electronics

MDPI

Article

Design and Evaluation of a Focus Area Maturity Model for Privacy-by-Design

Friso van Dijk [1,*], Michel Muszynski [1], Marco Spruit [2,3], Sjaak Brinkkemper [1] and Matthieu Brinkhuis [1]

[1] Department of Information and Computing Sciences, Utrecht University, Princetonplein 5, 3584 CC Utrecht, The Netherlands; s.brinkkemper@uu.nl (S.B.); m.j.s.brinkhuis@uu.nl (M.B.)
[2] Department of Public Health and Primary Care, Leiden University, Albinusdreef 2, 2333 ZA Leiden, The Netherlands; m.r.spruit@liacs.leidenuniv.nl
[3] Leiden Institute of Advanced Computer Science, Leiden University, Einsteinweg 55, 2333 CC Leiden, The Netherlands
* Correspondence: research@frisovandijk.com

Abstract

Privacy-by-design (PbD) considers privacy in the entire lifecycle of information systems and personal data. Although a wide variety of techniques for PbD exist, a framework that considers privacy in the full context of both systems design and organizational development remains absent. This research aims to design, validate, implement, and evaluate a PbD Focus Area Maturity Model as a guiding artifact for the application of PbD (PbD-MM). The PbD-MM was created using a design science approach. A set of previously coded PbD activities were used to formulate capabilities for the maturity matrix. The PbD-MM describes 14 focus areas and 60 capabilities, with their dependencies creating 10 maturity levels. The PbD-MM was validated through a focus group with PbD practitioners and implemented in a web application offering self-assessment and reporting. A total of 46 completed assessments were collected through online distribution. We find a broad basis of capabilities in PbD practice, with further developed governance and compliance, and a positive correlation between the highest-scoring focus area and higher overall maturity. The PbD-MM offers a structuring of PbD activities and an assessment instrument to support the development of organizational PbD capabilities.

Keywords: privacy by design; maturity model; functional domain; maturity assessment instrument

1. Introduction

Privacy, digital security, and data breaches have become a mainstay in public awareness, with regulatory and legislative efforts enacting protections and guidelines for using personal data in response. Included in these privacy-regulating efforts is the inception of a new systems design approach: privacy-by-design (PbD) [1]. PbD states that privacy should be embedded throughout the entire system design process as an essential component, using a proactive approach to mitigate privacy concerns and data protection issues early in systems design. Approaching privacy as a value in the design stage aims to prevent time-consuming, expensive, and potentially ineffective solutions during later stages of systems design to address privacy concerns that could have been identified earlier.

PbD is introduced as a set of design principles [1], of which the translation to organizational practices is a non-trivial challenge. The conditions for the successful application of PbD throughout all phases of information systems design in an organization were criticized

Check for updates

Academic Editor: Cheonshik Kim

Received: 16 June 2026
Revised: 17 August 2026
Accepted: 18 August 2026
Published: 30 August 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

for being vague and open-ended [2,3]. New standards, for example the ISO/IEC 27701 and NIST Privacy Framework, high-level guidelines, design techniques, and Privacy Enhancing Technologies have addressed many of these concerns. However, a gap remains in the application and validation of PbD research in organizational environments [4], as well as the integration of different techniques and development of supporting tools in bringing PbD principles to the practice of software engineering [5]. Likewise, the application of the Privacy Impact Assessment (PIA) as a principal design instrument suffers from a lack of consistency. A PIA is often considered a one-time compliance effort rather than a continuous process, where theory and practice are often misaligned and dependent on individual skill rather than mature processes [6].

The above observations indicate that a lack of structure remains in the PbD field and that its practices are inconsistently applied. Considering the number of moving parts in the application of PbD and the observed disparity between research and practice, there is a need for structuring and guiding artefacts in the PbD domain [7]. Such artefacts should aid in the structured and repeatable application of PbD in an organization's information systems design projects, ensuring that organizations have the necessary capabilities to address privacy design challenges in new initiatives and the application of novel technologies. The rapid adoption of Artificial Intelligence and new privacy issues arising in both the development and use of AI systems provide a strong case for identifying and structuring PbD capabilities. The aim of this research is to create and evaluate such an artifact to identify and structure PbD practices, while providing guidance to practitioners looking to apply PbD.

Stages of growth models are commonly used in organizational research to structure the progressive development of capabilities [8], of which maturity models are a much-used form in the IS field [9–11]. They can be categorized into two archetypes [12]: fixed-level models and Focus Area Maturity Models (FAMMs). A FAMM determines its number of growth stages (levels) based on the capabilities and their dependencies in a functional domain, rather than fitting capabilities to a predetermined set of levels [13]. This approach provides more flexibility in mapping a complex domain and the relation between its capabilities, rather than constraining a structuring effort to a set number of capabilities.

Based on the identified knowledge gap, the objective of this research is to design, validate and evaluate a FAMM that structures the functional domain of PbD. The model would aid organizations in understanding and employing PbD in information systems design projects [9]. Using the design problem template [14], the design problem is formulated as:

How to design a maturity model *that satisfies* Focus Area Maturity Model components and quality attributes *so that* organizations can employ effective privacy-by-design *in* information systems design projects.

The next sections describe relevant background information and the research methodology. Section 4.1 presents the PbD maturity model (PbD-MM) with 60 capabilities in 14 focus areas. The designed artefact is validated in a focus group of expert practitioners. The artefact is implemented through a web application with an online self-assessment and maturity report generation, presented in Section 4.2. In Section 4.3, PbD practices and the artefact are evaluated with data collected through the online self assessment and evaluation questionnaire. The resulting PbD-MM offers a first structuring of PbD activities in the context of organizational development and demonstrates the consistent appearance of its capabilities in practice. We discuss the implications of our findings in Section 5.

2. Background

2.1. Privacy-by-Design

PbD is the embedding of privacy and data protection throughout the entire lifecycle of personal data and information systems, from early design to their deployment and ultimately disposal [15]. The PbD paradigm originated in 2009 in response to privacy challenges in global competition, increasing system complexity and rapid innovation [1]. The PbD process covers all lifecycle stages and applies privacy and data protection design patterns that are well understood best-practices for their particular domain; it aims to limit privacy invading activities in the produced design documents and information system [1].

PbD is an evolution from Privacy Enhancing Technologies (PETs), creating a broader scope that allows the consideration of technology, management functions, business processes, and other organizational activities relevant to information systems design [16]. The implementation of PbD suffers from difficulties such as legacy systems, lack of economic incentives and a lack of end-user trust [17,18]. The concept is perceived as vague [2], is shrouded in opaqueness and distrust [15] and the focus of PbD is too heavily on compliance with regulation rather than seeing to the needs and attitudes of users [19,20].

The lack of regulation pushes PbD towards an individualistic nature where everyone is free to assert their process as PbD [15]. This places a heavy burden on society to understand the differences and therefore inhibits transparency about privacy implications. This is illustrated through the General Data Protection Regulation [21], which prescribes the application of the principles of PbD and privacy-by-default. However, the regulation offers an open norm and 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 through further regulatory guidance and the design of PbD methods and instruments [15].

The Privacy Impact Assessment (PIA), or Data Protection Impact Assessment, is considered a central component to integrating privacy measures in the foundations of a system [22] and as a practical method to establish PbD [23]. The PIA is a key design instrument in inventorying the use of personal data and associated privacy risks, formulating mitigation measures, and demonstrating compliance with privacy legislation [24]. Legislators have incorporated the practice in their regulatory efforts, and it has been proposed as an instrument to substantiate the principles of PbD [21]. In practice, performing a PIA as intended is not without its challenges. Instead of the envisaged continuous PIA, organizations often perform a PIA as a one-off activity [6], and software architecture is often not adequately considered [25].

Studies investigating PbD from a developer viewpoint identify further issues in how developers handle privacy requirements. Organizational culture and policies play a significant role in both positively and negatively encouraging developers to consider privacy in their work [26]. A suitable organizational privacy climate can encourage developers to prioritize privacy by enforcing positive practices and norms [27]. This includes organizational guidelines for software developers to embed privacy into system designs [28]. Another issue in building privacy-friendly systems is that PbD architectures tend to be rejected if they do not align with existing software frameworks [27]. Further concrete examples of challenges faced by developers are offered by [29]: 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.

Various methods have been developed to address the issues with implementing PbD. One popular approach is PbD through software architecture by using privacy design strategies to bridge the gap between early design and architecture. Example design strategies are

minimizing, hiding, or aggregating personal data [30]. There are also privacy frameworks coupled to privacy architecture [25], personal data lifecycles [31], and various other techniques. Artifacts that cover the entirety of the functional domain can bring further clarity to the practices of PbD. Unexplored in the PbD domain are maturity models, which offer such a structuring with the added lens of organizational development.

2.2. Maturity Models

Stages of growth models are commonly used in organizational research and are well-established in the information systems (IS) field [9]. The foundations of maturity models were built in the 1930s with process improvement through quality control, providing a base for extension and adaptation. In 1979, the quality management maturity grid (QMMG) was introduced, which was the first model incorporating consecutive stages that build on each other, similar to many of today's maturity models. Current-day maturity models can be categorized into two archetypes [12]: fixed-level models and FAMMs.

Maturity models have varying purposes [9]: descriptive, comparative, and prescriptive. Descriptive usage entails assessing the as-is situation within an organization, providing a snapshot of the current performance without looking at potential improvements. A descriptive maturity assessment can be compared with as-is assessments of other organizations. This comparative usage allows organizations to benchmark themselves against similar organizations on various axes, such as organization size or sector. A maturity model's prescriptive use 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 organizational component.

FAMMs consist of a number of focus areas; these are coherently defined subsets of the respective functional domain [12,13]. For each focus area, a number of capabilities are defined, and the dependencies between the capabilities are determined. A major benefit of FAMMs is the ability to determine the number of levels necessary for the integrity of the domain it models, rather than fitting the identified capabilities to a predetermined set of levels. This contrasts FAMMs to fixed-level models that often have a set number of levels, often five, regardless of their contents. The number of levels in focus area models is not set a priori and depends on the number of capabilities and the dependencies between them. FAMMs have been developed for a wide range of functional domains within IS, including API Management [32], Cybersecurity [33] and Smart Cities [34].

Applied to the domain of PbD, maturity models offer a structure to incorporate the various proposed techniques in a more complete image of the functional domain. Among them, the open-ended nature of a FAMM allows for the full expression of the functional domain of PbD in as many maturity levels as are required by the identified capabilities and their dependency relationships.

3. Materials and Methods

The objective of this study is to design and evaluate a FAMM for the PbD domain, described as a design problem in Section 1. Maturity models must be developed with scientific rigor and validation in order to increase their scientific nature [35]. Design science has previously been applied for the creation of maturity models [13]. This research also uses the design science paradigm to construct a PbD FAMM. It follows the entire engineering cycle, which stands central to design science and offers four stages: (A) problem investigation, (B) treatment design, (C) treatment validation, and (D) treatment evaluation [14]. For the FAMM, we will use the definitions provided by [12].

