Universiteit Leiden

ICT in Business

Privacy Maturity Model:
Towards Privacy-by-Design Best Practices

Name: Xin Qi
Student-no: s1534408

Date: 18/07/2016

1st supervisor: Dr. Amr Ali-Eldin
2nd supervisor: Dr. Steve F. Foster

1st external supervisor: Dr. Haiyun Xu
2nd external supervisor: Dr. Bárbara Vieira

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)

Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

ABSTRACT

The rapid development of technologies has brought risks to data protection as a byproduct. Information Privacy therefore becomes increasingly crucial in the ICT environment. In this study, a Privacy Maturity Model is proposed to analyze real-world Privacy-by-Design best practices. Based on ISO/IEC 29100 (2011) privacy principles, a checklist of Privacy-by-Design activities is generated. Furthermore, each activity is assigned with a privacy maturity level. The model is analyzed by case studies, via a privacy questionnaire that measures the privacy aspects of ICT-systems. We believe that the Privacy Maturity Model indicates a systematic way of advising modern organizations on how to get privacy right.

Keywords: Information Privacy; Data Protection; Privacy-by-Design; Privacy Maturity Model.

ACKNOWLEDGEMENTS

It is of great experience to live and study in a different continent. During the past two years that I have spent with the Master Program *ICT in Business* in Leiden University, many professors, lecturers and staff have been supportive to me. I appreciate them for the academic knowledge I obtained, the amazing business events I attended, and the kind help I received as an international student.

Living in a remote country yet with little homesick, I would owe it to my family and friends. My family supported me both emotionally and financially, which made things so easy and comfortable. My friends, especially the ones I met in Holland, have added enjoyable flavors into my life. Besides, credits go to my ICTiB classmates from Leiden University as well as colleagues from Software Improvement Group B.V. (SIG); thanks to them, the previous two years were full of fun and inspiration.

At last, I would like to give my special thanks to my thesis advisors: Dr. Amr Ali-Eldin: my first university supervisor; Dr. Steve Foster: my second reader; Dr. Haiyun Xu: my first external supervisor at SIG; and Dr. Bárbara Vireira, my second external supervisor at SIG. They have sacrificed a great amount of time, from coaching me in the research design to reading my thesis and guiding me in writing. Their suggestions are always in time, and are more than valuable for me to conduct this six-month research.

TABLE OF CONTENTS

List of Abbreviations

AICPA/CICA: The American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants

BSIMM: Building Security-In Maturity Model

CMMI: Capability Maturity Model Integration

ENISA: European Network and Information Security Agency

GDPR: General Data Protection Regulation

ICT: Information and Communications Technology

ISO: International Organization for Standardization

IEC: International Electrotechnical Commission

OECD: Organization for Economic Co-operation and Development

OWASP: Open Web Application Security Project

(OWASP) ASVS: (OWASP) Application Security Verification Standard

PbD: Privacy-by-Design

PIA: Privacy Impact Assessment

PII: Personal Identifiable Information

PMM: Privacy Maturity Model

PRIPARE: PReparing Industry to Privacy-by-design by supporting its Application in REsearch

SDLC: Software Development Life Cycle

SNS: Social Networking Service

LIST OF FIGURES

LIST OF TABLES

1. Introduction

1.1. Privacy: State of the Art

The rapid evolution of technologies, along with the explosive growth of the amount of data, have been impacting the way we live. While enjoying the efficiency from newly available technologies, one thing that must not be neglected is the byproduct: risks to privacy.

Privacy breaches have been happening more often and bringing severer results than we thought.[1] In December 2015, 191 million U.S. voters' information was uncovered by an independent computer security researcher – due to an incorrect configuration, the database was exposed on the open Internet, which included names, phone numbers, emails, addresses, birth dates, and party affiliations [Finkle & Volz, 2015]. In March 2016, Verizon Enterprise Solutions, who conducts business in providing solutions in terms of privacy breaches, claimed that they suffered from their own breach of contact information of 1.5 million business customers [McGee, 2016]. In the first example, the individual victims got panicked: if we look at the types of the leaked personal data, the chance of individuals being identified and tracked became extremely high. In the second example, Verizon's clients had to deal with potential risks such as fraud and phishing attack. Facing privacy breaches, not only the victims become weak; The organization which holds the data also has to pay a huge amount of compensation, not to say the ruined reputation.

The mechanisms behind internet encourage people to post more and share more, not only about themselves, but sometimes about other people as well. However, neither sufficient number of people are aware of privacy issues – especially with the fact that Social Networking Service (SNS) tend to be much more popular among younger generations [Pew Research Center, 2013], nor sufficient number of SNS systems and applications are designed with appropriate privacy protection methods. Let us take the example of Google. When using Google Maps to browse a location, the option to add a picture of that location can be easily found. A claim appears before uploading, saying the picture will be shared with public. However, what happens if someone mistakenly uploads a selfie? An experiment has been

[1] There are currently multiple online resources recording the data breaches that happened in recent years. One of the visualizations is available at: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

conducted.[2] Google does not even remind the user whether the picture can still be removed (the answer is yes), not to say respecting the consent choice of the user. Google could have done more, for instance, implementing facial-recognition techniques to ask the user "We have detected human face(s) in your picture. Do you still want to share this picture to the public?" Unfortunately, this is not the case; and this is just one of the countless examples where both service users and service providers happen to "forget" about privacy.

An inspiring news in April 2016 is that, the *General Data Protection Regulation* (GDPR) has been adopted by the European Council and the European Parliament [European Commission, 2016]. This marks a replacement of the data protection directive (Directive 95/46/EC), which already has its history of more than 20 years. Soon after the adoption of GDPR, Facebook launched a special version of its facial-recognition App in Europe and Canada. The special version was designed in alignment with privacy laws and regulations. However, part of the functionality had to be disabled from the original version due to the legal requirements [Kelion, 2016]. In fact, how to balance between people's demand of using the service and pursuing a more mature level of privacy still remains a challenging topic.

1.2. Research Questions

Privacy is increasingly important to individuals as well as organizations. Information and Communications Technology (ICT) system and applications should play a better role in protecting privacy-sensitive data. While existing privacy assessment methods address privacy protection at a broad organizational level (which will be elaborated in Chapter 2), the need has been arising for practical approaches that do justice to this emerging role of ICT applications. Hence, the overall research question has been defined as:

How to design a Privacy Maturity Model that is applicable to assess Privacy-by-Design best practices?

To answer the main Research Question step by step, three sub-questions have been further developed:

- What Privacy-by-Design activities shall be included in the model?
- To reach a certain privacy maturity level, what are the requirements, i.e. which Privacy-by-Design activities shall be implemented?

[2] A random location on Google Maps was picked. When a picture which contains recognizable human faces is selected, it will be automatically uploaded to the system, and the picture is almost immediately available for everyone who has access to Google.

- Is the Privacy Maturity Model created in this research applicable, i.e. the gap between the activities that companies/organizations are expected to do and what they actually do is insignificant?

1.3. Research Objectives and Contributions

The research objectives are mentioned as the following aspects, each aligning with one sub- research question:

- Generate a concrete list of Privacy-by-Design activities.
- Derive the Privacy Maturity Model. That is, for each maturity level, define which Privacy-by-Design activities shall belong to that level.
- Assess the validity of the Privacy Maturity Model by case studies.

With an accomplishment of the research objectives, Privacy-by-Design activities of an ICT system or application can be practically analyzed. The list of Privacy-by-Design activities will lead to suggestions on how to further improve the system to move towards a higher privacy maturity level.

The Privacy Maturity Model is crucial for raising privacy alarms throughout the entire Software Development Life Cycle (SDLC) – and especially in the early stages. For companies and organizations, the model encourages them to proactively implement Privacy-by-Design. Having more safeguarded and trustworthy systems in the first place, the risk of paying for unwilling costs (such as large amounts of compensation caused by privacy breaches) can be minimized.

1.4. Research Methods

1.4.1. Exploratory Study

This study aims to first gather a list of practical Privacy-by-Design activities, and later create the Privacy Maturity Model by mapping each activity into a proper maturity level. The actual performance of the model shall be assessed by feedbacks from real world cases, and adjustments shall be made to the model whenever needed.

In order to inductively come up with an applicable Privacy Maturity Model, the research is designed as an analogue to both the Building Security-In Maturity Model version 6 [BSIMM6, 2015] and OWASP Application Security Verification Standard version 3.0 [OWASP ASVS 3.0, 2015].

More detailed research steps are explained separately in the following sections.

1.4.2. Literature Review

The Privacy-by-Design activities shall be listed in a clear and structured way. Ahead of creating the model, several concepts need to be elaborated to avoid ambiguity in later stages: 1) relevant information privacy terminologies, 2) various versions of wide-accepted privacy principles, and 3) previous studies, i.e., Privacy Impact Assessment (PIA) frameworks/models. The results of literature review will be presented in Chapter 2.

1.4.3. Model Construction and Questionnaire Improvement (iterative)

The Privacy Maturity Model consisting of Privacy-by-Design activities will be generated according to privacy principles. As the foundation of the model, the privacy principles used in this research will be based on an overall understanding of multiple existing privacy principles. Meanwhile, the construction of the model will be supervised by Software Improvement Group B.V. (SIG) experts.

The Privacy Maturity Model will contain a list of maturity levels, which act as measuring sticks for Privacy-by-Design activities. After that, an evaluation framework will be developed to analyze the actual performance of Privacy-by-Design activities. This means when a real-world case is collected by the privacy questionnaire, we will be able to approach the evaluation framework to determine the privacy maturity levels for that specific case.

Finally, the Privacy Maturity Model will be validated via case studies. In this research, a privacy questionnaire is used to collect information about the reality (i.e. what Privacy-by-Design activities companies/organizations actually conduct, how is the performance of these activities, etc.). Initially, SIG provides this research with a draft version questionnaire. Before sending out the copies to participants (i.e. SIG clients as well as external companies/organizations), the questionnaire requires to be revised to satisfy our research objectives. A thorough description about the design of the privacy questionnaire can be found in Chapter 4.1.

1.4.4. Data Collection and Interviews

The privacy maturity questionnaire needs to be filled-in on a “one specific system per questionnaire” basis. When our participants feel necessary, a semi-structured interview session will be arranged to discuss about the content of the questionnaire. Participants shall be well informed that interviews will be recorded. Estimated number of participants for the purpose of model validation is 5 – 10 in total. That is, 2 – 3 participants per company/organization: at least one being the system designer/architect, and the other being the person in charge of organization’s privacy policy. In return, participants will receive a Privacy Maturity Report along with an interactive session.

1.4.5. Data Analysis and Result Validation

Based on the data collected from questionnaires as well as feedbacks from participants, the Privacy Maturity Model will be evaluated. The mapping between Privacy-by-design activities and maturity levels might face with slight adjustments, due to the feedbacks from respondents. SIG experts shall be invited to supervise any modifications to the Privacy Maturity Model.

