



Privacy Management Reference Model and Methodology (PMRM) Version 1.0

Committee Specification Draft 04

31 March 2016

Specification URIs

This version:

<http://docs.oasis-open.org/pmr/PMRM/v1.0/csd04/PMRM-v1.0-csd04.pdf> (Authoritative)
<http://docs.oasis-open.org/pmr/PMRM/v1.0/csd04/PMRM-v1.0-csd04.html>
<http://docs.oasis-open.org/pmr/PMRM/v1.0/csd04/PMRM-v1.0-csd04.doc>

Previous version:

<http://docs.oasis-open.org/pmr/PMRM/v1.0/cs01/PMRM-v1.0-cs01.pdf> (Authoritative)
<http://docs.oasis-open.org/pmr/PMRM/v1.0/cs01/PMRM-v1.0-cs01.html>
<http://docs.oasis-open.org/pmr/PMRM/v1.0/cs01/PMRM-v1.0-cs01.doc>

Latest version:

<http://docs.oasis-open.org/pmr/PMRM/v1.0/PMRM-v1.0.pdf> (Authoritative)
<http://docs.oasis-open.org/pmr/PMRM/v1.0/PMRM-v1.0.html>
<http://docs.oasis-open.org/pmr/PMRM/v1.0/PMRM-v1.0.doc>

Technical Committee:

OASIS Privacy Management Reference Model (PMRM) TC

Chair:

John Sabo (john.annapolis@comcast.net) Individual

Editors:

Michele Drgon, (micheledrgon@dataprobity.com), DataProbity
Gail Magnuson (gail.magnuson@gmail.com), Individual
John Sabo (john.annapolis@comcast.net), Individual

Abstract:

The Privacy Management Reference Model and Methodology (PMRM, pronounced “pim-rim”) provides a model and a methodology to

- understand and analyze privacy policies and their privacy management requirements in defined Use Cases; and
- select the technical Services, Functions and Mechanisms that must be implemented to support requisite Privacy Controls.

It is particularly valuable for Use Cases in which Personal Information (PI) flows across regulatory, policy, jurisdictional, and system boundaries.

Status:

This document was last revised or approved by the OASIS Privacy Management Reference Model (PMRM) TC on the above date. The level of approval is also listed above. Check the “Latest version” location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pmrm#technical.

TC members should send comments on this specification to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "[Send A Comment](#)" button on the TC's web page at <https://www.oasis-open.org/committees/pmrm/>.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (<https://www.oasis-open.org/committees/pmrm/ipr.php>).

Citation format:

When referencing this specification the following citation format should be used:

[PMRM-v1.0]

Privacy Management Reference Model and Methodology (PMRM) Version 1.0. Edited by Michele Drgon, Gail Magnuson, and John Sabo. 31 March 2016. OASIS Committee Specification Draft 04. <http://docs.oasis-open.org/pmrm/PMRM/v1.0/csd04/PMRM-v1.0-csd04.html>. Latest version: <http://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.html>.

Notices

Copyright © OASIS Open 2016. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full [Policy](#) may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of [OASIS](#), the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <https://www.oasis-open.org/policies-guidelines/trademark> for above guidance.

Table of Contents

1	Introduction.....	6
1.1	General Introduction to the PMRM	6
1.2	Major Changes from PMRM V1.0 CS01.....	7
1.3	Context.....	7
1.4	Objectives and Benefits	8
1.5	Target Audiences.....	9
1.6	Specification Summary	9
1.7	Terminology	11
1.8	Normative References	12
1.9	Non-Normative References	12
2	Develop Use Case Description and High-Level Privacy Analysis.....	13
2.1	Application and Business Process Descriptions.....	13
	Task #1: Use Case Description	13
	Task #2: Use Case Inventory.....	14
2.2	Applicable Privacy Policies	14
	Task #3: Privacy Policy Conformance Criteria	14
2.3	Initial Privacy Impact (or other) Assessment(s) [optional]	15
	Task #4: Assessment Preparation	15
3	Develop Detailed Privacy Analysis.....	16
3.1	Identify Participants and Systems, Domains and Domain Owners, Roles and Responsibilities, Touch Points and Data Flows (Tasks # 5-10)	16
	Task #5: Identify Participants.....	16
	Task #6: Identify Systems and Business Processes	16
	Task #7: Identify Domains and Owners	17
	Task #8: Identify Roles and Responsibilities within a Domain	18
	Task #9: Identify Touch Points.....	18
	Task #10: Identify Data Flows.....	18
3.2	Identify PI in Use Case Domains and Systems.....	19
	Task #11: Identify Incoming PI.....	19
	Task #12: Identify Internally Generated PI	19
	Task #13: Identify Outgoing PI.....	19
3.3	Specify Required Privacy Controls Associated with PI	19
	Task #14: Specify Inherited Privacy Controls	19
	Task #15: Specify Internal Privacy Controls	20
	Task #16: Specify Exported Privacy Controls.....	20
4	Identify Services and Functions Necessary to Support Privacy Controls	21
4.1	Services and Functions Needed to Implement the Privacy Controls	21
4.2	Service Details and Function Descriptions	23
	4.2.1 Core Policy Services	23
	1. Agreement Service	23
	2. Usage Service	23
	4.2.2 Privacy Assurance Services.....	23
	3. Validation Service	23

4.	Certification Service	24
5.	Enforcement Service	24
6.	Security Service	24
4.2.3	Presentation and Lifecycle Services	25
7.	Interaction Service	25
8.	Access Service	25
4.3	Identify Services satisfying the Privacy Controls	25
	Task #17: Identify the Services and Functions necessary to support operation of identified Privacy Controls	25
5	Define Technical and Procedural Mechanisms Supporting Selected Services and Functions.....	27
5.1	Identify Mechanisms Satisfying the Selected Services and Functions.....	27
	Task #18: Identify the Mechanisms that Implement the Identified Services and Functions	27
6	Perform Operational Risk and/or Compliance Assessment	28
	Task #19: Conduct Risk Assessment	28
7	Initiate Iterative Process	29
	Task #20: Iterate the analysis and refine	29
8	Conformance	30
8.1	Introduction	30
8.2	Conformance Statement.....	30
9	Operational Definitions for Privacy Principles and Glossary	31
9.1	Operational Privacy Principles.....	31
9.2	Glossary	32
9.3	PMRM Acronyms	36
Appendix A.	Acknowledgments	37

1 Introduction

1.1 General Introduction to the PMRM

The Privacy Management Reference Model and Methodology (PMRM) addresses the reality of today's networked, interoperable systems, applications and devices coupled with the complexity of managing Personal Information (PI)¹ across legal, regulatory and policy environments in these interconnected Domains. It can be of great value both to business and program managers who need to understand the implications of Privacy Policies for specific business systems and to assess privacy management risks as well as to developers and engineers who are tasked with building privacy into Systems and Business Processes.