The PbD-MM is constructed following six steps, visualized in Figure 1:

(A1) *Problem investigation*. Studying the problem context of PbD and formulating the design problem for a PbD-MM [9,13].
(A2) *Domain investigation*. Two literature reviews to investigate the PbD domain through existing privacy maturity models and documented PbD practices [9,36].
(B) *Model design*. Determining PbD capabilities, focus areas, and dependencies. Creation of the PbD maturity matrix [13].
(C) *Model validation*. Validating the designed PbD-MM through a focus group with 5 practitioners [9].
(D1) *Instrument development*. Implementation of the PbD-MM in a web application with informational pages, a self-assessment instrument, improvement actions, reporting functionality, and an evaluation questionnaire. The implementation was validated with a pilot group of practitioners [9,13,36].
(D2) *Evaluation*. Analysis of 46 collected assessments and 16 evaluation responses from the PbD-MM web application [9,13,36].

The rest of this section follows the method structure, starting from the domain investigation. Additional research data is made available in the attached data repository, including all identified factors in the literature, the mapping from factors to capabilities, the resulting maturity model, its dependency relations, and the source code for the assessment instrument.

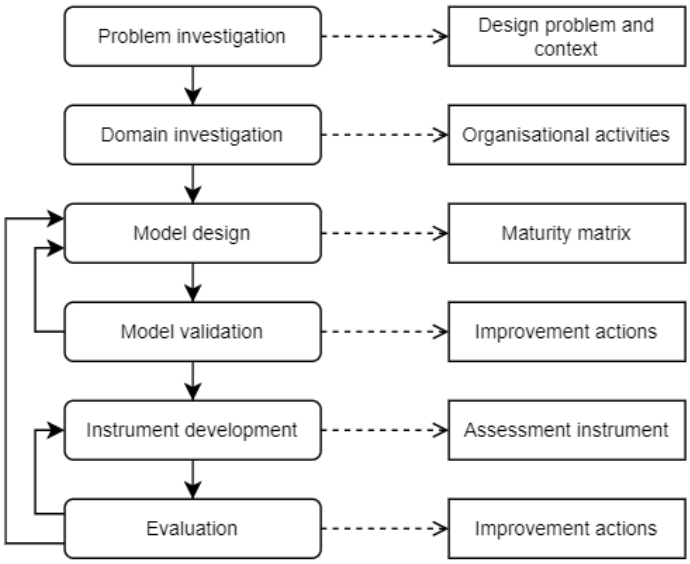


Figure 1. Research methodology overview displaying the process and outcomes for the design and validation of the PbD-MM.

3.1. Domain Investigation

The PbD-MM builds on a previously reported domain investigation consisting of two multivocal literature reviews [7]; structured literature reviews incorporating materials from scientific and practitioner publications, as well as guidance documents published by regulatory bodies. The first literature review identifies existing maturity models in the privacy domain and relevant adjacent domains. These models are compared and analyzed in order to get an understanding of what solutions already exist and demonstrate the necessity for a PbD-MM [36]. The second literature review investigates the organizational activities associated with the functional domain [9]. Both reviews were conducted in accordance with a literature review protocol and previously reported on.

In summary, no existing PbD maturity models were identified. A total of 847 privacy management and PbD activities were identified from 30 maturity models and 68 other

publications. Section 4 briefly describes the findings. The full results of the literature review are published in [7].

3.2. Model Design

The first step of the model creation process is to determine which activities are to be included for further processing. All 847 activities from the PbD domain model were assessed by the first two authors in order to achieve a consensus on the inclusion of each activity. The reductive criteria for the activities used during the inclusion assessment are:

1. *Fitness with the scope of PbD*. Privacy activities concern a broader scope than PbD alone. A multitude of activities describe organization-wide efforts that are outside the scope of PbD. Examples include the availability of an organizational privacy program or framework and organization-wide processes for general privacy awareness or reporting. While necessary for an organization, such activities are not directly concerned with designing information systems.
2. *Suitability of abstraction level for a maturity model*. Activities that are too concrete might not be suitable for a general maturity development path, for example, that a PIA report needs to contain a version log. Likewise, activities that are too abstract risk being perceived as vague or too open to interpretation, like PbD is integrated into business processes.
3. *Significance of contribution compared with previously included activities*. In order to reach theoretical saturation, activities were only included if they added new information.

A total of 371 activities were included in the creation of the maturity model.

The second phase of the model design entails creating the maturity matrix by determining the capabilities, focus areas, and dependency relationships [13]. These three activities are concurrent, since they are tightly coupled and iterative. Changing the wording of a capability could result in a necessary change in the dependency relationships of that capability, just as creating a new focus area would mean that new capabilities are introduced or moved from other focus areas. Of the 371 included activities, 257 activities were selected for best fit and combined to formulate 59 initial capabilities (60 after the validation) in 14 focus areas. A maturity matrix was populated with all focus areas on the vertical axis and all capabilities in the grid cells representing the appropriate focus area-maturity level combinations.

Both intra- and inter-focus area dependencies were modeled. The intra-focus area dependencies were identified by following a growth path where each capability builds on the previous. The inter-focus area dependencies were identified through intra-level assessment, where each level is assessed. A capability that depends on another capability at that level is shifted right to the next level, along with all following capabilities in that focus area. This results in a maturity matrix where the number of levels is dictated by the model's relationships. To validate the internal consistency of the created model, a directed dependency graph was created to confirm the absence of dependency cycles through a topological generation: 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 [37]. Analysis of the centrality of each node provided further insights into the key capabilities and relationships between focus areas.

3.3. Model Validation Design

The model validation for this research is conducted through a focus group [11,14]. A semi-structured interview protocol was created in a focus group protocol [38]. The interview protocol assigned fixed time slots for discussion on various elements of the model. First, the focus areas as a representation of the functional domain were discussed, followed

by evaluating the first level of the model across all focus areas. Finally, due to time constraints, a selection of five focus areas and their growth path in relation to other focus areas were discussed in more detail: roles, requirements, PIA process, architecture and risk management. These are the focus areas with the most connections in the model. The moderators guided these discussions along the maturity path of each focus area, describing the capability and requirements.

Written informed consent was obtained from all five participants, of which the demographics are described in Section 4.1.5. The focus group session was recorded and transcribed. Improvement actions were extracted from the transcript and applied to the PbD-MM before developing the assessment instrument.

3.4. Instrument Development

A maturity model is operationalized by an assessment instrument which allows an assessor to perform an assessment to ascertain the maturity level of an organization. Within the 30 identified maturity models that contain PbD capabilities, only 1 offered tool support and three more provided Excel sheets for self-assessments. One of the goals of this study is to create a model that can be applied by practitioners. Tool support would contribute significantly, as there are multiple automation opportunities in performing a maturity assessment and generating the results. To provide practitioners with an easy-to-use instrument and to support data collection, a web application was created as an implementation of the maturity model. This allows any user to access the assessment instrument from anywhere in the world, at any time, to perform an assessment and, if consenting, participate in the validation without the need to install additional software.

For the self-assessment, assessment questions typically have a binary yes/no response possibilities. In order to dissuade assessors from rounding up to a yes when they don't know the answer or when the accurate response is somewhat or partially, the design decision was made to add two additional response options: yes/somewhat/no/unknown. A conservative scoring method was used in the first iteration of the instrument. Only a confident yes for each question in a level will constitute maturity level achievement [12].

3.5. Evaluation Design

By validating the model through a single focus group, there is a need to introduce the artifact to a broader audience. We use a digital assessment instrument and a questionnaire to evaluate the model. The digital questionnaire allows for the easy introduction of the model to practitioners from diverse backgrounds, which increases the external validity of the results and can provide useful feedback from new perspectives [11,14]. Additionally, as the maturity assessment itself consists of a questionnaire, using an evaluative questionnaire allows for seamless integration of the evaluation activity in 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. Informed consent was requested prior to the assessment for use of the results in further analysis; non-consenting results were discarded.

The survey method for evaluation is a web questionnaire of 10 evaluation questions on a 5-point Likert scale (Section 4.3.3), three demographic questions, and optional text areas for positive and negative feedback. The evaluation criteria used for this questionnaire are selected from the taxonomy of evaluation methods for information systems artifacts [39]. A similar design has been used by [32] for the evaluation of a focus area maturity model for API management. The assessment instrument was tested by three practitioners before release to the public, and minor adjustments were made based on their feedback. The results were collected and analyzed, resulting in further suggestions for improvement.

4. Results

This section presents the outcomes of the maturity model design process. First, the PbD-MM is presented at the stage of its implementation in the assessment instrument (post-validation). Further attention is given to the dependency relationships between capabilities, the key design decisions, and the focus group validation with the incorporated improvement actions. Second, the online assessment instrument is described. Finally, the collected assessments are analyzed, and the evaluation questionnaire responses are used to formulate further improvement actions for the PbD-MM and assessment instrument.

4.1. Privacy-by-Design Maturity Model

4.1.1. Factor Selection and Capability Formulation

We provide a summary of the two MLRs published in [7] that this work builds upon. The purpose of MLR1 was to identify existing maturity models for PbD and related areas. A total of 30 maturity models were included in the results: 3 privacy maturity models from academic sources; 10 privacy maturity models from grey sources; 7 academic maturity models from reference disciplines; and 10 from reference disciplines from grey sources. No maturity models about PbD or sufficiently focused on PbD were identified. PbD was mentioned in two academic works [40,41]. The grey literature sources include privacy maturity models from standards bodies and governments: MITRE [42], AICPA and CICA [43], and the Dutch [44] and New Zealand [45] governments.

The identified maturity models were analyzed together with the outcomes of MLR2 on PbD activities from 68 academic, government, and industry publications. A notable observation is that the most used standards in practice, the ISO/IEC 27701:2025 and NIST Privacy Framework, did not appear in the literature reviews with a narrower scope of PbD. The NIST Privacy Framework, for example, is an "Enterprise privacy risk management framework" that provides "high-level privacy risk management outcomes that can be used by any organization to better understand, assess, prioritize, and communicate its privacy activities" [46]. Likewise, the ISO/IEC 27701:2025 as a privacy management standard does not detail the lower-level PbD activities identified in the domain model [47]. Included in the results are lower-level guidance documents that describe these activities in more detail, for example, the ISO/IEC 29134 on the PIA [48], the MITRE privacy engineering framework [49], and the UK Information Commissioner's Office guidance to PbD [50]. The resulting 847 privacy management and PbD activities form the PbD domain model dataset, with examples in Table 1.