1.5. Organization of the Thesis

The rest of the thesis is structured in the following way: Chapter 2 presents an overview of existing literatures and studies in the field of privacy, which performs as a scientific foundation of our research. Chapter 3 explains the processes of constructing the Privacy Maturity Model and the model itself. Chapter 4 describes the model validation by the analysis of real world cases. Following is Chapter 5, where findings from case studies and possible improvement to the model are discussed. At last, the conclusion and the limitation of this study, as well as further research paths can be found in Chapter 6.

2. Literature Review

This literature review builds a general research foundation by looking into a list of privacy-related issues and understanding them, such as privacy principles, the concept of Privacy-by-Design, and Privacy Impact Assessment. On the other hand, when reading about studies conducted on Privacy Maturity, insights as well as wonders popped up. Furthermore, to grasp the idea of how a maturity model works, other studies such as a process improvement program and security maturity models are being reviewed as an analogue. Note that, although Banisar & Davies [Banisar & Davies, 1999] and later researchers claimed that privacy could be specified in different categories, the term is used to refer information privacy (or, data protection) in our study.

2.1. Privacy and its Principles

Among the earliest privacy quotes, the most famous one describes privacy as the "right to be let alone" [Warren and Brandeis, 1890]. Privacy is such a common word in our society that giving an accurate definition to it becomes hard. Nevertheless, ISO/IEC 29100 – also known as "the Privacy Framework" [ISO/IEC 29100: 2011] has suggested us a possible definition:

"Privacy is the concern of nature persons and organizations specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology (ICT) systems or services where privacy controls are required for the processing of Personally Identifiable Information (PII)."

That is, privacy requires right people to conduct proper tasks towards specific pieces of personal information. Yet in another study [Schwaig, Kane & Storey, 2006], researchers argue that privacy in most contexts is no longer viewed as an absolute right, but must be balanced against the needs of society.

Privacy protection relies very much on obeying the instruction of privacy principles. In 1980, the Organization for Economic Co-operation and Development (OECD) [OECD, 1980] summarized 8 widely used privacy principles, and thus earned its global fame. The OECD privacy principles can be summarized as:

1. **Collection Limitation**: any collected data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data Quality**: personal data should be accurate, complete and kept up-to-date, and relevant to the purposes for which they are to be used and to the extent necessary for those purposes.

3. **Purpose Specification**: The purposes for personal data collection should be specified not later than at the time of data collection.
4. **Use Limitation**: personal data should not be disclosed, made available or otherwise used for purposes other than those specified (unless with the consent of the data subject, or by the authority of law).
5. **Security Safeguards**: data should be protected by reasonable security safeguards against risks such as loss, unauthorised access, destruction, use, modification or disclosure of data.
6. **Openness**: a general personal data policy should be introduced with openness on developments, practices and policies, for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identification and usual residence of the data controller.
7. **Individual Participation**: the individual should have the right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; to have communicated to him, data relating to him within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner; and in a form that is readily intelligible to him; to be given reasons if a request is denied, and to be able to challenge such denial; and to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
8. **Accountability**: data controller should be accountable for complying with measures, which give effect to the principles stated above.

Three decades later, facing rapid changes of both the society and technologies, OECD decided to publish an amendment version in 2013, adding details to the principles. But this new version has not become the same authority as the original one.

Apart from OECD, ISO/IEC 29100 defines 11 privacy principles for the privacy framework, which can be concluded as [ISO/IEC 29100: 2011]:

1. **Consent and choice:** PII principal's choice must be given freely, specific and on a knowledgeable basis;
2. **Purpose legitimacy and specification**: purpose of data processing complies with applicable legislation and is communicated to the PII principal before collection;
3. **Collection limitation**: limit data collection to the strictly necessary for the specific purpose (only collect the data indispensable for provisioning a particular service);
4. **Data minimization**: minimize the PII that is processed and avoid observability and linkability of PII collected; Delete and dispose of PII whenever the purpose for PII processing has expired;

5. **Use, retention and disclosure limitation**: limit the use, retention and disclosure of PII to specific purposes, unless a different purpose is required by law;
6. **Accuracy and quality**: PII processed must be accurate, complete and up-to-date;
7. **Openness, transparency and notice**: provide clear and easy to access information about policies, procedures and practices of PII processing;
8. **Individual participation and access**: provide PII principles the ability to access and review their own data; enforce access control;
9. **Accountability**: assign the task of implementing the privacy-related policies, procedures and practices to a particular individual within the organization; provide suitable training to the organization members handling PII;
10. **Information security**: enforce confidentiality, integrity and availability of PII; prevent unauthorised access, destruction, modification, disclosure and use of PII;
11. **Privacy compliance**: verify and demonstrate that PII processing meets data protection and privacy safeguarding requirements.

In addition, European Network and Information Security Agency (ENISA) [Danezis et al., 2014] provides a list of 9 privacy principles, which is on a basis of understanding the legal framework:

1. **Lawfulness**: data must be collected or processed either based on the data subject's explicit consent or there is legal obligation;
2. **Consent**: the data subject should give unambiguous and explicit consent on data collection and processing;
3. **Purpose binding**: a purpose must be well-defined for both data collection and processing;
4. **Necessity & Data minimisation**: only necessary data must be collected;
5. **Transparency & Openness**: privacy policies must be well defined and publicly known;
6. **Rights of the individual**: data subjects should have the right to access, change and delete (their own) collected data;
7. **Information security**: confidentiality, integrity and availability must be enforced;
8. **Accountability**: responsibilities on enforcing privacy policies should be clearly assigned to specific person(s) from the organisation;
9. **Data protection by design and by default**: data protection should be taken into account from the initial design phase of the system.

From the descriptions of the 3 groups of privacy principles, it is obvious to tell that, in different versions, different names have been given to the same content – and this is a common situation. On the one hand, with a comparison of the descriptions,

the ISO 29100 principles can be regarded as an extension of OECD's 8 principles. On the other hand, being an international standard, ISO 29100 describes privacy principles in a more structured and thorough way than OECD and ENISA. Therefore, to minimize ambiguity, this research will regard the ISO 29100 version descriptions as a foundation of creating the Privacy Maturity Model. The following table depicts a matching between ISO 29100 privacy principles and OECD as well as ENISA privacy principles. Although names in one specific row are different, they actually refer to the same content.

Table [2.1]. Matching of different versions of Privacy Principles

#	ISO/IEC 29100 (2011)	Matching Privacy Principles In OECD (1980)	Matching Privacy Principles In ENISA (2014)
1	Consent and choice	Collection Limitation, Use Limitation	Consent
2	Purpose legitimacy and specification	Purpose Specification	Lawfulness
3	Collection limitation	Collection Limitation	Purpose Binding
4	Data minimization	Collection Limitation	Purpose Binding, Necessity and Data Minimization
5	Use, retention and disclosure limitation	Use Limitation	Necessity and Data Minimization
6	Accuracy and quality	Data Quality	-
7	Openness, transparency and notice	Openness	Transparency and Openness
8	Individual participation and access	Individual Participation	Right of the Individual
9	Accountability	Accountability	Accountability
10	Information security	Security Safeguards	Information security
11	Privacy compliance	-	-
			Data protection by design and by default

2.2. Privacy-by-Design

The concept of Privacy-by-Design (PbD) was first developed in the 1990s. Over the years, it suggests that privacy can be better protected if it is embedded into the design specifications of technologies, business practices, and physical infrastructures[3]. Nowadays, because of the urgency in data protection, PbD has

[3] To view a detailed introduction to Privacy-by-Design, readers are suggested to visit: https://www.ipc.on.ca/english/privacy/introduction-to-pbd/

received its even more proponents. ENISA is one of the organizations that advocate PbD. According to ENISA's definition, PbD is a process of implementing privacy and data protection principles, which involves not only technological but also organizational components [Danezis et al., 2014].

Privacy-Enhancing Technologies (PETs) is regarded as a toolkit to assist the implementation of PbD. PETs are defined as "coherent ICT measures that protect privacy by eliminating or reducing personal data, or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system" [Borking & Raab, 2001]. Standard technologies used for privacy protections are: pseudo-identity, encryption, digital signatures, privacy policy languages (P3P), etc. However, relying only on implementing PETs is far less sufficient to realize PbD [Heurix et al., 2015].

2.3. Privacy Impact Assessment

In the European Data Protection Directive [Directive 95/46/EC, 1995], Recital 71a claims: "Data protection impact assessments should consequently have regard to the entire lifecycle management of personal data".

One widely accept deliverable of privacy safeguarding requirements is Privacy Impact Assessment (PIA). Being a risk assessment tool for decision-makers, PIA is able to address legal as well as moral and ethical issues, and it helps to ring the privacy alarm for organizations at the planning stage [Flaherty, 2000]. A PIA checklist can be found at Dutch Professional Association for IT-auditors (NOREA)[4]. This PIA checklist is based on the OECD privacy principles.

Up until today, more and more countries and alliances have set regulations to enforce PIA as a mandatory process.

In the report of Paul de Hert and his colleagues [De Hert, Kloza & Wright, 2012], the authors mentioned that PIA could run the risk of being too complicated and burdensome for organizations to conduct actual privacy acts. It is a fact that PIA will lead to increasing cost, which is depending on the complexity and seriousness of the privacy risks. However, researchers hold an optimistic view on PIA, because PIA is valuable in reducing cost in terms of management time, legal expenses, and

[4] A presentation on NOREA PIA (cache): https://webcache.googleusercontent.com/search?q=cache:naeZQ1PHSr8J:https://www.pilab.nl/wp-content/uploads/2013/12/2013-12-05-PIL-Presentatie-PIA-namens-NOREA.pdf+&cd=6&hl=en&ct=clnk&gl=nl&client=safari

potential media or public concerns [Wright, 2013]. A 16-step optimized PIA methodology is also proposed in the same paper as an outline.

2.4. Related studies on Privacy Maturity

An ideal Privacy Maturity Model (PMM), in our opinion, should be more down-to-the-earth. It should be able to first suggest practical PbD activities, and then examine how the privacy in an organization performs according to the maturity level of each activity that are defined in the PMM. The PMM will then pragmatically guide the organizations to implement privacy by design and by default, and thus benefit the control of PII.

Nowadays, due to the urgency of data protection, the number of studies that desire to analyze privacy activities and their maturity levels keeps increasing, and it becomes common to use the term "Privacy Maturity Model". However, these studies either focus on a relatively narrow domain, such as the study of *A Privacy Maturity Model for Cloud Storage Service* [Revoredo et al., 2014], or merely function as a legislation/management-oriented PIA. The PMM proposed by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants [AICPA/CICA, 2011] is a good example of high-level guidelines, rather than a practical model that is easy to follow.

