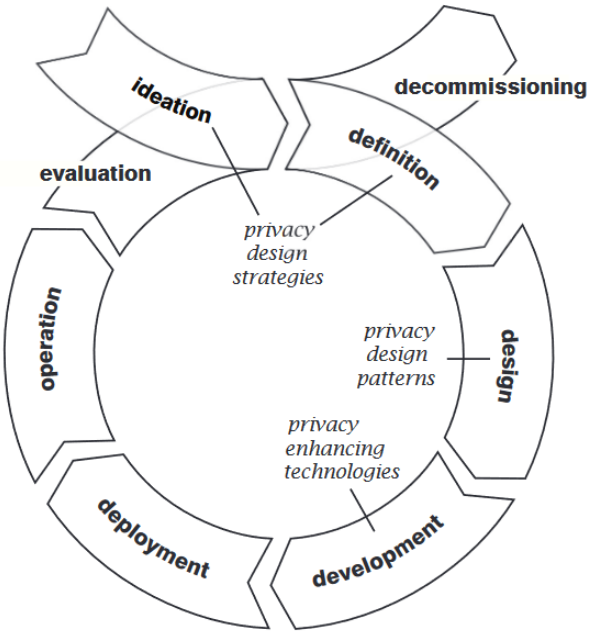

Figure 44: Hoepman's design elements integrated in the system lifecycle (Hoepman, 2022).

The use of strategies, tactics, patterns, and PETs as a design system for the application of privacy-by-design throughout the system lifecycle seems to have gained traction in the privacy (research) community. Looking at the citation count per year on Google Scholar (2023), the 2014 paper gained popularity for the first six years and has enjoyed a citation count in the range of 60–65 for the past three years. Hoepman's work is manifesting itself as a promising approach in guiding developers in addressing privacy concerns in system design and has been adopted throughout various capabilities in the privacy-by-design maturity model.

The MITRE Corporation presents a privacy engineering framework in their Privacy Engineering Framework and Lifecycle Adaptation Guide (2019b). This framework is an adaptation of the traditional V-model lifecycle for systems engineering (K. Forsberg & Mooz, 1991), quite similar to the earlier shown framework of the La Agencia Española de Protección de Datos (2019) in Figure 19. The MITRE framework is shown in Figure 45 and consists of three broad categories of phases: *Privacy Requirements Definition*, *Privacy Design and Development*, and *Privacy Verification and Validation*.

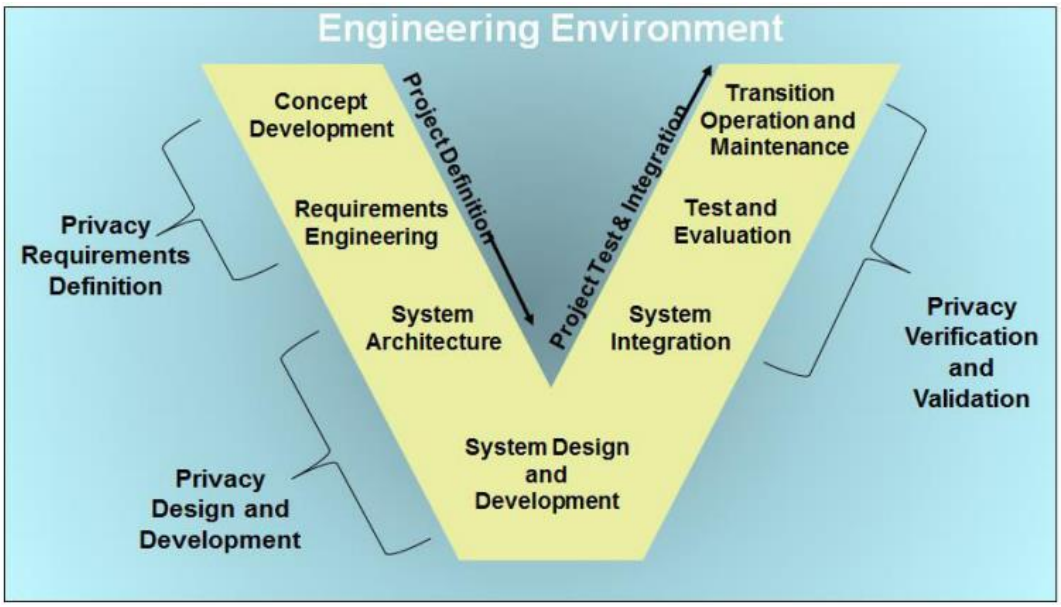

Figure 45: Privacy framework based on the V-model (The MITRE Corporation, 2019b).

The framework recognises that privacy policy alone is not enough to proactively address privacy risks and that there exists an untapped potential in embedding privacy requirements into organisational activities through systems engineering processes. Each phase category of the model is detailed with input artifacts, activities, and output artifacts. Notably, the *Privacy Design and Development* category contains an activity that prescribes the identification of privacy design strategies and patterns. What makes this framework additionally of interest is the inclusion of a life cycle adaptation guide. The base framework consists of a sequential Waterfall-type life cycle but can be adapted to other life cycles such as DevOps and Agile.

A different view on addressing privacy concerns with the V-model is presented by Al-Momani et al. (2019). They propose a privacy-aware variant of the V-model: the *W-model*—in reference to its new shape (Figure 46). This model integrates privacy into the original V-model by enhancing existing phases as well as introducing two new completely privacy-oriented phases: *Privacy Analysis* and *Privacy-Enhanced Architecture (PEAR)*. The first new phase, *Privacy Analysis*, focusses on analysing the initial somewhat privacy-preserving design of a system to ensure regulatory compliance and privacy preservation. It includes performing a PIA to identify privacy threats and formulate suitable mitigation measures, as well as addressing privacy requirements that are conflicting with business requirements. The second new phase, *Privacy-Enhanced Architecture (PEAR)*, aims to deliver a privacy-enhanced architecture that unifies both privacy and business requirements. Designing the PEAR is divided into two stages: a high-level privacy-preserving design and a low-level privacy-preserving design. The envisioned result of this phase is a privacy-preserving design that includes low-level components and that is suitable to be implemented in the next phase.

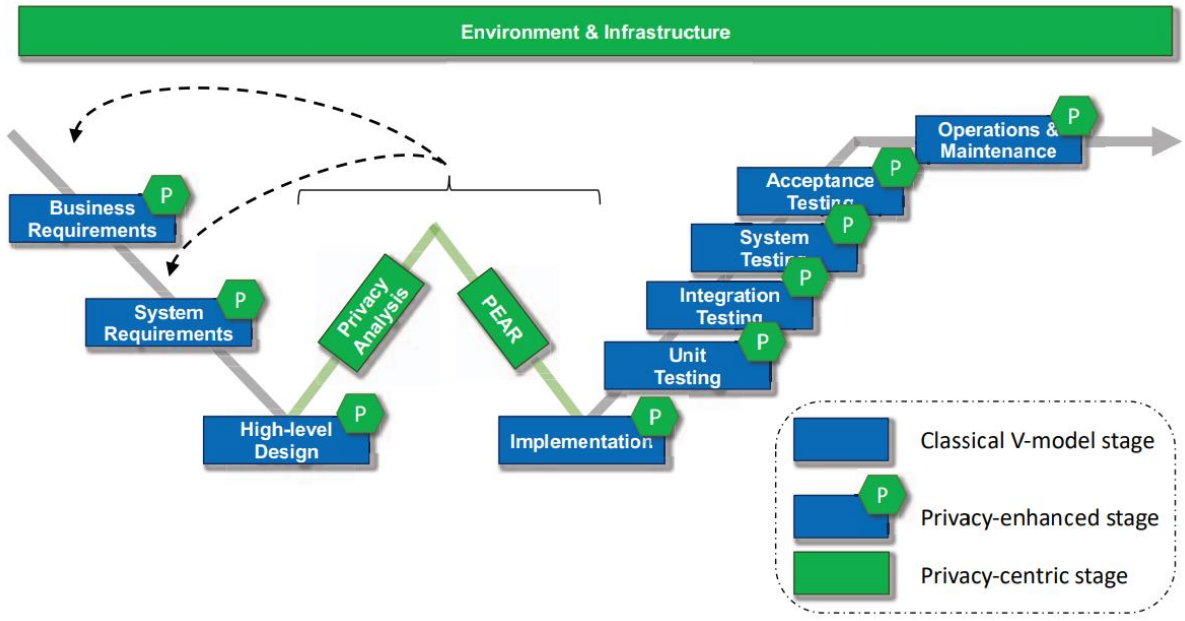

Figure 46: The W-model as a privacy-aware variant of the V-model (Al-Momani et al., 2019).

The examples shown in this subsection expose a focus on the system engineering side of PbD in terms of privacy embedding. Existing artifacts only seem to address limited aspects, disregarding many other relevant topics. The contribution of this thesis addresses that shortcoming. Reflecting on the role of the proposed PbD maturity model, it provides a more comprehensive and holistic approach that is better equipped to support the broader scope of PbD. The maturity model has focus areas such as *requirements*, *architecture*, and *development* which encompass the topics that some of the artifacts in this section discuss. But in contrast to those artifacts, it contains 11 more focus areas that address various organisation-wide topics related to governance, awareness, and processes, as well as fields and domains related to PbD which have been discussed extensively in previous chapters.

9.1.3 Privacy architecture

The architecture of a system is crucial for reasoning about system components and for guiding system development. Its importance in the context of privacy-by-design is evident as it is one of the vital components of the design phase of a system's lifecycle. This significance is reflected in the contribution of this thesis by its inclusion as a full-fledged focus area in the privacy-by-design maturity model. Capability A of architecture prescribes the creation of a privacy architecture as part of the project architecture. Several works in MLR 2 describe this notion, yet the evaluation results show that this capability is not implemented that often and is, in fact, one of the lowest in full implementation of the first three maturity levels. This subsection further explores how a privacy architecture could take shape and what its added value could be.

According to A. Jansen and Bosch (2005), architecture can be viewed as a collection of design decisions. In the application of privacy-by-design, privacy-oriented design decisions are inescapably generated—designs must integrate business requirements as well as privacy requirements which can originate from both a goal-oriented approach and a risk-based approach. There are inevitable requirement conflicts that will have to be resolved as well as trade-offs that will have to be made between privacy and other quality attributes or functional requirements (Senarath & Arachchilage, 2018). This notion raises the question of whether there is potential merit in formalising these privacy-oriented design decisions in a *privacy architecture*. Not only would a privacy architecture serve as a reference artifact for historical design decisions related to privacy or data protection with corresponding motivation, it can additionally function as a communication vehicle between different groups of stakeholders which, considering the multidisciplinary nature of the PbD domain, could enable enhanced understanding between practitioners from different fields such as legal and engineering.

Sion et al. (2019) propose an architectural viewpoint for data protection by design, incorporating data protection as an explicit viewpoint in existing software architecture documentation practices. They provide a meta-model (Figure 47) for the creation of data protection view diagrams based on the criteria for system description in the context of suitable DPIA methods, published by the Article 29 Working Party (2017). Sion et al. mainly take a legal perspective on the matter, modelling actors, processing activities, data subject types, and personal data types.

This stands in contrast to the PEAR concept (as used in the W-model) which is a more engineering-focussed approach for harmonising privacy and architecture. Kung (2014) describes how a PEAR can be constructed using the concept of quality attribute scenarios (Bass et al., 2013) and a collection of self-proposed tactics for the privacy quality attribute. Since this method sticks close to the conventional approach for software architecture, as outlined by Bass et al. (2013), Kung's tactics are equally based on the conventional architectural style of a tactic—differing from Hoepman's (2022) notion of a privacy design tactic. On that note, documenting the decisions related to Hoepman's design system in a project could be the first step in creating a formal privacy architecture. Such a privacy architecture can formalise the decisions related to the choice of strategies, tactics, patterns, and PETs. It can describe what decisions were made, how they relate to each other, their motivation, and which alternative solutions were considered but not used, including the reason they were not chosen.

Morales-Trujillo and Garcia-Mireles (2018) embedded privacy in the software engineering lifecycle profiles for very small entities (ISO/IEC, 2011). They too recognise the importance of addressing privacy in architecture, which is exemplified by one of their modified tasks which prescribes taking privacy scenarios into account when generating architectural design. On top of that, their suggestion of creating a PbD manager role can be pivoted into a suggestion for a privacy architect or technical privacy officer role that can support any activities related to the architectural embedding of privacy—or perhaps more broadly, support any engineering activity where privacy concerns need to be addressed. Additional research will have to discern what is appropriate and desired to be included in a potential privacy architecture and what the responsible roles should be, yet Hoepman's design system could serve as a natural inception point. Whether a privacy architecture needs to stand on its own legs or should be incorporated as part of the conventional software architecture, for example as a viewpoint, is another topic for potential future work.

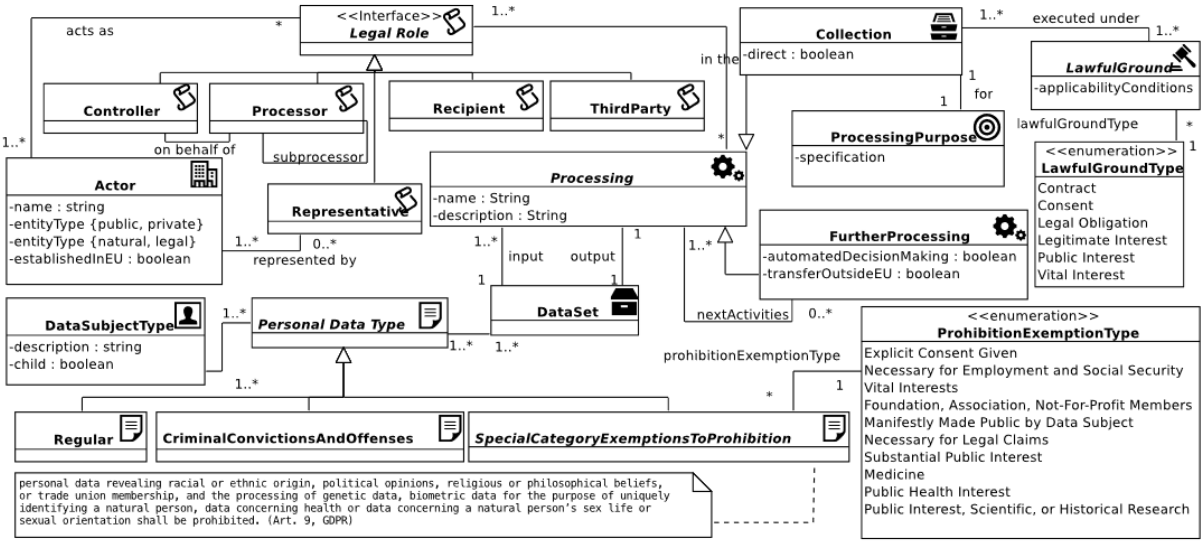

Figure 47: Meta-model for data protection view diagrams (Sion et al., 2019).

9.1.4 Maturity level zero definitions

The maturity model proposed in this work contains 60 capabilities spread over 10 levels, starting at level 1. Implicitly, there exists a start-state, i.e., a level zero, in which no capabilities of a focus area are implemented. This begs the question of what this state looks like and how it can be defined. The definition has implications for the assumptions related to the circumstances that an organisation that wants to apply the model is in. Subsection 5.3.2 defines level zero for each focus area.

Most level zero definitions revolve around not explicitly considering or addressing privacy concerns in the respective focus area. Some focus areas have a more specific level zero definition. For *PIA process*, level zero is defined as: "A PIA is a one-time process and product". For *PIA report*: "The PIA report is tightly coupled with the PIA process. There is one report for all audiences". For *Third-party management*: "Data processing agreements are established on an individual basis". For *Transparency*: "A privacy notice exists on a public website and data subjects are referred to it". These examples indicate that the model assumes an organisation to be already conducting certain activities before looking into PbD capability development. This thesis argues that an organisation that is starting from scratch should invest resources into getting the basics of privacy protection up and running before actively engaging in focused PbD maturity development. These basics include familiarising oneself with conducting PIAs, signing data processing agreements, and doing the bare minimum in terms of transparency.

The level zero definitions were formulated by working backwards from the first capability of each focus area and determining what basic activities would be expected from an organisation that aims to develop its PbD practices. While an expert practitioner was involved in this process, the strictness and specificity of the level zero definitions have some wiggle room. On top of that, one could argue that the model should incorporate the very basics so that it can be used by any organisation regardless of the current level of privacy protection offered. Some participants during the focus group voiced this suggestion. Future work can look to extend the model with early capabilities and should investigate what the optimal organisational state is to start PbD maturity development using this model.

9.1.5 Decoupling PIA process and PIA report

One of the design decisions of the maturity model discussed in subsection 5.3.5 is the decoupling of the PIA process and PIA report. This decision is not obvious and not explicitly supported by literature and thus requires more elaboration. Typically, in practice, the PIA process and report are the same. Practitioners take a PIA report template and work through it top-to-bottom filling out all necessary elements—this is their process, thus process and report are tightly coupled. The resulting artifact is a singular document, often referred to as 'the PIA'. This same document is used in all further activities related to the PIA, regardless of relevance, purpose, or involved stakeholders.

The multidisciplinary nature of PbD is also evident when examining the PIA. Conducting a PIA typically involves product owners, engineers, privacy officers, data protection officers, and legal advisors. Additionally, found literature prescribes the involvement of executives (Wright, 2012), users (Vicini et al., 2016), ethical experts (Vicini et al., 2016), and third-party auditors (Wright, 2012), all-in-all, various stakeholders are involved in the execution of the process and composition of the report. Timón López et al. (2021) indicate that a PIA report should be understandable for technical and non-technical experts, which signifies that the audience of the PIA report is a relevant factor in its composition. Semantha et al. (2020) recommend publishing the PIA report or summary thereof. This indicates that multiple different artifacts can exist simultaneously of which some would be publicly accessible. Combining these two inferences and expanding upon them, this thesis argues that the PIA process and PIA report should be decoupled. This allows for the creation and use of different types of PIA reporting and presentation artifacts which are composed for a specific purpose and tailored to a specific audience, i.e., stakeholder.

A PIA report contains numerous topics including requirements, risks, mitigating measures, technologies, and legal principles. All these elements will not be relevant to every stakeholder. While no found work explicitly recommends or prescribes this, it seems like a natural improvement of the PIA to service the various involved stakeholders as best as possible, suitable for their domain expertise and goals. The idea of stakeholder-tailored (sub)artifacts is not new, it is widely applied in the software architecture domain where different views and viewpoints provide a particular perspective of the same system for different stakeholders (Bass et al., 2013). In a similar fashion, different *PIA views* could provide a particular perspective on the entire PIA for different involved stakeholders.

This design decision was received somewhat sceptically during the focus group validation. Participants did not seem to fully understand the implications of this decision and considering the limited time this topic should be investigated further in the future. This includes the suitability of different artifact types for different purposes and stakeholders. One example in which this could be applied is for transparency towards users. From a transparency perspective, an organisation can show their commitment to privacy protection by publishing its PIA report. Internal PIA reports might contain highly specific, technical, and sensitive information which is unsuitable and undesirable to share publicly. In this case, a public version of the PIA report can be created according to a user viewpoint which contains enough information to inform users adequately and appropriately.

9.2 Limitations

This research is subject to several limitations. Starting with the two multivocal literature reviews that were performed, these use a stopping criterion where only the first 100 grey works are considered. This cut-off point mainly serves a pragmatic purpose since it is infeasible to consider potential millions of hits resulting from a Google search query. Because of this, we are at the mercy of the search engine's algorithm for choosing which 100 works to present first. Knowledge saturation can therefore not be guaranteed and there exists a possibility that relevant and insightful works were missed. Considering that most found grey works were excluded and taking the total volume of found factors into account, the impact of missed works is expected to be minimal. Additionally, the Google search engine maintains a limit of 32 keywords per query, this made it necessary to cut the generic search string shorter for the grey literature part of MLR 2.

In regards to the validation and evaluation, the focus group was conducted with a limited number of participants, all from the same organisation. These participants were mainly gathered through convenience sampling for accessibility and availability reasons. The result of this approach is that the sampling is subject to bias and introduces validity threats, specifically threats to the generalisability of the results which are discussed in more detail in the next section. Similarly, the evaluation was conducted with a limited sample and limited participant variety resulting in generalisability threats.

This research has completed the full design cycle of Wieringa (2014) once. Naturally, time is a pragmatic constraint that decides how much effort can be allocated to certain activities. One validation activity and one evaluation activity have been performed. More time would allow for more iterations of the design cycle including more validations and evaluations which would mitigate validity threats to a degree. Especially long-term observations and evaluations of improvement action implementation are required since the validation of these has been insufficient in this research project.

9.3 Validity threats

Ascertaining to what degree the results of a study are true, trustworthy, and to what extent the subjective perceptions of the researchers have had a biased effect are captured by the concept of validity. This subsection outlines the threats to the validity of this study and accompanying mitigations by employing the validity scheme by Runeson and Höst (2009). Four different aspects of study validity are discussed: *construct validity*, *internal validity*, *external validity*, and *reliability*.

9.3.1 Construct validity

Construct validity entails to what extent a study truly measures what it intends to measure. For this research, construct validity refers to the degree that the privacy-by-design focus area maturity model truly measures privacy-by-design maturity. There are two components to this validity: the validity of the type of artifact as an artifact for maturity measurement and the validity of the contents of the specific artifact introduced by this research to measure the maturity of specifically privacy-by-design.

In regards to the validity of the artifact to measure maturity, maturity models are an established artifact for maturity assessment in IS research. More specifically, focus area maturity models are widely used for maturity assessments in different domains with positive results, see the work by Sanchez-Puchol and Pastor-Collado (2017) for examples. Based on previous research, this thesis thus places a level of trust in the ability of this type of artifact to indeed measure organisational maturity for a particular functional domain. The meta-model for focus area maturity models by van Steenbergen et al. (2010) was used to mitigate the threat of the designed artifact deviating from the desired artifact type.

The second component of construct validity is accompanied by the threat that the model does not measure the maturity of privacy-by-design specifically. This threat was mitigated by employing two extensive literature reviews, examining both existing treatments as well as privacy-by-design factors originating from both academic literature and grey literature. Extracted factors were analysed and used to formulate PbD capabilities and focus areas with an additional researcher who is also an expert practitioner in the privacy domain which mitigates researcher bias in factor selection and model element formulation. On top of that, a focus group validation was performed with a varied group of privacy professionals who provided feedback on the model.