Additionally, the PMRM is a valuable tool to achieve Privacy by Design, particularly for those seeking to improve privacy management, compliance and accountability in complex, integrated information systems and solutions - such as health IT, financial services, federated identity, social networks, smart grid, mobile apps, cloud computing, Big Data, Internet of Things (IoT), etc. Achieving Privacy by Design is challenging enough in relatively simple systems, but can present insurmountable challenges in the complex systems we see today, where the use of PI across the entire ecosystem is governed by a web of laws, regulations, business contracts, operational policies and technologies.

The PMRM is neither a static model nor a purely prescriptive set of rules (although it includes characteristics of both). It utilizes the development of a Use Case that is clearly bounded, and which forms the basis for a Privacy Management Analysis (PMA). Implementers have flexibility in determining the level and granularity of analysis required for their particular Use Case.

A Use Case can be scoped narrowly or broadly. Although its granular-applicability is perhaps most useful to practitioners, it can also be employed at a broader level, encompassing an entire enterprise, product line or common set of functions within a company or government agency. From such a comprehensive level, the privacy office could establish broad Privacy Controls, implemented by Services and their underlying Functionality in manual and technical Mechanisms – and these, in turn, would produce a high level PMA and could also inform a high-level Privacy Architecture. Both the PMA and a Privacy Architecture could then be used to incorporate these reusable Services, Functions and Mechanisms in future initiatives, enabling improved risk assessment, compliance and accountability.

In order to ensure Privacy by Design at the granular level, a Use Case will more likely be scoped for a specific design initiative. However, the benefit of having used the PMRM at the broadest level first is to inform more-granular initiatives with guidance from an enterprise perspective, potentially reducing the amount of work for the privacy office and engineers.

Even if the development of an overarching PMA is not appropriate for an organization, the PMRM will be useful in fostering interoperable policies and policy management standards and solutions. In this way, the PMRM further enables Privacy by Design because of its analytic structure and primarily operational focus. A PMRM-generated PMA, because of its clear structure and defined components, can be valuable as a tool to inform the development of similar applications or systems that use PI.

As noted in Section 8, the PMRM as a “model” is abstract. However, as a Methodology it is through the process of developing a detailed Use Case and a PMA that important levels of detail emerge, enabling a complete picture of how privacy risks and privacy requirements are being managed. As a Methodology

¹ Note: We understand the important distinction between ‘Personal Information’ (PI) and ‘Personally-Identifiable Information’ (PII) and that in specific contexts a clear distinction must be made explicitly between the two, which should be reflected as necessary by users of the PMRM. However, for the purposes of this document, the term ‘PI’ will be used as an umbrella term to simplify the specification. Section 9.2 Glossary addresses the distinctions between PI and PII.

41 the PMRM – richly detailed and having multiple, iterative task levels - is intentionally open-ended and can
42 help users build PMAs at whatever level of complexity they require.

43

44 *Note: It is strongly recommended that Section 9 Operational Definitions for Privacy Principles and*
45 *Glossary is read before proceeding. The Operational Privacy Principles and the Glossary are key to a*
46 *solid understanding of Sections 2 through 8.*

47

48 **1.2 Major Changes from PMRM V1.0 CS01**

49

50 This version of the PMRM incorporates a number of changes that are intended to clarify the PMRM
51 methodology, resolve inconsistencies in the text, address the increased focus on accountability by privacy
52 regulators, improve definitions of terms, expand the Glossary, improve the graphical figures used to
53 illustrate the PMRM, and add references to the OASIS Privacy by Design Documentation for Software
54 Engineers committee specification. Although the PMRM specification has not fundamentally changed, the
55 PMRM technical committee believes the changes in this version will increase the clarity of the PMRM and
56 improve its usability and adoption by stakeholders who are concerned about operational privacy,
57 compliance and accountability.

58

59 **1.3 Context**

60 Predictable and trusted privacy management must function within a complex, inter-connected set of
61 networks, Business Processes, Systems, applications, devices, data, and associated governing policies.
62 Such a privacy management capability is needed in traditional computing, Business Process engineering,
63 in cloud computing capability delivery environments and in emerging IoT environments.

64 An effective privacy management capability must be able to instantiate the relationship between PI and
65 associated privacy policies. The PMRM supports this by producing a PMA, mapping Policy to Privacy
66 Controls to Services and Functions, which in turn are implemented via Mechanisms, both technical and
67 procedural. The PMA becomes the input to the next iteration of the Use Case and informs other initiatives
68 so that the privacy office and engineers are able to apply the output of the PMRM analysis to other
69 applications to shorten their design cycles.

70 The main types of Policy covered in this specification are expressed as classes of Privacy Controls:
71 Inherited, Internal or Exported. The Privacy Controls must be expressed with sufficient granularity as to
72 enable the design of Services consisting of Functions, instantiated through implementing Mechanisms
73 throughout the lifecycle of the PI. Services must accommodate a changing mix of PI and policies,
74 whether inherited or communicated to and from external Domains, or imposed internally. The PMRM
75 methodology makes possible a detailed, structured analysis of the business or application environment,
76 creating a custom PMA for the particular Use Case.

77 A clear strength of the PMRM is its recognition that today's systems and applications span jurisdictions
78 that have inconsistent and conflicting laws, regulations, business practices, and consumer preferences.
79 This creates huge challenges to privacy management and compliance. It is unlikely that these challenges
80 will diminish in any significant way, especially in the face of rapid technological change and innovation
81 and differing social and national values, norms and policy interests.

82 It is also important to note that in this environment agreements may not be enforceable in certain
83 jurisdictions. And a dispute over jurisdiction may have significant bearing over what rights and duties the
84 participants have regarding use and protection of PI. Even the definition of PI will vary. The PMRM may
85 be useful in addressing these issues. Because data can in many cases easily migrate across
86 jurisdictional boundaries, rights cannot necessarily be protected without explicit specification of what
87 boundaries apply. Proper use of the PMRM will however expose the realities of such environments
88 together with any rules, policies and solutions in place to address them.

89 1.4 Objectives and Benefits

90 The PMRM's primary objectives are to enable the analysis of complex Use Cases, to understand and
91 design appropriate operational privacy management Services and their underlying Functionality, to
92 implement this Functionality in Mechanisms and to achieve compliance across Domains, systems, and
93 ownership and policy boundaries. A PMRM-derived PMA may also be useful as a tool to inform policy
94 development applicable to multiple Domains, resulting in Privacy Controls, Services and Functions,
95 implementing Mechanisms and – potentially - a Privacy Architecture.