In addition to that, there also exists several published studies, which have been using the terms of PIA and PMM interchangeably. One example is the Privacy Maturity Assessment Framework of New Zealand government [New Zealand government, 2014 (1) & (2)]. While the document claims itself to be "simple, pragmatic, and easy to use", the content does not reflect so – unless the user is enthusiastic about reading through pages of policies. Actually, this PMM contains more of general risk-reducing strategies for decision makers, rather than an easy-to-follow action plan on PbD activities.

Moreover, Hinde proposed a PMM for assessing South Africa organizations information privacy on the topic of Protection of Personal Information (PoPI) [Hinde, 2014]. But the emphasis of this dissertation was still privacy policies, and some discussions seemed to be too wide and off-topic.

To the best of our knowledge, a Privacy Maturity Model that assigns maturity levels to PbD activities according to their real performance still does not exist. Therefore, it is crucial to introduce such model that can really assist organizations to recognize the maturity level of their privacy, to compare with same-industry organizations, or to implement sufficient PbD activities for a certain privacy maturity level.

2.5. Maturity Model as an Analogue

Developed by Carnegie Mellon University, the Capability Maturity Model Integration (CMMI) is used for process improvement by a wide-range of domains and industries. CMMI v1.3 [CMMI v1.3, 2011] mentioned five maturity levels, namely Initial, Managed, Defined, Quantitatively Managed, and Optimizing. Maturity levels in different process areas may vary. For example, Risk Management has been integrated with maturity level three, while Organizational Performance Management has been integrated with maturity level five.

Apart from CMMI, two security maturity models have also been examined in order to develop the Privacy Maturity Model as an analogue. The first one is Application Security Verification Standard 3.0, which provides a basis for testing web application technical security controls, as well as a list of secure development requirements for developers [OWASP ASVS 3.0, 2015]. OWASP ASVS v3.0 defined three levels for application security verifications, and each level contains a list of security requirements. To reach a certain level, the being-analyzed software should bind with all requirements under that level.

The second security maturity model is Building Security-In Maturity Model 6, which pays more attention on the management side of software security. By interviewing both security experts and 78 firms, BSIMM6 defined 4 domains for the Software Security Framework (SSF), namely: Governance, Intelligence, Secure Software Development Lifecycle (SSDL) Touch points, and Deployment. Each domain contains 3 practices and several software security activities. The SSF includes 112 activities in total, and each activity is assigned with a certain maturity level according to its actual performance in the firms. Therefore, BSIMM can help organizations compare their software security maturity levels to the others [BSIMM6, 2015].

3. Development of Privacy Maturity Model

The Privacy Maturity Model is valuable in examining to which level Privacy-by-Design is embedded into real-world ICT systems. Of course in reality, not all organizations are expected to achieve the same level of privacy maturity. For instance, while the privacy requirements for a library registration system may just be ranked as average among different industries, an insurance application system should reach a higher level of privacy maturity, since it collects, stores and processes much more sensitive PIIs (such as health conditions and bank details of individuals). But being a measuring instrument, all organizations can benefit from the Privacy Maturity Model, i.e. they can receive not only a clear view of the status quo of their own system's privacy maturity, but also an instruction on how to better conduct activities to pursue a higher privacy maturity level.

As Figure 3.1 shows, the Privacy Maturity Model is formatted as a Privacy-by-Design checklist, in which different categories of PbD activities are arranged under their belonging privacy principles. The ISO 29100 privacy principles are summarized and known as SIG privacy principles (which will be explained in Chapter 3.1). Furthermore, the model defines a list of maturity level which increases in depth. Each PbD activity is assigned with one of the maturity levels.

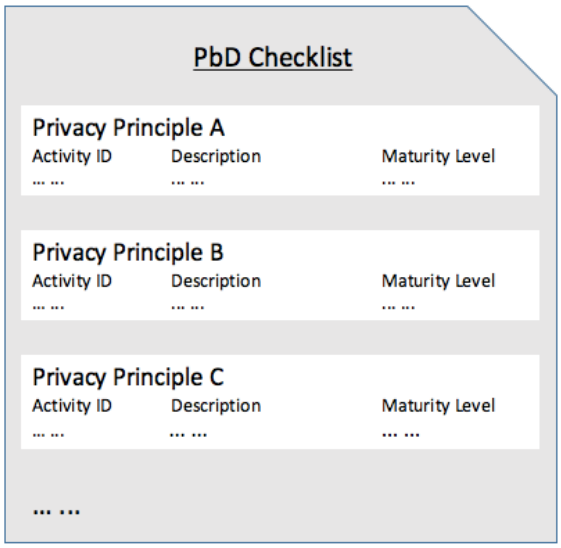

Figure [3.1]. The Composition of the Privacy Maturity Model

Following sections will explain the construction of Privacy Maturity Model step by step.

3.1. The Merge of ISO 29100 Privacy Principles

An upfront and consistent understanding of privacy principles is valuable for a later attempt to generate PbD activities. Thus, the aim of this section is to provide the foundation for our study in terms of privacy principles.

It is obvious that the ISO 29100's 11 privacy principles are more or less overlapping with each other in contents. To enhance the consistency of our work, the 11 ISO 29100 principles have been grouped into 7 by an interpretation of the descriptions in the ISO 29100 Privacy Framework. Besides, the result of grouping is also aligning with the ENISA's 9 privacy principles.

Table [3.1]. Summarizing ISO 29100 Privacy Principles

ISO 29100 Privacy Principle	Summarized Privacy Principle (SIG Principle)	collection	process	protection
Consent and choice	Lawfulness & Consent	x		
Purpose legitimacy and specification				
Data minimization	Data Minimization	x		
Individual participation and access	Individual Rights & Data Quality	x		
Accuracy and quality				
Collection limitation	Purpose Binding & Limitation		x	
Use, retention and disclosure limitation				
Openness, transparency and notice	Transparency & Openness		x	
Information security	Information Security			x
Privacy compliance	Accountability & Compliance			x
Accountability				

The above table indicates a way of merging the ISO 29100 principles, with an aim of minimizing the overlaps and redundancy.

- *Consent and choice* and *Purpose legitimacy and specification* are merged into *Lawfulness & Consent*, which means that PII should be collected with either consent of data subject or law requirements;
- *Data Minimization* remains *Data Minimization*, which means only necessary PII should be collected;

- *Individual participation and access* and *Accuracy and quality* are merged into *Individual Rights & Data Quality*, which means PII should be kept up to date, and data subjects should be allowed to add, change or delete associated PII;
- *Collection limitation* and *Use, retention and disclosure limitation* are merged into *Purpose Binding & Limitation*, which means PII being collected should have a well-defined purpose as well as binding with the law requirements;
- *Openness, transparency and notice* becomes *Transparency & Openness*, which means the purposes of PII collection and processing should be publicly known;
- *Information security* remains *Information Security*, which means the confidentiality, integrity and availability of system information should be enforced;
- Finally, *Privacy compliance* and *Accountability* are merged into *Accountability & Compliance*, which means the privacy-related responsibilities should be assigned and enforced.

The columns "collection", "process" and "protection" refer to the main stages where PII is involved. On a most relevant basis, the merged principles are mapped into these stages. In the PII collection stage, the principles that apply are: *Lawfulness & Consent*, *Data Minimization*, and *Individual Rights & Data Quality*. Later, when PII are being processed, the principles that apply are: *Purpose Binding & Limitation* and *Transparency & Openness*. Apart from PII collection and processing, PII protection must also not be neglected, and the principles that apply are: *Information Security* and *Accountability & Compliance*.

3.2. The Checklist of Privacy-by-Design Activities

In the ISO/IEC 29100 document, each privacy principle is followed by several suggestions, sometimes along with a few lines of description. For a specific privacy principle, the suggestions bring up guidelines for the adherent design and implementation of ICT systems; and the description instructs on how to conduct privacy-preserving activities, and sometimes contains additional information about legislations.

However, for a rather large number of organizations, the systematic implementation of PbD activities still remains pretty vague, because these organizations either do not have sufficient time/personnel to derive a to-do list by themselves, or conduct merely PIA and/or privacy auditing instead of Privacy-by-Design. Thus, a doable checklist of PbD activities becomes a premise for these organizations to get privacy right.

The checklist was generated iteratively. The following paragraphs explain on the construction of the PbD checklist. The overall checklist is provided at the end of this section.

The original version of PbD checklist was purely based on an interpretation of ISO 29100 privacy principles, and contained 92 activities in total. Later, the size of the checklist expanded into 108: on the one hand, with a comparison between ISO 29100-based activities and PRIPARE's suggestion on PbD activities [Le et al., 2015 (Annex B)], a few activities that were initially missing in our checklist but mentioned by PRIPARE were adopted. Some activities were also renamed according to the PRIPARE paper to enhance clarity. On the other hand, since the necessity of taking into account what is actually being conducted in reality, several activities were generated from a comprehension of privacy policies of world-leading companies/organizations. 5 different industries were chosen: Communications, Accommodations, Banking, Transportation, and Consulting. All of the chosen companies/organizations have their operations binding with the European legal framework. In case of any future updates, the being-examined privacy policies have been archived.

A discussion with SIG's experts revealed that, a number of PbD activities in checklist version 2 were overlapping with each other. The reason behind this problem was, although these activities were lying under different ISO 29100 privacy principles, they actually described similar situations. Hence, the overlapping activities were either merged into one, or redefined to be distinctive from each other. In addition, SIG's experts considered that some activities generated from the policies were only applicable in one or two specific industries. Therefore, a few activities were removed due to their inapplicability in more than half of the industries that were looked into (That is, more than 3 out of 5).

The following tables present an overview of the finalized checklist.