Table 1. Coded activities used in formulating the first capability of the Requirements focus area.

ID	MLR ID	Activity	Origin	Source
159	2-18	Privacy requirements are formulated before the design stage.	Academic	[51]
178	2-54	A gap analysis is performed to identify legal requirements.	Academic	[52]
238	2-187	Engineers are provided an evolving catalog of privacy patterns that instructs how to meet privacy requirements	Academic	[53]
325	2-367	High-level privacy requirements are derived from general privacy principles and the PIA.	Academic and grey	[49,53–56]

Through iterative open coding and categorization, a first PbD domain model was created. The inter-rater reliability was measured using Cohen's kappa, where the raters had an agreement of 89% and Cohen's kappa of 0.771. Disagreements were resolved between the two raters through discussion, resulting in a final set of 371 included activities. In this

section, we describe the creation process and traceability of the activities for one capability, with the full set available in Appendix A.

Using the categorization available in the dataset from the PbD domain model, 16 categories were included. A first mapping was made for each category by placing the capabilities in order of required maturity. Two categories did not offer distinct enough capabilities to warrant their inclusion as separate focus areas.

From this point, the capability formulation happened iteratively. For the first capability of *FA1. Requirements*, 4 activities were used in its final formulation (Table 1): 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, and privacy-violating requirements are discarded.

4.1.2. Maturity Matrix

The final PbD-MM maturity matrix (Table 2) consists of 60 capabilities in 14 focus areas, 10 maturity levels, and are based on 95 dependency relationships. A total of 59 capabilities were defined during the creation stage, and 1 was added after the validation. The focus areas are derived from the functional domain model presented in [7]. The capabilities are reasonably evenly distributed across the maturity levels up to level seven, after which there are fewer capabilities per level. Identified sources offered fewer activities for the higher maturity levels in the PbD domain, as opposed to the early levels whose activities are mentioned more in source works. Individual capability descriptions are available in Appendix A.

Each focus area in the model has between 3 and 6 capabilities, totaling 60 capabilities. A brief description of the development path for each focus area is provided below.

Table 2. The PbD-MM maturity matrix with 14 focus areas and 60 capabilities. The levels are organically generated by modeling dependency relationships between capabilities.

	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		

FA1 **Requirements** deals with explicitly formulating privacy requirements to translate a need to design. At level zero, privacy requirements are not explicitly formulated. The maturity development starts with formulating privacy requirements, followed

by validating privacy requirements, involving stakeholders and, finally, consulting ethical experts.

FA2 **Architecture** concerns the formal incorporation of privacy requirements in system design. At level zero, privacy is not explicitly considered in the software architecture. The maturity path consists of creating a privacy architecture viewpoint, modeling personal data flows, and validating models against requirements. Finally, it considers using and cataloging the use of privacy strategies, tactics, design patterns, and PETs.

FA3 **Development** entails the implementation of the information system and selected privacy measures. It starts with privacy not being addressed explicitly during development. Maturity grows by ensuring that the system meets privacy requirements, integrating privacy in the development lifecycle, applying PbD within change management, and documenting privacy design patterns.

FA4 **Technology** contains capabilities related to technological measures, PETs and privacy-by-architecture. Level zero states that PETs are not explicitly implemented. The maturity development includes purpose-based data access, implementing PETs, assessing selected technologies, enforcing privacy policies through technical design, and implementing revocable privacy.

FA5 **PIA process** deals with the management and execution of the PIA. Level zero describes the PIA as a one-off process. It is assumed that organizations know what a PIA is and that they can perform one from a template. At increasing maturity levels, this includes periodic revision of the PIA, conducting a threshold analysis, decoupling the process and report, senior accountability, and continuous process improvement.

FA6 **PIA report** is concerned with the reported outcomes of the PIA process. At first, the report is tightly coupled with its process, and one report exists for all audiences. Maturity develops by formally reviewing the report, storing PIA reports in a centralized registry, auditing the report, and generating different PIA reports based on audience needs.

FA7 **Risk management** is integrating privacy risks into the organizational risk management. At level zero, privacy is not part of the organization's risk management approach. The maturity development includes employing a privacy risk analysis framework, keeping a privacy risk inventory, policies to monitor and optimize privacy risk management, and using predictive analytics.

FA8 **Processing principles** details capabilities related to the application of PbD processing principles, such as data minimization, to guide data processing activities. Level zero stands for no proactive application of processing principles. Maturity development includes selecting and applying a set of standard principles to all processing activities, periodically evaluating their application, using a lawfulness dashboard, and proactively managing adherence to the principles.

FA9 **Subject rights** deals with individual rights relating to the use of personal data. At level zero, data subject rights are not actively facilitated through design. The growth path entails recording and documenting subject requests, using technology to facilitate data rights, creating an overview through a dashboard, and employing user-driven control.

FA10 **Transparency** concerns informing data subjects about processing activities. Level zero states that 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.

FA11 **Third party management** is the management of third parties in the data processing chain. At level zero, data processing agreements are established on an individual basis. The development path for this focus area concerns conducting a privacy risk assessment for third parties, using exception reports to record unacceptable activities, and making privacy level agreements.

FA12 **Roles** are capabilities related to the formulation and formalization of roles and responsibilities in privacy activities. Level zero describes that privacy-related roles are not formally defined for the entirety of the PbD process. The maturity development includes identifying relevant stakeholders, appointing a chief privacy officer, assigning a technical privacy officer, and appointing a privacy committee.

FA13 **Awareness** concerns stimulating privacy awareness among people who are involved in applying PbD. At level zero, privacy awareness is not actively stimulated. The maturity development includes awareness of the basics of PbD and broader privacy management, training PbD target groups, obtaining management commitment for PbD, and interacting with the PbD body of knowledge.

FA14 **Monitoring** is the monitoring, validating, and improving of privacy activities. Level zero describes that relevant activities are not structurally monitored. Its growth path focuses on technical compliance monitoring, and entails having a regulatory compliance assurance process, logging all processing activities, continuously monitoring policy compliance, performing periodic reviews and independent audits.

For each capability, a set of 1–4 atomic improvement actions were formulated to transition from one capability to the next within a focus area. An example of the improvement actions is shown in Table 3.

Table 3. Improvement actions to achieve capability A for the Requirements focus area.

	Improvement Action
1	Formulate the privacy requirements based on general privacy principles and the PIA.
2	Formulate privacy requirements before the design stage.
3	Elicit business and legal requirements with privacy in mind.
4	Discard business requirements that violate privacy.

4.1.3. Dependency Relationships

A total of 45 intra-focus area dependency relationships were mapped, where each capability in a focus area follows on the previous, such as (1A, 1B). The inter-focus area dependency relationships are more complex, with each capability exerting 0 or more relationships (Table 4). A total of 50 inter-focus area dependencies were identified. The combined set of 95 dependencies between capabilities in the PbD-MM was modeled as a directed graph. Figure 2 shows the full dependency graph.

Centrality measures offer some insights into the composition of the PbD-MM. No particular capability stands out for the in-degree distribution, although of the 10 capabilities with the highest in-degree, only 2 appear below the letter C. Capabilities at a higher maturity level are, on average, more complex and depend on more prerequisite capabilities. For the out-degree distribution, node 12B has an out-degree of 7, suggesting this is a key node in the graph. 12B entails appointing a chief privacy officer and formalizing stakeholder roles and responsibilities, which is a central component of a formalized PbD function within an organization.

Table 4. Subset of the inter-focus area dependency relationships for capability 1A (FA1 Requirements capability A) to other capabilities in the model. The capability labels correspond with Table 2.

Dependency	Motivation
(1A, 2A)	Privacy requirements must be formulated before a privacy architecture can be created that maps privacy requirements on the project architecture
(1A, 5A)	Privacy requirements must be formulated before a PIA can document how they are implemented.
(1A, 11A)	Privacy requirements must be formulated before risks related to third parties can be identified.
(1A, 14A)	Legal (privacy) requirements must be formulated before compliance with regulation can be demonstrated.

As a final step, the aggregate degree distribution was analysed at the level of focus areas. *FA5. PIA process* has the highest in-degree (5), a higher out-degree (6), and the highest total degree (11). It depends on four focus areas, and five focus areas depend on the PIA process. The Risk management focus area shares the highest total dependencies with the PIA process (11). Seven focus areas depend on capabilities from *FA7. Risk management*, while it depends on three focus areas. This suggests that the PIA process and risk management represent the core of the PbD-MM. An additional noteworthy observation is that *FA10 transparency* and *FA13 awareness* have an out-degree of zero. No capabilities from other focus areas directly depend on these focus areas.

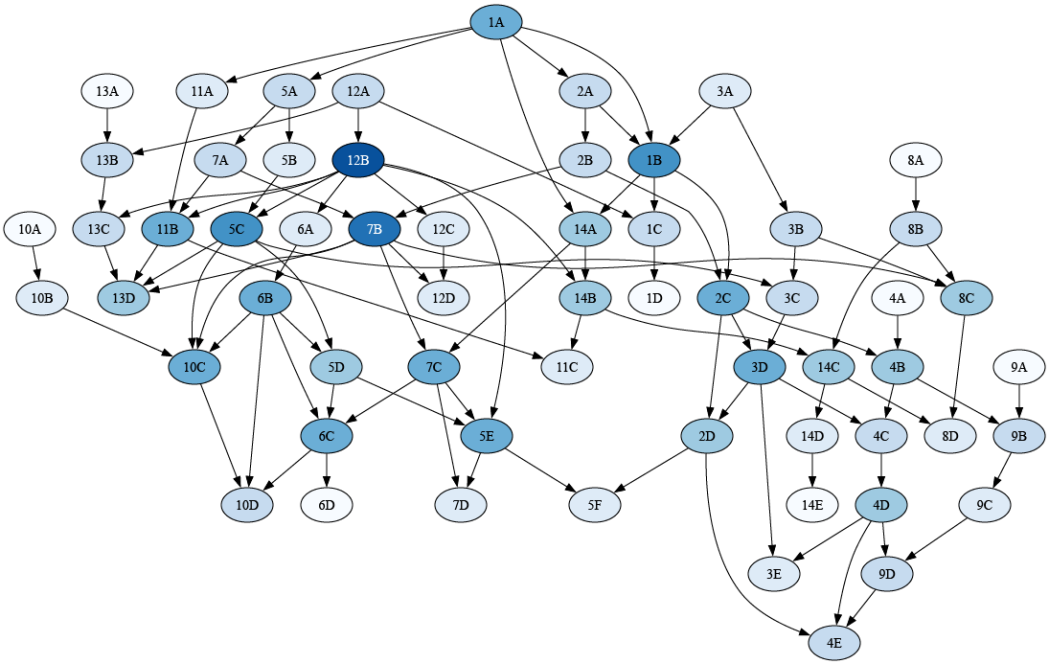


Figure 2. Dependency model of the PbD-MM generated from the directed graph of dependency relationships between capabilities with a gradient for the degree of each node (darker is higher). The capability labels correspond with Table 2.