96 *Note: Unless otherwise indicated specifically or by context, the use of the term 'policy' or 'policies' in this*
97 *document may be understood as referencing laws, regulations, contractual terms and conditions, or*
98 *operational policies associated with the collection, use, transmission, sharing, cross-border transfers,*
99 *storage or disposition of personal information or personally identifiable information.*

100 While serving as an analytic tool, the PMRM also supports the design of a Privacy Architecture (PA) in
101 response to Use Cases and, as appropriate, for a particular operational environment. It also supports the
102 selection of integrated Services, their underlying Functionality and implementation Mechanisms that are
103 capable of executing Privacy Controls with predictability and assurance. Such an integrated view is
104 important, because business and policy drivers are now both more global and more complex and must
105 thus interact with many loosely coupled systems.

106 The PMRM therefore provides policymakers, the privacy office, privacy engineers, program and business
107 managers, system architects and developers with a tool to improve privacy management and compliance
108 in multiple jurisdictional contexts while also supporting delivery and business objectives. In this Model, the
109 Services associated with privacy (including Security) will be flexible, configurable and scalable and make
110 use of technical Functionality, Business Process and policy components. These characteristics require a
111 specification that is policy-configurable, since there is no uniform, internationally adopted privacy
112 terminology and taxonomy.

113 Analysis and documentation produced using the PMRM will result in a PMA that serves multiple
114 Stakeholders, including privacy officers and managers, general compliance managers, system
115 developers and even regulators in a detailed, comprehensive and integrated manner. The PMRM creates
116 an audit trail from Policy to Privacy Controls to Services and Functions to Mechanisms. This is a key
117 difference between the PMRM and a PIA.

118 There is an additional benefit. While other privacy instruments such as PIAs also serve multiple
119 Stakeholders, the PMRM does so in a way that is different from these others. Such instruments, while
120 nominally of interest to multiple Stakeholders, tend to serve particular groups. For example, PIAs are
121 often of most direct concern to privacy officers and managers, even though developers are often tasked
122 with contributing to them. Such privacy instruments also tend to change hands on a regular basis. As an
123 example, a PIA may start out in the hands of the development or project team, move to the privacy or
124 general compliance function for review and comment, go back to the project for revision, move back to
125 the privacy function for review, and so on. This iterative process of successive handoffs is valuable, but
126 can easily devolve into a challenge and response dynamic that can itself lead to miscommunication and
127 misunderstandings. Typically PIA's do not trace compliance from Policies to Privacy Controls to Services
128 and Functions on to Mechanisms. Nor are they performed at a granular level.

129 In contrast, the resulting output of using the PMRM - the PMA - will have direct and ongoing relevance for
130 all Stakeholders and is less likely to suffer the above dynamic. This is because the PMA supports
131 productive interaction and collaboration among multiple communities. Although the PMA is fully and
132 continuously a part of each relevant community, each community draws its own meanings from it, based
133 on their needs and perspectives. As long as these meanings are not inconsistent across communities, the
134 PMA can act as a shared, yet heterogeneous, understanding. Thus, the PMA is accessible and relevant
135 to all Stakeholders, facilitating collaboration across relevant communities in a way that other privacy
136 instruments often cannot.

137 This multiple stakeholder capability is especially important today, given the growing recognition that
138 Privacy by Design principles and practices cannot be adopted effectively without a common, structured
139 protocol that enables the linkage of business requirements, policies, and technical implementations.

140 Finally, the PMA can also serve as an important artifact of accountability, in two ways. First, a rigorously
141 developed and documented PMA itself reveals all aspects of privacy management within a Domain or

142 Use Case, making clear the relationship between the Privacy Services, Functionality and Mechanisms in
143 place and their associated Privacy Controls and Policies. Second, in addition to proactively
144 demonstrating that Privacy Controls are in place and implemented via the PMA, the Services may also
145 include functionality that demonstrates accountability at a granular level. Such Functionality implemented
146 in Mechanisms confirms and reports that the Privacy Controls are correctly operating. Thus the privacy
147 office can demonstrate compliance on demand for both design and operational stages.

148 1.5 Target Audiences

149 The intended audiences of this document and expected benefits to be realized by each include:

- 150 • **Privacy and Risk Officers and Engineers** will gain a better understanding of the specific privacy
151 management environment for which they have compliance responsibilities as well as detailed policy
152 and operational processes and technical systems that are needed to achieve their organization's
153 privacy compliance objectives..
- 154 • **Systems/Business Architects** will have a series of templates for the rapid development of core
155 systems functionality, developed using the PMRM as a tool.
- 156 • **Software and Service Developers** will be able to identify what processes and methods are required
157 to ensure that PI is collected, stored, used, shared, transmitted, transferred across-borders, retained
158 or disposed in accordance with requisite privacy control requirements.
- 159 • **Public policy makers and business owners** will be able to identify any weaknesses or
160 shortcomings of current policies and use the PMRM to establish best practice guidelines where
161 needed. They will also have stronger assurance that the design of business systems and
162 applications, as well as their operational implementations, comply with privacy control requirements.

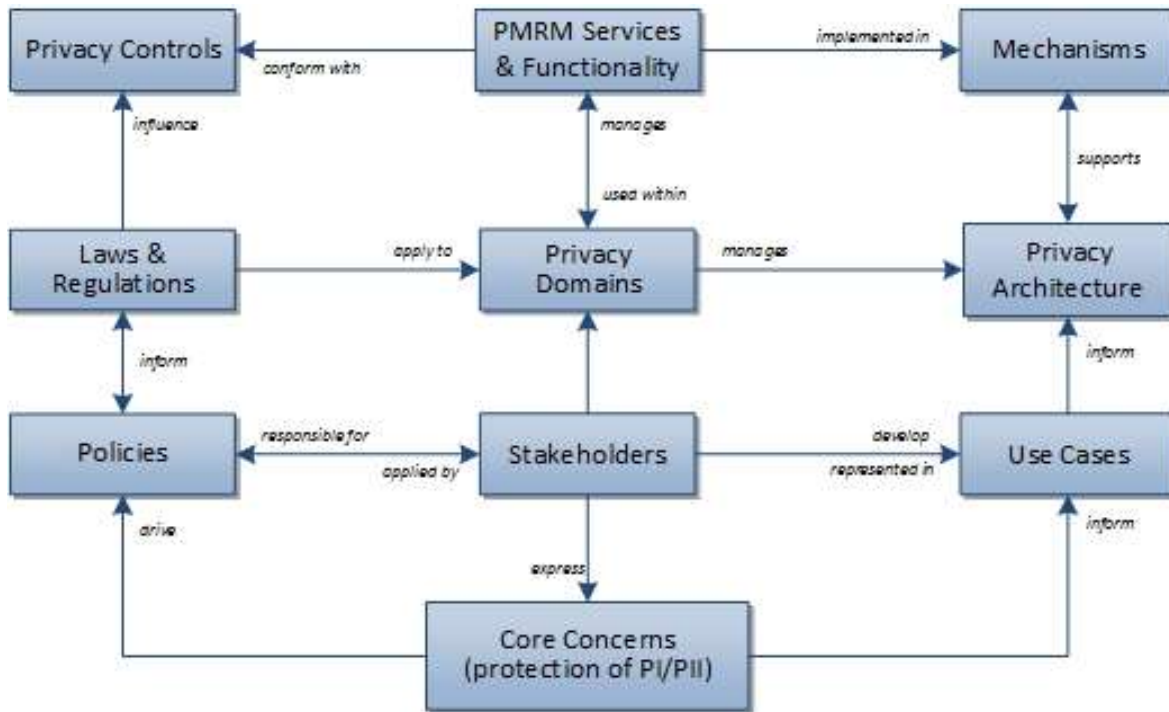
163 1.6 Specification Summary

164 The PMRM consists of:

- 165 • A conceptual model of privacy management, including definitions of terms;
- 166 • A methodology; and
- 167 • A set of operational Services and Functions, together with the inter-relationships among these three
168 elements.