Table [3.2]. Privacy-by-Design Activities: *Lawfulness & Consent (LC)*

Activity ID	Lawfulness & Consent (LC)
LC 1	Allow PII principal to freely opt-in and opt-out
LC 2	Define lawful purposes for collecting and processing PII before PII collection
LC 3	Notify PII principals about mandatory collection of PII (e.g. for legal purpose)
LC 4	Ensure PII principals understand the privacy policies before providing consent without special knowledge
LC 5	Provide easy to access and understandable information regarding PII collection
LC 6	Display notifications of privacy policies at the entrance of physical locations where PII is collected
LC 7	Collect PII in a privacy friendly way
LC 8	Specify the tracking technologies that have been used (cookies, web beacons, clicking behavior, etc.) for PII collection
LC 9	Notify PII principals that providing additional PII (e.g. for marketing purpose) is optional
LC 10	Obtain consent before using or disclosing PII
LC 11	Make provisions for PII principals to withdraw consent
LC 12	Inform PII principals about the consequences of approve or decline the consent
LC 13	Offer equitable conditions to PII principals who do not consent to provide PII
LC 14	Conduct activities on any PII only with user consent or on a legal basis

Table [3.3]. Privacy-by-Design Activities: *Data Minimization (DM)*

Activity ID	Data Minimization (DM)
DM 1	Minimize PII collected for each purpose
DM 2	Separate the storage of PII collected from different sources
DM 3	Set up aggregation mechanisms before PII processing and storage
DM 4	Set up anonymization mechanisms before PII collection, processing and storage

Table [3.4]. Privacy-by-Design Activities: *Individual rights & Data Quality (IRDQ)*

Activity ID	Individual rights & Data quality (IRDQ)
IRDQ 1	Collect PII directly from PII principals whenever possible
IRDQ 2	Only collect PII from sources whose reliability can be attested
IRDQ 3	Make sure that the automatically generated PII does not lead to false judgements
IRDQ 4	Allow PII principals to access their individualized PII stored in the system
IRDQ 5	Allow PII principals to amend, correct and remove their own PII
IRDQ 6	Allow PII principals to object the collection, processing, and sharing of their PII at any time
IRDQ 7	Enable timely and free-of-charge individual participation
IRDQ 8	Check regularly the accuracy, completeness, up-to-date, adequacy and relevance of PII
IRDQ 9	Provide PII changes in time to any relevant privacy stakeholders
IRDQ 10	Record the unresolved PII challenges
IRDQ 11	Inform privacy stakeholders in time about the unresolved PII challenges

Table [3.5]. Privacy-by-Design Activities: *Purpose binding & limitation (PBL)*

Activity ID	Purpose binding & limitation (PBL)
PBL 1	Notify PII principals about the legal reason for mandatory processing of PII
PBL 2	Identify and document the purposes for conducting activities involving PII
PBL 3	Define and document the purposes and technologies used for PII processing
PBL 4	Inform PII principals/service users about the purposes/services for which PII is used
PBL 5	Periodically evaluate the alignment between PII and its purpose
PBL 6	Exclude unnecessary PII which needs to be retained from regular processing
PBL 7	Reveal PII principals identity as less as possible (e.g. avoid creating de-anonymized profiles)
PBL 8	Delete and dispose non-purpose binding PII and back-ups as soon as the purpose expires
PBL 9	Retain PII for a limited time span only as needed or as required by law
PBL 10	Evaluate whether the privacy policy needs to be expanded for sharing new types of PII

Table [3.6]. Privacy-by-Design Activities: *Transparency & Openness (TO)*

Activity ID	Transparency & Openness (TO)
TO 1	Document the type of PII collected
TO 2	Define any cases that may disclose PII
TO 3	Make PII processing explicitly announced and described
TO 4	Specify policies and practices about public-available PII
TO 5	Ensure the policy is available in any natural languages that PII principals might use
TO 6	Inform PII principals about their rights and choices
TO 7	Provide contact information for questions and complaints
TO 8	Inform PII principals about privacy stakeholders and PII controller
TO 9	Archive and provide easy access to the historical versions of policy
TO 10	Design and maintain a Privacy Dashboard
TO 11	Make sure the PII principal read the privacy notice (by implementing an affordance)
TO 12	Specify a PII decommission plan in the system design

Table [3.7]. Privacy-by-Design Activities: *Information Security (IS)*

Activity ID	Information Security (IS)
IS 1	Restrict the number of PII stakeholders and their access to the minimum need of PII
IS 2	Minimize risks such as unauthorized access, destruction, use, modification, disclosure or loss
IS 3	Conduct attack surface analysis and privacy threat modeling
IS 4	Identify and prioritize privacy threats
IS 5	Validate and verify the system's alignment with the privacy requirements
IS 6	Define privacy requirements explicitly
IS 7	Design and implement adequate Privacy-Enhancing Technologies (PETs)
IS 8	Prevent third parties from profiling PII

Table [3.8]. Privacy-by-Design Activities: *Accountability & Compliance (AC)*

Activity ID	Accountability & Compliance (AC)
AC 1	Notify PII principals about privacy breaches
AC 2	Notify the Supervisory Authority when there are privacy breaches
AC 3	Provide sanction and/or remedy procedures for privacy breaches
AC 4	Place internal controls that align with external supervision mechanisms
AC 5	Specify an entity responsible for privacy related issues
AC 6	Arrange regular personnel training
AC 7	Check regularly if security safeguards are up-to-date
AC 8	Set up policy for internal PII sharing
AC 9	Choose reliable PII processors that have an equivalent privacy maturity
AC 10	Specify the responsibilities of external entities
AC 11	Minimize PII shared with external entities
AC 12	Inform PII principals about sharing their PII
AC 13	Conduct privacy risk assessments (PIA) and implement periodic review and reassessment
AC 14	Implement PII protection mechanisms when conducting testing, research or training
AC 15	Conduct either internal or third-party privacy auditing
AC 16	Cooperate with supervisory and regulatory authorities

3.3. Privacy Maturity Levels

Maturity level 1 to 3 are defined for the Privacy Maturity Model. The maturity levels increase in depth:

- Level 1 is the initial privacy maturity level. It requires the implementation of both the most fundamental PbD activities regardless of industries, and the law-binding PbD activities. Level 1 is regarded as the privacy level for all companies/organizations to achieve in order to “make privacy work”.
- Level 2 is the standard privacy maturity level, which is for data-sensitive companies/organizations to reach. It requires the implementation of all PbD activities from Level 1, plus a list of PbD best practices regarding to the privacy status-quo;
- Level 3 is the cutting-edge privacy maturity level. To reach Level 3, a company/organization should not only implement all PbD activities from the previous two maturity levels, but also more advanced ones which are

supposed to be more proactive acts, and cost more resources (i.e. time, money and knowledge) in theory.

To reach any of the maturity levels, requirements in the implementation of PbD activities differ. The requirement for each maturity level is defined accordingly, namely *Basic*, *Intermediate*, and *Advanced*.

- *Basic* (B) is the minimum privacy requirement. It refers to a PbD activity that is either mandatory for legal reason, or is expected (by expert opinion) to be implemented by every organization despite which industry the organization belongs to. Besides, a *Basic* activity is always easy to be implemented, in terms of lower costs. Sometimes a *Basic* activity is the precondition for *Intermediate* and/or *Advanced* activities;
- *Intermediate* (I) is the average privacy requirement. It refers to a PbD activity that has not yet set as mandatory by laws/regulations, but the prerequisite for implementing that activity does not significantly vary from industry to industry. An intermediate PbD activity is expected to be implemented by around half of the overall population in the real world. In a few cases, an *Intermediate* activity is a precondition for *Advanced* activities;
- *Advanced* (A) is the most complex privacy requirement. It refers to a PbD activity that is neither mandated by law, nor considered to be popular with the majority yet, and the implementing rate can be strongly distinctive among different industries.

For the classification of PbD activities, 3 indicators are analyzed: *Mandatory*, *Popularity*, and *Complexity*. A comparison of the 3 privacy requirements can be found in the following table:

Table [3.9]. A Comparison of Privacy Requirements

Requirement / Indicator	*Basic*	*Intermediate*	*Advanced*
Mandatory	In most cases*	Non-mandatory	Non-mandatory
Popularity	High	Medium	Low
Complexity	Low	Medium	High

*: *Mandatory* is a sufficient (but not necessary) condition for *Basic* PbD activity.

Then, each PbD activity in the checklist are matched with one of the requirements. In order to examine the indicators *Popularity* and *Complexity*, previous real-world privacy policies were also taken into account. The result has been validated along with SIG expert opinions.

In the end, each of the 75 PbD activities received a matching: in total, 23 being *Basic*, 28 being *Intermediate*, and 24 being *Advanced*. This distribution is aligning with the status-quo of the implementation of PbD activities.

Table 3.10 presents the classification of PbD activities in terms of different requirements. Under each privacy principle, the 3 columns stand for *Basic*, *Intermediate*, and *Advanced* from left to right, which are marked by the color of yellow, green, and blue, respectively.

Table [3.10]. Privacy Maturity Levels of PbD Activities

Lawfulness & Consent (LC)		
LC 1	LC 6	LC 12
LC 2	LC 7	
LC 3	LC 8	
LC 4	LC 9	
LC 5	LC 10	
LC 13	LC 11	
LC 14		
Individual rights & Data quality (IRDQ)		
IRDQ 1	IRDQ 2	IRDQ 3
IRDQ 4	IRDQ 7	IRDQ 6
IRDQ 5	IRDQ 9	IRDQ 8
		IRDQ 10
		IRDQ 11
Purpose binding & limitation (PBL)		
PBL 1	PBL 3	PBL 6
PBL 2	PBL 4	PBL 7
	PBL 5	
	PBL 8	
	PBL 9	
	PBL 10	

Data Minimization (DM)		
	DM 1	DM 2
		DM 3
		DM 4
Transparency & Openness (TO)		
TO 6	TO 3	TO 1
TO 7	TO 4	TO 2
TO 8	TO 5	TO 9
		TO 10
		TO 11
		TO 12
Information Security (IS)		
IS 1	IS 3	IS 6
IS 2	IS 4	IS 7
	IS 5	IS 8
Accountability & Compliance (AC)		
AC 1	AC 6	AC 8
AC 2	AC 7	AC 9
AC 3	AC 10	AC 14
AC 4	AC 11	AC 15
AC 5	AC 13	
AC 12	AC 16	

3.4. The Privacy Questionnaire

As discussed in the Research Methods section (Chapter 1.4), the validation of the Privacy Maturity Model relies on a privacy questionnaire that collect information about real-world IT systems. Initially, SIG provided the study with a draft version of the privacy questionnaire (v1.1), which contained 35 questions in total. Later, based on the iterative matching with the PbD checklist, the questionnaire was enlarged to 50 questions.

The questionnaire contains a combination of close-end and open-end questions. With closed-end questions, the participants are required to pick up the choice(s) that could most closely describe the status quo of their system. With open-end questions, the participants are required to specify the unique aspect(s) of their system.

The sequence of questions follows the 3 stages of PII workflow (which has been specified in Chapter 3.1). Questions under each PII workflow are further grouped to indicate different privacy principles. A separate section is being added at the end of the questionnaire to collect information about the system design and implementation. Below is an outline of the questionnaire, with each section followed by the number of questions asked in that part.