4.1.4. Design Decisions

This section details the significant decisions made during the design of the PbD-MM. While a structured approach was applied to create a reproducible maturity model, decisions were made during the process that influenced its outcome.

1. *The PbD-MM is scoped towards PbD and not privacy management*. PbD is not a logical first step for an organization concerned with its privacy practices, as it is a domain

within privacy management. As a result, certain basic capabilities were absent from specialized PbD materials. For example, descriptions exist on the activities of a PIA process and when to perform one, but not the basic capability of simply performing a one-off PIA. Level zero capabilities were formulated to establish the minimum practices assumed necessary for PbD for the focus areas PIA process, PIA report, Transparency and Third-party management. Likewise, general privacy awareness was deemed to be out of scope, and activities related to stimulating the organizational privacy culture were excluded.

2. *Excluded Policy and Asset inventory focus areas*. Two focus areas were excluded because they added little value to the model. Policy lacked individual capabilities that existed separate from the other identified focus areas. Asset inventory primarily described basic capabilities with no suitable development path.
3. *Distinguished PIA process from PIA report*. The PIA as a process was separated from its presentation. This allows for the PIA process to continue independently of its reporting, while at any time different reports can be generated for a particular purpose or audience. This decision was made upon encountering activities describing various audiences and report contents, as well as its structural similarity to software architecture where different views and viewpoints are tailored to the expectations and expertise of the intended audience.
4. *Excluded specifics of legal frameworks*. Many activities implement specifics of the GDPR. However, the design goal of the PbD-MM is to employ effective PbD, not to assess compliance with any specific legal framework. While the GDPR unmistakably has an effect on what is considered PbD, the decision was made to exclude activities prescribing specific legal requirements where a more generalized alternative was available.
5. *Excluded contents of PIA report*. Descriptions of the contents of a PIA report were discarded. For example, listing processing activities, selected privacy controls, and the PIA approval process. A wide variety of templates exist with specifics for a legal jurisdiction or market. The PIA report focus area in the PbD-MM is limited to how the report is used, reviewed, updated, and who is responsible for it, not what it contains.

4.1.5. Model Validation

The model was validated using a focus group. A variety of occupations and roles were selected to ensure a multi-perspective examination of PbD. The participants were employed at three Dutch government organizations, with the full group composition shown in Table 5. The organizations differ in function by the type of services they provide. One organization is an internal IT service provider for multiple government organizations as a "customer ", one is a service provider with the same scope, and one is a public service. In this section, we highlight the discussion points leading to changes in the PbD-MM.

Table 5. Overview of participants in the focus group with their function, years of experience in the function, organization size and type of organization.

	Function	Experience	Org. Size	Org. Type
1	Security/privacy officer	2.5 years	1000–2000	Service provider
2	Data scientist	3.5 years	500–1000	IT service provider
3	Data protection officer	4 years	5000+	Public service
4	Product owner	4 years	500–1000	IT service provider
5	Security architect	5 years	500–1000	IT service provider

The capabilities of the awareness focus area prompted a first discussion. The 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. In support of adding a capability for general PbD awareness at level one, 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, 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].*"

Improvement 1. *A new capability A is added to FA13 Awareness at level 1, which includes general PbD awareness and management support. The other awareness capabilities move up a level.*

The second topic of discussion was the level one capability of the technology focus area, prescribing the usage of encryption-at-rest and encryption-in-transit. Participant 2 commented, "*I find that 'personal data is encrypted in transit and at rest' quite impressive 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, concluding that encryption at rest could not be a level one capability because barely any company would get past level zero. 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.*" Participant 4 continued by proposing access to personal data as a level one capability in the technology focus area, ensuring separation of responsibilities through an authorization matrix. While both role-based and purpose-based access were identified in the PbD activities, purpose-based access better aligns with the purpose limitation principle. Within PbD, the main limitation for data access is the motivation rather than the person.

Improvement 2. *In FA4 Technology, capability A, the mention of encryption at rest is removed, and purpose-based access is added.*

Another discussion centered around the omission of most legal requirements from the model and the assumption that an organization should first focus on compliance before focusing on PbD. The discussion led to the consideration of the goal of a PbD-MM. The group came to the consensus that the goal of such a model is not to measure compliance but to develop PbD capabilities. With that in mind, participants 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:

> "*I do not expect that. I think that is a whole different story. You will get a ruckus about how to interpret 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.*"

While most specific legal requirements were removed from this version of the model, continuing this discussion led to formulating an additional improvement to address inconsistencies.

Improvement 3. *The GDPR specificity is removed from the capabilities in FA8 Processing principles.*

4.2. Online Assessment Instrument

A complete web application (https://www.privacymaturity.org) was developed using the Django Python framework version 2.2.3. The source code for this application is available alongside the research dataset.

The application consists of a homepage with an informational video about the PbD-MM and initial information. Visitors are prominently presented with a link to start a PbD-MM self-assessment. From the homepage, there are also links to additional information about the full model and the research project. Upon starting the assessment survey, practitioners are presented with an informed consent form and then assess their organization's capabilities for each maturity level through multiple-choice questions (Figure 3). If an assessor did not respond yes to all questions on the previous level, the option is offered to skip to the end and generate the final report.

After completing the assessment, the assessor is presented with a report page showing a filled maturity matrix: their maturity profile (Figure 4) and an atomic breakdown of the capabilities required for the next level as improvement actions (Figure 5). This report can also be downloaded as a PDF. From this page, the user is directed towards an optional evaluation questionnaire.

The assessment instrument was piloted with three practitioners. Overall, the assessment instrument was perceived positively. The practitioners preferred the convenience of an online survey and the generated report compared with earlier experiences with maturity model assessments through spreadsheets. One suggestion was made regarding the usefulness of the report. The desire was expressed to visualize partially developed capabilities, as this would better reflect current efforts when sharing the results inside the organization, for example, reporting to upper management.

Improvement 4. *A striped demarcation is used to display partially achieved maturity levels in the maturity matrix.*

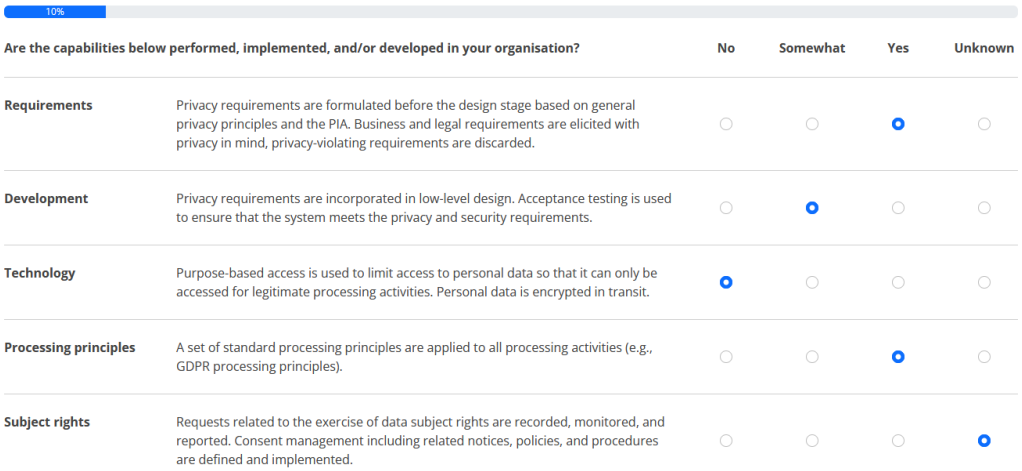


Figure 3. Partial screenshot of level 3 of the PbD-MM assessment questionnaire in the online assessment instrument.

4.3. Evaluation

The data collection started in the spring of 2023 by spreading the assessment instrument in the network of the researchers. Data collection from passive online discovery continued until June 2026. A total of 104 self-assessments and 16 evaluation questionnaires were performed. A total of 37 assessments were discarded during the data cleaning stage due to a combination of answering patterns and short assessment duration. It is likely that these respondents were testing the assessment instrument instead of performing an

assessment. A total of 25 valid assessments did not provide consent for further analysis. The remaining 46 assessments are described. This section begins with the analysis of the maturity assessments, followed by the outcomes of the evaluation questionnaire. Of the 71 valid assessments, 23 (3 without consent) were completed during the development phase and the first three months after active dissemination. Participants spent an average of 21 min 57 s on the assessment instrument. Shorter when using the skip function, and full assessments took between one and two hours.

		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		

Fully developed Partially developed

Figure 4. Screenshot displaying the maturity profile of the highest-scoring evaluation assessment. The final maturity score is calculated only accounting for the fully developed capabilities, in this instance level 0.

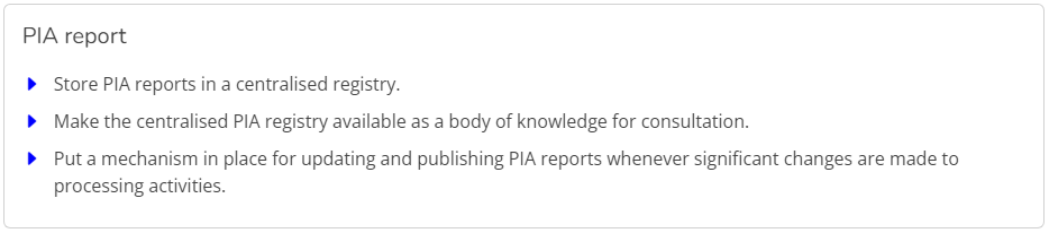


Figure 5. Screenshot from the PDF maturity report displaying the next capability the assessing organization should improve for the PIA report focus area. Improvement actions are presented as atomic components that together make up the assessed capability.

4.3.1. Maturity Assessment

The assessment results provide a high-level overview of the assessed PbD maturity. The aggregated responses (Figure 6) show that organizations implement a diverse range of PbD capabilities. A broad basis of early capabilities was accomplished, with the most

developed focus areas at level 1 leaning towards governance and compliance: *FA9. Subject rights*, *FA8. Processing principles* and *FA12. Roles*.

The least developed focus areas are *FA14. Monitoring*, *FA2. Architecture* and *FA3. Development*. Capabilities in these focus areas are more technically oriented. They include more extensive modeling of personal data processing within and between information systems, and the application of privacy design patterns and PETs. *FA14. Monitoring* concerns setting up continuous monitoring using logs and technical data to demonstrate compliance, which has a multitude of prerequisite capabilities and is thus unsurprising to be widely adopted.