9.3.2 Internal validity

Internal validity entails to what extent the artifact makes a difference in the context of this study in terms of cause and effect. For this research, internal validity refers to the degree that the privacy-by-design focus area maturity model makes a difference in achieving the intended maturity assessment and maturity development.

In regards to facilitating maturity assessment, providing a smooth assessment experience with automatic results generation through a web application mitigates some of the risk of errors occurring during the assessment while fiddling with formulas in a spreadsheet approach. On top of that, a pilot test was performed with the assessment instrument and evaluation questions to determine if there were any problems before widescale distribution. Nonetheless, there are threats to the validity of the results of the maturity assessments. The assessment instrument has been developed with a self-assessment approach in mind—while this allows anyone to perform the assessment, it introduces interpretation discrepancies, biases, socially desired behaviour (Hawthorne effect), and the results become somewhat dependent on the skill, knowledge, and organisational understanding of the assessor. These threats are inherent to the approach and are difficult to mitigate from an artifact design perspective, organisations can mitigate these threats by employing a neutral third-party expert, appointing an experienced employee with a deep understanding of the domain and the organisation, or using a panel of assessors to perform the assessment.

Whether this artifact makes a difference in developing maturity is difficult to ascertain at this point. Maturity development can take many months if not years just to advance a single level. Long-term studies would have to be conducted with observations, interviews, and evaluations to determine whether organisations are implementing the proposed improvement actions, whether these actions are being implemented as a result of using the privacy-by-design maturity model or because of some other

confounding variables, and whether the effects of the improvement actions are contributing positively to reaching organisational goals. These activities are beyond the scope and outside the pragmatic limits of this research project and will have to be explored in future work.

9.3.3 External validity

External validity entails to what extent the results of a study can be generalised to other demographics and application contexts. Since the application of privacy-by-design is mandatory per GDPR, the results of this study are inherently of relevance to organisations that process personal data within the European Union or process personal data of European citizens or residents. Since the validation and evaluation were performed with practitioners from an EU country, there is a potential threat to the generalisability of the model outside of a GDPR application context. This threat is partially mitigated by the MLRs which also considered sources originating from outside the EU. Pragmatically, specific mentions of the GDPR were also removed from the capabilities in favour of generalised terms. Whether the model is truly applicable in other legal jurisdictions will have to be established with additional future validation/evaluation efforts by introducing the model in those jurisdictions. Additionally, the validation was only performed with practitioners from the same organisation, which was a government entity. Thus, there also exists a threat to the generalisability of the model to other types of organisations. Lastly, the limited sample size of the validation and evaluation is another threat to the generalisability of the results.

9.3.4 Reliability

Reliability entails to what extent the result of a study is dependent on the specific researcher conducting it. The main threats to reliability are related to the replicability and subjectivity of the research, including the work selection and assessment activities of both MLRs, the factor coding and extraction, and the formulation of capabilities, focus areas, and dependency relationships. In general, these threats are mitigated by the modelled and documented steps for each phase of the research. The research design makes use of the overarching established design science paradigm with specific method fragments, taken from existing maturity model methods, forming the concrete phases.

For the MLRs, a protocol was used which includes the used search strings, used data sources, inclusion/exclusion criteria, quality assessment criteria, and data extraction forms. The entire process of both MLRs has been documented describing how many records were found, excluded, and what the exclusion reason was. While the search strings for the grey literature queries are documented, the Google search algorithm uses more variables, such as browser history, to choose which results to display first. It can therefore not be guaranteed that the same search string will always return the same results. While the extraction of factors was guided by extraction forms, it was entirely performed by one researcher thus the threat of subjectivity has only been partially mitigated. Regarding the data synthesis of the factors and model construction, an additional researcher was involved in the formulation of capabilities and focus areas to decrease the level of subjectivity. The formulation of dependency relationships was additionally guided by heuristics. The motivation for the formulation of all capabilities has been documented, ensuring full traceability of literature sources and factors that were used to substantiate each capability. The validation, which was performed through a focus group interview, was guided by a documented interview protocol and resulting model changes have been linked to quotes originating from said focus group, again ensuring full transparency and traceability. The source code of the created assessment instrument has been made available publicly and can be referenced by any researcher. The survey evaluation has been documented as well, including a full specification of its design including the questions and answer possibilities.

Overall, this study has provided a good-faith effort at documenting the research design and the steps taken in its application to allow other researchers to replicate this study. The process of transforming collected data into model elements has been documented, describing the full traceability of used factors to maintain a transparent chain of evidence which substantiates the design decisions and study results.

10 Conclusion

This chapter provides a summary of the main findings of this study, answers the research questions, outlines the main theoretical and practical contributions, and provides ideas for future research avenues.

10.1 Research question answers

The motivation for this research came from the observation that there is a need for practitioners to receive guidance in the application of the privacy-by-design paradigm. This observation has led to the formulation of the following objective: design a focus area maturity model that structures the privacy-by-design domain and allows organisations to effectively employ privacy-by-design practices in information systems design projects. The accompanying main research question has been formulated as:

> **MRQ**: How can organisations assess their privacy-by-design practices through a maturity model approach in order to understand the progression of, and the relationships between, various domain factors?

The main research question decomposes into four research questions which are subsequently discussed and answered in the following four subsections.

10.1.1 Research question 1

The goal of the first half of the domain investigation phase is to get an overview of existing solutions in order to collect the relevant factors that these solutions might contain as well as create a base of operation to build upon. To this end, the following research question was formulated:

> **RQ1**: What maturity models exist in the relevant and adjacent domains?

The first research question is a knowledge question that requests information from its environment. The formulation of this question is motivated by Wieringa's (2014) notion that before a new artifact can be designed, existing artifacts must be examined. This question thus asks for the examination of existing maturity models in the relevant domains. To answer this question, a multivocal literature review (MLR 1) was performed, taking an inventory of existing maturity models in the privacy and data governance domains.

The results of this MLR revealed a collection of 30 maturity models related to privacy or data governance (Table 7). Most of the models adhere to or are based on, the standard five-level approach of the widely known CMM(I) type maturity model. A wide variety of abstraction levels and number of attributes were found between the models. Looking at scientific rigour, only 5 out of the 13 academic models contain a definition for *maturity* and only 11 works in total describe some sort of validation or evaluation activity, mostly in academic works. Tool support was likewise found lacking with only one work describing a dedicated tool and three other works providing an Excel spreadsheet.

10.1.2 Research question 2

The goal of the second half of the domain investigation phase is to elicit privacy-by-design factors in order to gain insight into the practices of this domain which can be used to populate the privacy-by-design maturity model. The following research question was formulated accordingly:

> **RQ2**: What are the relevant factors that influence privacy-by-design?

The second research question is also a knowledge question that requests information from its environment. The purpose of this question is to gather domain factors that serve as basic building blocks for capabilities and focus areas. This question thus asks for the examination of the privacy-by-design domain and the identification of relevant factors. To answer this question, factors were extracted from

the models found in the first multivocal literature review (MLR 1). These were combined with factors extracted through another multivocal literature review (MLR 2), which had the goal of taking an inventory of best practices, success factors, guidelines, recommendations, and other factors in the privacy-by-design domain that are recommended or regarded positively.

The results of MLR 1 show that while 16 works contained relevant factors, only 8 works mentioned privacy-by-design explicitly. Nonetheless, a total of 620 factors were extracted. Using a coding approach, the factors were consolidated into a slimmed-down collection of 401 factors (Appendix C) and grouped into 9 main themes. The *data processing* theme was found to encompass the most factors (178), indicating a clear focus on a more legal perspective which includes data subject rights and data processing principles (Figure 14).

The results of MLR 2 revealed 713 factors extracted from 64 works. The reviewed works were found to discuss privacy-by-design in various application domains, healthcare and IoT were found to be common domains. The review did not only find works from academic and industry sources, multiple government sources were found to elaborately discuss privacy-by-design, including the data protection authorities of New Zealand, Spain, and the UK. The same coding, aggregation, and distillation approach of MLR 1 was used for MLR 2. The 446 factors of the slimmed-down list (Appendix E) were grouped into 10 themes. The *privacy-by-design* theme was numerically the largest with 260 factors, indicating that more emphasis is placed on PbD, the PIA, and development. This shifts the weight of the distribution from legal concepts to more technical concepts compared to the results of MLR 1.

In summary, the domain investigation phase found a total of 1333 factors for privacy-by-design which were consolidated into 847 factors and grouped into 12 distinct themes.

10.1.3 Research question 3

The treatment design phase follows the domain investigation phase and consists of model design and instrument development. The goal of this phase is to aggregate and distil the elicited privacy-by-design factors to formulate capabilities and focus areas, create a populated maturity matrix, and create an accompanying assessment instrument. Therefore, the following research question was formulated:

RQ3: What does a privacy-by-design focus area maturity model look like?

a. What focus areas does a privacy-by-design focus area maturity model have?

b. What capabilities does a privacy-by-design focus area maturity model have?

c. What are the dependencies between the capabilities in a privacy-by-design focus area maturity model?

d. What does the accompanying assessment instrument look like?

The third research question revolves around the design problem and encompasses the design activities. It has four subquestions related to the design of the focus areas, capabilities, dependency relationships, and the assessment instrument. During the model design phase, the factors acquired from both MLRs were consolidated and used to formulate focus areas and capabilities. This led to the initial formulation of 14 focus areas which can be found in Figure 29, 59 capabilities which are described in Appendix H, and 50 dependency relationships which are outlined in Table 10. Following the focus group validation, several changes were made, including adding an additional capability and upping the total number to 60 capabilities.

The last subquestion is concerned with the assessment instrument which is required to operationalise the model and perform an assessment to determine the maturity. The assessment instrument was constructed by formulating assessment questions: for each capability, an assessor is asked to indicate to what degree the capability is implemented in the organisation. Answering all questions pertaining to a maturity level positively would constitute the organisation having achieved that maturity level. One of the observations from MLR 1 indicates that tool support for maturity models is rare, hence to support the application of the focus area maturity model for privacy-by-design, a web application was developed that allows a user to perform a self-assessment by answering the assessment questions. The answers to

the questions are automatically collected and processed, providing the user with a maturity report that denotes the overall maturity level as well as providing a more detailed breakdown per focus area. Additionally, it provides concrete improvement actions in the form of practices which the organisation can start incorporating into a maturity development plan to grow to the next level.

The developed tool support allows practitioners to conduct an assessment and receive a dynamically generated organisation-tailored maturity report, providing a fluid and polished experience in guiding the maturity assessment and formulating a development path.

10.1.4 Research question 4

The two remaining phases of this research are the validation phase and the evaluation phase. The goal of these phases is to ascertain to what degree the real effects of the developed artifact correspond to the expected benefits. This is embodied by the following research question:

RQ4: How does a privacy-by-design focus area maturity model perform in practice?

The validation of the maturity model was conducted through a focus group interview with practitioner experts. The results of the validation led to eight changes being made to the model (Table 16): multiple capabilities were reformulated or relabelled, and one new capability was added in the first level of the *awareness* focus area.

The evaluation was performed through a questionnaire asking users that performed a self-assessment to rate the model following an assessment according to five evaluation criteria using a Likert scale. An initial small-scale pilot was conducted to test-run the assessment process. The feedback included a suggestion for the visualisation of partial development which was integrated into the maturity report, no major problems were reported. An invitation to the full wide-scale evaluation was publicly distributed. The results indicate that PbD maturity overall is low with most organisations not reaching the first maturity level. Practitioner attitude was neutral to moderately positive, with effectiveness and usefulness scoring the highest, yet the small sample size is a glaring limitation that should be overcome through additional research.

10.2 Contributions

This work makes several contributions to the scientific body of knowledge as well as contributions to practice, these are outlined in this section.

The main theoretical contribution of this work consists of providing a previously undefined structure to the privacy-by-design domain. This is done by identifying subdomains which are expressed as focus areas and by identifying the best practices which are expressed as capabilities. By identifying the dependency relationships between capabilities, they can be divided into maturity levels. This allows each capability to be linked to a degree of maturity which provides insight into the priority of each capability in the maturity development process. Using a maturity model approach, the privacy-by-design domain is organically categorised into subdomains based on the identified recommended practices. This provides insight into what exactly constitutes the privacy-by-design domain and can be used as a starting point for the creation of a PbD conceptual model. Future researchers can reference the collection of practices to get an understanding of what the PbD domain entails and to use it for the development of more concrete artifacts for the implementation of individual or smaller groups of capabilities or to adapt existing methods and paradigms to embed privacy concerns.

The main practical contribution of this work consists of an artifact in the form of a focus area maturity model that provides practitioners guidance in the application of the privacy-by-design paradigm. The focus area maturity model for privacy-by-design allows practitioners to determine what the PbD maturity of their organisation is through an assessment. Not only does this provide the organisation in question with valuable insight into the standing of the organisation regarding its PbD practices, but it also allows the organisation to set a maturity ambition and formulate a maturity development plan to fulfil that ambition. The dependencies in the model provide a natural order to the development of the capabilities which guides organisations in determining which capabilities it should develop next on the way to its maturity ambition. The need for guidance in the application of privacy-

by-design has been mentioned multiple times before in this thesis. The artifact presented in this work can fulfil that role by advising an organisation on what to do and in what order to do it, providing the organisation with a way to navigate this complex domain in a structured manner.

Additional contributions are made in the elaboration and formalisation of the focus area maturity model design process. This work provides a step-by-step overview of how a focus area maturity model can be constructed from start to finish. Using the overarching design science paradigm and a design method built from a maturity model design method base, which includes validation and evaluation activities, results in a rigorous approach which addresses the common criticism that maturity models lack scientific rigour. Other researchers can use this work as a reference template for their research method for the creation of a focus area maturity model. This work functions as a proof of concept for heuristics which can be used to determine dependency relationships between capabilities and shows that a low-effort algorithmic approach to generate the maturity matrix, once the dependencies have been identified, is possible. On top of that, this work uses, to the best of its knowledge, a novel approach for the analysis of focus area maturity models by modelling the dependencies in a graph data structure, opening the possibility of applying graph operations, such as checking for dependency cycles, as well as using graph attributes for the analysis, such as in/out-degrees to identify key capabilities or focus areas in the model.

The final contribution that this work makes relates to the observation that there is a lack of tool support for maturity models. The results of MLR 1 show that only one found work describes a dedicated tool and two others provide a spreadsheet for the assessment. This thesis argues that the assessment instrument is a vital part of a maturity model since it operationalises the model allowing practitioners to apply it—a model without an assessment instrument is a job unfinished. Not only does this work provide an assessment instrument, but it also elevates it by providing tool support in the form of a web application. This thesis shows that a tool-supported assessment instrument can be developed and implemented with limited resources, in a reasonable timeframe, by using common lightweight libraries and frameworks. The entire source code for the tool is provided in Appendix M as a reference example for other researchers as to how tool support can be implemented. The intention is to stimulate other researchers to provide assessment instruments with their maturity models and to encourage them to consider providing tool support.

10.3 Future work

There are multiple avenues for future work in relation to the topics discussed in this thesis. The rest of this section discusses research opportunities related to focus area maturity models, the PIA, domain integration, and the creation of concrete implementation artifacts.

10.3.1 General maturity models

Focus area maturity model design guidelines
Regarding focus area maturity models, there do not seem to be concrete guidelines regarding the construction of the maturity matrix. Using the two heuristics mentioned in subsection 5.3.3 and subsequently generating the matrix through an algorithmic approach worked well in this research project. Additional research could help formalise guidelines or incorporate additional activities in the focus area maturity model design method in order to provide more concrete guidance on focus area maturity matrix construction.

Focus area maturity model external dependencies
Additionally, in light of the multidisciplinary nature of the domain under investigation in this research, the observation was made that while a focus area maturity model depicts internal dependencies, it does not explicitly define external dependencies. For example, capability C of the *development* focus area prescribes applying and documenting privacy-by-design in change management procedures. This requires the existence of such a change management programme, which could be defined as an external dependency; a requirement that is out of scope for the model but which is required for the implementation of a capability from the model. Future research could investigate whether it is desired

to expand a focus area maturity model with the formulation of major prerequisites that do not directly fit the maturity scope of the domain addressed by the model. A suggestion for this consists of adding an *external* or *prerequisites* section to a focus area maturity model which contains the major external dependencies. Alternatively, this could be defined per level or even be turned into a capability property.

Maturity assessment results presentation artifact
The next suggestion regarding general maturity models pertains to the presentation of the results of a maturity assessment. Chapter 7 describes how the assessment instrument in this research was supported by a web application, including the presentation of the results in a maturity report. Additional research could investigate the design of such a maturity results presentation artifact to ascertain what content and visualisations practitioners perceive positively and what is best to support practitioners in formulating a maturity development path.

Maturity model tool support template
The last suggestion related to maturity models is regarding tool support. This work provides a prototype implementation of tool support for the PbD focus area maturity model. Expanding this prototype into a more generalised software template for any focus area maturity model is achievable. This template solution would already contain all the processing logic and would only require a model designer to input the respective model and assessment instrument elements such as capabilities, focus areas, dependency relationships, and assessment questions. Such a solution would simplify the implementation of tool support even further for the future development of new focus area maturity models.

10.3.2 Privacy-by-design focus area maturity model

Additional validation and evaluation
Chapter 9 has already touched on the limitations regarding the generalisability of this study. Additional research should be performed to increase the generalisability of the model by performing additional validation/evaluation activities. Expert practitioners from different organisation types should be involved such as semi-public organisations (e.g., education or healthcare) or even for-profit businesses that offer goods or services as practitioners working for these companies might have differing views compared to public servants considering the strong legal component that is in play. Since this research was conducted in Europe, in a GDPR environment, introducing the model to different legal jurisdictions could provide new insights and increase the generalisability of the model outside of the GDPR application context. Future work could investigate the formulation of a general PbD maturity model with several specific situational maturity models tailored to different legal application domains.

Long-term improvement action implementation
The effects of the privacy-by-design maturity model beyond getting an understanding of the current situation are in need of in-depth investigation. The maturity report following a maturity assessment does not only provide the current maturity level, but it also provides improvement actions which guide the organisation to reaching the next level. Future work should investigate how organisations respond to these suggested improvement actions. Especially if an organisation decides to implement them, long-term observation of the process and analysis of the resulting organisational changes could provide valuable insight into the maturity development process as well as the suitability of the improvement action.

PIA model and view decoupling
A different interesting suggestion that was already made in subsection 5.3.5, is the proposal of introducing PIA views. Future research could focus on ascertaining the extent of the added value of separating the PIA model from its presentation artifact allowing different PIA artifacts to exist simultaneously, tailored to a specific purpose or audience akin to software architecture documentation.

10.3.3 Privacy-by-design

Concrete privacy-by-design artifacts
While this maturity model provides a start in guiding organisations, additional guiding artifacts, such as development methods, could provide even more direction on a lower abstraction level—going as far as touching on the *how*, rather than just sticking to the *what*. Having software development methods that incorporate privacy concerns and holistically outline the use of reusable design elements (strategies, tactics, patterns, and PETs) could help development teams with addressing privacy concerns in system design and development. The incorporation of privacy considerations in existing widely used methods and paradigms, such as Agile or DevOps, should be investigated. In the same vein, a PbD-oriented method for conducting a PIA could be beneficial to practitioners.

Privacy architecture
One of the important artifacts in software development is the software architecture. Recognising that privacy-related decisions in system development are subject to trade-offs and design choices, it is reasonable to propose that these design decisions must be documented and formalised. A privacy architecture could serve as an artifact for this purpose. Future work can focus on investigating whether a standalone privacy architecture is desired, what such an artifact should contain, what roles should be involved in its creation and maintenance, and who is responsible for its quality.

Maturity-aware methods
Extending the thought of the previous paragraph, methods could potentially be enhanced by incorporating the maturity concept, creating a sort of situational method that embeds privacy concerns and that is maturity-aware. This type of method would be able to adapt itself to the maturity level of the organisation in question, preventing organisations from having to look for different methods once their maturity increases causing current methods to become insufficient in supporting the new higher maturity level. At the same time, such a method would allow organisations to focus on activities appropriate for their maturity level and not get lost in higher maturity activities.

Privacy, security, and ethics integration
The relation between privacy and security has been briefly touched upon, future work could investigate the integration of these domains leveraging their overlap in search of a holistic approach. Furthermore, considering the rise of artificial intelligence (AI) algorithm usage, the ethics domain is expected to play a bigger role in the future. The Dutch government has already introduced the impact assessment mensenrechten en algoritmes (IAMA) [impact assessment for human rights and algorithms] which is performed on top of the PIA when AI algorithms are in play (Gerards et al., 2021). This assessment is not mandatory by law currently, yet looking at how the PIA is legally anchored, it is plausible to expect an AI algorithm impact assessment to follow suit. While privacy and ethics are distinct domains, future integration is a reasonable suggestion which could see the development of an ethics-by-design paradigm that employs a broader view of moral and ethical considerations in information system development, encompassing privacy as a subset.

Multidisciplinary coordination of privacy-by-design
The last suggestion for future work that this thesis makes is related to the multidisciplinary nature of the privacy-by-design domain. PbD influences and is influenced by various factors, domains, and disciplines. Examples include software development, project management, risk management, data governance, legal, and ethical dilemmas. This requires coordination and cooperation between practitioners who have varying backgrounds, skills, expertise, roles, and responsibilities. Future work could investigate how the communication and coordination surrounding privacy-by-design practices between different practitioner demographics within an organisation can be structured and organised efficiently and effectively.