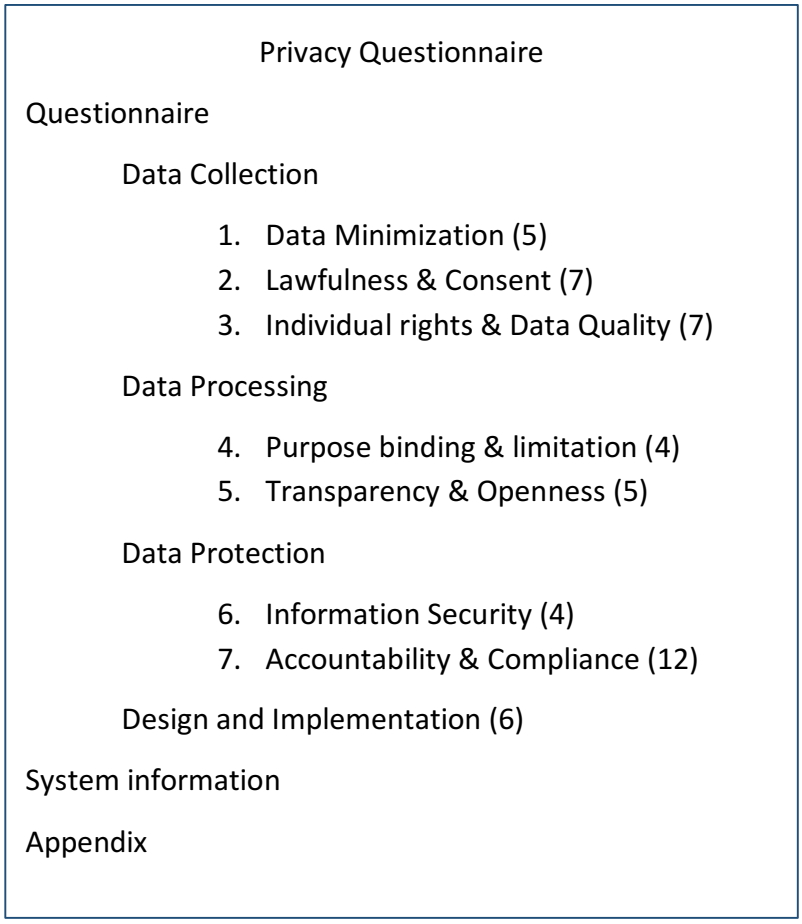

Figure [3.2]. Outline of the Privacy Questionnaire

The 50 questions ensure all the 75 PbD activities in our checklist are measurable – the mapping between the PbD activities and the questions is multiple to multiple. In some cases, one PbD activity refers to multiple questions; in others, several PbD activities are measured by one question. Besides, some questions are system-specific for gaining an impression of the context. Examples of different question types are given by the following tables.

Table [3.18]. Question Example 1: One Activity – Multiple Questions

Activity ID	Question	6. Which of the following actives regarding data collection are performed by the organization? (Please, check all that apply.)
LC 2	Options	The organization defines lawful purposes for collecting and processing PII before PII collection;
LC 3		The organization notify PII principals about mandatory collection of PII (e.g. for legal purpose);
LC 4		The organization ensures that data subjects understand the privacy policies when giving consent upon PII collection;
LC 5		The organization provides understandable information regarding PII purpose and collection;
LC 6		Upon PII collection, the organization displays notifications of the associated privacy policies.

Table [3.19]. Question Example 2: Multiple Activities – One Question

Activity ID	Question	39.c. (If the organisation shares PII with external entities) with which type of organisation(s) is PII shared? (Please check all that apply)
AC 11	Options	Outsourced IT partner
		Legal entity
		Government
		Other(s)
	Question	39.d. If yes, how often is the PII shared with external parties?
	Options	One time
		Periodically
		Continuously

Table [3.20]. Question Example 3: System-specific Question

Question	45. Does the organization host the application within its own premises?
Options	Yes, the organization locally hosts and manages the application and all elements that interact with it (e.g.: data stores, proxy, firewall, etc.);
	Yes, the organization hosts the application within its own premises, but an external party is responsible for managing the application and all its associated elements;
	No, the organization does not host the application and an external party is responsible for managing the application and all its associated elements;
	Others:

3.5. The Evaluation Framework

Based on the system facts collected by the privacy questionnaire, the PbD checklist can be reviewed and evaluated.

The evaluation of privacy maturity is two-fold: Firstly, the compliance with privacy maturity levels will be checked. Secondly, an action plan will be provided to the company/organization. The two parts function together to give an insight on what PbD activities are currently being implemented, and therefore encourages the company/organization to move towards a higher privacy maturity level.

3.5.1. Compliance with Privacy Maturity Levels

Instead of merely providing an overall result of compliance based on the whole model, the evaluation aims to provide a series of results based on each of the 7 privacy principles.

Rules for a *full compliance* with a specific privacy principle are defined as below:

- A *full compliance* with Privacy Maturity Level 1 is achieved by a 100% implementation of *Basic* PbD activities;
- A *full compliance* with Privacy Maturity Level 2 is achieved on top of a *full compliance* with Level 1, but also requires a 100% implementation of *Intermediate* PbD activities;
- A *full compliance* with Privacy Maturity Level 3 is achieved on top of a *full compliance* with Level 2, but also requires a 100% implementation of *Advanced* PbD activities.

The above rules indicate that, only when a system/application reaches a *full compliance* with the previous maturity level, can the compliance with next level be achieved.

If a system does not fully implement *Basic* PbD activities which is required by Level 1, then it is regarded as Level 1 *non-compliance*. Any unimplemented *Intermediate* or *Advanced* PbD activities under a specific privacy principle will stop it from being Level 2 or Level 3 *full compliance*, respectfully; these cases are thus classified as *non-compliance* with that privacy maturity level, and therefore the result will degrade to the previous level.

The privacy maturity level determination process is depicted as the following flowchart:

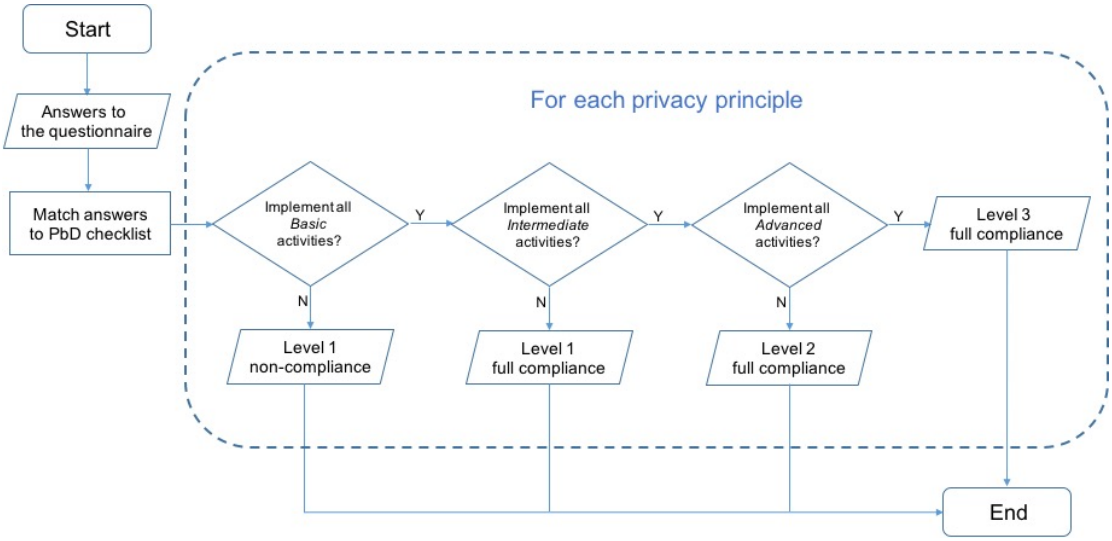

Figure [3.3]. The Composition of the Privacy Maturity Model

Tables below represents the *full compliance* circumstance of each privacy principle. Note that the privacy maturity evaluation always starts from the minimum level. Unless all PbD activities under the minimal privacy requirement (*Basic*) are "checked", or alternatively, a *full compliance* with Level 1 is achieved, can the evaluation move forward to the next level. Since the privacy maturity levels are in line with the privacy requirements (see Chapter 3.3), the same color set {yellow, green, and blue} has been adopted in the following tables to represent the conditions for achieving different maturity levels.

Table [3.11]. Evaluation of Compliance: *Lawfulness & Consent (LC)*

Activity ID	Lawfulness & Consent (LC)	L1	L2	L3
LC 1	Allow PII principal to freely opt-in and opt-out	✓	✓	✓
LC 2	Define lawful purposes for collecting and processing PII before PII collection	✓	✓	✓
LC 3	Notify PII principals about mandatory collection of PII (e.g. for legal purpose)	✓	✓	✓
LC 4	Ensure PII principals understand the privacy policies before providing consent without special knowledge	✓	✓	✓
LC 5	Provide easy to access and understandable information regarding PII collection	✓	✓	✓
LC 6	Display notifications of privacy policies at the entrance of physical locations where PII is collected	✓	✓	✓
LC 7	Collect PII in a privacy friendly way		✓	✓
LC 8	Specify the tracking technologies that have been used (cookies, web beacons, clicking behavior, etc.) for PII collection		✓	✓
LC 9	Notify PII principals that providing additional PII (e.g. for marketing purpose) is optional		✓	✓
LC 10	Obtain consent before using or disclosing PII		✓	✓
LC 11	Make provisions for PII principals to withdraw consent		✓	✓
LC 12	Inform PII principals about the consequences of approve or decline the consent		✓	✓
LC 13	Offer equitable conditions to PII principals who do not consent to provide PII			✓
LC 14	Conduct activities on any PII only with user consent or on a legal basis	✓	✓	✓

Table [3.12]. Evaluation of Compliance: *Data Minimization (DM)*

Activity ID	Data Minimization (DM)	L1	L2	L3
DM 1	Minimize PII collected for each purpose		✓	✓
DM 2	Separate the storage of PII collected from different sources			✓
DM 3	Set up aggregation mechanisms before PII processing and storage			✓
DM 4	Set up anonymization mechanisms before PII collection, processing and storage			✓

Table [3.13]. Evaluation of Compliance: *Individual rights & Data Quality (IRDQ)*

Activity ID	Individual rights & Data quality (IRDQ)	L1	L2	L3
IRDQ 1	Collect PII directly from PII principals whenever possible	✓	✓	✓
IRDQ 2	Only collect PII from sources whose reliability can be attested		✓	✓
IRDQ 3	Make sure that the automatically generated PII does not lead to false judgements			✓
IRDQ 4	Allow PII principals to access their individualized PII stored in the system	✓	✓	✓
IRDQ 5	Allow PII principals to amend, correct and remove their own PII	✓	✓	✓
IRDQ 6	Allow PII principals to object the collection, processing, and sharing of their PII at any time			✓
IRDQ 7	Enable timely and free-of-charge individual participation		✓	✓
IRDQ 8	Check regularly the accuracy, completeness, up-to-date, adequacy and relevance of PII			✓
IRDQ 9	Provide PII changes in time to any relevant privacy stakeholders		✓	✓
IRDQ 10	Record the unresolved PII challenges			✓
IRDQ 11	Inform privacy stakeholders in time about the unresolved PII challenges			✓