169
170 **The PMRM, as a conceptual model**, addresses all Stakeholder-generated requirements, and is
171 anchored in the principles of Service-Oriented Architecture. It recognizes the value of services operating
172 across departments, systems and Domain boundaries. Given the reliance by the privacy policy
173 community (often because of regulatory mandates in different jurisdictions) on what on inconsistent, non-
174 standardized definitions of fundamental Privacy Principles, the PMRM includes a *non-normative*, working
175 set of *Operational* Privacy Principle definitions (see section 9.1). These definitions may be useful to
176 provide insight into the Model. With their operational focus, these working definitions are not intended to
177 supplant or to in any way suggest a bias for or against any specific policy or policy set. However, they
178 may prove valuable as a tool to help deal with the inherent biases built into current terminology
179 associated with privacy by abstracting specific operational features and assisting in their categorization.

180 In Figure 1 below we see that the core concern of privacy protection and management, is expressed by
181 Stakeholders (including data subjects, policy makers, solution providers, etc.) who help, on the one hand,
182 drive policies (which both reflect and influence actual regulation and lawmaking), and on the other hand,
183 inform the Use Cases that are developed to expose and document specific Privacy Control requirements
184 and the Services and Functions necessary to implement them in Mechanisms.



187 *Figure 1 – The PMRM Model - Achieving Comprehensive Operational Privacy*

189 **The PMRM, as a methodology** covers a series of tasks, outlined in the following sections of the
 190 document, concerned with:

- 191 • defining and describing the scope of the Use Cases, either broad or narrow;
- 192 • identifying particular business Domains and understanding the roles played by all participants and
 193 systems within the Domains in relation to privacy policies;
- 194 • identifying the data flows and Touch Points for all personal information within a Domain or Domains;
- 195 • specifying various Privacy Controls;
- 196 • identifying the Domains through which PI flows and which require the implementation of Privacy
 197 Controls;
- 198 • mapping Domains to the Services and Functions and then to technical and procedural Mechanisms;
- 199 • performing risk and compliance assessments;
- 200 • documenting the PMA for future iterations of this application of the PMRM, for reuse in other
 201 applications of the PMRM, and, potentially, to inform a Privacy Architecture.

202 The specification defines a set of Services and Functions deemed necessary to implement the
 203 management and compliance of detailed privacy policies and Privacy Controls within a particular Use
 204 Case. The Services are sets of Functions, which form an organizing foundation to facilitate the
 205 application of the model and to support the identification of the specific Mechanisms, which will implement
 206 them. They may optionally be incorporated in a broader Privacy Architecture.

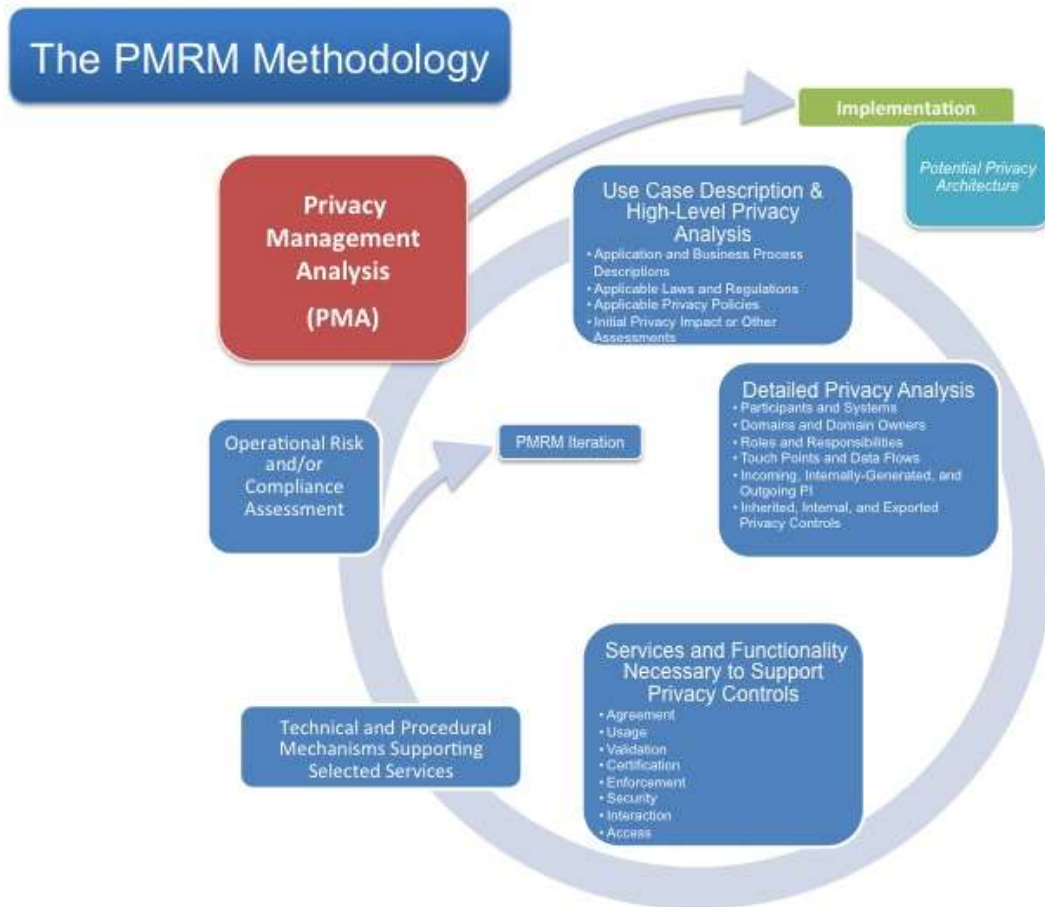
207 The set of operational Services (Agreement, Usage, Validation, Certification, Enforcement, Security,
 208 Interaction, and Access) is described in Section 4 below and in the Glossary in section 9.2.