Focus Area	1	2	3	4	5	6	7	8	9	10
Requirements	17	-	4	3	1	-	-	-	-	-
Architecture	-	7	5	0	-	-	0	-	-	-
Development	10	5	-	-	2	0	-	-	0	-
Technology	16	-	-	-	3	-	1	1	-	1
PIA process	-	17	14	9	5	3	-	3	-	-
PIA report	-	-	11	6	-	4	3	-	-	-
Risk management	-	-	11	4	3	-	2	-	-	-
Processing principles	22	12	-	-	1	-	0	-	-	-
Subject rights	23	-	-	-	-	1	1	-	0	-
Transparency	19	4	-	-	1	-	0	-	-	-
Third-party management	-	14	-	7	-	4	-	-	-	-
Roles	21	13	9	-	5	-	-	-	-	-
Awareness	19	6	4	-	3	-	-	-	-	-
Monitoring	-	-	-	4	4	0	0	0	-	-
Average focus area	**34**	**16**	**6**	**3**	**2**	**0**	**0**	**0**	**0**	**0**

Figure 6. Heat map of the PbD maturity profile of 46 self-assessments. Represents the total percentage of assessors that have achieved a capability and all preceding capabilities in that focus area.

The average maturity of each assessment was calculated by the maturity achieved in each focus area. The minimum average maturity observed is 0.71, equating to achieving no capabilities and automatically achieving the levels up to the lowest capability in each focus area. The highest average maturity is 5.93, with a mean of 1.80 and a standard deviation of 1.17. When observing responses that achieve high average maturity, the capabilities are spread across the model up to level 3 or 4. All capabilities up to level 4 were reached by multiple assessors. 6 of 46 responses (13%) did not achieve any capability in the model. Altogether, the responses show a diverse set of PbD capabilities achieved in organisations, where achieving high maturity in one focus area corresponds with achieving a higher average maturity. This shows that organizations tend to follow a development path in their PbD capabilities, where excelling in one area relates to a higher overall maturity.

The first three maturity levels were assessed using Cronbach's alpha on the collected assessments. All questions on each of the maturity levels were grouped, as well as each set omitting one item. Maturity level 1 has a Cronbach's alpha of 0.773; level 2, 0.875; and level 3, 0.918. Only omitting the level 2 capability for *FA10. Transparency* scored marginally higher, at 0.876.

4.3.2. Assessment Scoring

While participants achieved a wide variety of capabilities in the PbD-MM, the overall PbD maturity from the assessments is level 0. Participants were presented with a detailed maturity profile based on their responses (Figure 4), whereas overall maturity is determined by the lowest focus area. Only two assessments reached the first capability in every focus area on level 1 through fully responding yes, one of which achieved maturity level 3. The assessment results show that the most common reason was the use of somewhat responses, achieving a partial score in the maturity profile.

Assessments that achieve a higher average maturity on some focus areas often have one or more *somewhat* responses at maturity level 1, limiting maturity progression. Whether this is a result of the assessment design, a too strict capability formulation, or a capability that the organization needs to develop further, cannot be determined from these results.

Performing a sensitivity analysis on the responses provides additional insight into the effects of changing the scoring method. A full sensitivity analysis is outside the scope of this publication, so we provide a shallow analysis only on the number maturity levels achieved. Two factors were assessed: changing the scoring of Somewhat and Unknown responses, and changing the threshold for achieving a maturity level. The scoring was assessed by weighing Somewhat as (0, 0.25, 0.50, 0.75) and Unknown as (0, 0.25). Each scenario was compared with the thresholds 100%, 90%, 80%, 75%, and 67% of all points to consider a level achieved.

Six relevant scenarios from the sensitivity analysis are shown in Table 6. Scenario 1 is the current scoring method. Scenario 2 shows that reducing the threshold to 75% of capabilities achieved significantly increases the overall maturity levels, even when considering only Yes responses. A Somewhat weight of 0.25 sees a comparable increase at a higher threshold in scenario 3, and produces a longer tail of maturity achievement at a lower threshold in scenario 4. Scenario 5 shows that weighing somewhat answers at 0.5 produces a much stronger effect. Finally, scoring Unknown answers had a minimal effect on the overall maturity achieved, as can be seen when comparing scenarios 4 and 6.

Table 6. Sensitivity analysis of scoring methods for different weights of Somewhat and Unknown answers, and varying thresholds for achieving a maturity level.

Scenario	**1**	**2**	**3**	**4**	**5**	**6**
Somewhat weight	0	0	0.25	0.25	0.50	0.25
Unknown weight	0	0	0	0	0	0.25
Threshold ine Level 1	100% 2	75% 8	90% 6	75% 8	75% 17	75% 8
Level 2	2	5	2	5	9	5
Level 3	4	4	4	6	7	6
Level 4	1	2	1	5	7	5
Level 5	1	1	1	2	5	3
Level 6	0	0	0	0	2	0
Level 7	0	1	0	1	1	1
Level 8	0	0	0	2	2	2
Level 9	0	0	0	0	1	0
Level 10	0	0	0	0	0	0

Suggestion 1. *Implement and evaluate a more lenient scoring strategy for calculating overall PbD maturity.*

From the outcomes of a first analysis of scoring sensitivity, a future version of the PbD-MM should consider alternative scoring scenarios. Scenario 5 (Table 6) appears to produce results that better reflect the aggregate maturity level achieved (Figure 6).

For individual capabilities, the assessments show that all capabilities are responded to with yes or somewhat by at least 10 assessors. This confirms that the PbD-MM and the underlying works represent PbD capabilities that are recognized by practitioners and, at least partially, applied in practice, albeit less often for capabilities that require a higher PbD maturity.

4.3.3. Evaluation Questionnaire

A total of 16 participants filled out the evaluation questionnaire. Participants were asked to indicate how important privacy and data protection issues are to their organization. From very low (1) to very high (5), the results show a mean value of 4.38, which indicates that privacy and data protection are indeed seen as important issues. A total of seven evaluations originate from the Netherlands, with the others showing diverse demographics from four continents. The majority of evaluation responses come from practitioners in large organizations (500+ employees).

From Table 7, a generally neutral to moderately positive attitude can be observed for the evaluation criteria. The statements in the assessment instrument were presented in the order: 1a, 5b, 3a, 2b, 4a, 5a, 4b, 1b, 3b, 2a. Statements 1b, 3a, and 4a were formulated negatively and had their scores reversed for analysis.

Structural completeness is the highest evaluation criterium at 3.54. Operational feasibility (3.47) also achieves an above-average score. Ease of use falls behind at 2.57, primarily with statement 4a having the lowest mean. Opinions seem to differ on how difficult it is to assess PbD maturity using the proposed model and assessment instrument. Possible explanations include unfamiliarity with PbD practices, improper wording of capabilities, or misaligned capabilities and maturity levels. However, as all three negatively formulated statements (1b, 3a and 4a) score lower and have a higher standard deviation, there may also be some participant misinterpretation.

Suggestion 2. *Further investigate and improve the ease of use for assessing PbD maturity.*

Two participants commented on the capability granularity, describing how some topics are implemented while others are not and suggested splitting capabilities up, possibly needing more levels. Currently, the model contains 60 capabilities that indeed consist of multiple practices each. Compared with other FAMMs, for example [12,57,58], we argue that 60 is a reasonable number. Another explanation may be that the capabilities at maturity level 1 need to be reworded. The Cronbach's alpha for level 1 is lower than for later levels, yet it also is the first, and in some cases only, level assessed.

Suggestion 3. *Create a customizable assessment instrument to provide a more accessible overview of relevant PbD practices.*

Two participants commented that the questionnaire could be split up in different ways. Both suggested excluding focus areas for specific user groups. Specific mention was made to allow separating operational and governance functions. One participant suggested a shorter questionnaire to create an introductory overview of the PbD domain. Both options warrant further exploration. From these comments, we understand some participants act as

responsible parties but rarely engage with these activities themselves and instead develop a higher maturity in *FA11. Third-party management*.

Table 7. Average outcomes of the evaluation questionnaire based on a five-point Likert scale, with the evaluation criteria and questions.

Criterion	#	Statement	Mean
-	0	How important are privacy and data protection to your organization?	4.38
Effectiveness	1a	I am able to assess the privacy-by-design maturity by using the privacy-by-design focus area maturity model.	3.81
	1b	I am able to formulate a development path by using the privacy-by-design focus area maturity model.	2.44
Operational feasibility	2a	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.	3.50
	2b	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.	3.44
Usefulness	3a	The privacy-by-design focus area maturity model positively impacts my ability to perform a privacy-by-design maturity assessment.	2.63
	3b	The privacy-by-design focus area maturity model positively impacts my ability to formulate a privacy-by-design development path.	3.75
Ease of use	4a	I find it easy to assess the privacy-by-design maturity by using the privacy-by-design focus area maturity model.	1.69
	4b	I find it easy to formulate a privacy-by-design maturity development path by using the privacy-by-design focus area maturity model.	3.44
Structural completeness	5a	The privacy-by-design focus area maturity model contains all required focus areas.	3.44
	5b	The privacy-by-design focus area maturity model contains all required capabilities.	3.63

For the positive comments, three participants commented that the assessment was comprehensive and thorough. Two participants mentioned that the maturity report would be immediately usable for a project plan. Finally, two participants complimented the assessment instrument on helping them expand their understanding of the functional domain of PbD.

5. Discussion

PbD has seen widespread adoption since the introduction of its foundational principles in 2009. With its application, it aims to offer a universal framework for strong privacy protections [1]. However, PbD was criticized for the vagueness of its principles [2,15]. The application of PbD requires specific expertise and the necessity to balance privacy with other requirements [3,6]. As a result, organizations implement their own vision on

PbD with the expertise they have at hand, leading to a lack of uniformity in its application. To structure our discussion, we pose four statements on the current state of the field, the relevance of the PbD-MM, our findings in practice, and the placement of PbD within privacy management.

Statement 1. *PbD has matured to offer methods and techniques that address specific practitioner needs but often lack connection to an overarching domain structure.*

Recent reviews of PbD in software engineering have encountered no shortage of practical solutions for PbD. However, this has created a new need for validation research [4,5]. In the evaluation of the PbD-MM, we find sufficient recognition of its capabilities to state that the PbD-MM represents capabilities actively used in practice. While there is a need to validate individual capabilities and their development, these findings reaffirm that PbD researchers and grey literature are addressing problems relevant to its practitioners.

What distinguishes the PbD-MM from earlier work is that it provides an overarching structure and more generalized PbD capabilities, rather than specific techniques. The PbD-MM originates from a PbD domain model demonstrating that PbD is in need of more detailed artefacts [7]. The PbD-MM is such an artifact, with sufficient granularity to describe the development of PbD capabilities. The provided framework builds on existing methods and techniques that provide the concrete implementation of its capabilities, while keeping a level of detail necessary to provide a concrete guideline. The PbD-MM should help future research to better contextualize their proposed solutions and account for the application of techniques at different stages of organizational development.