Bibliography

Abou Jaoude, A., Foss, A., Arafat, Y., & Dixon, B. (2021). *An Economics-by-Design Approach Applied to a Heat Pipe Microreactor Concept* (INL/EXT-21-63067-Rev000, 1811894; p. INL/EXT-21-63067-Rev000, 1811894). https://doi.org/10.2172/1811894

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 23. https://aisel.aisnet.org/icis2006/94

Adams, J., Hillier-Brown, F. C., Moore, H. J., Lake, A. A., Araujo-Soares, V., White, M., & Summerbell, C. (2016). Searching and synthesising 'grey literature' and 'grey information' in public health: Critical reflections on three case studies. *Systematic Reviews*, *5*(1), 164. https://doi.org/10.1186/s13643-016-0337-y

Agarwal, J., Malhotra, N. K., & Kim, S. S. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Ahmadian, A. S., Strüber, D., Riediger, V., & Jürjens, J. (2018). Supporting Privacy Impact Assessment by Model-based Privacy Analysis. *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 1467–1474. https://doi.org/10.1145/3167132.3167288

AICPA/CICA. (2011). *Privacy Maturity Model*. https://vvena.nl/wp-content/uploads/2018/04/aicpa_cica_privacy_maturity_model.pdf

Aljeraisy, A., Barati, M., Rana, O., & Perera, C. (2020). Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective. *ACM Computing Surveys*, *54*(5), 1–38. https://doi.org/10.1145/3450965

Alkubaisy, D., Piras, L., Al-Obeidallah, M. G., Cox, K., & Mouratidis, H. (2022). A Framework for Privacy and Security Requirements Analysis and Conflict Resolution for Supporting GDPR Compliance Through Privacy-by-Design. In R. Ali, H. Kaindl, & L. A. Maciaszek (Eds.), *Evaluation of Novel Approaches to Software Engineering* (Vol. 1556, pp. 67–87). Springer International Publishing. https://doi.org/10.1007/978-3-030-96648-5_4

Al-Momani, A., Kargl, F., Schmidt, R., Kung, A., & Bosch, C. (2019). A Privacy-Aware V-Model for Software Development. *2019 IEEE Security and Privacy Workshops (SPW)*, 100–104. https://doi.org/10.1109/SPW.2019.00028

Al-Ruithe, M., & Benkhelifa, E. (2017). Cloud Data Governance Maturity Model. *Proceedings of the Second International Conference on Internet of Things, Data and Cloud Computing*, 1–10. https://doi.org/10.1145/3018896.3036394

Alshammari, M., & Simpson, A. (2017). Towards a Principled Approach for Engineering Privacy by Design. In E. Schweighofer, H. Leitold, A. Mitrakas, & K. Rannenberg (Eds.), *Privacy Technologies and Policy* (Vol. 10518, pp. 161–177). Springer International Publishing. https://doi.org/10.1007/978-3-319-67280-9_9

Alshammari, M., & Simpson, A. (2018). Privacy Architectural Strategies: An Approach for Achieving Various Levels of Privacy Protection. *Proceedings of the 2018 Workshop on Privacy in the Electronic Society*, 143–154. https://doi.org/10.1145/3267323.3268957

Alsheiabni, S., Cheung, Y., & Messom, C. (2019). Towards An Artificial Intelligence Maturity Model: From Science Fiction To Business Facts. *PACIS 2019 Proceedings. 46*, 9. https://aisel.aisnet.org/pacis2019/46

Al-Slais, Y. (2020). Privacy Engineering Methodologies: A survey. *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, 1–6. https://doi.org/10.1109/3ICT51146.2020.9311949

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Brooks-Cole Publ. Comp.

Amazon.com, Inc. (2021). *FORM 10-Q QUARTERLY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934 For the quarterly period ended June 30, 2021*. https://www.sec.gov/ix?doc=/Archives/edgar/data/0001018724/000101872421000020/amzn-20210630.htm#i5986f88ea1e04d5c91ff09fed8d716f0_103

American Psychological Association. (2017). *Ethical principles of psychologists and code of conduct*. https://www.apa.org/ethics/code/ethics-code-2017.pdf

Antignac, T., Scandariato, R., & Schneider, G. (2018). Privacy Compliance Via Model Transformations. *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 120–126. https://doi.org/10.1109/EuroSPW.2018.00024

Arfaoui, S., Mezrioui, A., & BelmekkI, A. (2020). A Methodology for Assuring Privacy by Design in Information Systems. *International Journal of Communication Networks and Information Security (IJCNIS)*, *12*(3), 12. https://doi.org/10.17762/ijcnis.v12i3.4852

Article 29 Working Party. (2017). *Guidelines on Data Protection Impact Assessment (DPIA) (WP248 rev.01)*. https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711

Association of Corporate Counsel. (2019). *U.S. States' Privacy Laws Capability Maturity Model*. https://www.acc.com/sites/default/files/resources/upload/ACC%20Privacy%20Capability%20Maturity%20Model%20v2-0.pdf

Ayalon, O., & Toch, E. (2021). User-Centered Privacy-by-Design: Evaluating the Appropriateness of Design Prototypes. *International Journal of Human-Computer Studies*, *154*, 102641. https://doi.org/10.1016/j.ijhcs.2021.102641

Ayalon, O., Toch, E., Hadar, I., & Birnhack, M. (2017). How Developers Make Design Decisions about Users' Privacy: The Place of Professional Communities and Organizational Climate. *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 135–138. https://doi.org/10.1145/3022198.3026326

Bach, J. (1994). The Immaturity of CMM. *American Programmer*, 7.

Baldassarre, M. T., Santa Barletta, V., Caivano, D., & Piccinno, A. (2021). Integrating Security and Privacy in HCD-Scrum. *CHItaly 2021: 14th Biannual Conference of the Italian SIGCHI Chapter*, 1–5. https://doi.org/10.1145/3464385.3464746

Bass, L., Clements, P., & Kazman, R. (2013). *Software architecture in practice* (3rd ed). Addison-Wesley.

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management: A Procedure Model and its Application. *Business & Information Systems Engineering*, *1*(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5

Belanger, F., & Crossler, R. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*, 1017–1041. https://doi.org/10.2307/41409971

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, *11*(3–4), 245–270. https://doi.org/10.1016/S0963-8687(02)00018-5

Belli, L., Schwartz, M., & Louzada, L. (2017). Selling your soul while negotiating the conditions: From notice and consent to data control by design. *Health and Technology*, *7*(4), 453–467. https://doi.org/10.1007/s12553-017-0185-3

Bharadwaj, A. S. (2000). A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. *MIS Quarterly*, *24*(1), 169. https://doi.org/10.2307/3250983

Biberoglu, E., & Haddad, H. (2002). A Survey Of Industrial Experiences With Cmm And The Teaching Of Cmm Practices. *Journal of Computing Sciences in Colleges*, *18*(2), 143–152.

Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., & Rost, M. (2016). A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation. In S. Schiffner, J. Serna, D. Ikonomou, & K. Rannenberg (Eds.), *Privacy Technologies and Policy* (Vol. 9857, pp. 21–37). Springer International Publishing. https://doi.org/10.1007/978-3-319-44760-5_2

Bincoletto, G. (2019). A Data Protection by Design Model for Privacy Management in Electronic Health Records. In M. Naldi, G. F. Italiano, K. Rannenberg, M. Medina, & A. Bourka (Eds.), *Privacy Technologies and Policy* (Vol. 11498, pp. 161–181). Springer International Publishing. https://doi.org/10.1007/978-3-030-21752-5_11

Bisztray, T., & Gruschka, N. (2019). Privacy Impact Assessment: Comparing Methodologies with a Focus on Practicality. In A. Askarov, R. R. Hansen, & W. Rafnsson (Eds.), *Secure IT Systems* (Vol. 11875, pp. 3–19). Springer International Publishing. https://doi.org/10.1007/978-3-030-35055-0_1

Boswell, M., & Courtright, A. (2022). *Data governance overview—Cloud Adoption Framework.* https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/cloud-scale-analytics/govern

Brinkkemper, S. (1996). Method engineering: Engineering of information systems development methods and tools. *Information and Software Technology*, *38*(4), 275–280. https://doi.org/10.1016/0950-5849(95)01059-9

Campbell, J. E., & Carlson, M. (2002). Panopticon.com: Online Surveillance and the Commodification of Privacy. *Journal of Broadcasting & Electronic Media*, *46*(4), 586–606. https://doi.org/10.1207/s15506878jobem4604_6

Capgemini. (2021). *World Quality Report (WQR) 2021-22*. https://www.capgemini.com/insights/research-library/world-quality-report-wqr-2021-22/

Carretero, A. G., Gualo, F., Caballero, I., & Piattini, M. (2017). MAMD 2.0: Environment for data quality processes implantation based on ISO 8000-6X and ISO/IEC 33000. *Computer Standards & Interfaces*, *54*, 139–151. https://doi.org/10.1016/j.csi.2016.11.008

Castillo-Montoya, M. (2016). Preparing for Interview Research: The Interview Protocol Refinement Framework. *The Qualitative Report*, *21*(5), 811–831. https://doi.org/10.46743/2160-3715/2016.2337

Cavoukian, A. (2009). *Privacy by Design The 7 Foundational Principles*. https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

Cavoukian, A. (2010). Privacy by design: The definitive workshop. A foreword by Ann Cavoukian, Ph.D. *Identity in the Information Society*, *3*(2), 247–251. https://doi.org/10.1007/s12394-010-0062-y

Cavoukian, A. (2011). *Privacy by Design Strong Privacy Protection – Now, and Well into the Future*. https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf

Cavoukian, A. (2012). *Operationalizing privacy by design: A Guide to Implementing Strong Privacy Practices*. https://gpsbydesigncentre.com/wp-content/uploads/2021/08/Doc-5-Operationalizing-pbd-guide.pdf

Cavoukian, A., & Dixon, M. (2013). *Privacy and Security by Design: An Enterprise Architecture Approach*. https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf

Centre for Reviews and Dissemination. (2009). *Systematic reviews: CRD's guidance for undertaking reviews in health care*. University of York.

Centrum Informatiebeveiliging en Privacybescherming (CIP). (2017). *Privacy Volwassenheidsmodel*. https://www.cip-overheid.nl/media/1141/20171102-privacy-volwassenheidsmodel-v3_0_9.pdf

Centrum Informatiebeveiliging en Privacybescherming (CIP). (2019). *Privacy Impact Assessment: Een door de SVB ontwikkeld template voor de uitvoering van PIA's*. https://www.cip-overheid.nl/media/1456/20190807-pia-template-v11.pdf

Charmaz, K. (2014). *Constructing grounded theory* (2nd edition). Sage.

Chaudhuri, A. (2018). *Smart Products and Services Adopt a Privacy-by-Design Approach to Build Trust*. Tata Consultancy Services.

Chaudhuri, A., & Cavoukian, A. (2018). The Proactive and Preventive Privacy (3P) Framework for IoT Privacy by Design. *EDPACS*, *57*(1), 1–16. https://doi.org/10.1080/07366981.2017.1343548

Chen, W. (2010). *Kalido Data Governance Maturity Model*. https://docplayer.net/2788287-Kalido-data-governance-maturity-model.html

Cheng, G., Li, Y., Gao, Z., & Liu, X. (2017). Cloud Data Governance Maturity Model. *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 517–520. https://doi.org/10.1109/ICSESS.2017.8342968

Chhetri, T. R., Kurteva, A., DeLong, R. J., Hilscher, R., Korte, K., & Fensel, A. (2022). Data Protection by Design Tool for Automated GDPR Compliance Verification Based on Semantically Modeled Informed Consent. *Sensors*, *22*(7), 2763. https://doi.org/10.3390/s22072763

Chiesa, V., Coughlan, P., & Voss, C. A. (1996). Development of a Technical Innovation Audit. *Journal of Product Innovation Management*, *13*(2), 105–136. https://doi.org/10.1016/0737-6782(95)00109-3

Clarke, R. (2009). Privacy impact assessment: Its origins and development. *Computer Law & Security Review*, *25*(2), 123–135. https://doi.org/10.1016/j.clsr.2009.02.002

Cleven, A., Winter, R., & Wortmann, F. (2012). Managing Process Performance to Enable Corporate Sustainability: A Capability Maturity Model. In J. vom Brocke, S. Seidel, & J. Recker (Eds.), *Green Business Process Management* (pp. 111–129). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-27488-6_7

CMMI Institute. (2019). *Data Management Maturity (DMM) Model*. https://stage.cmmiinstitute.com/getattachment/cb35800b-720f-4afe-93bf-86ccefb1fb17/attachment.aspx

CMS. (2022). *GDPR Enforcement Tracker—List of GDPR fines*. Enforcementtracker. https://www.enforcementtracker.com

Cohen, J. E. (2001). Privacy, Ideology, and Technology: A Response to Jeffrey Rosen. *THE GEORGETOWN LAW JOURNAL*, *89*, 18.

Commission Nationale de l'Informatique et des Libertés. (2019). *The open source PIA software helps to carry out data protection impact assessment*. CNIL. https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment

Compliance, Governance and Oversight Council (CGOC). (2018). *Information Governance Maturity Model*. https://community.ibm.com/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=fa0b2e30-817b-b948-1833-c097d6eb651e&forceDialog=0

Corbin, J. M., & Strauss, A. L. (2015). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (Fourth edition). SAGE.

Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2022). *Introduction to algorithms* (Fourth edition). The MIT Press.

Crosby, P. B. (1979). *Quality is Free: The Art of Making Quality Certain*. McGraw-Hill. https://archive.org/details/qualityisfree00cros/mode/2up

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Ćurković, M., & Košec, A. (2018). Bubble effect: Including internet search engines in systematic reviews introduces selection bias and impedes scientific reproducibility. *BMC Medical Research Methodology*, *18*(1), 130. https://doi.org/10.1186/s12874-018-0599-2

Data Protection Commission. (2021). *In the matter of WhatsApp Ireland Limited: DECISION*. https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf

DataFlux Corporation. (2007). *The Data Governance Maturity Model*.

Datatilsynet. (2017). *Software development with Data Protection by Design and by Default*. Datatilsynet. https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/

de Bruin, T., Rosemann, M., Freeze, R., & Kaulkarni, U. (2005). Understanding the Main Phases of Developing a Maturity Assessment Model. *ACIS 2005 Proceedings*, 11. https://www.researchgate.net/publication/27482282_Understanding_the_Main_Phases_of_Developing_a_Maturity_Assessment_Model/link/00b7d51f71c388cc54000000/download

Demir, C., & Kocabaş, İ. (2010). Project Management Maturity Model (PMMM) in educational organizations. *Procedia - Social and Behavioral Sciences*, *9*, 1641–1645. https://doi.org/10.1016/j.sbspro.2010.12.379

Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Joosen, W. (2011). A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*, *16*(1), 3–32. https://doi.org/10.1007/s00766-010-0115-7

Denscombe, M. (2014). *The good research guide: For small-scale social research projects* (5. ed). Open University Press.

Diamantopoulou, V., Kalloniatis, C., Gritzalis, S., & Mouratidis, H. (2017). Supporting Privacy by Design Using Privacy Process Patterns. In S. De Capitani di Vimercati & F. Martinelli (Eds.), *ICT Systems Security and Privacy Protection* (Vol. 502, pp. 491–505). Springer International Publishing. https://doi.org/10.1007/978-3-319-58469-0_33

Diamantopoulou, V., & Karyda, M. (2022). Integrating Privacy-By-Design with Business Process Redesign. In S. Katsikas, C. Lambrinoudakis, N. Cuppens, J. Mylopoulos, C. Kalloniatis, W. Meng, S. Furnell, F. Pallas, J. Pohle, M. A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. Maestre Vidal, & M. A. Sotelo Monge (Eds.), *Computer Security. ESORICS 2021 International Workshops* (Vol. 13106, pp. 127–137). Springer International Publishing. https://doi.org/10.1007/978-3-030-95484-0_8

Digital.ai. (2021). *15th Annual State Of Agile Report*. https://digital.ai/resource-center/analyst-reports/state-of-agile-report

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Drev, M., & Delak, B. (2022). Conceptual Model of Privacy by Design. *Journal of Computer Information Systems*, *62*(5), 888–895. https://doi.org/10.1080/08874417.2021.1939197

EDM Council. (2021). *The DCAM Framework*. https://cdn.ymaws.com/edmcouncil.org/resource/collection/AC65DC50-5687-4942-9B53-3398C887A578/DCAM_Overview_2021_update.pdf

Egelman, S., Felt, A. P., & Wagner, D. (2013). Choice Architecture and Smartphone Privacy: There's a Price for That. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 211–236). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39498-0_10

Eliot & associates. (2005). *Guidelines for Conducting a Focus Group*. https://datainnovationproject.org/wp-content/uploads/2017/04/4_How_to_Conduct_a_Focus_Group-2-1.pdf

European Commission. (2010). *A Digital Agenda for Europe*. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF

European Commission. (2016). *Regulation EU 2016/679 of the European Parliament and of the Council (GDPR)*.

European Commission. (2021). *Digital Rights and Principles* (No. 518; Special Eurobarometer). Publications Office. https://data.europa.eu/doi/10.2759/30275

European Network and Information Security Agency (ENISA). (2014). *Privacy and data protection by design: From policy to engineering.* Publications Office. https://data.europa.eu/doi/10.2824/38623

European Parliament and Council of the European Union. (2016). *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)*. http://data.europa.eu/eli/reg/2016/679/2016-05-04

Federal Trade Commission. (2022). *Privacy and Security Enforcement Cases*. Federal Trade Commission. http://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement

Felt, A. P., Egelman, S., & Wagner, D. (2012). *I've got 99 problems, but vibration ain't one: A survey of smartphone users' concerns*. 11.

Fhom, H. S., & Bayarou, K. M. (2011). Towards a Holistic Privacy Engineering Approach for Smart Grid Systems. *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, 234–241. https://doi.org/10.1109/TrustCom.2011.32

Forsberg, C., Foss, A., & Abou-Jaoude, A. (2022). Fission battery economics-by-design. *Progress in Nuclear Energy*, *152*, 104366. https://doi.org/10.1016/j.pnucene.2022.104366

Forsberg, K., & Mooz, H. (1991). The Relationship of System Engineering to the Project Cycle. *INCOSE International Symposium*, *1*(1), 57–65. https://doi.org/10.1002/j.2334-5837.1991.tb01484.x

Fort Privacy. (2022). *The Fort Privacy GDPR Compliance Framework*. https://www.fortprivacy.ie/insights/introducing-the-fort-privacy-maturity-model-framework-whitepaper/#framework-download

Fox, C. (2022, May 6). IKEA Canada confirms data breach involving personal information of approximately 95,000 customers. *CTV News Channel*. https://toronto.ctvnews.ca/ikea-canada-confirms-data-breach-involving-personal-information-of-approximately-95-000-customers-1.5892457

Fraser, P., Moultrie, J., & Gregory, M. (2002). *The use of maturity models / grids as a tool in assessing product development capability: A review*. *1*, 244–249. https://doi.org/10.1109/IEMC.2002.1038431

Garcia, A., Calle, L., Raymundo, C., Dominguez, F., & Moguerza, J. M. (2018). Personal data protection maturity model for the micro financial sector in Peru. *2018 4th International Conference on Computer and Technology Applications (ICCTA)*, 20–24. https://doi.org/10.1109/CATA.2018.8398649

Garousi, V., Felderer, M., & Mäntylä, M. V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology*, *106*, 101–121. https://doi.org/10.1016/j.infsof.2018.09.006

Garousi, V., & Mäntylä, M. V. (2016). When and what to automate in software testing? A multi-vocal literature review. *Information and Software Technology*, *76*, 92–117. https://doi.org/10.1016/j.infsof.2016.04.015

Gerards, J., Schäfer, M. T., Vankan, A., & Muis, I. (2021). *Impact Assessment Mensenrechten en Algoritmes*. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. https://open.overheid.nl/documenten/ronl-c3d7fe94-9c62-493f-b858-f56b5e246a94/pdf

Gkotsopoulou, O., Charalambous, E., Limniotis, K., Quinn, P., Kavallieros, D., Sargsyan, G., Shiaeles, S., & Kolokotronis, N. (2019). Data Protection by Design for cybersecurity systems in a Smart Home environment. *2019 IEEE Conference on Network Softwarization (NetSoft)*, 101–109. https://doi.org/10.1109/NETSOFT.2019.8806694

Gökalp, M. O., Gökalp, E., Kayabay, K., Koçyiğit, A., & Eren, P. E. (2021). The development of the data science capability maturity model: A survey-based research. *Online Information Review*. https://doi.org/10.1108/OIR-10-2020-0469

Google Scholar. (2023). *Privacy design strategies Total citations*. Google Scholar. https://scholar.google.nl/citations?view_op=view_citation&hl=en&user=QWyYRlkAAAAJ&citation_for_view=QWyYRlkAAAAJ:_xSYboBqXhAC

Gotterbarn, D., Miller, K., & Rogerson, S. (1997). Software engineering code of ethics. *Communications of the ACM*, *40*(11), 110–118. https://doi.org/10.1145/265684.265699

Gürses, F. S. (2010). *Multilateral Privacy Requirements Analysis in Online Social Network Services*. Katholieke Universiteit Leuven.

Gurses, S., Troncoso, C., & Diaz, C. (2011). *Engineering Privacy by Design*. 25.

Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S., & Balissa, A. (2018). Privacy by designers: Software developers' privacy mindset. *Empirical Software Engineering*, *23*(1), 259–289. https://doi.org/10.1007/s10664-017-9517-1

Hammer, M. (2007). The Process Audit. *Harvard Business Review*.

Hansen, B., Rose, J., & Tjørnehøj, G. (2004). Prescription, description, reflection: The shape of the software process improvement field. *International Journal of Information Management*, *24*(6), 457–472. https://doi.org/10.1016/j.ijinfomgt.2004.08.007

Hayes, W., & Zubrow, D. (1995). *Moving On Up: Data and Experience Doing CMM-Based Process Improvement* (CMU/SEI-95-TR-008; p. 41). Software Engineering Institute, Carnegie Mellon University.

Herbsleb, J. D., & Goldenson, D. R. (1996). A systematic survey of CMM experience and results. *Proceedings of IEEE 18th International Conference on Software Engineering*, 323–330. https://doi.org/10.1109/ICSE.1996.493427

Hevner, A., & Chatterjee, S. (2010). *Design Research in Information Systems* (Vol. 22). Springer US. https://doi.org/10.1007/978-1-4419-5653-8

Hevner, A., March, S., Jinsoo, P., & Ram, S. (2004). Design Science In Information Systems Research. *MIS Quarterly*, 75–105.

Higgins, J. P. T., Thomas, J., Chandler, J., Cumpston, M., Li, T., Page, M. J., & Welch, V. A. (Eds.). (2020). *Cochrane handbook for systematic reviews of interventions* (Second edition). Wiley-Blackwell.

Hirsch, D. D. (2011). The law and policy of online privacy: Regulation, self-regulation, or co-regulation. *Seattle University Law Review*, *34*(2), 439–480.