209 The core of this specification is expressed in three major sections: Section 2, “Develop Use Case
 210 Description and High-Level Privacy Analysis,” Section 3, “Develop Detailed Privacy Analysis,” and
 211 Section 4, “Identify Services and Functions Necessary to Support Privacy Controls.” The detailed analysis
 212 is informed by the general findings associated with the high level analysis. However, it is much more
 213 granular and requires documentation and development of a Use Case which clearly expresses the
 214 complete application and/or business environment within which personal information is collected, stored,
 215 used, shared, transmitted, transferred across-borders, retained or disposed.

216 It is important to point out that the model is not generally prescriptive and that users of the PMRM may
 217 choose to adopt some parts of the model and not others. They may also address the tasks in a different
 218 order, appropriate to the context or to allow iteration and discovery of further requirements as work
 219 proceeds. Obviously, a complete use of the model will contribute to a more comprehensive PMA. As
 220 such, the PMRM may serve as the basis for the development of privacy-focused capability maturity
 221 models and improved compliance frameworks. As mentioned above, the PMRM may also provide a
 222 foundation on which to build Privacy Architectures.

223 Again, the use of the PMRM, for a particular business Use Case will lead to the production of a PMA. An
 224 organization may have one or more PMAs, particularly across different business units, or it may have a
 225 unified PMA. Theoretically, a PMA may apply across organizations, states, and even countries or other
 226 geo-political boundaries.

227 Figure 2 below shows the high-level view of the PMRM methodology that is used to create a PMA.
 228 Although the stages are sequenced for clarity, no step is an absolute pre-requisite for starting work on
 229 another step and the overall process will usually be iterative. Equally, the process of conducting an
 230 appropriate PMA, and determining how and when implementation will be carried out, may be started at
 231 any stage during the overall process.



232
 233 *Figure 2 - The PMRM Methodology*

234 **1.7 Terminology**

235 References are surrounded with [square brackets] and are in **bold** text.

236 The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD
 237 NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described
 238 in **[RFC2119]**.

239 A glossary of key terms used in this specification as well as non-normative definitions for Operational
240 Privacy Principles are included in Section 9 of the document.

241 We note that words and terms used in the discipline of data privacy in many cases have meanings and
242 inferences associated with specific laws, regulatory language, and common usage within privacy
243 communities. The use of such well-established terms in this specification is unavoidable. However, we
244 urge readers to consult the definitions in the Glossary and clarifications in the text to reduce confusion
245 about the use of such terms within this specification. Readers should also be aware that terms used in the
246 different examples are sometimes more “conversational” than in the formal, normative sections of the text
247 and may not necessarily be defined in the Glossary.

248 1.8 Normative References

249 [RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*,
250 <http://www.ietf.org/rfc/rfc2119.txt>, IETF RFC 2119, March 1997.

251 1.9 Non-Normative References

252 [SOA-RM] OASIS Standard, "Reference Model for Service Oriented Architecture 1.0", 12
253 October 2006. <http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.pdf>

254 [SOA-RAF] OASIS Specification, "Reference Architecture Foundation for SOA v1.0",
255 November 2012. [http://docs.oasis-open.org/soa-rm/soa-ra/v1.0/cs01/soa-ra-v1.0-
256 cs01.pdf](http://docs.oasis-open.org/soa-rm/soa-ra/v1.0/cs01/soa-ra-v1.0-cs01.pdf)

257 [PBD-SE] OASIS Committee Specification, "Privacy by Design Documentation for Software
258 Engineers Version 1.0." [http://docs.oasis-open.org/pbd-se/pbd-
259 se/v1.0/csd01/pbd-se-v1.0-csd01.pdf](http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/csd01/pbd-se-v1.0-csd01.pdf)

260 [NIST 800-53] NIST Special Publication 800-53 "Security and Privacy Controls for Federal
261 Information Systems and Organizations" Rev 4 (01-22-2015) – Appendix J:
262 Privacy Controls Catalog.
263 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

264 [ISTPA-OPER] International Security Trust and Privacy Alliance (ISTPA) publication, "Analysis of
265 Privacy Principles: Making Privacy Operational," v2.0 (2007). [https://www.oasis-
266 open.org/apps/org/workgroup/pmrm/download.php/55945/ISTPAAnalysisofPrivac
267 yPrinciplesV2.pdf](https://www.oasis-open.org/apps/org/workgroup/pmrm/download.php/55945/ISTPAAnalysisofPrivacyPrinciplesV2.pdf)

268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286

2 Develop Use Case Description and High-Level Privacy Analysis

The first phase in applying the PMRM methodology requires the scoping of the Use Case in which PI is associated - in effect, identifying the complete description in which the environment, application or capabilities where privacy and data protection requirements are applicable. The extent of the scoping analysis and the definitions of “business environment” or “application” are set by the Stakeholders using the PMRM within a particular Use Case. These may be defined broadly or narrowly, and may include lifecycle (time) elements.

The high level analysis may also make use of Privacy Impact Assessments, previous risk assessments, privacy maturity assessments, compliance reviews, and accountability model assessments as determined by Domain Stakeholders. However, the scope of the high level privacy analysis (including all aspects of the business environment or application under review and all relevant privacy policies) must correspond with the scope of analysis covered in Section 3, “Develop Detailed Privacy Use Case Analysis,” below.

Note, that the examples below refer to a detailed Use Case. The same methodology and model can be used at more abstract levels. Using the PMRM to study an entire business environment to develop Policies, Privacy Controls, Services and Functions, Mechanisms, a PMA and perhaps a Privacy Architecture allows an entity to establish broad guidance for use in future application of the PMRM in another, more-detailed Use Case.

2.1 Application and Business Process Descriptions

Task #1: Use Case Description

Objective Provide a general description of the Use Case

Task 1 Example²

A California electricity supplier (Utility), with a residential customer base with smart meters installed in homes, offers-reduced electricity rates for evening recharging of vehicles’ batteries. The utility also permits the customer to use the charging station at another customer’s site [such as at a friend’s house] and have the system bill the vehicle owner instead of the customer whose charging station is used.

Utility customers register with the utility to enable electric vehicle (EV) charging. An EV Customer (Customer One) plugs in the car at her residence, and the system detects the connection. The utility system is aware of the car’s location, its registered ID number and the approximate charge required (estimated by the car’s onboard computer). Based on Customer One’s preferences, the utility schedules the recharge to take place during the evening hours and at times determined by the utility (for load balancing).

The billing department system calculates the amount of money to charge Customer One, based on EV rates, time of charging, and duration of the charge.

The following week, Customer One drives to a friend’s home (Customer Two) and needs a quick charge of her vehicle’s battery. When she plugs her EV into Customer Two’s EV charger, the utility system detects Customer Two’s location, vehicle ID number, the fact that the EV is using Customer Two’s system, the date and time, Customer One’s preferences and other operational information...

The billing department system calculates the invoice amount to bill the EV Customer One, based on Customer One’s account information and preferences.

² The boxed examples are not to be considered as part of the normative text of this document.

309
310
311

The utility has a privacy policy that includes selectable options for customers relating to the use of PI associated with location and billing information, and has implemented systems to enforce those policies.