Statement 2. *The PbD-MM offers a practical instrument to assess an organization's PbD capabilities and create a PbD development path.*

The PbD-MM provides a logical structuring of the PbD domain from the perspective of organizational development. The evaluation shows that achieving a higher maturity in one focus area correlates with a higher overall PbD maturity, demonstrating that we can indeed distinguish levels of development. While the evaluation questionnaire highlights points of improvement, especially the ease of use in assessing PbD maturity, the PbD-MM performs well on structural completeness and operational feasibility.

The comments on ease of use show a desire for role- or domain-specific assessment tracks. This could be achieved by identifying focus area sets that fit within a category, such as governance and technology. Another direction worth investigating is extracting a smaller model for organizations that do not develop their own software. For those participants, the focus areas *FA2. Architecture*, *FA3. Development*, *FA4. Technology* and *FA14. Monitoring* may be less relevant to their overall maturity. Finally, the capability text and presentation could be improved to make the instrument more accessible, for example, by providing practical examples for each capability. Case studies in different contexts and additional design iterations could help improve the ease of use of the PbD-MM.

The area we find most in need of improvement is the scoring, as a conservative scoring approach, where Somewhat or Unknown equals No, provides a maturity profile that does not adequately display the progress an organization has made. Other FAMMs have attempted different scoring approaches, which show promising results in practice but still lack accuracy and scientific grounding [33]. The PbD-MM applied a conservative scoring in combination with the somewhat option to encourage conservative assessment. While this leads to higher accuracy, it likely harms the practical usability of the instrument for organizations that have made significant efforts to improve their PbD capabilities. While the artifact validation led to the improvement of displaying partially achieved capabilities

in the maturity profile, this was a practical consideration and not frequently encountered in other works. The sensitivity analysis (Table 6) provides further guidance to improve the scoring mechanisms, with partially scoring Somewhat and lowering the required threshold for achieving a maturity level producing results that appear more representative of the underlying data. Future work should investigate the impact of different scoring approaches on the perceived usefulness of FAMMs, as well as attempt to determine what measure of achievement finds a balance between usability and accuracy.

The development of PbD in practice is less structured than the theory of the PbD-MM. In order to overcome the vagueness of earlier PbD, many organizations have defined and implemented PbD to their own best effort [6,15,29]. This results in diverse approaches to PbD practices, which is reflected in the diversity of capabilities achieved within each assessment. While it remains necessary to investigate improvements to the PbD-MM, it is difficult to validate the development path presented in the PbD-MM in this research design. Furthermore, assessing PbD practices that significantly differ in content or scope from the practices identified in the body of knowledge will require a considerable mental effort from the assessor. This may reflect in the ease of use evaluation, as this was considerably lower for assessing PbD than creating a development path. Other methods for evaluation, such as expert interviews, could offer additional insights in these areas [32].

Statement 3. *Organizations display a broad basis of PbD practices, with a focus towards governance and compliance.*

Considering the aggregated outcomes of the 46 assessments displayed in Figure 6, three categories of focus area progression can be distinguished: high baseline, basic capabilities and low scoring. The high baseline category is primarily concerned with governance and compliance: *FA5. PIA process*, *FA8. Processing principles* and *FA12. Roles*. The overall performance on these focus areas progressed furthest in maturity. The basic capabilities set of focus areas saw the adoption of its lower-level capabilities, but the majority of respondents did not achieve a higher maturity: *FA1. Requirements*, *FA4. Technology*, *FA13. Awareness* and *FA13. Awareness*. The low scoring focus areas are directly concerned with translating policy into design and implementation: *FA2. Architecture* and *FA3. Development*. According to the PbD-MM, *FA14. Monitoring* requires a higher base level of maturity to employ effectively, which is reflected in the assessment results.

These findings do not stand on their own. Earlier work argues that the focus of PbD is too much on compliance with regulation, rather than accounting for end-user needs like embedding technical privacy protections and transparency in the technology itself [19,59]. This viewpoint is supported by other PbD researchers recognizing that organizations generally prefer to implement privacy-by-policy rather than safeguarding it through system architecture [6,60].

In the PbD-MM assessments, we recognize the same pattern of organizations applying a governance and compliance-focused approach, taking measures through privacy-by-policy rather than developing technical capabilities. The high baseline category includes not only focus areas directly involving software development but also *FA3. Architecture* and achieving a higher maturity in *FA1. Requirements*. The consequences are that the technical implementation of an information system differs significantly from its design, and end-users are not informed about how their personal data is actually used, if they receive information of sufficient quality at all [25,61].

Statement 4. *PbD is not a logical starting point for organizations implementing privacy protections, as effective PbD requires a foundation in privacy management.*

One notable aspect of the PbD-MM from other FAMMs is the formulation of capabilities at maturity level 0. These definitions were formulated by working backward from the first capability of each focus area to determine what would be expected from an organization that aims to develop its PbD practices. Four focus areas have a level 0 that presumes the presence of a capability, albeit in an unstructured manner: some manner of PIA process is implemented (as opposed to a repeatable method), the PIA process is tightly coupled to its report, processing agreements with third parties are established on an individual basis, and a public privacy notice exists. Establishing these basic capabilities are part of privacy management frameworks that consider the entirety of the organization [62].

The leading thought for FAMMs is that they should incorporate the very basics of a functional domain, so that it can be used by any organization regardless of current ability. We argue that PbD is entangled with privacy management in a manner that prevents this approach. An organization starting from scratch should invest resources in implementing the basics of privacy management before actively engaging in focused PbD maturity development. Among these basic capabilities are instituting a privacy office team with the required expertise to start on PbD, a strategic direction to guide structured development of privacy capabilities, a first mapping of the organization's processing activities, and implementing breach management procedures [62]. Starting a PbD effort without first establishing such basics for organization-wide privacy management will hinder the effectiveness of these efforts by burdening the professionals holding the required expertise with inefficient and insufficient processes in other areas of their work. The availability of this privacy expertise strongly impacts the quality of the outcomes [30,63].

Once a basic framework is established, organizations can opt to achieve further depth in PbD by improving specific capabilities. This is the gap filled by the PbD-MM: it expands on a single, though crucial and expansive, aspect of privacy management. Compared with other privacy maturity models [42–44] and privacy (risk) management standards [46,47], it covers a narrower scope of capabilities. In turn, the depth of PbD capabilities in the PbD-MM will enhance the ability of an organization to perform effective privacy management. Either by designing more privacy-friendly information systems or by demanding more mature practices from third parties.

5.1. Practical Implications

The PbD-MM provides a structure to implementing PbD in an organization. It supports assessing the current capabilities of an organization and creating an improvement plan for PbD. Rather than prescribing specific techniques to accomplish PbD, it helps guide an informed selection of techniques to apply. The web application provides the PbD-MM, as well as assessment and reporting tooling, at a low barrier of entry.

In the validation focus group and through personal interactions with practitioners, the most interest was given to the contents of the model. It provides answers to the question of what needs to be accomplished to implement and improve PbD, rather than how this can be done. While other maturity models reference PbD or privacy as a single focus area, the PbD-MM distinguishes itself by providing a complete view of the complexity involved in achieving PbD in designing information systems. Its focus areas reflect the connection of PbD to other disciplines, among them architecture, development and contract management. The model guides practitioners to integrating PbD into existing practices by providing specific capabilities that need to be achieved in these areas. The PbD-MM also offers freedom in the selection of methods and techniques used, allowing for a best-fit selection with the methods already in use in the organization. The PbD-MM thus helps practitioners effectively assess and improve their PbD practices based on a logical development path of best practices.

5.2. Limitations and Future Work

This research has completed the engineering cycle once, including one validation activity and one evaluation activity. Long-term observations and evaluations of improvement action implementation are validity threats, as the validation of these has been out of scope for this research project. Similarly, additional validation is recommended for the development path laid out in the PbD-MM. Although the dependencies between and placement of capabilities were not validated separately, the outcomes support the applicability of organizational development in PbD. Additional iterations of the engineering cycle with a focus on one of these aspects would mitigate validity threats to a degree.

Although significant effort was made to distribute the PbD-MM, the population reached remains limited. The focus group was conducted with a limited number of participants, all from a similar background in Dutch government organizations, and time-sensitive. This poses a threat to the external validity of the PbD-MM and the higher maturity of focus areas that were not assessed. This threat is partially mitigated by the MLRs, which considered sources originating from diverse contexts. Specific mentions of the GDPR were also removed from the capabilities in favor of generalized terms. Finally, the evaluation (Table 7) shows that the model scores well on being able to effectively assess PbD maturity, structural completeness, and ease of formulating a development path. To further address validity threats, we suggest that a new iteration of the engineering cycle includes different populations and methods, for example, case studies and expert interviews, in assessing the PbD-MM.

While the evaluation included a broader population, the invitation was distributed targeting privacy practitioners through existing and accessible networks. A significant number of the included assessments (20 of 46) were collected during the first three months after spreading the model in personal networks. Little demographic data was collected, but we expect an overrepresentation of Dutch, as well as public sector organizations in that portion of the dataset. 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, such as only considering the GDPR and not other legal frameworks or an absence thereof, which may influence the generalizability of this research. While no extensive analysis was performed, we do observe a slightly lower average overall maturity (-0.12) of the final dataset in comparison with an earlier analysis of the first 24 valid results, which is most strongly pronounced in the focus areas *FA5. PIA process* (-0.62), *FA6. PIA report* (-0.55) and *Third-party management* (-0.29). Both versions of the analysis are available in the published dataset.

Finally, the collection of only single snapshots of PbD maturity limits our ability to determine whether the PbD-MM holds prescriptive value. Future work on the PbD-MM would benefit from applying a different methodology, for example, a series of case studies or expert interviews covering a wider variety of organizations or as a longitudinal investigation of maturity development, to address these validity concerns.

Throughout the paper, we mentioned various avenues for future work. Directions for further improvements and validation of the PbD-MM artifact are presented in Sections 4.3 and 5. For researchers looking towards FAMMs, we suggest strengthening the validity of various scoring methods that were developed for practical considerations, such as progressive scoring based on how advanced capabilities are [33] or applying various scoring scenarios as shown in Table 6. Differences in scoring methods for FAMMs now come from practical considerations, showing the need for a scientifically grounded approach.

We invite PbD researchers to continue developing and validating the PbD techniques that fit with the capabilities described in the PbD-MM. Taking into account organizational development will strengthen the positioning and validity of PbD approaches, as not all

methods are suited for all levels of PbD maturity. Finally, we encourage further investigation into the interdependencies between PbD and privacy management. While PbD garners attention within privacy management, its representation remains shallow when compared with the diversity of activities identified in the PbD body of knowledge.