Hoepman, J.-H. (2014). Privacy Design Strategies. In N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, & T. Sans (Eds.), *ICT Systems Security and Privacy Protection* (Vol. 428, pp. 446–459). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-55415-5_38

Hoepman, J.-H. (2022). *Privacy Design Strategies (The Little Blue Book)*. https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf

Huang, S.-J., & Han, W.-M. (2006). Selection priority of process areas based on CMMI continuous representation. *Information & Management*, *43*(3), 297–307. https://doi.org/10.1016/j.im.2005.08.003

Huth, D., & Matthes, F. (2019). "Appropriate Technical and Organizational Measures": Identifying Privacy Engineering Approaches to Meet GDPR Requirements. *AMCIS 2019 Proceedings*, 10.

iapp. (2020). *Private Sector PIA Template*. https://iapp.org/resources/article/private-sector-privacy-impact-assessment-template/

IBM. (2007). *The IBM Data Governance Council Maturity Model: Building a roadmap for effective data governance*. http://www.databaser.net/moniwiki/pds/DataWarehouse/leverage_wp_data_gov_council_maturity_model.pdf

Iezzi, M. (2021). *The Evolving Path of 'the Right to Be Left Alone'—When Privacy Meets Technology* (arXiv:2111.12434). arXiv. http://arxiv.org/abs/2111.12434

Information and privacy commission New South Wales. (2020). *Fact Sheet—Privacy by design*. https://www.ipc.nsw.gov.au/fact-sheet-privacy-design

Information Commissioner's Office (ICO). (2018). *Sample DPIA template*. https://ico.org.uk/media/2258461/dpia-template-v04-post-comms-review-20180308.pdf

Information Commissioner's Office (ICO). (2022, October 17). *Data protection by design and default*. Ico. Information Commissioner's Office; ICO. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

Intel Privacy Office. (2013). *Managing the Privacy Maturity of a Standalone Subsidiary*.

International Conference of Data Protection and Privacy Commissioners. (2010). *Resolution on Privacy by Design*. 32nd International Conference of Data Protection and Privacy Commissioners. https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf

Isaksson, R., & Cöster, M. (2018). *Testing a Maturity Grid for Assessing Sustainability Reports*. 13. https://uu.diva-portal.org/smash/get/diva2:1267383/FULLTEXT01.pdf

ISO/IEC. (2011). *ISO/IEC TR 29110-5-1-2 Software engineering—Lifecycle profiles for Very Small Entities (VSEs)—Part 5-1-2: Management and engineering guide: Generic profile group: Basic profile*.

ISO/IEC. (2017). *INTERNATIONAL STANDARD ISO/IEC 29134 Information technology—Security techniques—Guidelines for privacy impact assessment*.

IT GOVERNANCE. (2021). *Privacy by Design – Step by step*. https://www.itgovernance.eu/blog/en/the-gdpr-why-you-need-to-adopt-the-principles-of-privacy-by-design

Jansen, A., & Bosch, J. (2005). Software Architecture as a Set of Architectural Design Decisions. *5th Working IEEE/IFIP Conference on Software Architecture (WICSA'05)*, 109–120. https://doi.org/10.1109/WICSA.2005.61

Jansen, S. (2020). A focus area maturity model for software ecosystem governance. *Information and Software Technology*, *118*, 106219. https://doi.org/10.1016/j.infsof.2019.106219

Jansen, S., & Yang, Z. (2020). Source Data for the Focus Area Maturity Model for Software Ecosystem Governance. *Data in Brief*, *31*, 105656. https://doi.org/10.1016/j.dib.2020.105656

Johnson, C. A. (1974). *PRIVACY AS PERSONAL CONTROL*. 18.

Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2008). Addressing privacy requirements in system design: The PriS method. *Requirements Engineering*, *13*(3), 241–255. https://doi.org/10.1007/s00766-008-0067-3

Kalloniatis, C., Lambrinoudakis, C., Musahl, M., Kanatas, A., & Gritzalis, S. (2021). Incorporating privacy by design in body sensor networks for medical applications: A privacy and data protection framework. *Computer Science and Information Systems*, *18*(1), 323–347. https://doi.org/10.2298/CSIS200922057K

Karlsson, F., & Ågerfalk, P. J. (2004). Method configuration: Adapting to situational characteristics while creating reusable assets. *Information and Software Technology*, *46*(9), 619–633. https://doi.org/10.1016/j.infsof.2003.12.004

King, J. L., & Kraemer, K. L. (1984). Evolution and organizational information systems: An assessment of Nolan's stage model. *Communications of the ACM*, *27*(5), 466–475. https://doi.org/10.1145/358189.358074

Kitchenham, B. (2004). *Procedures for Performing Systematic Reviews* (NICTA Technical Report 0400011T.1; p. 34). Keele University. https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf

Kitchenham, B., Budgen, D., & Brereton, P. (2015). *Evidence-Based Software Engineering and Systematic Reviews*. Chapman and Hall/CRC. https://doi.org/10.1201/b19467

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering* (EBSE Technical Report EBSE-2007- 01) [Technical Report]. Keele University and Durham University.

Klimko, G. (2001). Knowledge Management and Maturity Models: Building Common Understanding. *Proceedings of the 2nd European Conference on Knowledge Management*, *2*, 269–278.

Kohl, C., McIntosh, E. J., Unger, S., Haddaway, N. R., Kecke, S., Schiemann, J., & Wilhelm, R. (2018). Online tools supporting the conduct and reporting of systematic reviews and systematic maps: A case study on CADIMA and review of existing tools. *Environmental Evidence*, *7*(1), 8. https://doi.org/10.1186/s13750-018-0115-5

Kohlegger, M., Maier, R., & Thalmann, S. (2009). Understanding maturity models Results of a Structured Content Analysis. *Proceedings of I-KNOW '09 and I-SEMANTICS '09*, 12. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=0d74407d74883760c630aa41699a5c3028573c75

Koops, B.-J., Hoepman, J.-H., & Leenes, R. (2013). Open-source intelligence and privacy by design. *Computer Law & Security Review*, *29*(6), 676–688. https://doi.org/10.1016/j.clsr.2013.09.005

Koops, B.-J., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. *International Review of Law, Computers & Technology*, *28*(2), 159–171. https://doi.org/10.1080/13600869.2013.801589

Koorn, R., & ter Hart, J. (2011). Privacy by design: From privacy policy to privacy-enhancing technologies. *Compact_ IT Advisory*, 11.

Kost, M., Freytag, J.-C., Kargl, F., & Kung, A. (2011). Privacy Verification Using Ontologies. *2011 Sixth International Conference on Availability, Reliability and Security*, 627–632. https://doi.org/10.1109/ARES.2011.97

Kroener, I., & Wright, D. (2014). A Strategy for Operationalizing Privacy by Design. *The Information Society*, *30*(5), 355–365. https://doi.org/10.1080/01972243.2014.944730

Krueger, R. A., & Casey, M. A. (2015). *Focus groups: A practical guide for applied research* (5th edition). SAGE.

Kulkarni, U., & St. Louis, R. (2003). *Organizational Self Assessment of Knowledge Management Maturity*. 10. https://www.researchgate.net/publication/220892849_Organizational_Self_Assessment_of_Knowledge_Management_Maturity/link/0c96052e908e39454c000000/download

Kung, A. (2014). PEARs: Privacy Enhancing ARchitectures. In B. Preneel & D. Ikonomou (Eds.), *Privacy Technologies and Policy* (Vol. 8450, pp. 18–29). Springer International Publishing. https://doi.org/10.1007/978-3-319-06749-0_2

Kung, A., Freytag, J.-C., & Kargl, F. (2011). Privacy-by-design in ITS applications. *2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 1–6. https://doi.org/10.1109/WoWMoM.2011.5986166

La Agencia Española de Protección de Datos. (2019). *A Guide to Privacy by Design*. https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

Labadie, C., & Legner, C. (2019). Understanding Data Protection Regulations from a Data Management Perspective: A Capability-Based Approach to EU-GDPR. *WIRTSCHAFTSINFORMATIK 2019 PROCEEDINGS*, 15.

Lane, J., & Schur, C. (2010). Balancing Access to Health Data and Privacy: A Review of the Issues and Approaches for the Future: Balancing Access to Health Data and Privacy. *Health Services Research*, *45*(5p2), 1456–1467. https://doi.org/10.1111/j.1475-6773.2010.01141.x

Lanier, C. D., & Saini, A. (2008). Understanding Consumer Privacy: A Review and Future Directions. *Academy of Marketing Science Review*, *12*(2), 1–45.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, *33*(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Let's Encrypt. (2023). *Let's Encrypt*. https://letsencrypt.org/

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471–481. https://doi.org/10.1016/j.dss.2012.06.010

Lin, H. (2007). Knowledge sharing and firm innovation capability: An empirical study. *International Journal of Manpower*, *28*(3/4), 315–332. https://doi.org/10.1108/01437720710755272

London Economics. (2010). *Study on the economic benefits of privacy-enhancing technologies (PETs)* (p. 259). https://londoneconomics.co.uk/wp-content/uploads/2011/09/17-Study-on-the-economic-benefits-of-privacy-enhancing-technologies-PETs.pdf

Maier, A. M., Moultrie, J., & Clarkson, P. J. (2012). Assessing Organizational Capabilities: Reviewing and Guiding the Development of Maturity Grids. *IEEE Transactions on Engineering Management*, *59*(1), 138–159. https://doi.org/10.1109/TEM.2010.2077289

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251–266. https://doi.org/10.1016/0167-9236(94)00041-2

Marchildon, P., Bourdeau, S., Hadaya, P., & Labissière, A. (2018). Data governance maturity assessment tool: A design science approach: *Projectics / Proyéctica / Projectique*, *n°20*(2), 155–193. https://doi.org/10.3917/proj.020.0155

Margulis, S. T. (1977). Conceptions of Privacy: Current Status and Next Steps. *Journal of Social Issues*, *33*(3), 5–21. https://doi.org/10.1111/j.1540-4560.1977.tb01879.x

Marshall, S., & Mitchell, G. (2002). An E-Learning Maturity Model? *Proceedings of the 19th Annual Conference of the Australian Society for Computers in Learning in Tertiary Education*, 10.

Martin, Y.-S., del Alamo, J. M., & Yelmo, J. C. (2014). Engineering privacy requirements valuable lessons from another realm. *2014 IEEE 1st International Workshop on Evolving Security and*

Privacy Requirements Engineering (ESPRE), 19–24. https://doi.org/10.1109/ESPRE.2014.6890523

Martin, Y.-S., & Kung, A. (2018). Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering. *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 108–111. https://doi.org/10.1109/EuroSPW.2018.00021

Matavire, R., & Brown, I. (2013). Profiling grounded theory approaches in information systems research. *European Journal of Information Systems*, *22*(1), 119–129. https://doi.org/10.1057/ejis.2011.35

McCormack, K., Willems, J., van den Bergh, J., Deschoolmeester, D., Willaert, P., Indihar Štemberger, M., Škrinjar, R., Trkman, P., Bronzo Ladeira, M., Paulo Valadares de Oliveira, M., Bosilj Vuksic, V., & Vlahovic, N. (2009). A global investigation of key turning points in business process maturity. *Business Process Management Journal*, *15*(5), 792–815. https://doi.org/10.1108/14637150910987946

McGrath, Y., Sumnall, H., Edmonds, K., McVeigh, J., & Bellis, M. (2006). *Review of grey literature on drug prevention among young people*. National Institute for Health and Clinical Excellence. http://www.publichealth.nice.org.uk/download.aspx?o=316428

Mead, N. R., Miyazaki, S., & Zhan, J. (2011). Integrating privacy requirements considerations into a security requirements engineering method and tool. *International Journal of Information Privacy, Security and Integrity*, *1*(1), 106. https://doi.org/10.1504/IJIPSI.2011.043733

Merkus, J. (2015). *Data Governance Maturity Model* [Master Thesis, Open University]. http://rgdoi.net/10.13140/RG.2.2.19274.16321

Merkus, J., Helms, R., & Kusters, R. (2021). Data Governance Capabilities: Maturity Model Design with Generic Capabilities Reference Model: *Proceedings of the 13th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*, 102–109. https://doi.org/10.5220/0010651300003064

Merriam-Webster. (2022a). *Definition of Capability*. https://www.merriam-webster.com/dictionary/capability

Merriam-Webster. (2022b). *Definition of Capable*. https://www.merriam-webster.com/dictionary/capable

Merriam-Webster. (2022c). *Definition of Mature*. https://www.merriam-webster.com/dictionary/mature

Merriam-Webster. (2022d). *Definition of Maturity*. https://www.merriam-webster.com/dictionary/maturity

Mettler, T. (2010). Thinking in Terms of Design Decisions When Developing Maturity Models: *International Journal of Strategic Decision Sciences*, *1*(4), 76–87. https://doi.org/10.4018/jsds.2010100105

Mettler, T. (2011). Maturity assessment models: A design science research approach. *International Journal of Society Systems Science*, *3*(1/2), 81. https://doi.org/10.1504/IJSSS.2011.038934

Mettler, T., & Rohner, P. (2009). Situational maturity models as instrumental artifacts for organizational design. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology - DESRIST '09*, 1. https://doi.org/10.1145/1555619.1555649

Mettler, T., Rohner, P., & Winter, R. (2010). Towards a Classification of Maturity Models in Information Systems. In A. D'Atri, M. De Marco, A. M. Braccini, & F. Cabiddu (Eds.), *Management of the Interconnected World* (pp. 333–340). Physica-Verlag HD. https://doi.org/10.1007/978-3-7908-2404-9_39

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information Privacy: Corporate Management and National Regulation. *Organization Science*, *11*(1), 35–57. https://doi.org/10.1287/orsc.11.1.35.12567

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook* (Third edition). SAGE Publications, Inc.

Morales-Trujillo, M. E., & Garcia-Mireles, G. A. (2018). Extending ISO/IEC 29110 Basic Profile with Privacy-by-Design Approach: A Case Study in the Health Care Sector. *2018 11th International Conference on the Quality of Information and Communications Technology (QUATIC)*, 56–64. https://doi.org/10.1109/QUATIC.2018.00018

Moultrie, J., Sutcliffe, L., & Maier, A. (2016). A maturity grid assessment tool for environmentally conscious design in the medical device industry. *Journal of Cleaner Production*, *122*, 252–265. https://doi.org/10.1016/j.jclepro.2015.10.108

Mylopoulos, J. (1992). Conceptual Modelling and Telos. *Conceptual Modelling, Databases, and CASE: An Integrated View of Information System Development*, 49–68.

NetworkX. (2022). *topological_generations—NetworkX 2.8.8 documentation*. https://networkx.org/documentation/stable/reference/algorithms/generated/networkx.algorithms.dag.topological_generations.html#networkx.algorithms.dag.topological_generations

Niazi, M., Saeed, A. M., Alshayeb, M., Mahmood, S., & Zafar, S. (2020). A maturity model for secure requirements engineering. *Computers & Security*, *95*, 101852. https://doi.org/10.1016/j.cose.2020.101852

Niazi, M., Wilson, D., & Zowghi, D. (2005). A maturity model for the implementation of software process improvement: An empirical study. *Journal of Systems and Software*, *74*(2), 155–172. https://doi.org/10.1016/j.jss.2003.10.017

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Normann Andersen, K., Lee, J., Mettler, T., & Moon, M. J. (2020). Ten Misunderstandings about Maturity Models. *The 21st Annual International Conference on Digital Government Research*, 261–266. https://doi.org/10.1145/3396956.3396980

Notario, N., Crespo, A., Martin, Y.-S., Del Alamo, J. M., Metayer, D. L., Antignac, T., Kung, A., Kroener, I., & Wright, D. (2015). PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology. *2015 IEEE Security and Privacy Workshops*, 151–158. https://doi.org/10.1109/SPW.2015.22

Oetzel, M. C., & Spiekermann, S. (2014). A systematic methodology for privacy impact assessments: A design science approach. *European Journal of Information Systems*, *23*(2), 126–150. https://doi.org/10.1057/ejis.2013.18

Oetzel, M. C., Spiekermann, S., Grüning, I., Kelter, H., & Mull, S. (2011). *Privacy Impact Assessment Guideline for RFID Applications* (J. Cantella, Ed.). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf%3F__blob%3DpublicationFile%26v%3D1

Office of management & enterprise services. (2020). *Data governance maturity model*. https://hnu.edu/wp-content/uploads/2020/03/Data-Governance-Maturity-Model.pdf

Overeem, M., Mathijssen, M., & Jansen, S. (2022). API-m-FAMM: A focus area maturity model for API Management. *Information and Software Technology*, *147*, 106890. https://doi.org/10.1016/j.infsof.2022.106890

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M.,

Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 1–9. https://doi.org/10.1136/bmj.n71

Patten, M. L. (2017). *Questionnaire research: A practical guide* (Fourth edition). Routledge.

Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). *Capability Maturity Model for Software, Version 1.1:* Defense Technical Information Center. https://doi.org/10.21236/ADA263403

Pedroza, G., Muntes-Mulero, V., Martin, Y. S., & Mockly, G. (2021). A Model-based Approach to Realize Privacy and Data Protection by Design. *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 332–339. https://doi.org/10.1109/EuroSPW54576.2021.00042

Perera, C., McCormick, C., Bandara, A. K., Price, B. A., & Nuseibeh, B. (2016). Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms. *Proceedings of the 6th International Conference on the Internet of Things*, 83–92. https://doi.org/10.1145/2991561.2991566

Pfeffer, J., & Sutton, R. I. (1999). Knowing "What" to do is not Enough: Turning Knowledge into Action. *California Management Review*, *42*(1), 26. https://doi.org/10.1177/000812569904200101

Pflügler, C., Böhm, M., & Krcmar, H. (2015). *Coping with IT Carve-out Projects – Towards a Maturity Model*. 16.

Piras, L., Al-Obeidallah, M. G., Pavlidis, M., Mouratidis, H., Tsohou, A., Magkos, E., Praitano, A., Iodice, A., & Crespo, B. G.-N. (2020). DEFeND DSM: A Data Scope Management Service for Model-Based Privacy by Design GDPR Compliance. In S. Gritzalis, E. R. Weippl, G. Kotsis, A. M. Tjoa, & I. Khalil (Eds.), *Trust, Privacy and Security in Digital Business* (Vol. 12395, pp. 186–201). Springer International Publishing. https://doi.org/10.1007/978-3-030-58986-8_13

Ponemon Institute & IBM. (2021). *Cost of a Data Breach Report 2021* (p. 73). https://www.ibm.com/downloads/cas/OJDVQGRY

Pöppelbuß, J., Niehaves, B., Simons, A., & Becker, J. (2011). Maturity Models in Information Systems Research: Literature Search and Analysis. *Communications of the Association for Information Systems*, *29*. https://doi.org/10.17705/1CAIS.02927

Pöppelbuß, J., & Röglinger, M. (2011). What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management. *ECIS 2011 Proceedings. 28*, *19*, 28. http://aisel.aisnet.org/ecis2011/28

Prat, N., Comyn-Wattiau, I., & Akoka, J. (2015). A Taxonomy of Evaluation Methods for Information Systems Artifacts. *Journal of Management Information Systems*, *32*(3), 229–267. https://doi.org/10.1080/07421222.2015.1099390

PricewaterhouseCoopers. (2021). *Privacy by Design as license to operate for new business initiatives*. https://www.pwc.nl/nl/digital/cybersecurity/documents/pwc-privacy-by-design.pdf

Privacy Company. (2019). *Privacy-by-design framework*. https://www.privacycompany.eu/knowledge-base-nl/privacy-by-design-framework

privacypatterns.org. (2023). *Privacy Patterns*. https://privacypatterns.org/

Proença, D., & Borbinha, J. (2016). Maturity Models for Information Systems—A State of the Art. *Procedia Computer Science*, *100*, 1042–1049. https://doi.org/10.1016/j.procs.2016.09.279

Proenca, D., Vieira, R., & Borbinha, J. (2016). A maturity model for information governance. *2016 11th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6. https://doi.org/10.1109/CISTI.2016.7521480

Pullen, W. (2007). A public sector HPT maturity model. *Performance Improvement*, *46*(4), 9–15. https://doi.org/10.1002/pfi.119

Qi, X. (2016). *Privacy Maturity Model: Towards Privacy-by-Design Best Practices* [Master Thesis, Leiden University]. https://theses.liacs.nl/pdf/Qi-Xin-non-confidential.pdf

Raulamo-Jurvanen, P., Kakkonen, K., & Mäntylä, M. (2016). Using Surveys and Web-Scraping to Select Tools for Software Testing Consultancy. In P. Abrahamsson, A. Jedlitschka, A. Nguyen Duc, M. Felderer, S. Amasaki, & T. Mikkonen (Eds.), *Product-Focused Software Process Improvement* (Vol. 10027, pp. 285–300). Springer International Publishing. https://doi.org/10.1007/978-3-319-49094-6_18

Raza, A., Capretz, L. F., & Ahmed, F. (2012). An open source usability maturity model (OS-UMM). *Computers in Human Behavior*, *28*(4), 1109–1121. https://doi.org/10.1016/j.chb.2012.01.018

Reuters. (2021, October 7). Amazon's Twitch blames configuration error for data breach. *Reuters*. https://www.reuters.com/technology/amazons-twitch-hit-by-data-breach-2021-10-06/

Rivera, S., Loarte, N., Raymundo, C., & Dominguez, F. (2017). Data Governance Maturity Model for Micro Financial Organizations in Peru: *Proceedings of the 19th International Conference on Enterprise Information Systems*, 203–214. https://doi.org/10.5220/0006149202030214

Roberts, R. (2020). Qualitative Interview Questions: Guidance for Novice Researchers. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2020.4640

Robson, C., & McCartan, K. (2016). *Real world research* (4th ed.). John Wiley & Sons Ltd.

Röglinger, M., Pöppelbuß, J., & Becker, J. (2012). Maturity models in business process management. *Business Process Management Journal*, *18*(2), 328–346. https://doi.org/10.1108/14637151211225225

Romme, G. (2016). *The Quest for Professionalism: The Case of Management and Entrepreneurship*. Oxford University Press.

Rosemann, M., & de Bruin, T. (2005). *Towards a Business Process Management Maturity Model*. 13.