312 **Task #2: Use Case Inventory**

313 **Objective** Provide an inventory of the business environment, capabilities, applications and policy
314 environment under review at the level of granularity appropriate for the analysis covered
315 by the PMRM and define a High Level Use Case, which will guide subsequent analysis.
316 In order to facilitate the analysis described in the Detailed Privacy Use Case Analysis in
317 Section 3, the components of this Use Case inventory should align as closely as possible
318 with the components that will be analyzed in the corresponding Detailed Privacy Use
319 Case Analysis in Section 4.

320 **Note** *The inventory can include organizational structures, applications and Business
321 Processes; products; policy environment; legal and regulatory jurisdictions; Systems
322 supporting the capabilities and applications; PI; time; and other factors impacting the
323 collection, storage, usage, sharing, transmitting, transferred across-borders, retained or
324 disposed of PI. The inventory should also include the types of data subjects covered by
325 the Use Case together with specific privacy options (such as policy preferences, privacy
326 settings, etc. if these are formally expressed) for each type of data subject.*

327 **Task 2 Example**

328 Systems: Utility Communications Network, Customer Billing System, EV On Board System...

329 Legal and Regulatory Jurisdictions:

330 California Constitution, Article 1, section 1 gives each citizen an "inalienable right" to
331 pursue and obtain "privacy."

332 Office of Privacy Protection - California Government Code section 11549.5.

333 Automobile Black Boxes" - Vehicle Code section 9951.

334 ...

335 Personal Information Collected on Internet:

336 Government Code section 11015.5. This law applies to state government agencies...

337 The California Public Utilities Commission, which "serves the public interest by protecting
338 consumers and ensuring the provision of safe, reliable utility service and infrastructure at
339 reasonable rates, with a commitment to environmental enhancement and a healthy
340 California economy"...

341 Utility Policy: The Utility has a published Privacy Policy covering the EV recharging/billing application

342 Customer: The customer's selected settings for policy options presented via customer-facing
343 interfaces.

344 **2.2 Applicable Privacy Policies**

345 **Task #3: Privacy Policy Conformance Criteria**

346 **Objective** Define and describe the criteria for conformance of the organization or a System or
347 Business Process (identified in the Use Case and inventory) with an applicable Privacy
348 Policy or policies. As with the inventory described in Task #2 above, the conformance
349 criteria should align with the equivalent elements in the Detailed Use Case Analysis
350 described in Section 3. Wherever possible, they should be grouped by the relevant
351 Operational Privacy Principles and required Privacy Controls.

352 **Note** *Whereas Task #2 itemizes the environmental elements relevant to the Use Case, Task #
353 3 focuses on the privacy requirements specifically.*

354
355
356
357
358
359
360
361

Task 3 Example
Privacy Policy Conformance Criteria:
(1) Ensure that the utility does not share PI with third parties without the customer's consent...etc. For example a customer may choose to not share their charging location patterns
(2) Ensure that the utility supports strong levels of:
 (a) Identity authentication
 (b) Security of transmission between the charging stations and the utility information systems...etc.
(3) Ensure that PI is deleted on expiration of retention periods...

362

2.3 Initial Privacy Impact (or other) Assessment(s) [optional]

363

Task #4: **Assessment Preparation**

364
365
366
367

Objective Include, or prepare, an initial Privacy Impact Assessment, or as appropriate, a risk assessment, privacy maturity assessment, compliance review, or accountability model assessment applicable to the Use Case. Such an assessment can be deferred until a later iteration step (see Section 7) or inherited from a previous exercise.

368
369
370
371
372
373
374
375
376
377

Task 4 Example
Since the EV has a unique ID, it can be linked to a specific customer. As such, customer's whereabouts may be revealed and tracked through utility transaction's systems.
The EV charging and vehicle management systems may retain data, which can be used to identify charging time and location information that can constitute PI (including driving patterns).
Unless safeguards are in place and (where appropriate) under the customer's control, there is a danger that intentionally anonymized PI nonetheless becomes PII.
The utility may build systems to capture behavioral and movement patterns and sell this information to potential advertisers or other information brokers to generate additional revenue. The collection and use of such information requires the explicit, informed consent of the customer.

378 **3 Develop Detailed Privacy Analysis**

379 **Goal** Prepare and document a detailed PMA of the Use Case, which corresponds with the
380 High Level Privacy Analysis and the High Level Use Case Description.
381 The Detailed Use Case must be clearly bounded and must include the components in the
382 following sections.

383 **3.1 Identify Participants and Systems, Domains and Domain Owners,** 384 **Roles and Responsibilities, Touch Points and Data Flows (Tasks # 5-** 385 **10)**

386 **Task #5: Identify Participants**

387 **Objective** Identify Participants having operational privacy responsibilities.
388 A Participant is any Stakeholder responsible for collecting, storing, using, sharing,
389 transmitting, transferring across-borders, retaining or disposing PI, or is involved in the
390 lifecycle of PI managed by a Domain, or a System or Business Process within a Domain.

392 **Task 5 Example**

393 *Participants Located at the Customer Site:*

394 Registered Customers (Customers One and Two)

395 *Participants Located at the EV's Location:*

396 Registered Customer Host (Customer Two - Temporary host for EV charging), Customer One -
397 Registered Customer Guest

398 *Participants Located within the Utility's Domain:*

399 Service Provider (Utility)

400 Contractors and Suppliers to the Utility

401 **Task #6: Identify Systems and Business Processes**

402 **Objective** Identify the Systems and Business Processes where PI is collected, stored, used,
403 shared, transmitted, transferred across-borders, retained or disposed within a Domain.

404 **Definition** For purposes of this specification, a System or Business Process is a collection of
405 components organized to accomplish a specific function or set of functions having a
406 relationship to operational privacy management.

407 **Task 6 Example**

408 *System Located at the Customer Site(s):*

409 Customer Communication Portal

410 EV Physical Re-Charging and Metering System

411 *System Located in the EV(s):*

412 EV: Device

413 EV On-Board System

414 *System Located within the EV Manufacturer's Domain:*

415 EV Charging Data Storage and Analysis System

416 *System Located within the Utility's Domain:*

- 417 EV Program Information System (includes Rates, Customer Charge Orders, Customers enrolled
- 418 in the program, Usage Info etc.)
- 419 EV Load Scheduler System
- 420 Utility Billing System
- 421 Remote Charge Monitoring System
- 422 Selection System for selecting and transferring PI to the third party

423 **Task #7: Identify Domains and Owners**

424 **Objective** Identify the Domains included in the Use Case definition together with the respective
 425 Domain Owners.

426 **Definition** A Domain includes both physical areas (such as a customer site or home, a customer
 427 service center, a third party service provider) and logical areas (such as a wide-area
 428 network or cloud computing environment) that are subject to the control of a particular
 429 Domain owner.