Table [3.14]. Evaluation of Compliance: *Purpose binding & limitation (PBL)*

Activity ID	Purpose binding & limitation (PBL)	L1	L2	L3
PBL 1	Notify PII principals about the legal reason for mandatory processing of PII	✓	✓	✓
PBL 2	Identify and document the purposes for conducting activities involving PII	✓	✓	✓
PBL 3	Define and document the purposes and technologies used for PII processing		✓	✓
PBL 4	Inform PII principals/service users about the purposes/services for which PII is used		✓	✓
PBL 5	Periodically evaluate the alignment between PII and its purpose		✓	✓
PBL 6	Exclude unnecessary PII which needs to be retained from regular processing			✓
PBL 7	Reveal PII principals identity as less as possible (e.g. avoid creating de-anonymized profiles)			✓
PBL 8	Delete and dispose non-purpose binding PII and back-ups as soon as the purpose expires		✓	✓
PBL 9	Retain PII for a limited time span only as needed or as required by law		✓	✓
PBL 10	Evaluate whether the privacy policy needs to be expanded for sharing new types of PII		✓	✓

Table [3.15]. Evaluation of Compliance: *Transparency & Openness (TO)*

Activity ID	Transparency & Openness (TO)	L1	L2	L3
TO 1	Document the type of PII collected			✓
TO 2	Define any cases that may disclose PII			✓
TO 3	Make PII processing explicitly announced and described		✓	✓
TO 4	Specify policies and practices about public-available PII		✓	✓
TO 5	Ensure the policy is available in any natural languages that PII principals might use		✓	✓
TO 6	Inform PII principals about their rights and choices	✓	✓	✓
TO 7	Provide contact information for questions and complaints	✓	✓	✓
TO 8	Inform PII principals about privacy stakeholders and PII controller	✓	✓	✓
TO 9	Archive and provide easy access to the historical versions of policy			✓
TO 10	Design and maintain a Privacy Dashboard			✓
TO 11	Make sure the PII principal read the privacy notice (by implementing an affordance)			✓
TO 12	Specify a PII decommission plan in the system design			✓

Table [3.16]. Evaluation of Compliance: *Information Security (IS)*

Activity ID	Information Security (IS)	L1	L2	L3
IS 1	Restrict the number of PII stakeholders and their access to the minimum need of PII	✓	✓	✓
IS 2	Minimize risks such as unauthorized access, destruction, use, modification, disclosure or loss	✓	✓	✓
IS 3	Conduct attack surface analysis and privacy threat modeling		✓	✓
IS 4	Identify and prioritize privacy threats		✓	✓
IS 5	Validate and verify the system's alignment with the privacy requirements		✓	✓
IS 6	Define privacy requirements explicitly			✓
IS 7	Design and implement adequate Privacy-Enhancing Technologies (PETs)			✓
IS 8	Prevent third parties from profiling PII			✓

Table [3.17]. Evaluation of Compliance: *Accountability & Compliance (AC)*

Activity ID	Accountability & Compliance (AC)	L1	L2	L3
AC 1	Notify PII principals about privacy breaches	✓	✓	✓
AC 2	Notify the Supervisory Authority when there are privacy breaches	✓	✓	✓
AC 3	Provide sanction and/or remedy procedures for privacy breaches	✓	✓	✓
AC 4	Place internal controls that align with external supervision mechanisms	✓	✓	✓
AC 5	Specify an entity responsible for privacy related issues	✓	✓	✓
AC 6	Arrange regular personnel training		✓	✓
AC 7	Check regularly if security safeguards are up-to-date		✓	✓
AC 8	Set up policy for internal PII sharing			✓
AC 9	Choose reliable PII processors that have an equivalent privacy maturity			✓
AC 10	Specify the responsibilities of external entities		✓	✓
AC 11	Minimize PII shared with external entities		✓	✓
AC 12	Inform PII principals about sharing their PII	✓	✓	✓
AC 13	Conduct privacy risk assessments (PIA) and implement periodic review and reassessment		✓	✓
AC 14	Implement PII protection mechanisms when conducting testing, research or training			✓
AC 15	Conduct either internal or third-party privacy auditing			✓
AC 16	Cooperate with supervisory and regulatory authorities		✓	✓

3.5.2. The Action Plan

Compliance with privacy maturity levels reflect how well an ICT system or application is doing in terms of privacy protection. Apart from that, having an action plan providing feedbacks and tailored suggestions is crucial for companies and organizations; despite that the Privacy Maturity Model shows maturity levels under 7 privacy principles, it is believed that company and organizations would like to know the meaning behind the results, as well as how to conduct PbD activities in a more consistent way.

The potential benefits of having an action plan along with the maturity results can be distinguished as such: Firstly, a list of unimplemented PbD activities is able to be identified from the specific answers to the questionnaire; Secondly, a prioritization of these unimplemented PbD activities can be determined by conducting risk analysis based on relevant factors (such as likelihood/impact/cost, etc.). However, since each company/organization has its specification in terms of business resources,

it will not be further discussed on how to calibrate the risk management process in this Privacy Maturity Model research.

4. Case Studies

Figure 4.1 represents a flowchart about the adoption of the Privacy Maturity Model. It will be described in detail in the following sections.

Figure [4.1]. Process of Adopting the Privacy Maturity Model

4.1. Outcomes of Case Study

Overall, two case studies have been performed to analyze the Privacy Maturity Model. Due to a consideration of protecting the participants from being disclosed, the two participants will be anonymized and referred as Organization *X* and Company *Y* throughout the text. Organization *X* resides in the Dutch Government sector (51–200 employees, retrieved from the organization's LinkedIn page); Company *Y* is a leading Dutch company in the Utilities industry (1,001 – 5,000 employees, retrieved from the company's LinkedIn page).

Both participants have answered the privacy questionnaire in the first place, each with their own system serving their core business operations. Later, an interview with Company *Y* have also been conducted (Chapter 4.2 will focus on this interview). The two sets of responses to the questionnaire are processed in the same way: first of all, the answers are mapped into the PbD checklist. Then, the implementation of PbD activities is checked by the evaluation framework mentioned in Chapter 3.5.

One thing needed to be clarified before showing the maturity level results is that, in both case studies, there are a few questions that haven't been answered. This is due to the iterative improvement of the privacy questionnaire, i.e., new questions have been added. Comparatively, Company *Y* participated in a later stage of this research, so they have less unanswered questions than Organization *X*. These unanswered questions lead to the unknown implementation of PbD activities. The way of dealing with this situation is to check the unanswered questions additionally. Take privacy requirement *Basic* as an example, this means, if the question(s) mapping into a *Basic* PbD activity is unanswered, which indicates the implementation of that *Basic* activity is unknown, then the privacy maturity will be considered as Level 1: *partial compliance* rather than Level 1: *full compliance*, despite that it might be the case that the rest of *Basic* activities are fully implemented.

4.1.1. Case Study 1

The following table indicates the results of privacy maturity levels received by Organization *X*:

Table [4.4]. Privacy Maturity Levels: Organization *X*

Privacy Principles	Maturity Level
Lawfulness & Consent (LC)	Level 1: *partial compliance*
Data Minimization (DM)	Level 1: *non-compliance*
Individual rights & Data quality (IRDQ)	Level 2: *partial compliance*
Purpose binding & limitation (PBL)	Level 1: *partial compliance*
Transparency & Openness (TO)	Level 1: *non-compliance*
Information Security (IS)	Level 1: *partial compliance*
Accountability & Compliance (AC)	Level 1: *non-compliance*

4.1.2. Case Study 2

The following table indicates the results of privacy maturity levels received by Company *Y*:

Table [4.5]. Privacy Maturity Levels: Company *Y*

Privacy Principles	Maturity Level
Lawfulness & Consent (LC)	Level 2: *full compliance*
Data Minimization (DM)	Level 2: *full compliance*
Individual rights & Data quality (IRDQ)	Level 3: *partial compliance*
Purpose binding & limitation (PBL)	Level 2: *partial compliance*
Transparency & Openness (TO)	Level 2: *full compliance*
Information Security (IS)	Level 3: *partial compliance*
Accountability & Compliance (AC)	Level 3: *full compliance*

4.2. Feedbacks on the Privacy Maturity Model

After filling out the questionnaire, Company *Y* showed willingness to participate in a further discussion on the privacy topic. This was mainly because Company *Y* felt that during filling out the questionnaire, they encountered several situations that the system facts were more of ambiguity rather than black-and-white. Therefore, a face to face discussion was planned between SIG Privacy Researchers and the Chief Privacy Officer of Company *Y*, along with his colleague, the Security Officer.

During the meeting, fundamental information has been briefly shared with Company *Y*, such as the initial motivation of having this research on privacy, the overall research process, the summarizing of privacy principles, and the distribution of PbD activities under each privacy principle. Then, the answers provided by Company *Y* were reviewed together. On the one hand, SIG experts pointed out several cases that Company *Y* might misunderstood the questions, and these cases were clarified during the discussion; On the other hand, Company *Y* strengthened their answers by explaining more according to the system facts.

Most crucially, the meeting with Company *Y* reveals that having the Privacy Maturity Model in place will be valuable in guiding the implementation of PbD activities. The opinions held by Company *Y* are three-fold, each followed by a brief explanation:

- *Overall, having a roadmap for solving privacy issues is of increasingly higher importance to modern organizations*. Although many privacy acts have been regulated as mandatory, it is still rare that an organization immediately owns a privacy checklist containing best practices to follow. To create a to-do list for privacy, the organization has to either approach in-house development, or hire someone outside. Both are expensive and time-consuming, and might run the risk of being involved with red tape or lawyers;
- *Implementing only Privacy-Enhancing Technologies will not always be sufficient for the protection of personal data, especially sensitive data*. Apart from purely implementing PETs, the emerging issues such as governance and compliance are crucial to be solved by the organization. Besides, customers are becoming more and more eager to protecting their PII, which requires the organization to be more transparent on sharing the information of how PII is used;
- *Organizations need to be aware of, and consider more on how to provide services as much as possible with less PII*. The organization should always think more about the question “Is the PII we collect really necessary for providing service?”. Previously, the trend was “collect as much as data at first, and think how to use the data later”; but nowadays, the organization is warned by the fact that, the more PII the organization holds, the larger

amount of compensation the organization has to pay once the data breach happens.

Regarding the above opinions provided by Company *Y*, it is convincing that the Privacy Maturity Model will be able to not only act as a guidance in terms of conducting PbD activities, but also better prevent cases such as relying on PETs as panacea, or "act before think" from happening.

4.3. Findings from Case Studies

The focus of this section is on presenting the findings in terms of privacy issues when applying the Privacy Maturity Model. Apart from describing the problems occurred in the two case studies, this section also explains the reasons behind those problems, and purposes possible solutions.

4.3.1. Non-Compliance with *Basic* Activities

When looking at the maturity levels of Organization *X*, it appears that compliance with Privacy Maturity Level 1 has not been fulfilled by the system under 3 privacy principles: *Lawfulness & Consent*, *Transparency & Openness*, and *Accountability & Compliance*. This means that the system is missing out the implementation of some *Basic* PbD activities, which should be the most common privacy practices, or even might be mandated by law.