Rosen, J. (2001). *The unwanted gaze: The destruction of privacy in America* (1st Vintage Books ed). Vintage Books. https://archive.org/details/unwantedgazedest0000rose/page/94/mode/2up

Rubin, H., & Rubin, I. (2005). *Qualitative Interviewing: The Art of Hearing Data* (2nd ed.). SAGE Publications, Inc. https://doi.org/10.4135/9781452226651

Rubinstein, I. S., & Good, N. (2013). Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents. *Berkeley Tech. LJ*, *28*, 1333.

Runeson, P., & Höst, M. (2009). Guidelines for conducting and reporting case study research in software engineering. *Empirical Software Engineering*, *14*(2), 131–164. https://doi.org/10.1007/s10664-008-9102-8

Sabo, J., Drgon, M., & Magnuson, G. (2016). *Privacy Management Reference Model and Methodology (PMRM) Version 1.0*. https://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.pdf

Sanchez-Puchol, F., & Pastor-Collado, J. A. (2017). Focus Area Maturity Models: A Comparative Review. In M. Themistocleous & V. Morabito (Eds.), *Information Systems* (pp. 531–544). Springer International Publishing.

Schaar, P. (2010). Privacy by Design. *Identity in the Information Society*, *3*(2), 267–274. https://doi.org/10.1007/s12394-010-0055-x

Schoeman, F. D. (Ed.). (1984). *Philosophical dimensions of privacy: An anthology* (Digitally pr). Cambridge Univ. Pr. https://archive.org/details/philosophicaldim0000unse_g8h7

Secure Controls Framework. (2022). *Cybersecurity & privacy capability maturity model*. https://securecontrolsframework.com/capability-maturity-model/

Seidman, I. (2006). *Interviewing as qualitative research: A guide for researchers in education and the social sciences* (3rd ed). Teachers College Press.

Semantha, F. H., Azam, S., Shanmugam, B., Yeo, K. C., & Beeravolu, A. R. (2021). A Conceptual Framework to Ensure Privacy in Patient Record Management System. *IEEE Access*, *9*, 165667–165689. https://doi.org/10.1109/ACCESS.2021.3134873

Semantha, F. H., Azam, S., Yeo, K. C., & Shanmugam, B. (2020). A Systematic Literature Review on Privacy by Design in the Healthcare Sector. *Electronics*, *9*(3), 452. https://doi.org/10.3390/electronics9030452

Senarath, A., & Arachchilage, N. A. G. (2018). Why developers cannot embed privacy into software systems? An empirical investigation. *Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering 2018*, 211–216. https://doi.org/10.1145/3210459.3210484

Sheth, S., Kaiser, G., & Maalej, W. (2014). Us and them: A study of privacy requirements across North America, Asia, and Europe. *Proceedings of the 36th International Conference on Software Engineering*, 859–870. https://doi.org/10.1145/2568225.2568244

Shewart, W. A. (1931). *Economic Control of Quality of Manufactured Product*. Macmillan and Co.

Singer, J., & Vinson, N. G. (2002). Ethical issues in empirical studies of software engineering. *IEEE Transactions on Software Engineering*, *28*(12), 1171–1180. https://doi.org/10.1109/TSE.2002.1158289

Sion, L., Dewitte, P., Van Landuyt, D., Wuyts, K., Emanuilov, I., Valcke, P., & Joosen, W. (2019). An Architectural View for Data Protection by Design. *2019 IEEE International Conference on Software Architecture (ICSA)*, 11–20. https://doi.org/10.1109/ICSA.2019.00010

Sion, L., Dewitte, P., Van Landuyt, D., Wuyts, K., Valcke, P., & Joosen, W. (2020). DPMF: A Modeling Framework for Data Protection by Design. *Enterprise Modelling and Information Systems Architectures (EMISAJ)*, 10:1-53 Pages. https://doi.org/10.18417/EMISA.15.10

Sion, L., Landuyt, D. V., & Joosen, W. (2020). The Never-Ending Story: On the Need for Continuous Privacy Impact Assessment. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 314–317. https://doi.org/10.1109/EuroSPW51379.2020.00049

Sivakumar, S., Wilkinson, D., Cherry, D., Knijnenburg, B. P., Raybourn, E. M., Wisniewski, P., & Sloan, H. (2017). *User-Tailored Privacy by Design*. 14. https://www.researchgate.net/publication/316065468_User-Tailored_Privacy_by_Design/link/58eeab8aa6fdcc61cc12691f/download

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*, 989–1015. https://doi.org/10.2307/41409970

Smits, D., & van Hillegersberg, J. (2015). IT Governance Maturity: Developing a Maturity Model Using the Delphi Method. *2015 48th Hawaii International Conference on System Sciences*, 4534–4543. https://doi.org/10.1109/HICSS.2015.541

Solli-Sæther, H., & Gottschalk, P. (2010). The Modeling Process for Stage Models. *Journal of Organizational Computing and Electronic Commerce*, *20*(3), 279–293. https://doi.org/10.1080/10919392.2010.494535

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477. https://doi.org/10.2307/40041279

Sonnenberg, C., & vom Brocke, J. (2012). Evaluations in the Science of the Artificial – Reconsidering the Build-Evaluate Pattern in Design Science Research. In K. Peffers, M. Rothenberger, & B. Kuechler (Eds.), *Design Science Research in Information Systems. Advances in Theory and Practice* (Vol. 7286, pp. 381–397). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-29863-9_28

Spiekermann, S. (2012). The challenges of privacy by design. *Communications of the ACM*, *55*(7), 38–40. https://doi.org/10.1145/2209249.2209263

Spiekermann, S., & Cranor, L. F. (2009). *Engineering Privacy* (SSRN Scholarly Paper ID 1085333). Social Science Research Network.

Spiekermann, S., Korunovska, J., & Langheinrich, M. (2019). Inside the Organization: Why Privacy and Security Engineering Is a Challenge for Engineers. *Proceedings of the IEEE*, *107*(3), 600–615. https://doi.org/10.1109/JPROC.2018.2866769

Spruit, M., & Röling, M. (2014). Isfam: The Information Security Focus Area Maturity Model. *Proceedings of the European Conference on Information Systems (ECIS) 2014*, 16. https://www.researchgate.net/publication/288134391_ISFAM_The_information_security_focus_area_maturity_model/link/56a775fc08ae0fd8b3fe05dc/download

Stallings, W. (2019). *Information privacy engineering and privacy by design: Understanding privacy threats, technology, and regulations based on standards and best practices* (1st ed.). Pearson Education, Inc.

Stanford Legal Design Lab. (2022). *Privacy Design Pattern Library*. Legal Communication Design. https://legaltechdesign.com/communication-design/privacy-design-pattern-library/

State of Oregon. (2022). *State of Oregon Data Governance Maturity Model*. https://www.oregon.gov/das/Policies/Data%20Governance%20Maturity%20Model.xlsx

Tamò-Larrieux, A. (2018). *Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things* (Vol. 40). Springer International Publishing. https://doi.org/10.1007/978-3-319-98624-1

Teo, T. S. H., & King, W. R. (1997). Integration between Business Planning and Information Systems Planning: An Evolutionary-Contingency Perspective. *Journal of Management Information Systems*, *14*(1), 185–214. https://doi.org/10.1080/07421222.1997.11518158

The Department of Internal Affairs Te Tari Taiwhenua. (2014). *Privacy Maturity Assessment Framework: Elements, attributes, and criteria (version 2.0)*. Department of Internal Affairs on behalf of the New Zealand Government. https://www.digital.govt.nz/assets/Documents/Privacy-Maturity-Assessment-Elements-and-Attributes.pdf

The MITRE Corporation. (2019a). *Privacy Maturity Model Version 1*. https://www.mitre.org/sites/default/files/2021-11/pr-19-3384-privacy-maturity-model.pdf

The MITRE Corporation. (2019b). *MITRE Privacy Engineering Framework and Life Cycle Adaptation Guide*. https://www.mitre.org/sites/default/files/2021-11/pr-19-00598-5-privacy-engineering-framework-v2.pdf

Thomson, J. J. (1975). The Right to Privacy. *Philosophy & Public Affairs*, *4*(4), 295–314.

Timón López, C., Alamillo Domingo, I., & Valero Torrijos, J. (2021). Approaching the Data Protection Impact Assessment as a legal methodology to evaluate the degree of privacy by design achieved in technological proposals. A special reference to Identity Management systems. *The 16th International Conference on Availability, Reliability and Security*, 1–9. https://doi.org/10.1145/3465481.3469207

Tuncel, D., Korner, C., & Plosch, R. (2020). Comparison of Agile Maturity Models: Reflecting the Real Needs. *2020 46th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, 51–58. https://doi.org/10.1109/SEAA51224.2020.00019

van de Weerd, I., & Brinkkemper, S. (2009). Meta-Modeling for Situational Analysis and Design Methods. In *Handbook of research on modern systems analysis and design technologies and applications* (pp. 35–54). IGI Global.

van Dijk, F., Gadellaa, J., van Toledo, C., Spruit, M., Brinkkemper, S., & Brinkhuis, M. (2023). Uncovering the structures of privacy research using bibliometric network analysis and topic

modelling. *Organizational Cybersecurity Journal: Practice, Process and People*. https://doi.org/10.1108/OCJ-11-2021-0034

van Dijk, F., Spruit, M., van Toledo, C., & Brinkhuis, M. (2021). Pillars of Privacy: Identifying Core Theory in a Network Analysis of Privacy Literature. *Proceedings of the Twenty-Ninth European Conference on Information Systems (ECIS 2021)*. Twenty-Ninth European Conference on Information Systems (ECIS 2021). https://aisel.aisnet.org/ecis2021_rp/84

van Dijk, F., van Toledo, C., Spruit, M., Brinkkemper, S., & Brinkhuis, M. (2023). *Explaining organisational privacy behaviour through a privacy calculus model: A theory-building case study of privacy tradeoffs in government systems design [working paper]*.

van Lieshout, M., & Hoepman, J.-H. (2015). *The PI.lab—Four years later*. The Privacy & Identity Lab. https://doi.org/10.13140/RG.2.1.1210.7600

van Lieshout, M., Kool, L., van Schoonhoven, B., & de Jonge, M. (2011). Privacy by Design: An alternative to existing practice in safeguarding privacy. *Info*, *13*(6), 55–68. https://doi.org/10.1108/14636691111174261

van Looy, A., Poels, G., & Snoeck, M. (2017). Evaluating Business Process Maturity Models. *Journal of the Association for Information Systems*, *18*(6), 461–486. https://doi.org/10.17705/1jais.00460

van Puijenbroek, J., & Hoepman, J.-H. (2017). Privacy impact assessments in practice: Outcome of a descriptive field research in the Netherlands. *3rd International Workshop on Privacy Engineering*, 8.

van Rest, J., Boonstra, D., Everts, M., van Rijn, M., & van Paassen, R. (2014). Designing Privacy-by-Design. In B. Preneel & D. Ikonomou (Eds.), *Privacy Technologies and Policy* (Vol. 8319, pp. 55–72). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-54069-1_4

van Steenbergen, M., Bos, R., & Brinkkemper, S. (2013). Improving IS Functions Step by Step: The Use of Focus Area Maturity Models. *Scandinavian Journal of Information Systems*, *25*(2), 35–56.

van Steenbergen, M., Bos, R., Brinkkemper, S., Weerd, I. van de, & Bekkers, W. (2010). *The design of focus area maturity models*. 317–332.

Vemou, K., & Karyda, M. (2019). Evaluating privacy impact assessment methods: Guidelines and best practice. *Information & Computer Security*, *28*(1), 35–53. https://doi.org/10.1108/ICS-04-2019-0047

Venable, J., Pries-Heje, J., & Baskerville, R. (2012). A Comprehensive Framework for Evaluation in Design Science Research. In K. Peffers, M. Rothenberger, & B. Kuechler (Eds.), *Design Science Research in Information Systems. Advances in Theory and Practice* (Vol. 7286, pp. 423–438). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-29863-9_31

Verykios, V. S., Bertino, E., Fovino, I. N., Provenza, L. P., Saygin, Y., & Theodoridis, Y. (2004). State-of-the-art in privacy preserving data mining. *ACM SIGMOD Record*, *33*(1), 50–57. https://doi.org/10.1145/974121.974131

Vicini, S., Alberti, F., Notario, N., Crespo, A., Pastoriza, J. R. T., & Sanna, A. (2016). Co-creating Security-and-Privacy-by-Design Systems. *2016 11th International Conference on Availability, Reliability and Security (ARES)*, 768–775. https://doi.org/10.1109/ARES.2016.74

Vinson, N. G., & Singer, J. (2008). A Practical Guide to Ethical Research Involving Humans. In F. Shull, J. Singer, & D. I. K. Sjøberg (Eds.), *Guide to Advanced Empirical Software Engineering* (pp. 229–256). Springer London. https://doi.org/10.1007/978-1-84800-044-5_9

Walsh, D., Parisi, J. M., & Passerini, K. (2017). Privacy as a right or as a commodity in the online world: The limits of regulatory reform and self-regulation. *Electronic Commerce Research*, *17*(2), 185–203. https://doi.org/10.1007/s10660-015-9187-2

Wang, H., Chen, K., & Xu, D. (2016). A maturity model for blockchain adoption. *Financial Innovation*, *2*(1), 12. https://doi.org/10.1186/s40854-016-0031-z

Wang, Y., Mäntylä, M. V., Liu, Z., Markkula, J., & Raulamo-jurvanen, P. (2022). Improving test automation maturity: A multivocal literature review. *Software Testing, Verification and Reliability*, *32*(3). https://doi.org/10.1002/stvr.1804

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, *20*(3), 267–284. https://doi.org/10.1057/ejis.2010.72

Weinstein, M. A. (1971). The uses of privacy in the good life. In J. R. Pennock & J. W. Chapman (Eds.), *Privacy & personality* (1st ed., pp. 88–104). Transaction Publishers. https://archive.org/details/privacypersonali0000unse/page/n5/mode/2up

Weiss, R. S. (1994). *Learning from strangers: The art and method of qualitative interview studies* (First Free Press paperback ed). Free Press.

Wendler, R. (2012). The maturity of maturity model research: A systematic mapping study. *Information and Software Technology*, *54*(12), 1317–1339. https://doi.org/10.1016/j.infsof.2012.07.007

Westin, A. F. (1967). *Privacy And Freedom*. https://archive.org/embed/privacyfreedom0000west_r3c7

Wieringa, R. J. (2014). *Design Science Methodology for Information Systems and Software Engineering*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-43839-8

Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering - EASE '14*, 1–10. https://doi.org/10.1145/2601248.2601268

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). *Experimentation in Software Engineering*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-29044-2

World Health Organization. (2017). *Code of Conduct for responsible Research*. https://www.who.int/about/ethics/code-of-conduct-for-responsible-research

Wright, D. (2012). The state of the art in privacy impact assessment. *Computer Law & Security Review*, *28*(1), 54–61. https://doi.org/10.1016/j.clsr.2011.11.007

Wuyts, K., & Joosen, W. (2015). *LINDDUN privacy threat: A tutorial* (Volume C685) [Technical Report (CW Reports)]. KU Leuven. https://lirias.kuleuven.be/1652885?limo=0

Wuyts, K., Sion, L., & Joosen, W. (2020). LINDDUN GO: A Lightweight Approach to Privacy Threat Modeling. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 302–309. https://doi.org/10.1109/EuroSPW51379.2020.00047

Yaqiong, C., Zijie, Y., Feng, L., & Jiayin, Q. (2020). Data Privacy Maturity Assessment Practice of Digital Transformation Enterprises under the COVID-19: Taking an Industrial Company in Xiamen as an Example. *Proceedings of the 2020 International Conference on Big Data in Management*, 33–40. https://doi.org/10.1145/3437075.3437084

Zapata, M. L., Berrah, L., & Tabourot, L. (2020). Is a digital transformation framework enough for manufacturing smart products? The case of Small and Medium Enterprises. *Procedia Manufacturing*, *42*, 70–75. https://doi.org/10.1016/j.promfg.2020.02.024

Zhou, Y., Zhang, H., Huang, X., Yang, S., Babar, M. A., & Tang, H. (2015). Quality assessment of systematic reviews in software engineering: A tertiary study. *Proceedings of the 19th International Conference on Evaluation and Assessment in Software Engineering*, 1–14. https://doi.org/10.1145/2745802.2745815

Appendices

Appendix A: PDD definitions

Table A1: PDD activity table.

Activity	Subactivity	Description
Problem investigation	Identify & scope domain	Identify the relevant FUNCTIONAL DOMAIN and create a demarcation to conduct the investigation, design, and development within.
	Specify objectives	Determine the OBJECTIVES of the project by asking what the desired achievements of the existence of the maturity model are.
	Identify stakeholders	Determine which STAKEHOLDERS have a vested interest in the design, development, or application of the maturity model.
	Specify requirements	Define REQUIREMENTS for the maturity model that form the base for the design and development.
Domain investigation	Identify existing maturity models	Perform a literature review to gain an inventory of EXISTING MODELS within the FUNCTIONAL DOMAIN.
	Analyse existing maturity models	Perform a COMPARISON STUDY of EXISTING MODELS to identify patterns, shortcomings, and practices which can form the basis for INFLUENTIAL FACTORS.
	Identify influential factors	Take the results of the COMPARISON STUDY and supplement it with a literature review of the FUNCTIONAL DOMAIN within the BODY OF KNOWLEDGE, in order to identify INFLUENTIAL FACTORS.
Model design	Determine capabilities	Take the identified INFLUENTIAL FACTORS and distil them into CAPABILITIES.
	Determine focus areas	Aggregate the CAPABILITIES into appropriate FOCUS AREAS.
	Determine dependencies	Determine the DEPENDENCY relationships between the CAPABILITIES and attach them to a MATURITY LEVEL.
	Position capabilities in matrix	Construct the MATURITY MATRIX by populating it with the FOCUS AREAS and CAPABILITIES, ensuring that the DEPENDENCY relationships are respected by taking the corresponding MATURITY LEVELS into account.
Validation	Gather feedback	Validate the MATURITY MATRIX by performing a validation activity to gain FEEDBACK on the maturity model design.
	Identify artifact improvements	Convert the gathered FEEDBACK into actionable ARTIFACT IMPROVEMENTS that can be applied to the MATURITY MATRIX in a following iteration.

Instrument development	Specify assessment questions	For each FOCUS AREA, formulate ASSESSMENT QUESTIONS in order to determine which CAPABILITIES are developed, and thus, what the MATURITY LEVEL is.
	Develop assessment instrument	Present the collection of ASSESSMENT QUESTIONS in a pragmatic ASSESSMENT INSTRUMENT that can be applied in the field.
	Define improvement actions	Define for each CAPABILITY an IMPROVEMENT ACTION that guides the development of that CAPABILITY.
Evaluation	Implement maturity model	Introduce the maturity model and ASSESSMENT INSTRUMENT to their natural context.
	Gather feedback	Evaluate the MATURITY MATRIX by performing an evaluation activity to gain FEEDBACK on the maturity model design or application.
	Identify artifact improvements	Convert the gathered FEEDBACK into actionable ARTIFACT IMPROVEMENTS that can be applied to the MATURITY MATRIX in a following iteration.
	Communicate results	Write a SCIENTIFIC PUBLICATION detailing the development, validation, and evaluation of the maturity model.

Table A2: PDD concept table.

Concept	Definition
FUNCTIONAL DOMAIN	A functional domain is the whole of activities, means, responsibilities and actors involved in the fulfilment of a well-defined function within an organisation (van Steenbergen et al., 2013, p. 11).
OBJECTIVE	An objective is a desire for which resources have been committed. (Wieringa, 2014, p. 38).
STAKEHOLDER	A stakeholder of a problem is a person, group of persons, or institution affected by treating the problem. Stakeholders are the source of goals and constraints of the project, which are in turn the source of requirements in the model (Wieringa, 2014, p. 35).
REQUIREMENT	A requirement is a property of the maturity model desired by some stakeholder, who has committed resources to realise the property (Wieringa, 2014, p. 51).
EXISTING MODEL	An existing model is a maturity model that is already contained in the current body of knowledge (Becker et al., 2009).
COMPARISON STUDY	A comparison study analyses existing maturity models to identify shortcomings which can incentivise modification of one's own maturity model (Becker et al., 2009).
INFLUENTIAL FACTOR	Influential factors are functional domain components and subcomponents that are mutually exclusive and collectively exhaustive (de Bruin et al., 2005). They are specific, measurable and independent elements which reflect a fundamental and distinct characteristic of the domain (Rosemann & de Bruin, 2005, p. 5).
BODY OF KNOWLEDGE	A body of knowledge is the systematic collection of activities and outcomes in terms of their values, constructs, models, principles, and instantiations that arise from continuous discovery and validation work by practitioners and scholars, and enables self-reflective growth and reproduction (Romme, 2016, p. 76).
CAPABILITY	A capability is the ability to achieve a predefined goal (van Steenbergen et al., 2013, p. 11).
FOCUS AREA	A focus area is a well-defined coherent subset of a functional domain. The total set of focus areas is a partition of the functional domain, i.e., different focus areas are disjoint and the union of all these focus areas is the complete functional domain (van Steenbergen et al., 2013, p. 11).
DEPENDENCY	A capability is dependent on another capability if it can only be achieved after that other capability has been achieved (van Steenbergen et al., 2013, p. 11).
MATURITY LEVEL	A maturity level is a well-defined evolutionary plateau within a Functional Domain (van Steenbergen et al., 2013, p. 11).
MATURITY MATRIX	A maturity matrix provides a partial ordering of capabilities within a functional domain across focus areas over a sequence of maturity levels (van Steenbergen et al., 2013, p. 11).
FEEDBACK	The result of the systematic determination of merit, worth, and significance of something or someone (Hevner & Chatterjee, 2010, p. 109).
ARTIFACT IMPROVEMENT	The formulation of a design modification following the investigation of feedback resulting from validation or evaluation activities (Hevner & Chatterjee, 2010; Wieringa, 2014).

ASSESSMENT QUESTION	Assessment questions are used to determine the current or target maturity level of an organisation within a functional domain (van Steenbergen et al., 2013, p. 11).
ASSESSMENT INSTRUMENT	An assessment instrument is a tool to determine maturity within a functional domain (van Steenbergen et al., 2013, p. 11).
IMPROVEMENT ACTION	An improvement action is the description of an activity that is expected to result in achieving a specific capability (van Steenbergen et al., 2013, p. 11).
SCIENTIFIC PUBLICATION	A scientific publication is a work of science detailing the maturity model design procedure in detail, considering all process steps, the applied methods, the parties involved, and the results (Becker et al., 2009).