430 A Domain Owner is the Participant responsible for ensuring that Privacy Controls are
 431 implemented in Services and Functions within a given Domain.

432 **Note** *Domains may be under the control of Data Subjects or Participants with a specific
 433 responsibility for privacy management within a Domain, such as data controllers;
 434 capability providers; data processors; and other distinct entities having defined
 435 operational privacy management responsibilities. Domains can be "nested" within wider,
 436 hierarchically-structured Domains, which may have their own defined ownership, roles
 437 and responsibilities. Individual data subjects may also have Domain Owner characteristics
 438 and obligations depending on the specific Use Case.*

439 *Domain Owner identification is important for purposes of establishing accountability.*

440 **Task 7 Example**

441 *Utility Domain:*

442 The physical premises, located at... which includes the Utility's program information system, load
 443 scheduling system, billing system, remote monitoring system and the selection system

444 This physical location is part of a larger logical privacy Domain, owned by the Utility and extends
 445 to the Customer Portal Communication system at the Customer's site, and the EV On-Board
 446 Metering software application System installed in the EV by the Utility, together with cloud-based
 447 services hosted by....

448 *Customer Domain:*

449 The physical extent of the customer's home and associated property as well as the EV, wherever
 450 located, together with the logical area covered by devices under the ownership and control of the
 451 customer (such as mobile devices).

452 *Vehicle Domain:*

453 The Vehicle Management System, installed in the EV by the manufacturer.

454 *Ownership*

455 The Systems listed above as part of the Utility's Systems belong to the Utility Domain Owner

456
 457 The EV Vehicle Management System belongs to the Customer Domain Owner but is controlled
 458 by the Vehicle Manufacturer

459 The EV (with its ID Number) belongs to the Customer Domain Owner and the Vehicle
 460 Manufacturer Domain Owners, but the EV ID may be accessed by the Utility.

461 **Task #8: Identify Roles and Responsibilities within a Domain**

462 **Objective** For any given Use Case, identify the roles and responsibilities assigned to specific
463 Participants, Business Processes and Systems within a specific Domain

464 **Note** *Any Participant may carry multiple roles and responsibilities and these need to be
465 distinguishable, particularly as many functions involved in processing of PI are assigned
466 to functional roles, with explicit authority to act, rather than to a specific Participant.*

467 **Task 8 Example**

468 **Role:** EV Manufacturer Privacy Officer

469 **Responsibilities:** Ensure that all PI data flows from EV On-Board System that communicate with or
470 utilize the Vehicle Management System conform with contractual obligations
471 associated with the Utility and vehicle owner as well as the Collection Limitation and
472 Information Minimization privacy policies.

473 **Role:** Utility Privacy Officer

474 **Responsibilities** Ensure that the PI data flows shared with the Third Party Marketing Domain are
475 done so according to the customer's permissions and that the Third Party
476 demonstrates the capability to enforce agreed upon privacy management obligations

477 **Task #9: Identify Touch Points**

478 **Objective** Identify the Touch Points at which the data flows intersect with Domains or Systems or
479 Business Processes within Domains.

480 **Definition** Touch Points are the intersections of data flows across Domains or Systems or
481 Processes within Domains.

482 **Note** *The main purpose for identifying Touch Points in the Use Case is to clarify the data flows
483 and ensure a complete picture of all Domains and Systems and Business Processes in
484 which PI is used.*

485 **Task 9 Example**

486 The Customer Communication Portal provides an interface through which the Customer communicates
487 a charge order to the Utility. This interface is a touch point.

488 When Customer One plugs her EV into the charging station, the EV On-Board System embeds
489 communication functionality to send EV ID and EV Charge Requirements to the Customer
490 Communication Portal. This functionality provides a further touch point.

491 **Task #10: Identify Data Flows**

492 **Objective** Identify the data flows carrying PI and Privacy Controls among Domains within the Use
493 Case.

494 Data flows may be multidirectional or unidirectional.

495 **Task 10 Example**

496 When a charging request event occurs, the Customer Communication Portal sends Customer
497 information, EV identification, and Customer Communication Portal location information to the EV
498 Program Information System managed by the Utility.

499 This Program Information System application uses metadata tags to indicate whether or not customer's
500 identification and location data may be shared with authorized third parties, and to prohibit the sharing
501 of data that provides customers' movement history, if derived from an aggregation of transactions.

502 3.2 Identify PI in Use Case Domains and Systems

503 **Objective** Specify the PI collected, stored, used, shared, transmitted, transferred across-borders,
504 retained or disposed within Domains or Systems or Business Processes in three
505 categories, (Incoming, Internally-Generated and Outgoing)

506 Task #11: Identify Incoming PI

507 **Definition** Incoming PI is PI flowing into a Domain, or a System or Business Process within a
508 Domain.

509 **Note** *Incoming PI may be defined at whatever level of granularity appropriate for the scope of*
510 *analysis of the Use Case and its Privacy Policies and requirements.*

511 Task #12: Identify Internally Generated PI

512 **Definition** Internally Generated PI is PI created within the Domain or System or Business Process
513 itself.

514 **Note** *Internally Generated PI may be defined at whatever level of granularity appropriate for*
515 *the scope of analysis of the Use Case and its Privacy Policies and requirements.*

516 *Examples include device information, time-stamps, location information, and other*
517 *system-generated data that may be linked to an identity.*

518 Task #13: Identify Outgoing PI

519 **Definition** Outgoing PI is PI flowing from one System to another, or from one Business Process to
520 another, either within a Domain or to another Domain.

521 Note: Outgoing PI may be defined at whatever level of granularity appropriate for the
522 scope of analysis of the Use Case and its Privacy Policies and requirements.

523 Tasks 11, 12, 13 Example

524 *Incoming PI:*

525 Customer ID received by Customer Communications Portal

526 *Internally Generated PI:*

527 Current EV location associated with customer information, and time/location information logged
528 by EV On-Board system

529 *Outgoing PI:*

530 Current EV ID and location information transmitted to Utility Load Scheduler System

531 3.3 Specify Required Privacy Controls Associated with PI

532 **Goal** For Incoming, Internally Generated and Outgoing PI, specify the Privacy Controls
533 required to enforce the privacy policy associated with the PI. Privacy controls may be pre-
534 defined or may be derived.

535 **Definition** Control is a process designed to provide reasonable assurance regarding the
536 achievement of stated objectives.

537 **Definition** Privacy Controls are administrative, technical and physical requirements employed within
538 an organization or Domain in order to protect and manage PI. They express how privacy
539 policies must be satisfied in an operational setting.

540 Task #14: Specify Inherited Privacy Controls

541 **Objective** Specify the required Privacy Controls that are inherited from Domains or Systems or
542 Processes.

543
544
545
546
547
548
549
550
551
552
553
554
555

Task 14 Example:

The utility inherits a Privacy Control associated with the Electric Vehicle’s ID (EVID) from the vehicle manufacturer’s privacy policies.