6. Conclusions

In the presented research, PbD activities from two multivocal literature reviews were used to structure the functional domain of PbD in a maturity model. With a web application, online self-assessment and reporting, the PbD-MM supports organizations wanting to investigate and improve their PbD practices. The PbD-MM is well received, and achieving high capabilities in one focus area correlates with better performance in other focus areas.

From 46 maturity assessments, we find that organizations have implemented different interpretations of PbD with diverse maturity profiles. The responses show a broad development of lower-level capabilities in the PbD-MM, with a focus towards governance and compliance capabilities. While this contrasts with the best-practice approach of applying both privacy-by-policy and privacy-by-architecture techniques, these results follow a trend seen in previous findings. The PbD-MM was evaluated positively on structural completeness and operational feasibility, with improvement suggestions for its ease of use. Overall, the PbD-MM provides recognizable practices to assessors and supports assessing maturity and formulating a development path.

The PbD-MM fills a gap in PbD research by applying the lens of organizational development to its practices and logically structuring them as a single functional domain. It offers a structure to contextualize existing works describing specific PbD techniques within the PbD domain. The PbD-MM and its assessment instrument provide an artifact that supports identifying an organization's current capabilities and areas for improvement to effectively design, develop, and operate privacy-friendly information systems.

Author Contributions: Conceptualization, F.v.D., M.M., M.B., and S.B.; methodology, F.v.D., M.M., M.B., and S.B.; software, M.M.; validation, formal analysis, investigation, resources, F.v.D. and M.M.; data curation, F.v.D. and M.M.; writing—original draft preparation, F.v.D. and M.M.; writing—review and editing, M.S., S.B., and M.B.; visualization, F.v.D. and M.M.; supervision, M.S., S.B., and M.B.; project administration, F.v.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The original data presented in the study are openly available in Zenodo at https://doi.org/10.5281/zenodo.20668760 (accessed on 17 August 2026) (model data) and in Github at https://github.com/MichelMuszynski/PbD-Maturity-Tool (accessed on 17 August 2026) (assessment instrument).

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

FA	Focus Area
FAMM	Focus Area Maturity Model
IS	Information Systems
MLR	Multi-vocal Literature Review
PbD	Privacy-by-Design

PbD-MM	Privacy-by-Design Maturity Model
PET	Privacy Enhancing Technology
PIA	Privacy Impact Assessment

Appendix A. PbD-MM Capabilities

FA1. Requirements

0 Privacy requirements are not explicitly formulated.

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.

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.

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.

D Advice from ethical experts is gained regarding requirements for sensitive personal data.

FA2. Architecture

0 Privacy is not explicitly considered in the software architecture.

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 datasets, processing purposes, lawful grounds, actors, legal roles, and personal data types.

B The data flows for all processing activities are modeled 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.

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.

D Processing activities and related information elements are exhaustively modeled and traceable through all layers of architecture. Privacy design patterns and PETs are selected from a centralized catalog in a structured manner.

FA3. Development

0 Privacy is not explicitly addressed during development.

A Privacy requirements are incorporated in low-level design. Acceptance testing is used to ensure that the system meets the privacy and security requirements.

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.

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 organizations processing activities.

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.

E Privacy policies are embedded in system design and are automatically enforced.

FA4. Technology

0 Privacy enhancing technologies are not explicitly implemented.

A 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.

B Privacy-enhancing technologies (PETs) are selected, developed, and used to implement privacy design patterns.

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 cataloged.

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 catalog while taking into account the quantitative and qualitative costs and benefits. The privacy protection technology is continuously monitored, optimized, and upgraded.

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.

FA5. PIA process

0 A PIA is a one-time process and product.

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.

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.

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

D The PIA process and the PIA reporting activities are decoupled. PIAs reference PIA reports from the centralized registry, ensuring that subsequent changes build upon previous analysis. Privacy controls are methodically assessed using metrics. The design of the physical environment is included.

E A formalized 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.

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.

FA6. PIA report

0 The PIA report is tightly coupled with the PIA process. There is one report for all audiences.

A The PIA report is reviewed and is tied to budget submissions for new projects.

B PIA reports are stored in a centralized 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.

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.

D Different PIA reports can exist per PIA process; these reports are adapted to their intended audience in both content and form.

FA7. Risk management

0 Privacy is not integrated into the organization's risk management program.

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 modeling, risk prioritization, and formulating mitigation measures. Residual risks are identified and documented.

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.

C The entity has implemented documented policies and procedures to monitor and to optimize 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.

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 and compliance dashboard that provides a continuous view of the system.

FA8. Processing principles

0 Data processing principles are not actively applied.

A A set of standard processing principles are applied to all processing activities (e.g., GDPR processing principles).

B The processing principles are documented, applied in a structured and methodical manner, and are periodically evaluated.

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.

D Compliance with the processing principles is proactively managed to deliver deliberate process optimization. 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.

FA9. Subject rights

0 Data subject rights are not actively facilitated through design.

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.

B Data subject rights are facilitated through automated technical mechanisms such as self-service dashboards. Consent processes are periodically reviewed, and improvements are made where necessary. Automated processes are followed to test consent prior to use of personal information.

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.

D User-driven control of personal data is employed. Data subjects who 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.

FA10. Transparency

0 A privacy notice exists on a public website and data subjects are referred to it.

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, and feedback on the readability and content of the privacy policy is analyzed and incorporated. Historical versions of the policy are archived and accessible.

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.

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.

D Summaries of PIAs, TRAs, and independent third-party audit results are published.

FA11. Third-party management

0 Data processing agreements are established on an individual basis.

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.

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 authorization, 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.

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 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.

FA12. Roles

0 Privacy-related roles are not formally defined for the entirety of the privacy-by-design process.

A Stakeholders, roles, and responsibilities related to privacy activities are identified and assigned.

B The management of privacy-related roles and responsibilities is formalized in a role/functionality matrix to ensure accountability. A chief privacy officer is appointed.

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.

D Appoint a central entity responsible for privacy-related issues such as a privacy committee.

FA13. Awareness

0 Privacy awareness is not actively stimulated.

A The organization is aware of the basic principles of privacy-by-design and management is committed to applying them.

B Different target groups involved in privacy-by-design are identified and receive training for raising awareness as well as transmitting knowledge relevant to their specialization.

C Resources are provided, such as manuals, guides, and handbooks, to support consistent implementation of privacy policies, procedures, and standards, as required and appropriate.

D The organization 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.

FA14. Monitoring

0 Privacy-related activities are not structurally monitored or validated.

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.

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.

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.

D Periodic reviews and audits are performed on processing activities to ensure personal information uses are appropriate and lawful.

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.

References

1. Cavoukian, A. *Privacy by Design the 7 Foundational Principles*; Technical Report; Office of the Information and Privacy Commissioner of Ontario: Toronto, ON, Canada, 2009.
2. Gürses, S.; Troncoso, C.; Diaz, C. Engineering privacy by design. In Proceedings of the Computers, Privacy & Data Protection (CPDP 2011), Brussels, Belgium, 25–28 January 2011.
3. Rubinstein, I.; Good, N. Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. *Berkeley Tech. LJ.* **2013**, *28*, 1333. [CrossRef]
4. de Chaves, S.A.; Barreto Vavassori Benitti, F. Privacy by Design in Software Engineering: An update of a Systematic Mapping Study. In *SAC '23: Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*; Association for Computing Machinery: New York, NY, USA, 2023; pp. 1362–1369. [CrossRef]
5. Andrade, V.C.; Gomes, R.D.; Reinehr, S.; Freitas, C.O.D.A.; Malucelli, A. Privacy by Design and Software Engineering: A Systematic Literature Review. In *SBQS '22: Proceedings of the XXI Brazilian Symposium on Software Quality*; Association for Computing Machinery: New York, NY, USA, 2023; pp. 1–10. [CrossRef]

6. van Puijenbroek, J.; Hoepman, J.H. Privacy impact assessments in practice: Outcome of a descriptive field research in The Netherlands. In *Proceedings of the 3rd International Workshop on Privacy Engineering*; CEUR: Aachen, Germany, 2017; p. 8.
7. Muszynski, M.; van Dijk, F.; Brinkkemper, S. Mapping the Privacy-by-Design domain and its organisational activities: Two multivocal literature reviews. In *Proceedings of the Thirty-Second European Conference on Information Systems (ECIS 2024)*; AIS Library: Auckland, New Zealand, 2024.
8. Solli-Sæther, H.; Gottschalk, P. The Modeling Process for Stage Models. *J. Organ. Comput. Electron. Commer.* **2010**, *20*, 279–293. [CrossRef]
9. de Bruin, T.; Rosemann, M.; Freeze, R.; Kaulkarni, U. Understanding the Main Phases of Developing a Maturity Assessment Model. In *Proceedings of the ACIS 2005 Proceedings, Sydney, Australia, 29 November–2 December 2005*; AIS Library: Auckland, New Zealand, 2005; p. 11.
10. van Looy, A.; Poels, G.; Snoeck, M. Evaluating Business Process Maturity Models. *J. Assoc. Inf. Syst.* **2017**, *18*, 461–486. [CrossRef]
11. Cleven, A.; Winter, R.; Wortmann, F. Managing Process Performance to Enable Corporate Sustainability: A Capability Maturity Model. In *Green Business Process Management*; vom Brocke, J., Seidel, S., Recker, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 111–129. [CrossRef]
12. van Steenbergen, M.; Bos, R.; Brinkkemper, S. Improving IS Functions Step by Step: The Use of Focus Area Maturity Models. *Scand. J. Inf. Syst.* **2013**, *25*, 35–56.
13. Van Steenbergen, M.; Bos, R.; Brinkkemper, S.; Van De Weerd, I.; Bekkers, W. The Design of Focus Area Maturity Models. In *Global Perspectives on Design Science Research*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 317–332.
14. Wieringa, R.J. *Design Science Methodology for Information Systems and Software Engineering*; Springer: Berlin/Heidelberg, Germany, 2014. [CrossRef]
15. van Rest, J.; Boonstra, D.; Everts, M.; van Rijn, M.; van Paassen, R. Designing Privacy-by-Design. In *Privacy Technologies and Policy*; Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J.M., Mattern, F., Mitchell, J.C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B., et al., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8319, pp. 55–72. [CrossRef]
16. Cavoukian, A. Privacy by design: The definitive workshop. A foreword by Ann Cavoukian, Ph.D. *Identity Inf. Soc.* **2010**, *3*, 247–251. [CrossRef]
17. van Lieshout, M.; Hoepman, J.H. *The PI.Lab—Four Years Later*; The Privacy & Identity Lab: Nijmegen, The Netherlands, 2015. [CrossRef]
18. London Economics. *Study on the Economic Benefits of Privacy-Enhancing Technologies (PETs)*; Technical Report; London Economics: London, UK, 2010.
19. Ayalon, O.; Toch, E. User-Centered Privacy-by-Design: Evaluating the Appropriateness of Design Prototypes. *Int. J. Hum.-Comput. Stud.* **2021**, *154*, 102641. [CrossRef]
20. Clarke, R. Privacy impact assessment: Its origins and development. *Comput. Law Secur. Rev.* **2009**, *25*, 123–135. [CrossRef]
21. European Parliament; Council of the European Union. Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Off. J. Eur. Union* **2016**, *L 119*, 1–88.
22. Oetzel, M.C.; Spiekermann, S. A systematic methodology for privacy impact assessments: A design science approach. *Eur. J. Inf. Syst.* **2014**, *23*, 126–150. [CrossRef]
23. Ahmadian, A.S.; Strüber, D.; Riediger, V.; Jürjens, J. Supporting privacy impact assessment by model-based privacy analysis. In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing, Pau, France, 9–13 April 2018*; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1467–1474. [CrossRef]
24. Tancock, D.; Pearson, S.; Charlesworth, A. *The Emergence of Privacy Impact Assessments*; HP Laboratories: Palo Alto, CA, USA, 2010; p. 35.
25. Sion, L.; Dewitte, P.; Van Landuyt, D.; Wuyts, K.; Emanuilov, I.; Valcke, P.; Joosen, W. An Architectural View for Data Protection by Design. In *Proceedings of the 2019 IEEE International Conference on Software Architecture (ICSA), Hamburg, Germany, 25–29 March 2019*; IEEE: New York, NY, USA, 2019; pp. 11–20. [CrossRef]
26. Hadar, I.; Hasson, T.; Ayalon, O.; Toch, E.; Birnhack, M.; Sherman, S.; Balissa, A. Privacy by designers: Software developers' privacy mindset. *Empir. Softw. Eng.* **2018**, *23*, 259–289. [CrossRef]
27. Ayalon, O.; Toch, E.; Hadar, I.; Birnhack, M. How Developers Make Design Decisions about Users' Privacy: The Place of Professional Communities and Organizational Climate. In *Proceedings of the Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, Portland, OR, USA, 25 February–1 March 2017*; Association for Computing Machinery: New York, NY, USA, 2017; pp. 135–138. [CrossRef]
28. Sheth, S.; Kaiser, G.; Maalej, W. Us and them: A study of privacy requirements across North America, Asia, and Europe. In *Proceedings of the 36th International Conference on Software Engineering, Hyderabad, India, 31 May–7 June 2014*; Association for Computing Machinery: New York, NY, USA, 2014; pp. 859–870. [CrossRef]