Appendix B: MLR 1 Protocol

Name of reviewer	Michel Muszynski
Date of search	11-07-2022

Background

This protocol describes the steps for the execution of a multivocal literature review (MLR) as part of a design science project that aims to design a maturity model for the application of the privacy-by-design paradigm in information systems design. This protocol is created according to the guidelines and principles of Kitchenham and Charters (2007) and Garousi et al. (2019). First, the research question, objectives, and rationale are presented, after which the following five phases of this MLR are further elaborated on: search process/strategy, source selection process, source quality assessment, data extraction, and data synthesis.

Research question

RQ1: What maturity models exist in the relevant and adjacent domains?

Objectives & rationale

This multivocal literature review aims to identify and take an inventory of existing maturity models in order to answer the research question. Wieringa's (2014) engineering cycle indicates that available treatments should be considered before creating new treatments, similarly, Becker et al. (2009) have an explicit step in their maturity model design method that prescribes a comparison with existing maturity models. The purpose is to compare existing models in order to gain an understanding of which model types are used, what domains they service, and how they compare to each other. Additionally, these models can contain information in regards to privacy-by-design practices which are of interest.

This protocol describes a multivocal literature review, this means that grey literature sources are considered next to academic literature sources. The privacy-by-design paradigm is very much relevant for practitioners since legislators are increasingly adopting its principles, forcing practitioners to think about how they can implement them. For this review, the inclusion of grey literature adds value and can give insight into valuable practitioner experiences and perspectives.

Tool support

This literature review is partially conducted with the CADIMA tool (Kohl et al., 2018). This online tool provides support for the literature review process, including merging reference lists from different sources, duplicate identification and removal, title & abstract screening, full-text screening, critical appraisal, and data extraction. The tool is intended for academic references and is used for the white literature component of this multivocal literature review. The grey literature component is performed using Excel sheets.

Search process/strategy

For this review, an automated literature search is performed by querying literature databases through a search string. The search terms are formulated in the English language. Preliminary exploratory searches have been performed to identify relevant search terms and synonyms or equivalents. Table B1 provides an overview of the data sources, six databases for academic works and Google Search mainly for grey literature. In addition, Google Scholar is used for exploratory and supplementary searches.

Table B1: Data sources.

Academic literature	Grey literature
AIS Electronic Library SCOPUS Web of Science Science Direct IEEE Xplore ACM Digital Library Google Scholar	Google Search

Search string

To search through the listed data sources, a search string is used. For this review, the string consists of two parts. The first part consists of synonyms or equivalents of *maturity model*, connected by Boolean OR operators. The second part consists of the relevant domains, connected in a similar fashion. These two parts are combined with a Boolean AND operator, meaning that the search query aims to find maturity/capability assessment artifacts in the specified domains. Where possible, the search string specifies the inclusion of the title, abstract, and keywords, these are the fields that will be searched. Due to the limitations of the search engine, the strings for Google Scholar and Science Direct are split into multiple strings. The following overview in Table B2 presents the generic search string first, followed by the search engine-specific strings for each data source.

Table B2: Search strings.

Generic string
("maturity model" OR "maturity framework" OR "maturity assessment" OR "maturity matrix" OR "capability model" OR "capability framework" OR "capability assessment" OR "capability matrix" OR "stages of growth") AND ("privacy" OR "data protection" OR "data governance")
AIS Electronic Library
Fields: Title & abstract
((title:"maturity model" OR title:"maturity framework" OR title:"maturity assessment" OR

```
title:"maturity matrix" OR
title:"capability model" OR
title:"capability framework" OR
title:"capability assessment" OR
title:"capability matrix" OR
title:"stages of growth")
AND
(title:"privacy" OR
title:"data protection" OR
title:"data governance"))
OR
((abstract:"maturity model" OR
abstract:"maturity framework" OR
abstract:"maturity assessment" OR
abstract:"maturity matrix" OR
abstract:"capability model" OR
abstract:"capability framework" OR
abstract:"capability assessment" OR
abstract:"capability matrix" OR
abstract:"stages of growth")
AND
(abstract:"privacy" OR
abstract:"data protection" OR
abstract:"data governance"))
```

SCOPUS

Fields: Title, abstract, & keywords

```
TITLE-ABS-KEY ( ( "maturity model"  OR
"maturity framework"  OR
"maturity assessment"  OR
"maturity matrix" OR
"capability model"  OR
"capability framework"  OR
"capability assessment"  OR
"capability matrix" OR
"stages of growth" )
AND
( "privacy"  OR
"data protection"  OR
"data governance" ) )
```

Web of Science

Fields: Title, abstract, & keywords

```
TI=(("maturity model" OR
"maturity framework" OR
"maturity assessment" OR
"maturity matrix" OR
"capability model" OR
"capability framework" OR
"capability assessment" OR
"capability matrix" OR
"stages of growth")
```

```
AND
("privacy" OR
"data protection" OR
"data governance"))
OR
AB=(("maturity model" OR
"maturity framework" OR
"maturity assessment" OR
"maturity matrix" OR
"capability model" OR
"capability framework" OR
"capability assessment" OR
"capability matrix" OR
"stages of growth")
AND
("privacy" OR
"data protection" OR
"data governance"))
OR
AK=(("maturity model" OR
"maturity framework" OR
"maturity assessment" OR
"maturity matrix" OR
"capability model" OR
"capability framework" OR
"capability assessment" OR
"capability matrix" OR
"stages of growth")
AND
("privacy" OR
"data protection" OR
"data governance"))
```

Science Direct

Fields: Title, abstract, & keywords

```
("maturity model" OR
"maturity framework" OR
"maturity assessment" OR
"maturity matrix" OR
"capability model")
AND
("privacy" OR
"data protection" OR
"data governance")

("capability framework" OR
"capability assessment" OR
"capability matrix" OR
"stages of growth")
AND
("privacy" OR
"data protection" OR
"data governance")
```

IEEE Xplore

Fields: Title, abstract, & keywords

```
(("Document Title":"maturity model" OR
"Document Title":"maturity framework" OR
"Document Title":"maturity assessment" OR
"Document Title":"maturity matrix" OR
"Document Title":"capability model" OR
"Document Title":"capability framework" OR
"Document Title":"capability assessment" OR
"Document Title":"capability matrix" OR
"Document Title":"stages of growth")
AND
("Document Title":"privacy" OR
"Document Title":"data protection" OR
"Document Title":"data governance"))
OR
(("Abstract":"maturity model" OR
"Abstract":"maturity framework" OR
"Abstract":"maturity assessment" OR
"Abstract":"maturity matrix" OR
"Abstract":"capability model" OR
"Abstract":"capability framework" OR
"Abstract":"capability assessment" OR
"Abstract":"capability matrix" OR
"Abstract":"stages of growth")
AND
("Abstract":"privacy" OR
"Abstract":"data protection" OR
"Abstract":"data governance"))
OR
(("Author Keywords":"maturity model" OR
"Author Keywords":"maturity framework" OR
"Author Keywords":"maturity assessment" OR
"Author Keywords":"maturity matrix" OR
"Author Keywords":"capability model" OR
"Author Keywords":"capability framework" OR
"Author Keywords":"capability assessment" OR
"Author Keywords":"capability matrix" OR
"Author Keywords":"stages of growth")
AND
("Author Keywords":"privacy" OR
"Author Keywords":"data protection" OR
"Author Keywords":"data governance"))
```

ACM Digital Library

Fields: Title, abstract, & keywords

```
Title:(("maturity model" OR
"maturity framework" OR
"maturity assessment" OR
"maturity matrix" OR
"capability model" OR
```

```
"capability framework" OR
"capability assessment" OR
"capability matrix" OR
"stages of growth")
AND
("privacy" OR
"data protection" OR
"data governance"))
OR
Abstract:(("maturity model" OR
"maturity framework" OR
"maturity assessment" OR
"maturity matrix" OR
"capability model" OR
"capability framework" OR
"capability assessment" OR
"capability matrix" OR
"stages of growth")
AND
("privacy" OR
"data protection" OR
"data governance"))
OR
Keyword:(("maturity model" OR
"maturity framework" OR
"maturity assessment" OR
"maturity matrix" OR
"capability model" OR
"capability framework" OR
"capability assessment" OR
"capability matrix" OR
"stages of growth")
AND
("privacy" OR
"data protection" OR
"data governance"))
```

Google Scholar

Fields: Title

```
allintitle: "maturity model" OR
"maturity framework" OR
"maturity assessment" OR
"maturity matrix" OR
"capability model" OR
"capability framework" OR
"capability assessment" OR
"capability matrix" OR
"stages of growth"
"privacy"

allintitle: "maturity model" OR
"maturity framework" OR
"maturity assessment" OR
```

```
"maturity matrix" OR
"capability model" OR
"capability framework" OR
"capability assessment" OR
"capability matrix" OR
"stages of growth"
"data protection"

allintitle: "maturity model" OR
"maturity framework" OR
"maturity assessment" OR
"maturity matrix" OR
"capability model" OR
"capability framework" OR
"capability assessment" OR
"capability matrix" OR
"stages of growth"
"data governance"
```

Google Search

```
("maturity model" OR
"maturity framework" OR
"maturity assessment" OR
"maturity matrix" OR
"capability model" OR
"capability framework" OR
"capability assessment" OR
"capability matrix" OR
"stages of growth")
AND
("privacy" OR
"data protection" OR
"data governance")
```

Grey literature search considerations

The searches in academic databases are exhaustive, meaning that all hits are considered. These data sources are AIS Electronic Library, SCOPUS, Web of Science, Science Direct, IEEE Xplore, and ACM Digital Library. Google Scholar is used for exploratory searches and for finding supplementary works which are not found in the previously named data sources.

For the grey literature side of this review, the regular Google search engine at http://www.google.com is used. Because of its wide reach, a Google search is expected to return a high number of hits. It is therefore paramount to formulate a clear stopping criterion. For this search, an effort-bounded stopping criterion of $n = 100$ is used, meaning only the first 100 hits are considered. This particular stopping criterion is based on the work from Garousi and Mäntylä (2016) who also used the first 100 results in their review, stating that in their experience the most relevant results appear in the first few pages.

The Google search is conducted in an incognito tab of the Google Chrome web browser, logged out of any accounts, and with only the SEOquake[6] SERP tool extension enabled. This is done to mitigate the risks posed by the search bubble effect (Ćurković & Košec, 2018). The SERP tool is used to conveniently download the Google search results as a CSV-file for further processing.

[6] https://chrome.google.com/webstore/detail/seoquake/akdgnmcogleenhbclghghlkkdndkjdjc

Source selection process

A search is performed for each of the stated data sources by using their respective search strings. The resulting works are aggregated into a single list and checked for duplicates. Duplicate results are then removed so that the aggregated list of works contains only unique entries. The decision to include a found work in the review is based on several inclusion/exclusion criteria. Table B3 shows the five criteria that are used to determine the inclusion/exclusion of a work. These criteria aim to ensure that only works that introduce a relevant maturity model and that can be screened fully are included in the review.

For each work, a two-stage inclusion/exclusion assessment is performed. The first stage entails applying the criteria to the title and abstract of each work. For grey literature that does not adhere to a typical academic format, the following elements are screened: the title, (executive) summary, figures and tables, and the conclusion. In the second stage, a full-text screening is performed. The source selection phase results in a list of works that are accessible and relevant to answering the research question.

Table B3: Inclusion/exclusion criteria.

#	Criterion
1	The work introduces a new artifact.
2	The artifact is used for capability/maturity assessment.
3	The artifact addresses a relevant domain.
4	The work is accessible in full text.
5	The work is in English or Dutch.

Snowballing

The criteria specify that a work must introduce a new artifact. This means that works that apply, discuss, or mention an artifact introduced in a different work, will be excluded from the review. Snowballing is employed in these works to identify the original work that introduces the artifact so that it can be included, this is especially relevant for grey literature. Additionally, the same approach is used for included works that refer to relevant works not found in the initial search efforts.

Study quality assessment

The study quality assessment phase entails assessing the quality of the found works. Because of the different process of review and publication between academic literature and grey literature, two separate sets of criteria are used. For academic literature, the criteria and assessment questions by Wang et al. (2022) that are based on the guidelines by Zhou et al. (2015) and Kitchenham (2004) are used (Table B4). For grey literature, the criteria and assessment questions from Garousi et al. (2019) are used (Table B5). The majority of the criteria are employed as a checklist requiring a binary answer, for both academic literature and grey literature.

Table B4: Academic literature quality assessment checklist (Wang et al., 2022).

Criterion	Question
Methodology	Does the source clearly state objectives?
	Does the source clearly state methods?
	Does the source have specific questions to address?
	Does the source present work that is based on prior research?
Objectivity	Is there a clear statement of findings (data) and relationship to the objectives of research?
	Does the source answer the research question defined or presents the results in a clear way?
	Does the first author of the source have other publications related to the topic?
Impact	Does the source clearly state the contribution?
	Does the source clearly discuss the implications of practices?
	Does the source clearly discuss the future research?
Credibility	Does the source clearly present findings?
	Does the source present the findings based on the evidence and/or arguments?
	Does the source clearly discuss the validity of its results?
	Is the work (of the source) replicable?
	Are the findings credible?
Rigour	Has the work been validated (e.g., in academia or/and industry)?
	Does the source clearly describe and justify data collection methods?
	Are the collected data appropriate for addressing the objectives of the research?
	Does the source clearly describe and justify data analysis methods?
	Are the data analysis methods appropriate for addressing objectives of the research?

Table B5: Grey literature quality assessment checklist (Garousi et al., 2019).

Criterion	Question
Authority of the producer	Is the publishing organisation reputable? E.g., the Software Engineering Institute (SEI)
	Is an individual author associated with a reputable organisation?
	Has the author published other work in the field?
	Does the author have expertise in the area? (e.g., job title principal software engineer)
Methodology	Does the source have a clearly stated aim?
	Does the source have a stated methodology?
	Is the source supported by authoritative, contemporary references?
	Are any limits clearly stated?
	Does the work cover a specific question?
	Does the work refer to a particular population or case?
Objectivity	Does the work seem to be balanced in presentation?
	Is the statement in the sources as objective as possible? Or, is the statement a subjective opinion?
	Is there vested interest? E.g., a tool comparison by authors that are working for a particular tool vendor.
	Are the conclusions supported by the data?
Date	Does the item have a clearly stated date?
Position w.r.t. related sources	Have key related GL or formal sources been linked to / discussed?
Novelty	Does it enrich or add something unique to the research?
	Does it strengthen or refute a current position?
Impact	Normalise all the following impact metrics into a single aggregated impact metric (when data are available): Number of citations, Number of backlinks, Number of social media shares (the so-called “alt-metrics”), number of comments posted for a specific online entry like a blog post or a video, Number of page or paper views.
Outlet type	1st tier GL: High outlet control/ High credibility: Books, magazines, theses, government reports, white papers
	2nd tier GL: Moderate outlet control/Moderate credibility: Annual reports, news articles, presentations, videos, Q/A sites (such as StackOverflow), Wiki articles
	3rd tier GL: Low outlet control/ Low credibility: Blogs, emails, tweets

Data extraction

The data extraction phase aims to accurately record the relevant information from the works included in the review in order to answer the research question. To this end, a data extraction form is used, detailing all the elements that are extracted from each work. Table B6 shows the data extraction form used in this review. The form contains 16 extraction elements; the first two pertain to general attributes of a work, elements 3–15 are maturity model elements pertaining to maturity model properties and quality, and element 16 links this review to the greater topic under investigation to extract relevant privacy-by-design information for the design of a privacy-by-design maturity model. This data extraction form is used for each included work in the review.

Table B6: Data extraction form.

#	Extraction element	Description	Source
1	Name	The name of the maturity model and the main references.	-
2	Author	Source of the work.	-
3	Scope of model	The domain that the model considers and is to be applied in.	Pöppelbuß & Röglinger, (2011), Zapata et al. (2020)
4	Purpose of use	The purpose for which the model is intended to be used.	Pöppelbuß & Röglinger, (2011), Zapata et al. (2020)
5	Target group	The demographic that applies the maturity model and to whom the results are reported.	Pöppelbuß & Röglinger, (2011), Zapata et al. (2020)
6	Number of levels	The number of maturity levels of the model.	Pöppelbuß & Röglinger, (2011) Proença & Borbinha (2016) Zapata et al. (2020)
7	Level definitions	Does the model have clear definitions of the elements falling under the assessment category-level intersection?	Pöppelbuß & Röglinger, (2011), Tuncel et al. (2020)
8	Definition of maturity	Shows if the maturity model contains a definition of maturity.	Pöppelbuß & Röglinger, (2011), Proença & Borbinha (2016)
9	Name of the attributes	The name of attributes the maturity model uses.	Proença & Borbinha (2016)
10	Number of attributes	The number of attributes used by the maturity model.	Proença & Borbinha (2016)
11	Assessment instrument	Availability of a procedure that guides model users through the steps of the assessment.	Proença & Borbinha (2016), Zapata et al. (2020)
12	The origin of the model	Whether it originated from academia or from practitioners.	Proença & Borbinha (2016)
13	Validation/evaluation	The extent of empirical validation or evaluation.	Pöppelbuß & Röglinger (2011)
14	Reference model	Does the model follow any reference models or frameworks?	Tuncel et al. (2020)
15	Tool support	Does the model have a software service implementation to support its usage?	Tuncel et al. (2020)
16	Privacy-by-design relevance	What elements of the model are relevant to the privacy-by-design paradigm?	-

Data synthesis

The data synthesis phase concerns the aggregation, comparison, and presentation of the results of the review. For this review, the filled-out data extraction forms are aggregated in a tabular comparison for extraction elements 1-15. These elements are mostly short in nature and provide a quick overview of the general attributes of a maturity model, making them suitable for comparison in table format.

Extraction element 16 requires a lengthier elaboration since its comparison is more intricate. Moreover, this element is the most interesting for answering the main research question of the overarching research, thus a more elaborate descriptive narrative synthesis approach is used for this element in addition to using open coding for the factors.

Appendix C: MLR 1 Consolidated domain factors

This thesis is accompanied by a digital repository with supplementary data files that are not suitable to be added to this document. This appendix will provide a short description of what the data file that this appendix refers to entails and where it can be found.

Description
This appendix provides an overview of all consolidated domain factors that were found in the execution of the first multivocal literature review. The data file is a CSV-file which is formatted as a table and provides an overview of all factors with an identifier, the source work origin (e.g., academic, industry, or government), the domain that the work addresses, the type of factor (e.g., capability, recommendation, or principle), the source reference, the final grouping, the initial coding, and a description of what the factor entails.

Digital repository:
https://github.com/MichelMuszynski/PbD-maturity-data

Data file for this appendix:
https://github.com/MichelMuszynski/PbD-maturity-data/blob/main/data/MLR1/MLR%201%20Factors.csv

Appendix D: MLR 2 Protocol

Name of reviewer	Michel Muszynski
Date of search	13-09-2022

Background

This protocol describes the steps for the execution of a multivocal literature review (MLR) as part of a design science project that aims to design a maturity model for the application of the privacy-by-design paradigm in information systems design. This protocol is created according to the guidelines and principles of Kitchenham and Charters (2007) and Garousi et al. (2019). First, the research question, objectives, and rationale are presented, after which the following five phases of this MLR are further elaborated on: search process/strategy, source selection process, source quality assessment, data extraction, and data synthesis.

Research question

RQ2: What are the relevant factors that influence privacy-by-design?

Objectives & rationale

This multivocal literature review aims to identify and take an inventory of relevant factors in the privacy-by-design domain in order to answer the research question. The purpose is to find factors that can be used as candidate capabilities or that can provide input for the formulation of capabilities. These factors can be any type of construct which indicates practices or activities related to PbD application. Examples of factor constructs include but are not limited to, best practices, success factors, recommendations, principles, method fragments, guidelines, and techniques. Using a literature review to source capabilities for a maturity model is common practice (e.g., Overeem et al., 2022) and is part of the domain investigation phase of Wieringa's (2014) design cycle which is employed in the overarching research method.

This protocol describes a multivocal literature review, this means that grey literature sources are considered next to academic literature sources. The privacy-by-design paradigm is very much relevant for practitioners since legislators are increasingly adopting its principles, forcing practitioners to think about how they can implement them. For this review, the inclusion of grey literature adds value and can give insight into valuable practitioner experiences and perspectives.

Tool support

This literature review is partially conducted with the CADIMA tool (Kohl et al., 2018). This online tool provides support for the literature review process, including merging reference lists from different sources, duplicate identification and removal, title & abstract screening, full-text screening, critical appraisal, and data extraction. The tool is intended for academic references and is used for the white literature component of this multivocal literature review. The grey literature component is performed using Excel sheets.

Search process/strategy

For this review, an automated literature search is performed by querying literature databases through a search string. The search terms are formulated in the English language. Preliminary exploratory searches have been performed to identify relevant search terms and synonyms or equivalents. Table D1 provides an overview of the data sources, five databases for academic works and Google Search mainly for grey literature. In addition, Google Scholar is used for exploratory and supplementary searches.

Table D1: Data sources.

Academic literature	Grey literature
SCOPUS Web of Science IEEE Xplore ACM Digital Library Google Scholar	Google Search

Search string

To search through the listed data sources, a search string is used. For this review, the string consists of two parts. The first part consists of synonyms or equivalents of *privacy-by-design*, connected by Boolean `OR` operators. The second part consists of the relevant constructs that denote domain factors as input for capabilities, connected in a similar fashion. These two parts are combined with a Boolean `AND` operator, meaning that the search query aims to find domain factors in the privacy-by-design domain. This search string was constructed based on exploratory searches as well as string elements from Niazi et al. (2020). Where possible, the search string specifies the inclusion of the title and abstract, these are the fields that will be searched. The following overview in Table D2 presents the generic search string first, followed by the search engine-specific strings for each data source. Since Google Scholar does not accept a string as long as the generic string, multiple substrings have to be used where elements from the clause after the `AND` operator are combined. For the sake of brevity, these are not included in Table D2. The google search engine maintains a limit of 32 keywords in a query, thus the search string had to be cut short for the grey literature part of this MLR.