The reason behind non-compliance with Level 1 is that, Organization *X* is undergoing a system redesign. The previous version of their system was launched far ahead of the recent release of GDPR (April, 2016), so there exist quite a few issues that does not binding with the new privacy regulation. According to the communication between SIG and Organization *X*, non-compliance issues are not only lying in the system design, but also in the *X*'s organizational procedures. But the positive thinking in this case study is that, Organization *X* will take the evaluation results into serious consideration, and regard them as input for the system re-design.

4.3.2. The Non-Applicable Activities

There exist a few situations that a PbD activity is not applicable to the specific system. For example, under privacy principle *Accountability & Compliance*, one *Basic* PbD activity is "Make sure the automatically generated PII does not lead to false judgements". "Make sure the automatically generated PII does not lead to false judgements". But in the reality, since the being analyzed systems of our participants do not generate PII automatically, this activity is regarded as not applicable in both case studies.

When going through the process of matching answers to the PbD checklist, both participants have got around 3 non-applicable PbD activities. These non-applicable activities have not been taken into consideration for the evaluation. Therefore, they do not hamper the determination of privacy maturity levels.

4.3.3. Overall Comparison on the Case Studies

Before sending out the privacy questionnaire, it is known that Company *Y* emphasizes more on the privacy issue than Organization *X*. Therefore, the results of their privacy maturity levels are in line with the expectation.

The results also show that both participants have gained a higher maturity level in *Individual Rights & Data Quality* as well as *Information Security*. The comprehension to this result is that, these two privacy principles have covered more PbD activities which can be labeled as “do’s” rather than “notice’s”. Since Organization *X* and Company *Y* are both willing to get privacy right, the implementation of “do’s” are high. However, sometimes it might be the case that the organizations only focus on implementing, but forget to put those “do’s” into documentation. Although privacy principles such as *Transparency and Openness* suggest PbD activities more about publishing policies, they are regarded as of equal importance in the Privacy Maturity Model. To enhance the maturity level of these previously neglected privacy principles, both participants should focus more on the “notice’s” in the future.

5. Discussions

This chapter aims to provide refinement to the Privacy Maturity Model based on the company interview in the first place. Later, this chapter presents discussions on alternative approaches of conducting the evaluation framework of the Privacy Maturity Model.

5.1. Refinement on the Privacy Maturity Model

During the interview with Company Y, the participants were encouraged to share their opinions on the Privacy Maturity Model. The Chief Privacy Officer spoke out a concern with part of the model: According to the distribution of PbD activities under the *Data Minimization* principle, it might be confusing to have zero *Basic* activity for Maturity Level 1. Once a company implements nothing under *Data Minimization*, it can be judged as both *non-compliance* with Level 1 as well as *non-compliance* with Level 2.

Thus, a discussion on this activity distribution issue was taken place with SIG experts. However, because there is only 4 PbD activities lying under the *Data Minimization* principle, a comparison of the maturity of each activity was made. Therefore, activity DM 1 was re-assigned as a *Basic* activity, and DM 2 was re-assigned as an *Intermediate* activity. Besides, it has also resulted in a change to this part of the model evaluation:

Table [5.1]. Evaluation of Compliance (Updated): *Data Minimization (DM)*

Activity ID	Data Minimization (DM)	L1	L2	L3
DM 1	Minimize PII collected for each purpose	✓	✓	✓
DM 2	Separate the storage of PII collected from different sources		✓	✓
DM 3	Set up aggregation mechanisms before PII processing and storage			✓
DM 4	Set up anonymization mechanisms before PII collection, processing and storage			✓

The updated *Data Minimization* evaluation will be able to eliminate the ambiguity brought up by Company *Y*. Instead of confusingly being judged as non-compliance with either maturity level 1 or 2, a company/organization does not implement *DM 1* will now be judged as Level 1: *non-compliance* for certain.

5.2. Improvement on the Evaluation Framework

Due to the fact of fewer-than-expected data points collected by the privacy questionnaire, the current approach of evaluating the Privacy Maturity Model still

has its constraints. For example, the current evaluation does not indicate a benchmark. However, if more data points could be gathered via questionnaire in the future, the chance will be high that the evaluation framework differs from how it looks now. In the following sections, the reason of having a low response rate as well as a potential redesign of the evaluation framework (i.e. a star-rating system) are discussed.

5.2.1. A Limited Number of Data Points

During the whole research process, the most challenging issue is the unexpected few responses to our questionnaire. Originally, an *Invitation to Participate* letter has been sent out to more than 20 companies/organizations in total. However, among these potential participants, only half responded to the invitation, and eventually only 2 participated in answering the questionnaire (and Company *Y* participated in an interview). Later, the *Invitation to Participate* was iteratively (i.e. monthly, from April to June) spread via social networks, such as SIG official LinkedIn page, SIG experts personal LinkedIn pages, as well as SIG official Twitter accounts. Yet, no further response has been received until the end of model validation.

To summarize, the major reason behind the low motivation to participate can be identified from the communications with the invited companies/organizations: it is hard to avoid bureaucracy in large organizations, which really slowed things down. Especially, the research has faced more resistance when the internal communication procedures requires everything to be kept in track by various departments. The worst case was that the research even got rejected simply because of the ignorance of less relevant personnel.

5.2.2. The Partially Implemented PbD Activities

An issue on the implementation of PbD activities is that, for several activities, it is not enough to measure things as “either black, or white”. A few questions were designed to ask about the frequency of conducting a PbD activity. For instance, one question asks how often does the organization plan a personnel privacy training. The answers could be “frequently” “once” and “never”. The idea is, of course, not to merely look at if a training has ever been done or not to the personnel, but to see whether the training has been done regularly.

In that sense, the specific PbD activity can be measured as “partially done” if the participant answered “once”. To better understand the type of “partially done” situation, the respondents are also asked to specify the frequency by entering free text to the questionnaire.

The good news is that, the answers from both participants showed that entering free text is not a burden. Company *Y* is even happy to write down some extra information

to better describe the situation they are going through, which is indeed an appealing outcome that encourages the development of Privacy Maturity Model.

In order to take the partial implementation of PbD activities into account, the rule of current model evaluation can be further developed. Together with SIG experts, we suggest a possible definition of the *partial compliance* circumstance:

- A system/application reaches Level 1 *partial compliance* when every *Basic* activity is at least partially implemented;
- A system/application reaches Level 2 *partial compliance* when it has reached *full-compliance* with Level 1, and every *Intermediate* activity is at least partially implemented;
- A system/application reaches Level 3 *partial compliance* when it has reached *full-compliance* with Level 2, and every *Advanced* activity is at least partially implemented.

5.2.3. Possibility of A Privacy Maturity Rating System

A 5-star rating system is able to provide benchmark information once the amount of data points is ready. The stars will be a complete overwrite of the evaluation framework, and will provide a direct insight to a company/organization who would like to conduct self-positioning within either its industry or the general context.

The following transition table gives a first impression on how the star rating works. Overall, there are five rows specifying the number of stars from 1 to 5, respectively. For each row, a set of percentages is defined under all three privacy maturity levels. The percentages, P_{Bi}, P_{Ii}, and P_{Ai} ($i = \{1,2,3,4,5\}$), indicate that, for the total number of PbD activities (i.e., despite of the privacy principles) belonging to a specific maturity level, how many of them are actually being fully implemented. Each percentage determines the least amount of PbD activities that have to be implemented. For instance, a 3-star rating requires a system to conduct P_{B3} of all PbD activities that belong to *Basic*, P_{I3} of *Intermediate*, and P_{A3} of *Advanced*.

Although one argument can be that, in theory, a company can implement all PbD activities in *Basic* and yet none of the other two; but since the percentages will be determined by data, it is still possible to avoid this theoretical issue.

Table [5.2]. The Transition Table for Privacy Star Rating

Star	Basic	Intermediate	Advanced
★☆☆☆☆	P_{B1}	P_{I1}	P_{A1}
★★☆☆☆	P_{B2}	P_{I2}	P_{A2}
★★★☆☆	P_{B3}	P_{I3}	P_{A3}
★★★★☆	P_{B4}	P_{I4}	P_{A4}
★★★★★	P_{B5}	P_{I5}	P_{A5}

Furthermore, based on the actual data, 3 different scenarios can be suggested, each aiming at a specific purpose of analyzing the PbD checklist.

- *Basic*-focused: This scenario stresses the importance of Basic. To reach a higher star-rating, organizations should make a promise on implementing as many Basic PbD activities as possible;
- Optimistic: This scenario provides tolerant basis for reaching different stars, regarding to the current real-world implementations;
- Stringent: This scenario defines challenging percentages for organizations to receive a higher star-rating.

For each scenario, the example of percentage setting can be found in the following tables, respectively:

Table [5.3]. Thresholds of Privacy Star Rating: *Basic*-focused

Star	Basic	Intermediate	Advanced
★☆☆☆☆	0	0	0
★★☆☆☆	40%	25%	10%
★★★☆☆	60%	35%	20%
★★★★☆	80%	45%	30%
★★★★★	95%	55%	40%

Table [5.4]. Thresholds of Privacy Star Rating: Optimistic

Star	Basic	Intermediate	Advanced
★☆☆☆☆	0	0	0
★★☆☆☆	30%	25%	15%
★★★☆☆	50%	40%	30%
★★★★☆	70%	55%	45%
★★★★★	90%	70%	60%

Table [5.5]. Thresholds of Privacy Star Rating: Stringent

Star	Basic	Intermediate	Advanced
★☆☆☆☆	0	0	0
★★☆☆☆	35%	25%	15%
★★★☆☆	55%	45%	35%
★★★★☆	75%	65%	55%
★★★★★	95%	85%	75%

6. Conclusions

Living in the digital era, more and more people start to realize the criticalness of privacy issues. Apart from simply enjoying the advancement of technologies, the problems in collecting and processing (sometimes irrelevant) PIIs have long not been solved.

This research on Privacy Maturity Model, thus, has its significance in both academic and industrial field. On the one hand, this research is a breakthrough, for its distinctive technology-specific features from the existing PIA. On the other hand, with the Privacy Maturity Model working as a guideline for implementing PbD activities, modern companies and organizations whose services are relying on the collection and processing of PII will be able to build services and conduct activities with more mature privacy concerns.