29. Senarath, A.; Arachchilage, N.A.G. Why developers cannot embed privacy into software systems? An empirical investigation. In *Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering 2018, Christchurch, New Zealand, 28–29 June 2018*; Association for Computing Machinery: New York, NY, USA, 2018; pp. 211–216. [CrossRef]
30. Hoepman, J.H. *Privacy Design Strategies (The Little Blue Book)*; Radboud University: Nijmegen, The Netherlands, 2022.
31. Alshammari, M.; Simpson, A. Privacy Architectural Strategies: An Approach for Achieving Various Levels of Privacy Protection. In *Proceedings of the 2018 Workshop on Privacy in the Electronic Society, Toronto, ON, Canada, 15 October 2018*; Association for Computing Machinery: New York, NY, USA, 2018; pp. 143–154. [CrossRef]
32. Overeem, M.; Mathijssen, M.; Jansen, S. API-m-FAMM: A focus area maturity model for API Management. *Inf. Softw. Technol.* **2022**, *147*, 106890. [CrossRef]
33. Yigit Ozkan, B.; van Lingen, S.; Spruit, M. The Cybersecurity Focus Area Maturity (CYSFAM) Model. *J. Cybersecur. Priv.* **2021**, *1*, 119–139. [CrossRef]
34. Aljowder, T.; Ali, M.; Kurnia, S. Development of a Maturity Model for Assessing Smart Cities: A Focus Area Maturity Model. *Smart Cities* **2023**, *6*, 2150–2175. [CrossRef]
35. Wendler, R. The maturity of maturity model research: A systematic mapping study. *Inf. Softw. Technol.* **2012**, *54*, 1317–1339. [CrossRef]
36. Becker, J.; Knackstedt, R.; Pöppelbuß, J. Developing Maturity Models for IT Management: A Procedure Model and its Application. *Bus. Inf. Syst. Eng.* **2009**, *1*, 213–222. [CrossRef]
37. Cormen, T.H.; Leiserson, C.E.; Rivest, R.L.; Stein, C. *Introduction to Algorithms*, 4th ed.; The MIT Press: Cambridge, MA, USA, 2022.
38. Krueger, R.A.; Casey, M.A. *Focus Groups: A Practical Guide for Applied Research*, 5th ed.; SAGE: Thousand Oaks, CA, USA, 2015.
39. Prat, N.; Comyn-Wattiau, I.; Akoka, J. A Taxonomy of Evaluation Methods for Information Systems Artifacts. *J. Manag. Inf. Syst.* **2015**, *32*, 229–267. [CrossRef]
40. Labadie, C.; Legner, C. Understanding Data Protection Regulations from a Data Management Perspective: A Capability-Based Approach to EU-GDPR. In Proceedings of the WIrtschaftsinformatik 2019 Proceedings, Siegen, Germany, 24–27 February 2019; p. 15.
41. Yaqiong, C.; Zijie, Y.; Feng, L.; Jiayin, Q. Data Privacy Maturity Assessment Practice of Digital Transformation Enterprises under the COVID-19: Taking an Industrial Company in Xiamen as an Example. In *Proceedings of the 2020 International Conference on Big Data in Management, Manchester, UK, 15–17 May 2020*; Association for Computing Machinery: New York, NY, USA, 2020; pp. 33–40. [CrossRef]
42. The MITRE Corporation. *Privacy Maturity Model*, Version 1; The MITRE Corporation: McLean, VA, USA, 2019.
43. AICPA/CICA. *Privacy Maturity Model*; AICPA: Durham, NC, USA; CICA: Toronto, ON, Canada, 2011.
44. Centrum Informatiebeveiliging en Privacybescherming (CIP). *Privacy Volwassenheidsmodel*; Technical Report; Centrum Informatiebeveiliging en Privacybescherming (CIP): Amsterdam, The Netherlands, 2017.
45. The Department of Internal Affairs Te Tari Taiwhenua. *Privacy Maturity Assessment Framework: Elements, Attributes, and Criteria*, Version 2.0; The Department of Internal Affairs Te Tari Taiwhenua: Wellington, New Zealand, 2014.
46. National Institute of Standards and Technology. *NIST Privacy Framework 1.1*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2025.
47. *ISO/IEC 27701:2025*; Information Security, Cybersecurity and Privacy Protection—Privacy Information Management System—Requirements and Guidance. International Organization for Standardization: Geneva, Switzerland, 2025.
48. *ISO/IEC 29134*; Information Technology—Security Techniques—Guidelines for Privacy Impact Assessment. International Organization for Standardization: Geneva, Switzerland, 2017.
49. The MITRE Corporation. *MITRE Privacy Engineering Framework and Life Cycle Adaptation Guide*; The MITRE Corporation: McLean, VA, USA, 2019.
50. Information Commissioner's Office (ICO). *Data Protection by Design and Default*; Information Commissioner's Office (ICO): Wilmslow, UK, 2022.
51. Timón López, C.; Alamillo Domingo, I.; Valero Torrijos, J. 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. In *Proceedings of the 16th International Conference on Availability, Reliability and Security, Vienna, Austria, 17–20 August 2021*; Association for Computing Machinery: New York, NY, USA, 2021; pp. 1–9. [CrossRef]
52. Bincoletto, G. A Data Protection by Design Model for Privacy Management in Electronic Health Records. In *Privacy Technologies and Policy*; Naldi, M., Italiano, G.F., Rannenberg, K., Medina, M., Bourka, A., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2019; Volume 11498, pp. 161–181. [CrossRef]
53. Martin, Y.S.; del Alamo, J.M.; Yelmo, J.C. Engineering privacy requirements valuable lessons from another realm. In *Proceedings of the 2014 IEEE 1st International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE), Karlskrona, Sweden, 25 August 2014*; IEEE: New York, NY, USA, 2014; pp. 19–24. [CrossRef]

54. Morales-Trujillo, M.E.; Garcia-Mireles, G.A. Extending ISO/IEC 29110 Basic Profile with Privacy-by-Design Approach: A Case Study in the Health Care Sector. In *Proceedings of the 2018 11th International Conference on the Quality of Information and Communications Technology (QUATIC), Coimbra, Portugal, 4–7 September 2018*; IEEE: New York, NY, USA, 2018; pp. 56–64. [CrossRef]
55. van Lieshout, M.; Kool, L.; van Schoonhoven, B.; de Jonge, M. Privacy by Design: An alternative to existing practice in safeguarding privacy. *Info* **2011**, *13*, 55–68. [CrossRef]
56. Kost, M.; Freytag, J.C.; Kargl, F.; Kung, A. Privacy Verification Using Ontologies. In *Proceedings of the 2011 Sixth International Conference on Availability, Reliability and Security, Vienna, Austria, 22–26 August 2011*; IEEE: New York, NY, USA, 2011; pp. 627–632. [CrossRef]
57. Jansen, S. A focus area maturity model for software ecosystem governance. *Inf. Softw. Technol.* **2020**, *118*, 106219. [CrossRef]
58. Spruit, M.; Röling, M. Isfam: The Information Security Focus Area Maturity Model. In *Proceedings of the European Conference on Information Systems (ECIS 2014), Tel Aviv, Israel, 9–11 June 2014*; AIS Library: Auckland, New Zealand, 2014; p. 16.
59. Dorfleitner, G.; Hornuf, L.; Kreppmeier, J. Promise not fulfilled: FinTech, data privacy, and the GDPR. *Electron. Mark.* **2023**, *33*, 33. [CrossRef]
60. Spiekermann, S. The challenges of privacy by design. *Commun. ACM* **2012**, *55*, 38–40. [CrossRef]
61. Dehling, T.; Sunyaev, A. A Design Theory for Transparency of Information Privacy Practices. *Inf. Syst. Res.* **2023**, *35*, 956–977. [CrossRef]
62. Swartz, P.; Da Veiga, A.; Martins, N. A conceptual privacy governance framework. In *Proceedings of the 2019 Conference on Information Communications Technology and Society (ICTAS)*; IEEE: New York, NY, USA, 2019; pp. 1–6.
63. Spiekermann, S.; Korunovska, J.; Langheinrich, M. Inside the Organization: Why Privacy and Security Engineering Is a Challenge for Engineers. *Proc. IEEE* **2019**, *107*, 600–615. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.