Table D2: Search strings.

Generic string
("privacy-by-design" OR "privacy by design" OR "privacy engineering" OR "privacy system design" OR "data protection by design") AND ("practice*" OR "method*" OR "goal*" OR "guideline*" OR "principle*" OR "initiative*" OR "pattern*" OR "strateg*" OR "tactic*" OR "capabilit*" OR "activit*" OR "approach*" OR

```
"process*" OR
"step*" OR
"technique*" OR
"model*" OR
"framework*" OR
"scheme*" OR
"technolog*" OR
"success factor*" OR
"recommendation*" OR
"application*" OR
"implementation*" OR
"operation*" OR
"challenge*" OR
"privacy impact assessment" OR
"PIA" OR
"data protection impact assessment" OR
"DPIA")
```

SCOPUS

Fields: Title

```
TITLE ((
"privacy-by-design" OR
"privacy by design" OR
"privacy engineering" OR
"privacy system design" OR
"data protection by design")
AND  (
"practice*" OR
"method*" OR
"goal*" OR
"guideline*" OR
"principle*" OR
"initiative*" OR
"pattern*" OR
"strateg*" OR
"tactic*" OR
"capabilit*" OR
"activit*" OR
"approach*" OR
"process*" OR
"step*" OR
"technique*" OR
"model*" OR
"framework*" OR
"scheme*" OR
"technolog*" OR
"success factor*" OR
"recommendation*" OR
"application*" OR
"implementation*" OR
"operation*" OR
"challenge*" OR
"privacy impact assessment" OR
```

```
"PIA" OR
"data protection impact assessment" OR
"DPIA"))
```

Web of Science

Fields: Title & abstract

```
TI=((
"privacy-by-design" OR
"privacy by design" OR
"privacy engineering" OR
"privacy system design" OR
"data protection by design")
AND  (
"practice*" OR
"method*" OR
"goal*" OR
"guideline*" OR
"principle*" OR
"initiative*" OR
"pattern*" OR
"strateg*" OR
"tactic*" OR
"capabilit*" OR
"activit*" OR
"approach*" OR
"process*" OR
"step*" OR
"technique*" OR
"model*" OR
"framework*" OR
"scheme*" OR
"technolog*" OR
"success factor*" OR
"recommendation*" OR
"application*" OR
"implementation*" OR
"operation*" OR
"challenge*" OR
"privacy impact assessment" OR
"PIA" OR
"data protection impact assessment" OR
"DPIA"))
OR
AB=((
"privacy-by-design" OR
"privacy by design" OR
"privacy engineering" OR
"privacy system design" OR
"data protection by design")
AND  (
"practice*" OR
"method*" OR
"goal*" OR
```

```
"guideline*" OR
"principle*" OR
"initiative*" OR
"pattern*" OR
"strateg*" OR
"tactic*" OR
"capabilit*" OR
"activit*" OR
"approach*" OR
"process*" OR
"step*" OR
"technique*" OR
"model*" OR
"framework*" OR
"scheme*" OR
"technolog*" OR
"success factor*" OR
"recommendation*" OR
"application*" OR
"implementation*" OR
"operation*" OR
"challenge*" OR
"privacy impact assessment" OR
"PIA" OR
"data protection impact assessment" OR
"DPIA"))
```

IEEE Xplore

Fields: Title & abstract

```
(("Document Title":"privacy-by-design" OR
"Document Title":"privacy by design" OR
"Document Title":"privacy engineering" OR
"Document Title":"privacy system design" OR
"Document Title":"data protection by design")
AND
(
"Document Title":practice OR
"Document Title":method OR
"Document Title":goal OR
"Document Title":guideline OR
"Document Title":principle OR
"Document Title":initiateve OR
"Document Title":pattern OR
"Document Title":strategy OR "Document Title":strategies OR
"Document Title":tactic OR
"Document Title":capability OR "Document Title":capabilities OR
"Document Title":activity OR "Document Title":activities OR
"Document Title":approach OR
"Document Title":process OR
"Document Title":step OR
"Document Title":technique OR
"Document Title":model OR
"Document Title":framework OR
```

```
"Document Title":scheme OR
"Document Title":technology OR "Document Title":technologies OR
"Document Title":"success factor" OR "Document Title":"success factors"
OR
"Document Title":recommendation OR
"Document Title":application OR
"Document Title":implementation OR
"Document Title":operation OR
"Document Title":challenge OR
"Document Title":"privacy impact assessment" OR
"Document Title":"PIA" OR
"Document Title":"data protection impact assessment" OR
"Document Title":"DPIA"
))
OR
(("Abstract":"privacy-by-design" OR
"Abstract":"privacy by design" OR
"Abstract":"privacy engineering" OR
"Abstract":"privacy system design" OR
"Abstract":"data protection by design")
AND
(
"Abstract":practice OR
"Abstract":method OR
"Abstract":goal OR
"Abstract":guideline OR
"Abstract":principle OR
"Abstract":initiateve OR
"Abstract":pattern OR
"Abstract":strategy OR "Abstract":strategies OR
"Abstract":tactic OR
"Abstract":capability OR "Abstract":capabilities OR
"Abstract":activity OR "Abstract":activities OR
"Abstract":approach OR
"Abstract":process OR
"Abstract":step OR
"Abstract":technique OR
"Abstract":model OR
"Abstract":framework OR
"Abstract":scheme OR
"Abstract":technology OR "Abstract":technologies OR
"Abstract":"success factor" OR "Abstract":"success factors" OR
"Abstract":recommendation OR
"Abstract":application OR
"Abstract":implementation OR
"Abstract":operation OR
"Abstract":challenge OR
"Abstract":"privacy impact assessment" OR
"Abstract":"PIA" OR
"Abstract":"data protection impact assessment" OR
"Abstract":"DPIA"))
```

ACM Digital Library

Fields: Title & abstract

```
(Title:
(("privacy\-by\-design" OR
"privacy by design" OR
"data protection by design" OR
"privacy engineering" OR
"privacy system design")
AND
(
"practice*" OR
"method*" OR
"goal*" OR
"guideline*" OR
"principle*" OR
"initiative*" OR
"pattern*" OR
"strateg*" OR
"tactic*" OR
"capabilit*" OR
"activit*" OR
"approach*" OR
"process*" OR
"step*" OR
"technique*" OR
"model*" OR
"framework*" OR
"scheme*" OR
"technolog*" OR
"success factor*" OR
"recommendation*" OR
"application*" OR
"implementation*" OR
"operation*" OR
"challenge*" OR
"privacy impact assessment" OR
"PIA" OR
"data protection impact assessment" OR
"DPIA"
)))
OR
(
Abstract:
((
"privacy\-by\-design" OR
"privacy by design" OR
"data protection by design" OR
"privacy engineering" OR
"privacy system design")
AND
(
"practice*" OR
"method*" OR
"goal*" OR
"guideline*" OR
```

```
"principle*" OR
"initiative*" OR
"pattern*" OR
"strateg*" OR
"tactic*" OR
"capabilit*" OR
"activit*" OR
"approach*" OR
"process*" OR
"step*" OR
"technique*" OR
"model*" OR
"framework*" OR
"scheme*" OR
"technolog*" OR
"success factor*" OR
"recommendation*" OR
"application*" OR
"implementation*" OR
"operation*" OR
"challenge*" OR
"privacy impact assessment" OR
"PIA" OR
"data protection impact assessment" OR
"DPIA")))
```

Google Search

```
("privacy.by.design" OR
"privacy engineering" OR
"data protection by design")
AND
( "practice" OR
"method" OR
"goal" OR
"guideline" OR
"principle" OR
"initiative" OR
"pattern" OR
"strategy" OR
"tactic" OR
"capability" OR
"activity" OR
"approach" OR
"process" OR
"step" OR
"technique" OR
"model" OR
"framework" OR
"scheme" OR
"technology" OR
"success factor" OR
"recommendation" OR
"application")
```

Grey literature search considerations

The searches in academic databases are exhaustive, meaning that all hits are considered. These data sources are SCOPUS, Web of Science, IEEE Xplore, and ACM Digital Library. Google Scholar is used for exploratory searches and for finding supplementary works which are not found in the previously named data sources.

For the grey literature side of this review, the regular Google search engine at http://www.google.com is used. Because of its wide reach, a Google search is expected to return a high number of hits. It is therefore paramount to formulate a clear stopping criterion. For this search, an effort-bounded stopping criterion of $n = 100$ is used, meaning only the first 100 hits are considered. This particular stopping criterion is based on the work from Garousi and Mäntylä (2016) who also used the first 100 results in their review, stating that in their experience the most relevant results appear in the first few pages.

The Google search is conducted in an incognito tab of the Google Chrome web browser, logged out of any accounts, and with only the SEOquake[7] SERP tool extension enabled. This is done to mitigate the risks posed by the search bubble effect (Ćurković & Košec, 2018). The SERP tool is used to conveniently download the Google search results as a CSV-file for further processing.

[7] https://chrome.google.com/webstore/detail/seoquake/akdgnmcogleenhbclghghlkkdndkjdjc

Source selection process

A search is performed for each of the stated data sources by using their respective search strings. The resulting works are aggregated into a single list and checked for duplicates. Duplicate results are then removed so that the aggregated list of works contains only unique entries. The decision to include a found work in the review is based on several inclusion/exclusion criteria. Table D3 shows the four criteria that are used to determine the inclusion/exclusion of a work. These criteria aim to ensure that only works that introduce a relevant domain factor and that can be screened fully are included in the review.

For each work, a two-stage inclusion/exclusion assessment is performed. The first stage entails applying the criteria to the title and abstract of each work. For grey literature that does not adhere to a typical academic format, the following elements are screened: the title, (executive) summary, figures and tables, and the conclusion. In the second stage, a full-text screening is performed. The source selection phase results in a list of works that are accessible and relevant to answering the research question.

Table D3: Inclusion/exclusion criteria.

#	Criterion
1	The work discusses privacy-by-design.
2	The work contains factors that can be used as input for a privacy-by-design maturity model.
3	The work is accessible in full text.
4	The work is in English or Dutch.

Snowballing

In this review, snowballing is used to identify potential factors which are not found in the initial search. If a work references factors in other, not included works, those works will be added to the search results for review so that those factors can be examined and extracted if deemed relevant.

Study quality assessment

The study quality assessment phase entails assessing the quality of the found works. Because of the different process of review and publication between academic literature and grey literature, two separate sets of criteria are used. For academic literature, the criteria and assessment questions by Wang et al. (2022) that are based on the guidelines by Zhou et al. (2015) and Kitchenham (2004) are used (Table D4). For grey literature, the criteria and assessment questions from Garousi et al. (2019) are used (Table D5). The majority of the criteria are employed as a checklist requiring a binary answer, for both academic literature and grey literature.

Table D4: Academic literature quality assessment checklist (Wang et al., 2022).

Criterion	Question
Methodology	Does the source clearly state objectives?
	Does the source clearly state methods?
	Does the source have specific questions to address?
	Does the source present work that is based on prior research?
Objectivity	Is there a clear statement of findings (data) and relationship to the objectives of research?
	Does the source answer the research question defined or presents the results in a clear way?
	Does the first author of the source have other publications related to the topic?
Impact	Does the source clearly state the contribution?
	Does the source clearly discuss the implications of practices?
	Does the source clearly discuss the future research?
Credibility	Does the source clearly present findings?
	Does the source present the findings based on the evidence and/or arguments?
	Does the source clearly discuss the validity of its results?
	Is the work (of the source) replicable?
	Are the findings credible?
Rigour	Has the work been validated (e.g., in academia or/and industry)?
	Does the source clearly describe and justify data collection methods?
	Are the collected data appropriate for addressing the objectives of the research?
	Does the source clearly describe and justify data analysis methods?
	Are the data analysis methods appropriate for addressing objectives of the research?

Table D5: Grey literature quality assessment checklist (Garousi et al., 2019).

Criterion	Question
Authority of the producer	Is the publishing organisation reputable? E.g., the Software Engineering Institute (SEI)
	Is an individual author associated with a reputable organisation?
	Has the author published other work in the field?
	Does the author have expertise in the area? (e.g., job title principal software engineer)
Methodology	Does the source have a clearly stated aim?
	Does the source have a stated methodology?
	Is the source supported by authoritative, contemporary references?
	Are any limits clearly stated?
	Does the work cover a specific question?
	Does the work refer to a particular population or case?
Objectivity	Does the work seem to be balanced in presentation?
	Is the statement in the sources as objective as possible? Or, is the statement a subjective opinion?
	Is there vested interest? E.g., a tool comparison by authors that are working for a particular tool vendor.
	Are the conclusions supported by the data?
Date	Does the item have a clearly stated date?
Position w.r.t. related sources	Have key related GL or formal sources been linked to / discussed?
Novelty	Does it enrich or add something unique to the research?
	Does it strengthen or refute a current position?
Impact	Normalise all the following impact metrics into a single aggregated impact metric (when data are available): Number of citations, Number of backlinks, Number of social media shares (the so-called “alt-metrics”), number of comments posted for a specific online entry like a blog post or a video, Number of page or paper views.
Outlet type	1st tier GL: High outlet control/ High credibility: Books, magazines, theses, government reports, white papers
	2nd tier GL: Moderate outlet control/Moderate credibility: Annual reports, news articles, presentations, videos, Q/A sites (such as StackOverflow), Wiki articles
	3rd tier GL: Low outlet control/ Low credibility: Blogs, emails, tweets

Data extraction

The data extraction phase aims to accurately record the relevant information from the works included in the review in order to answer the research question. To this end, a data extraction form is used, detailing all the elements that are extracted from each work. Table D6 shows the data extraction form used in this review. The form contains five extraction elements, including the scope of the work, the origin type (e.g., academia, industry, or government), factor construct (e.g., capability, guideline, practice, etc.), and description. This data extraction form is used for each included work in the review.

Table D6: Data extraction form.

#	Extraction element	Description	Source
1	Author	Source of the work.	Jansen & Yang (2020)
2	Scope	The domain that the work considers or addresses.	-
3	Origin	The type of origin.	-
4	Factor construct	The type of construct denoting the factor.	-
5	Factor description	Description of the factor.	Jansen & Yang (2020)

Data synthesis

The data synthesis phase concerns the aggregation, comparison, and presentation of the results of the review. For this review, the filled-out data extraction forms are aggregated in a table where each row is dedicated to one factor. This allows for a clear presentation of each factor and its attributes as well as simple further processing of the factors. Additional notable findings and general patterns are presented through a descriptive narrative synthesis approach.

Appendix E: MLR 2 Consolidated domain factors

This thesis is accompanied by a digital repository with supplementary data files that are not suitable to be added to this document. This appendix will provide a short description of what the data file that this appendix refers to entails and where it can be found.

Description
This appendix provides an overview of all consolidated domain factors that were found in the execution of the second multivocal literature review. The data file is a CSV-file which is formatted as a table and provides an overview of all factors with an identifier, the source work origin (e.g., academic, industry, or government), the domain that the work addresses, the type of factor (e.g., capability, recommendation, or principle), the source reference, the final grouping, the initial coding, and a description of what the factor entails.

Digital repository:
https://github.com/MichelMuszynski/PbD-maturity-data

Data file for this appendix:
https://github.com/MichelMuszynski/PbD-maturity-data/blob/main/data/MLR2/MLR%202%20Factors.csv

Appendix F: MLR 1 & 2 included works

Table F1: Included works for both MLRs.

#	MLR 1	MLR 2
1	Labadie & Legner (2019)	Chhetri et al. (2022)
2	Garcia et al. (2018)	Diamantopoulou & Karyda (2022)
3	Carretero et al. (2017)	Alkubaisy et al. (2022)
4	Rivera et al. (2017)	Pedroza et al. (2021)
5	Cheng et al. (2017)	Timón López et al. (2021)
6	Al-Ruithe & Benkhelifa (2017)	Drev & Delak (2022)
7	Yaqiong et al. (2020)	Arfaoui et al. (2020)
8	Proenca et al. (2016)	Kalloniatis et al. (2021)
9	Merkus et al. (2021)	Piras et al. (2020)
10	Marchildon et al. (2018)	Huth & Matthes (2019)
11	Office of management & enterprise services (2020)	Bincoletto (2019)
12	AICPA/CICA (2011)	Morales-Trujillo & Garcia-Mireles (2018)
13	Merkus (2015)	Chaudhuri & Cavoukian (2018)
14	Boswell & Courtright (2022)	Alshammari & Simpson (2017)
15	New Zealand Government (2014)	Diamantopoulou et al. (2017)
16	Compliance, Governance and Oversight Council (CGOC) (2018)	Notario et al. (2015)
17	The MITRE Corporation (2019)	Kroener & Wright (2014)
18	State of Oregon (2022)	Oetzel & Spiekermann (2014)
19	Fort Privacy (2022)	Kung et al. (2011)
20	Qi (2016)	van Lieshout et al. (2011)
21	Association of Corporate Counsel (2019)	Sion, Dewitte, et al. (2020)
22	Secure Controls Framework (2022)	Semantha et al. (2020)
23	DataFlux Corporation (2007)	Koops et al. (2013)
24	Centrum Informatiebeveiliging en Privacybescherming (CIP) (2017)	Semantha et al. (2021)
25	IBM (2007)	Spiekermann & Cranor (2009)
26	CMMI Institute (2019)	Belli et al. (2017)
27	EDM Council (2021)	Fhom & Bayarou (2011)
28	Chen (2010)	Sion et al. (2019)
29	van Lieshout & Hoepman (2015)	Iezzi (2021)
30	Intel Privacy Office (2013)	Al-Momani et al. (2019)
31		Sion, Landuyt, et al. (2020)
32		Antignac et al. (2018)
33		Kost et al. (2011)
34		Martin et al. (2014)
35		Martin & Kung (2018)
36		Gkotsopoulou et al. (2019)
37		Vicini et al. (2016)
38		Perera et al. (2016)
39		Ahmadian et al. (2018)
40		Alshammari & Simpson (2018)
41		Baldassarre et al. (2021)
42		Aljeraisy et al. (2020)
43		Mead et al. (2011)
44		Kalloniatis et al. (2008)
45		Sivakumar et al. (2017)

46	Deng et al. (2011)
47	Hoepman (2014)
48	Wright (2012)
49	Privacy Company (2019)
50	Cavoukian (2009)
51	PricewaterhouseCoopers (2021)
52	Hoepman (2022)
53	European Network and Information Security Agency (ENISA) (2014)
54	Information and privacy commission New South Wales (2020)
55	Koorn & ter Hart (2011)
56	Tamò-Larrieux (2018)
57	La Agencia Española de Protección de Datos (2019)
58	Information Commissioner's Office (ICO) (2022)
59	Chaudhuri (2018)
60	Datatilsynet (2017)
61	IT GOVERNANCE (2021)
62	MITRE Privacy Engineering (2019)
63	Stallings (2019)
64	Cavoukian (2012)
65	ISO/IEC (2017)
66	Sabo et al. (2016)
67	Oetzel et al. (2011)
68	Gürses (2010)

Appendix G: Model factor selection

This thesis is accompanied by a digital repository with supplementary data files that are not suitable to be added to this document. This appendix will provide a short description of what the data file that this appendix refers to entails and where it can be found.

Description
This appendix provides an overview of all factors that were deemed relevant from both multivocal literature reviews and denotes which factors were selected to be included in the design of the maturity model. The data file is a CSV-file which is formatted as a table and provides an overview of all factors with MLR origin, identifier, a description of what the factor entails, the source work origin (e.g., academic, industry, or government), the focus area the factor belongs to, whether the factor is included or not, and the maturity level that the factor belongs to.

Digital repository:
https://github.com/MichelMuszynski/PbD-maturity-data

Data file for this appendix:
https://github.com/MichelMuszynski/PbD-maturity-data/blob/main/data/Model%20factor%20selection/Factor%20selection.csv

Appendix H: Capability definitions and traceability

This appendix contains the definitions for all capabilities per focus area. The third column denotes the factor traceability which indicates what factors from Appendix G are used to form the respective capability.