6.1. Privacy Requires a Proactive Thinking

Although modern companies and organizations are spending more time and resources on figuring out issues with privacy, the dominant trend is still "change once we are forced to". This can be supported by 3 aspects:

- A recent trigger for companies and organizations to rethink their privacy is not much than the newly released GDPR. Guidelines for how to conduct privacy-binding activities have been emerging and can be easily found online, but the contents of them are more on "how to avoid paying fines by conducting activities that have been set as mandatory in GDPR". For a company/organization who intend to implement Privacy by Design, approaching these regulation-based guidelines is obviously far from sufficient, because what can be found in these online accessible guidelines is merely several PbD activities categorized as *Basic* in our Privacy Maturity Model.
- It is commonly seen that companies/organizations only focus on data protection, without considering the whole PII workflow which includes data collection and data processing as well (see Chapter 3.1). Several companies and organizations we witnessed during this research are regarding privacy the same concept as information security; a common case is that at first they collect as much PII as possible to enhance security aspects, and later have to suffer from a higher risk of data breach. However, information security is only one of the seven privacy principles being covered by the Privacy Maturity Model.
- The group of people who hold a proactive thinking is comparatively small in the whole organization. This aspect of the problem is revealed by the interview with Company *Y*. Although Company *Y* has received higher privacy

maturity levels, employees who are eager to think proactively about privacy are still limited to the ones who directly deal with privacy issues. According to Company *Y*, it is still often the case that an ambitious plan on privacy receives ignorance by the management team, and might take several years to be actually implemented.

The aspects above reflect the importance of having a model that can better guide the companies/organizations to reach a higher privacy maturity level. The Privacy Maturity Model proposed in this research is possible to raise more privacy awareness, as well as encourage companies/organizations to implement PbD activities from reactively to proactively.

6.2. Improvement of the Privacy Maturity Model

During recent years, both BSIMM and OWASP ASVS have been going through the process of further development. BSIMM now reaches its sixth version and OWASP ASVS is in its third version. If looking at the history versions of both models, it is obvious to tell that both their size as well as the content have been refined. Designed analogously to these two maturity models, the Privacy Maturity Model will also be subject to change both in size and in content in the future.

Reviewing and revising the Privacy Maturity Model can be triggered by events such as the main update of ISO 29100 or any European/world-class privacy regulations. Two main aspects shall be considered in order to make adjustments to the Privacy Maturity Model:

- Completeness. This means to check if PbD activities mentioned under each privacy principle in the Privacy Maturity Model are complete. When there is the necessity of adding new PbD activities, modifying existing PbD activities, or removing outdated PbD activities, expert opinions shall be taken into consideration. This also ensures no overlap between activities will appear.
- Evolvement of privacy requirements. In Chapter 3.3, the privacy requirements are defined as *Basic*, *Intermediate*, and *Advanced*. The mapping between PbD activities and these requirements is dynamic. In the future, with the development on the concept of Privacy-by-Design, existing PbD activities in the current checklist might become more of common or even obligatory practices. Therefore, it is crucial to make sure that the mapping between PbD activities and the privacy requirements is up-to-date.

6.3. Limitations and Further Research

Having seen the facts of how modern companies and organizations are dealing with privacy issues, it has to be admitted that the improvement on information privacy is not, and will not be something that happens immediately. As discussed in Chapter 5.2.1, the most challenging issue in this research is the lower-than-expected response rate to the privacy questionnaire.

Nevertheless, this research on Privacy Maturity Model performs as an initializer in the field, and is expected to raise several relevant research topics in the near future. Once a larger number of data points is available, it will be interesting to automatically process the questionnaire results for the model evaluation. The further research will be focusing on developing a benchmark and model calibration which is based on data collected from various industries.

References

[AICPA/CICA, 2011] American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants. (2011). Privacy Maturity Model. Retrieved from http://www.kscpa.org/writable/files/AICPADocuments/10-229_aicpa_cica_privacy_maturity_model_finalebook.pdf

[Banisar & Davies, 1999] Banisar, D., & Davies, S. (1999). Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments. *Journal of Computer & Information Law*, *XVIII*, 1–111. Retrieved from http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jmjcila18&section=4

[Borking & Raab, 2001] Borking, J. J., & Raab, C. (2001). Laws, PETs and other technologies for privacy protection. *Journal of Information, Law and Technology*, *1*(February), 1–14.

[BSIMM6, 2015]]Mcgraw, G., Ph, D., Migues, S., West, J., Arkin, A. B., Routh, A. J., … Derdouri, S. (2015). *BSIMM6*. Retrieved from http://www.inf.ed.ac.uk/teaching/courses/sp/2015/lecs/BSIMM6.pdf

[CMMI v1.3, 2011] *CMMI for Development, Version 1.3*. (2010). Retrieved from http://resources.sei.cmu.edu/asset_files/TechnicalReport/2010_005_001_15287.pdf

[Comparison of International Privacy Concepts] *Comparison of International Privacy Concepts - AICPA*. *Aicpa.org*. Retrieved 2016, from http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/InternationalPrivacyConcepts.aspx

[Danezis et al., 2014] Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, D. Le, Tirtea, R., & Schiffner, S. (2014). Privacy and Data Protection by Design - from policy to engineering. Retrieved from http://arxiv.org/abs/1501.03726

[De Hert, Kloza & Wright, 2012] De Hert, P., Kloza, D., & Wright, D. (2012). *Recommendations for a privacy impact assessment framework for the European Union*.

[European Commission, 2016] *Reform of EU data protection rules - European Commission*. (2016). *ec.europa.eu*. Retrieved 2016, from http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[Directive 95/46/EC, 1995] European Parliament. (1995). Directive 95/46/EC. *Official Journal of the European Communities*, *L 281/31*(L).

[Finkle & Volz, 2015] Finkle, J. & Volz, D. (2015). *Database of 191 million U.S. voters exposed on Internet: researcher*. *Reuters UK*. Retrieved from http://uk.reuters.com/article/us-usa-voters-breach-idUKKBN0UB1E020151229

[Flaherty, 2000] Flaherty, D. (2000). Privacy impact assessments: an essential tool for data protection. In *Privacy Law and Policy Reporter* (Vol. 7, p. 85). Retrieved from http://www.austlii.edu.au/au/journals/PLPR/2000/45.html

[Heurix et al., 2015] Heurix, J., Zimmermann, P., Neubauer, T., & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers and Security*, *53*, 1–17. http://doi.org/10.1016/j.cose.2015.05.002

[Hinde, 2014] Hinde, C. (2014). A Model to Assess Organisational Information Privacy Maturity against the Protection of Personal Information Act. University of Cape Town.

[Huijben, 2014] Huijben, K. (2014). *A lightweight, flexible evaluation framework to measure the ISO 27002 information security controls*. Radboud University.

[ISO/IEC 29100: 2011] INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Privacy framework. (2011)

[Kelion, 2016] Kelion, L. (2016). *Facebook Moments facial-recognition app launches in Europe - BBC News*. *BBC News*. Retrieved from http://www.bbc.com/news/technology-36256765

[Le et al., 2015] Le, D., Inria, M., Trilateral, I. K., & María, J. (2015). PRIPARE: Privacy- and Security-by-Design Methodology Handbook.

[McGee, 2016] McGee, M. (2016). *Verizon Confirms Breach Affecting Business Customers*. *Databreachtoday.eu*. Retrieved from http://www.databreachtoday.eu/verizon-confirms-breach-affecting-business-customers-a-8991

[New Zealand Government, 2014 (1)] New Zealand Government. Privacy Maturity Assessment Framework: Elements, attributes, and criteria (version 2.0). (2014).

[New Zealand Government, 2014 (2)] New Zealand Government. User guide for the Privacy Maturity Assessment Framework. (2014).

[OECD, 1980] Organisation for Economic Cooperation and Development guidelines Annex to the recommendation of the Council of 23 September 1980: Guidelines governing the protection of privacy and transborder flows of personal data. (1980).

[OWASP ASVS 3.0, 2015] *Application Security Verification Standard 3.0*. (2015). Retrieved from https://www.owasp.org/images/6/67/OWASPApplicationSecurityVerificationStandard 3.0.pdf

[Pew Research Center, 2013] *Social Networking Fact Sheet*. (2013). *Pew Research Center: Internet, Science & Tech*. Retrieved September 2014, from http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/

[Revoredo et al., 2014] Revoredo, M., Marcelo, C., Lutiano, J., Melo, R. M., Batista, R., Lucien, L. R., … Garcia, V. C. (2014). A Privacy Maturity Model for Cloud Storage Services. http://doi.org/10.1109/CLOUD.2014.135

[Roger, 2015] Roger, H. (2015). *Right of Subject Access – From request to response: An analysis of process performance*. Leiden University.

[Schwaig, Kane & Storey, 2006] Schwaig, K. S., Kane, G. C., & Storey, V. C. (2006). Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures? *Information and Management*, *43*(7), 805–820. http://doi.org/10.1016/j.im.2006.07.003

[Thiesse, 2007] Thiesse, F. (2007). RFID, privacy and the perception of risk: A strategic framework. *Journal of Strategic Information Systems*, *16*(2), 214–232. http://doi.org/10.1016/j.jsis.2007.05.006

[Warren and Brandeis, 1890] Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Havard Law Review*, *4*(5), 193–220.

[Wright, 2013] Wright, D. (2013). Making Privacy Impact Assessment More Effective. *The Information Society: An International Journal*, *29*, 307–315. http://doi.org/10.1080/01972243.2013.825687

Appendices

Appendix A: The Privacy Questionnaire

This part has been removed from the thesis due to the concern of confidentiality. The questionnaire has been handed in separately to the thesis advisors.

Appendix B: The Invitation Letter

A practical approach to assess privacy protection in and around IT applications

Invitation to participate in research

Privacy is increasingly important to citizens and policy makers. Organizations that collect and process privacy-sensitive information are under rapidly increasing scrutiny.

IT applications play a key role in both processing and protecting privacy-sensitive information. While existing privacy assessment methods address privacy protection at a broad organizational level, the need arises for practical approaches that do justice to this key role of IT applications.

In joint research, Leiden University and the Software Improvement Group (SIG) are developing a Privacy Maturity Model that applies to an IT application in its organizational context.

We now invite organizations that rely on IT applications to process and protect privacy-sensitive information to participate in our research. Participating organizations are invited to go through the following steps:

1. Fill out a **questionnaire**. This will take approximately 2 hours in total, divided over two or three employees with knowledge of application functionality, architecture, and privacy requirements.

2. Partake in an **interview**. This will take approximately 1.5 hours. The interview includes a discussion of the filled-out questionnaire.

Feedback will be provided to the participating organizations in the form of a Privacy Maturity report together with an interactive session. All study results will remain anonymous.

Please express your interest to participate in this study via privacypractice@sig.eu. We will contact you to make all necessary arrangements.

We are looking forward to your contribution!

Prof. dr. ir. Joost Visser (Software Improvement Group & Radboud University Nijmegen)

Dr. Amr Ali-Eldin (Leiden Institute of Advanced Computer Science, Leiden University)

Appendix C: The Mapping between PbD Activities and Questions

This part has been removed from the thesis due to the concern of confidentiality. This part has been handed in separately to the thesis advisors.