#	Capability definition	Traceability
Requirements – 15 factors		
A	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.	159, 178, 238, 325
B	All privacy and security requirements are collected and validated for technical soundness and implementation viability. Adherence of the system to the requirements is verified during validation through pre-formulated requirement constraints and tests.	173, 177, 290, 291, 343
C	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.	146, 186, 201, 249, 297
D	Advice from ethical experts is gained regarding requirements for sensitive personal data.	251
Architecture – 27 factors		
A	A privacy architecture viewpoint is included in the project architecture for new initiatives. The privacy architecture maps privacy requirements onto the project architecture, translates privacy design strategies to tactics, and models data sets, processing purposes, lawful grounds, actors, legal roles, and personal data types.	8, 160, 191, 200, 218, 225, 226, 229, 257, 258, 265, 267, 269, 292
B	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.	23, 87, 158, 318, 210
C	Architecture models are verified for completeness and soundness. The architecture and models are validated to confirm that privacy requirements are implemented correctly. Selected privacy tactics are integrated by means of available privacy design patterns and PETs.	161, 182, 227
D	Processing activities and related information elements are exhaustively modelled and traceable through all layers of architecture. Privacy design patterns and PETs are selected from a centralised catalogue in a structured manner.	215, 236, 259, 355, 357
Development – 22 factors		
A	Privacy requirements are incorporated in low-level design. Acceptance testing is used to ensure that the system meets the privacy and security requirements.	54, 165, 231, 232, 287, 289
B	Privacy and data protection activities are integrated in the methods and workflows of the software development lifecycle. Operational behaviour is checked against applicable privacy policies and procedures.	241, 293, 353

C	Privacy-by-design is applied and documented within change management procedures. A process is in place to ensure that updates to privacy notices are considered for every significant change in the organisations processing activities.	10, 17, 110, 112, 113, 143, 147, 248, 285
D	Establish a catalogue of privacy patterns with relevant code excerpts to enable reusable design. Information systems are designed with automated privacy controls where possible.	102, 185, 238
E	Privacy policies are embedded in system design and are automatically enforced.	224

Technology – 15 factors

A	Personal data is encrypted in transit and at rest.	252, 253, 254
B	Privacy enhancing technologies (PETs) are selected, developed, and used to implement privacy design patterns.	55, 331, 362
C	The selected privacy enhancing technologies are assessed for effectiveness and added value to the provided degree of privacy, unnecessary PETs are removed. New and existing PETs are catalogued.	221, 274, 276
D	Enforcement of privacy policies is embedded in the technical design where suitable. The problem expressed by a privacy design pattern is mapped to a PET which is selected from a PETs catalogue while taking into account the quantitative and qualitative costs and benefits. The privacy protection technology is continuously monitored, optimised, and upgraded.	6, 209, 22, 260, 275
E	Revocable privacy is implemented through privacy-by-architecture, including PETs, limiting personal data access unless pre-established conditions are met that necessitate lawful access to the data.	216

PIA process – 33 factors

A	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.	19, 156, 175, 230, 246, 299, 319, 333
B	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.	34, 89, 140, 333, 358, 98
C	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.	313, 314, 347, 106, 164
D	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.	88, 108, 214
E	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.	85, 189, 315, 356, 364
F	A PIA covers not only information privacy issues, but all privacy issues and involves an assessment of positive and negative privacy impacts. There is more focus on applying privacy-by-architecture through the formulation of privacy targets in system design. The existing PIAs and the overall PIA process are constantly reviewed as part of a continuous improvement effort.	141, 202, 272, 332, 342, 344

PIA report – 7 factors

A	The PIA report is reviewed and is tied to budget submissions for new projects.	303, 316
B	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.	304, 317, 349
C	Reporting adheres to its own periodic reporting cycle independent of the PIA process and reports are submitted for audit to an independent third-party.	301
D	Different PIA reports can exist per PIA process, these reports are adapted to their intended audience in both content and form.	162

Risk management – 21 factors

A	Privacy-by-design and the privacy impact assessment are part of a formally defined risk management approach. A privacy risk analysis framework is employed that includes privacy risk modelling, risk prioritisation and formulating mitigation measures. Residual risks are identified and documented.	21, 52, 53, 144, 167, 198, 330
B	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.	20, 154, 172, 203, 298, 323, 336
C	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.	116, 145, 196, 280
D	Data risks are automatically identified, and early warnings are provided for high-risk operations by employing predictive analytics. Continuous risk assessment is supported by a privacy risk & compliance dashboard that provides a continuous view on the system.	5, 9, 235

Processing principles – 23 factors

A	The GDPR processing principles (lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability) are applied to all processing activities.	194, 208, 244, 308, 369, 367, 368
B	The GDPR processing principles are documented, applied in a structured and methodical manner, and are periodically evaluated.	46, 119, 120, 122, 123, 126, 127
C	Data past the retention period gets flagged or deleted automatically when no legal hold has been specified. Purpose limitation is supported by role concepts with graduated access rights. The data protection officer has a dashboard that provides an up-to-date view of the lawfulness of personal data processing activities.	29, 124, 149, 263
D	Compliance with the GDPR processing principles is proactively managed to deliver deliberate process optimisation. Issues of non-compliance are identified and remedial action is taken to ensure compliance in a timely	13, 14, 15, 16, 115

	fashion. Automated controls prevent the deletion of personal data that would violate legal retention requirements.	

Subject rights – 22 factors

A	Requests related to the exercise of data subject rights are recorded, monitored, and reported. Consent management including related notices, policies, and procedures are defined and implemented.	3, 11, 63, 92, 130, 310, 341
B	Data subject rights are facilitated through automated technical mechanisms such as self-service dashboards. Consent processes are periodically reviewed, improvements are made where necessary. Automated processes are followed to test consent prior to use of personal information.	65, 66, 137, 139, 222, 223, 245, 278, 340, 363
C	Policies and procedures related to subject rights facilitation are reviewed regularly. The data protection officer has a dashboard that provides an up-to-date view of data access requests and responses.	3, 30, 94
D	User-driven control of personal data is employed. Data subjects that do not consent to provide personal data are offered equitable conditions. Consent items are automatically updated in all affected processing systems whenever a change occurs.	40, 217

Transparency – 17 factors

A	Privacy policies are publicly available in clear and comprehensible language and contain contact information of the individuals responsible for privacy and security. Privacy policy revision meetings are conducted, feedback on the readability and content of the privacy policy is analysed and incorporated. Historical versions of policy are archived and accessible.	62, 188, 339, 359, 360
B	Policy communications are routine and semi-automated. Individual's general level of privacy policy understanding is assessed and feedback is used to improve communication methods. Procedures have been implemented that uniformly and consistently obtain consent for additional processing activities in the collection phase.	7, 39, 72, 74, 277
C	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.	26, 31, 187, 281, 311
D	Summaries of PIAs, TRAs, and independent third-party audit results are published.	32, 312

Third-party management – 15 factors

A	A privacy risk assessment for third parties is completed before any contract under which personal data is made available is granted. Existing contracts and agreements involving personal data provided to third parties are reviewed to ensure the appropriate information has been communicated.	76, 90, 371
B	Documented procedures exist and are consistently applied to ensure that third-parties have appropriate safeguards in place prior to transferring personal data. New instances of sharing personal data with third parties are assessed to determine authorisation, additional notice, and possible updates to existing agreements. Exception reports are used to record inappropriate, unacceptable, or misuse activities by third parties and to monitor the status of remedial activities.	12, 70, 77, 78, 79, 80, 133, 361
C	A privacy level agreement is made as part of a service level agreement, that addresses the level of privacy protection a service provider commits to	75, 132, 239, 240

	undertake and maintain. Changes in a third-party environment are monitored to ensure the processor can continue to meet its obligations. Management monitors compliance with privacy policies relating to disclosure to third parties.	

Roles – 13 factors

A	Stakeholders, roles, and responsibilities related to privacy activities are identified and assigned.	134, 166, 288, 351
B	The management of privacy related roles and responsibilities is formalised in a role/functionality matrix to ensure accountability. A chief privacy officer is appointed.	190, 192, 207, 212
C	The trust relationship between the stakeholders is defined. Data processing responsibilities are assigned to appropriate stakeholders including accompanying monitoring activities. A technical privacy officer is assigned to support operational privacy-by-design activities.	33, 193, 266
D	Appoint a central entity responsible for privacy related issues such as a privacy committee.	56, 213

Awareness – 6 factors

A	Different target groups involved in privacy-by-design are identified and receive training for raising awareness as well as transmitting knowledge relevant to their specialisation.	271
B	Management is committed to applying privacy-by-design and provides resources, such as manuals, guides, and handbooks, to support consistent implementation of privacy policies, procedures, and standards, as required and appropriate.	148, 282, 305
C	The organisation participates in learning from and contributing to the available body of knowledge amassed by the privacy community. Staff and management are comfortable identifying areas for improving privacy practices and discuss/raise these freely and proactively.	83, 242

Monitoring – 19 factors

A	An assurance process is in place, supporting the checking and demonstration of compliance with regulation, this includes overseeing the execution of cybersecurity and privacy controls. Systems should have functional audit logs and usage reports without disclosing identity information.	117, 243, 268, 295, 335
B	Log events during all processing activities. Privacy-related Key Performance Indicators are used to periodically track, measure, and monitor the performance of the privacy function. Performance is regularly reported to management and metrics are regularly reviewed.	84, 255, 306
C	Management continuously monitors compliance with privacy policies, regulations, and procedures related to personal data processing. The approach to privacy-by-design is continually reviewed and updated based on both internal review and external developments in best practice.	18, 64, 67, 69, 71, 81, 125
D	Periodic reviews and audits are performed on processing activities to ensure personal information uses are appropriate and lawful.	28, 37
E	Systematic and independent audit examinations of logs, procedures, processes, hardware and software specifications are performed. Audit and log systems are compliant with other privacy principles and track user activity to identify illegal processing.	256, 322

Appendix I: Intra-focus area dependencies

Table I1: All implicit intra-focus area dependencies.

$(1A, 1B)$	$(3D, 3E)$	$(5E, 5F)$	$(8C, 8D)$	$(12A, 12B)$
$(1B, 1C)$	$(4A, 4B)$	$(6A, 6B)$	$(9A, 9B)$	$(12B, 12C)$
$(1C, 1D)$	$(4B, 4C)$	$(6B, 6C)$	$(9B, 9C)$	$(12C, 12D)$
$(2A, 2B)$	$(4C, 4D)$	$(6C, 6D)$	$(9C, 9D)$	$(13A, 13B)$
$(2B, 2C)$	$(4D, 4E)$	$(7A, 7B)$	$(10A, 10B)$	$(13B, 13C)$
$(2C, 2D)$	$(5A, 5B)$	$(7B, 7C)$	$(10B, 10C)$	$(14A, 14B)$
$(3A, 3B)$	$(5B, 5C)$	$(7C, 7D)$	$(10C, 10D)$	$(14B, 14C)$
$(3B, 3C)$	$(5C, 5D)$	$(8A, 8B)$	$(11A, 11B)$	$(14C, 14D)$
$(3C, 3D)$	$(5D, 5E)$	$(8B, 8C)$	$(11B, 11C)$	$(14D, 14E)$

Appendix J: Topological generations code

This appendix contains the code that was used to calculate the topological generations of the graph representation of the PbD focus area maturity model. Python 3.9 was used with version 2.8.8 of the NetworkX[8] library for network analysis in Python.

```
import networkx as nx

elist = [

    # Intra-focus area dependencies

    # Requirements
    ("1A", "1B"),
    ("1B", "1C"),
    ("1C", "1D"),

    # Architecture
    ("2A", "2B"),
    ("2B", "2C"),
    ("2C", "2D"),

    # Development
    ("3A", "3B"),
    ("3B", "3C"),
    ("3C", "3D"),
    ("3D", "3E"),

    # Technology
    ("4A", "4B"),
    ("4B", "4C"),
    ("4C", "4D"),
    ("4D", "4E"),

    # PIA process
    ("5A", "5B"),
    ("5B", "5C"),
    ("5C", "5D"),
    ("5D", "5E"),
    ("5E", "5F"),

    # PIA report
    ("6A", "6B"),
    ("6B", "6C"),
    ("6C", "6D"),

    # Risk management
    ("7A", "7B"),
    ("7B", "7C"),
    ("7C", "7D"),

    # Processing principles
    ("8A", "8B"),
    ("8B", "8C"),
    ("8C", "8D"),

    # Subjects rights
    ("9A", "9B"),
    ("9B", "9C"),
    ("9C", "9D"),

    # Transparency
    ("10A", "10B"),
    ("10B", "10C"),
```

[8] https://networkx.org/documentation/stable/index.html#

```
    ("10C", "10D"),

    # Third-party
    ("11A", "11B"),
    ("11B", "11C"),

    # Roles
    ("12A", "12B"),
    ("12B", "12C"),
    ("12C", "12D"),

    # Awareness
    ("13A", "13B"),
    ("13B", "13C"),

    # Monitoring
    ("14A", "14B"),
    ("14B", "14C"),
    ("14C", "14D"),
    ("14D", "14E"),

    # Inter-focus area dependencies
    ("1A", "2A"),
    ("3A", "1B"),
    ("1A", "11A"),
    ("2D", "4E"),
    ("2B", "7B"),
    ("3D", "2D"),
    ("3D", "4C"),
    ("4D", "9D"),
    ("4D", "3E"),
    ("1A", "5A"),
    ("5A", "7A"),
    ("5D", "6C"),
    ("7A", "11B"),
    ("12A", "1C"),
    ("12A", "13A"),
    ("12B", "5E"),
    ("12B", "13B"),
    ("14A", "7C"),
    ("1A", "14A"),
    ("8B", "14C"),
    ("12B", "11B"),
    ("14C", "8D"),
    ("6C", "10D"),
    ("4B", "9B"),
    ("1B", "2C"),
    ("12B", "6A"),
    ("2A", "1B"),
    ("2C", "3D"),
    ("6B", "5D"),
    ("6B", "10D"),
    ("2C", "4B"),
    ("5C", "3C"),
    ("7B", "8C"),
    ("3B", "8C"),
    ("6B", "10C"),
    ("7B", "10C"),
    ("12B", "5C"),
    ("1B", "14A"),
    ("12B", "14B"),
    ("5C", "10C"),
    ("7B", "12D"),
    ("5C", "13C"),
    ("7B", "13C"),
    ("11B", "13C"),
    ("7C", "6C"),
    ("14B", "11C"),
    ("7C", "5E"),
    ("5E", "7D"),
```

```
    ("2D", "5F"),
    ("9D", "4E")
]

# Create directional graph from list with edges.
G = nx.DiGraph(elist)

# Calculate the topological generations and store them in a list.
TopGens = list(nx.topological_generations(G))

# Print the topological generations with each generation on a new line.
print(*TopGens, sep="\n")

```

Appendix K: Focus group informed consent

INFORMATIEBRIEF over deelname aan:

Focusgroep voor validatie privacy-by-design volwassenheidsmodel

Onderzoekstitel: A focus area maturity model for privacy-by-design

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?

Privacy-by-design is een begrip dat stelt dat privacybelangen vroeg in een ontwerpproces aan bod moeten komen en vervolgens in de gehele levenscyclus van systemen, verwerkingsactiviteiten en data mee moeten worden genomen. Privacy-by-design wordt omschreven als een vaag begrip ondanks de goede intenties, er is geen eenduidige visie voor hoe privacy-by-design in de praktijk toegepast moet worden en welke activiteiten hierbij horen. Dit onderzoek wil de beste privacy-by-design activiteiten vinden en die samenvoegen in een volwassenheidsmodel. Dit type model kan praktijkbeoefenaars begeleiden in wat er gedaan moet worden en in welke volgorde, zodat privacy-by-design effectief toegepast kan worden.

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 P-Direkt. Het onderzoek wordt uitgevoerd bij P-Direkt, 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 focusgroep sessie als onderdeel van de validatiefase. U bent onderdeel van de focusgroep samen met andere praktijkexperts. De gehele sessie neemt ongeveer twee uur tijd in beslag. Gedurende de sessie wordt een versie van het privacy-by-design volwassenheidsmodel getoond en toegelicht. Er wordt van u gevraagd om uw gedachten en meningen te delen en om feedback te geven op het model. Een groepsdiscussie wordt daarbij gestimuleerd. 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 de focusgroep sessie 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 de focusgroep sessie. 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 volwassenheidsmodel. 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	M. Muszynski, BSc	m.muszynski@students.uu.nl
Onderzoeker	F. van Dijk, MSc	f.w.vandijk@uu.nl

TOESTEMMINGSVERKLARING voor deelname aan:

Focusgroep voor validatie van privacy-by-design volwassenheidsmodel

Onderzoekstitel: A focus area maturity model for privacy-by-design

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: ___ / ___ / _____

Appendix L: Focus group protocol

Focusgroep protocol: Validatie privacy-by-design volwassenheidsmodel

Onderzoekstitel	A focus area maturity model for privacy-by-design
Onderzoeker	M. Muszynski
Datum	08-12-2022
Duur	2 uur
Aantal deelnemers	5

Tijd	**Onderdeel**	**Beschrijving**
2 min	Introductie	Goede middag, Welkom bij deze focusgroep voor de validatie van een privacy-by-design volwassenheidsmodel. Ik zal kort uitleggen hoe deze sessie eruit gaat zien en wat het doel is.
5 min	Doel	Het doel van deze sessie is om een eerste versie van een privacy-by-design focus area volwassenheidsmodel te valideren. Validatie houdt in dit geval in dat jullie, de praktijkexperts, jullie mening, visie, opmerkingen, of feedback geven op het model. Het is een vrije vorm discussie dus voel je vrij om iets te zeggen of om vragen te stellen als iets niet duidelijk is. We hebben een gevarieerd gezelschap dus het zou mooi zijn als we vanuit verschillende invalshoeken privacy-by-design kunnen belichten om tot een gezamenlijke visie te komen.
5 min	Toestemming	Voordat we inhoudelijk beginnen heb ik jullie toestemming nodig om alles wat uit deze validatie komt als onderzoeksdata te mogen gebruiken voor verdere ontwikkeling van het model. Jullie hebben een informatiebrief en toestemmingsverklaring ontvangen. Hebben jullie deze gelezen? Zijn hier vragen over? Jullie deelname is geheel vrijwillig, je mag stoppen wanneer je maar wilt, dit is geen probleem. <u>De audio van de sessie wordt opgenomen.</u> Is iedereen zich daarvan bewust en stemt iedereen daar mee in? De audio wordt alleen gebruikt voor een transcriptie en zal daarna worden vernietigd. De transcriptie en onderzoeksdata zullen verder niet persoonlijk herleidbaar zijn, jullie namen zullen nergens genoemd worden. **[Check toestemmingsverklaringen]**
5 min	Introductierondje	Het lijkt me goed om een kort introductierondje te houden zodat we elkaar iets beter kunnen leren kennen. Wie ben je en wat doe je? [Zelf introduceren, rondje aflopen]
1 min	Opname	Dan gaan we nu inhoudelijk beginnen en ga ik de audio opname starten. **[Opname starten!]**
10 min	Model presentatie	Ik zal eerst het model presenteren en kort toelichten hoe het tot stand is gekomen. • 2 literatuurstudies

		• Factoren verzameld uit het privacy, data governance, en PbD domein • Gefilterd op relevantie • In focus areas gegroepeerd • Afhankelijkheidsrelaties bepaald.
20 min	Vraag 1	Wat vinden jullie van de focus areas? • Komt het privacy-by-design domein hierin compleet terug? • Ontbreekt er iets? • FA: Asset inventory? • FA: Policy?
10 min	Vraag 2	[level 1 tonen] • Eerste niveau belangrijk omdat dit het startniveau is. • Doorlopen van de capabilities. • Goede entree voor het model? • Niet te intimiderend? • Ontbreekt er wat?
		Ruggengraat focus areas doorlopen: • Roles • Risk management • Requirements • Architecture • PIA process
10 min	Vraag 3	FA: Roles • Is het compleet, wat ontbreekt? • Is het PbD? • Is het generiek genoeg? • Goede volwassenheidsvoortgang?
10 min	Vraag 4	FA: PIA process • Is het compleet, wat ontbreekt? • Is het PbD? • Is het generiek genoeg? • Goede volwassenheidsvoortgang?
10 min	Vraag 5	FA: Requirements • Is het compleet, wat ontbreekt? • Is het PbD? • Is het generiek genoeg? • Goede volwassenheidsvoortgang?
10 min	Vraag 5	FA: Architecture • Is het compleet, wat ontbreekt? • Is het PbD? • Is het generiek genoeg? • Goede volwassenheidsvoortgang?
10 min	Vraag 6	FA: Risk management • Is het compleet, wat ontbreekt? • Is het PbD? • Is het generiek genoeg? • Goede volwassenheidsvoortgang?
10 min	Outro	De tijd zit er bijna op dus we moeten afronden. Bedankt voor jullie aanwezigheid en bijdrage. Zijn er nog afsluitende vragen of opmerkingen?

		Jullie kunnen via de mail nog altijd contact opnemen als er vragen zijn. **[Stop opname]**

Appendix M: Assessment tool source code

This thesis is accompanied by a digital repository with supplementary files that are not suitable to be added to this document. This appendix will provide a short description of what the files that this appendix refers to entail and where they can be found.

Description
This appendix provides the source code of a proof-of-concept prototype web-based tool to support the privacy-by-design focus area maturity model. This tool has been developed in the artifact design phase and has been built in the artifact implementation phase. The tool has subsequently been used in the pilot test and full evaluation of the privacy-by-design focus area maturity model. It makes use of a Python back-end running on the Flask framework and uses HTML, CSS, and JavaScript for front-end presentation.

Digital repository:
https://github.com/MichelMuszynski/PbD-Maturity-Tool

Appendix N: Maturity report example

Privacy-by-Design Maturity

2023-02-22
www.privacymaturity.org

Maturity assessment results

This report shows the maturity results based on the provided answers during the assessment. The coloured cells in the table below denote the maturity level per focus area. The last column that is entirely coloured will be the overall maturity level. The improvement actions tell you what must be done to reach the next maturity level.

		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		

Overall maturity	Lowest focus area	Highest focus area
3	PIA process: 3	Requirements: 10

Improvement actions

PIA process

- Determine and document the scope and scale of the PIA.
- Assign and document the PIA roles.
- Assign and document the PIA responsibilities.
- Assign and document the PIA approval process.
- Assign and document the needed PIA resources.
- Implement a privacy control selection process to evaluate the proportionality of selected measures.

PIA report

- Store PIA reports in a centralised registry.
- Make the centralised PIA registry available as a body of knowledge for consultation.
- Put a mechanism in place for updating and publishing PIA reports whenever significant changes are made to processing activities.

Privacy-by-Design Maturity - www.privacymaturity.org

Utrecht University

Sharing science, *shaping tomorrow*

Appendix O: Survey informed consent

Utrecht University

Informed consent

A focus area maturity model for privacy-by-design.

You are invited to participate in a research study about privacy-by-design maturity. Please read this informed consent notice carefully before participating. Privacy-by-design is a paradigm that prescribes embedding privacy concerns in the life cycle of systems, processing activities, and data. Often this term is described as vague and there is no consensus on what privacy-by-design entails or how it should be applied in practice.

The goal of this study is to identify and classify the best privacy-by-design activities and consolidate them in a maturity model. This type of model can guide practitioners in determining what has to be done and in what order so that privacy-by-design can be applied effectively.

Your participation in this study consists of completing a questionnaire as part of the evaluation of the model. You will perform the regular assessment which will include several additional questions about your opinion of the model, the assessment, and the resulting maturity results. Your answers to these questions will be used to further improve the model and support future research.

Your participation in this study is completely voluntary. You are not forced to participate and you may stop participating at any time, this will have no negative effects. There are no physical, legal, or economic risks tied to this research. There are no additional inducements or incentives apart from the maturity assessment results tied to this research.

The answers you provide during the assessment and evaluation questions will be stored and processed. The assessment questions ask for information regarding the privacy practices of your organisation while the evaluation questions ask for your opinion. We do not ask you to provide any personal data, all data is anonymised and will not be related to any specific person. Research data will be stored for 10 years following the policy framework for research data of Utrecht University.

This research study is conducted by researchers from Utrecht University. For questions or complaints regarding your data, you may contact the data protection officer of Utrecht University (privacy@uu.nl). For general questions or further information, you can contact the researchers:

Lead researcher	F. van Dijk, MSc	f.w.vandijk@uu.nl
Researcher	M. Muszynski, BSc	m.muszynski@students.uu.nl
Project supervisor	prof. dr. S. Brinkkemper	s.brinkkemper@uu.nl