The utility inherits Customer One’s Operational Privacy Control Requirements, expressed as privacy preferences, via a link with the customer communications portal when she plugs her EV into Customer Two’s charging station.

The utility must apply Customer One’s privacy preferences to the current transaction. The Utility accesses Customer One’s privacy preferences and learns that Customer One does not want her association with Customer Two exported to the Utility’s third party partners. Even though Customer Two’s privacy settings differ regarding his own PI, Customer One’s non-consent to the association being transmitted out of the Utility’s privacy Domain is sufficient to prevent commutative association. Similarly, if Customer Two were to charge his car’s batteries at Customer One’s location, the association between them would also not be shared with third parties.

556 **Task #15: Specify Internal Privacy Controls**

557 **Objective** Specify the Privacy Controls that are mandated by internal Domain Policies.

558
559
560
561
562
563
564
565
566

Task 15 Example

Use Limitation Internal Privacy Controls

The Utility has adopted and complies with California Code SB 1476 of 2010 (Public Utilities Code §§ 8380-8381 Use Limitation).

It also implements the 2011 California Public Utility Commission (CPUC) privacy rules, recognizing the CPUC’s regulatory privacy jurisdiction over it and third parties with which it shares customer data.

Further, it adopts NIST 800-53 Appendix J’s “Control Family” on Use Limitation – e.g. it evaluates any proposed new instances of sharing PI with third parties to assess whether they are authorized and whether additional or new public notice is required.

567 **Task #16: Specify Exported Privacy Controls**

568 **Objective** Specify the Privacy Controls that must be exported to other Domains or to Systems or
569 Business Processes within Domains.

570
571
572
573
574

Task 16 Example

The Utility exports Customer One’s privacy preferences associated with her PI to its third party partner, whose systems are capable of understanding and enforcing these preferences. One of her Privacy Control requirements is to *not* share her EVID and any PI associated with the use of the Utility’s vehicle charging system with marketing aggregators or advertisers.

575
576
577
578
579
580
581
582
583
584
585
586

4 Identify Services and Functions Necessary to Support Privacy Controls

Privacy Controls are usually stated in the form of a policy declaration or requirement and not in a way that is immediately actionable or implementable. Until now, we have been concerned with the real-world, human side of privacy but we need now to turn attention to the procedures, business processes and technical system-level, components that actually enable privacy. Services and their associated Functions provide the bridge between Privacy Controls and a privacy management implementation by instantiating business and system-level actions governing PI.

Note: The PMRM provides only a high level description of the functionality associated with each Service. A well-developed PMA will provide the detailed functional requirements associated with Services within a specific Use Case.

4.1 Services and Functions Needed to Implement the Privacy Controls

A set of operational Services and associated Functionality comprise the organizing structure that will be used to establish the linkage between the required Privacy Controls and the operational Mechanisms (both manual and automated) that are necessary to implement those requirements.

PMRM identifies eight Privacy Services, necessary to support any set of privacy policies and Controls, at a *functional level*. The eight Services can be logically grouped into three categories:

- **Core Policy:** Agreement, Usage
- **Privacy Assurance:** Validation, Certification, Enforcement, Security
- **Presentation and Lifecycle:** Interaction, Access

These groupings, illustrated in Table 1 below, are meant to clarify the “architectural” relationship of the Services in an operational design. However, the functions provided by all Services are available for mutual interaction without restriction.

600

Core Policy Services	Privacy Assurance Services		Presentation & Lifecycle Services
Agreement	Validation	Certification	Interaction
Usage	Enforcement	Security	Access

601
602

603
604

Table 1

A privacy engineer, system architect or technical manager must be able to define these privacy Services and Functions, and deliver them via procedural and technical Mechanisms. In fact, an important benefit of using the PMRM is to stimulate design and analysis of the specific Mechanisms - both manual and automated - that are needed to implement any set of privacy policies and Controls and their associated Services and Functions. In that sense, the PMRM can be a valuable tool for fostering privacy innovation.

610 The PMRM Services and Functions include important System and Business Process capabilities that are
 611 not described in privacy practices and principles. For example, functionality enabling the management of
 612 Privacy Policies and their associated Privacy Controls across integrated Systems is implied but not
 613 explicitly addressed in privacy principles. Likewise, interfaces and agency are not explicit in the privacy
 614 principles, but are necessary to make possible essential operational privacy capabilities.

615 Such inferred capabilities are necessary if information Systems and associated Business Processes are
 616 to be made “privacy-configurable and compliant” and to ensure accountability. Without them, enforcing
 617 privacy policies in a distributed, fully automated environment will not be possible; businesses, data
 618 subjects, and regulators will be burdened with inefficient and error-prone manual processing, inadequate
 619 privacy governance, compliance controls and reporting.

620 As used here,

- 621 - **Service** is defined as a collection of related Functions that operate for a specified purpose;
- 622 - **Actor** is defined as a human or a system-level, digital ‘proxy’ for either a (human) Participant, a (non-
 623 human) system-level process or other agent.

624 The eight privacy Services defined are **Agreement, Usage, Validation, Certification, Enforcement,**
 625 **Security, Interaction,** and **Access. These Services represent collections of functionality which**
 626 **make possible the delivery of Privacy Control requirements.** The Services are identified as part of the
 627 Use Case analysis. Practice with Use Cases has shown that the Services can, together, operationally
 628 encompass any arbitrary set of Privacy Control requirements.

629 One Service and its Functions may interact with one or more other Services and their Functions. In other
 630 words, Functions under one Service may “call” those under another Service (for example, “pass
 631 information to a new Function for subsequent action”). In line with principles of Service-Oriented
 632 Architecture (SOA)³, the Services can interact in an arbitrary, interconnected sequence to accomplish a
 633 privacy management task or set of privacy lifecycle policy and Control requirements. Use Cases will
 634 illustrate such interactions and their sequencing as the PMRM is used to instantiate a particular Privacy
 635 Control.

636 Table 2 below provides a description of each Service’s functionality and an informal definition of each
 637 Service:

SERVICE	FUNCTIONALITY	PURPOSE
AGREEMENT	Defines and documents permissions and rules for the handling of PI based on applicable policies, data subject preferences, and other relevant factors; provides relevant Actors with a mechanism to negotiate, change or establish new permissions and rules; expresses the agreements such that they can be used by other Services	Manage and negotiate permissions and rules
USAGE	Ensures that the use of PI complies with the terms of permissions, policies, laws, and regulations, including PI subjected to information minimization, linking, integration, inference, transfer, derivation, aggregation, anonymization and disposal over the lifecycle of the PI	Control PI use
VALIDATION	Evaluates and ensures the information quality of PI in terms of accuracy, completeness, relevance, timeliness, provenance, appropriateness for use and other relevant qualitative factors	Ensure PI quality
CERTIFICATION	Ensures that the credentials of any Actor, Domain, System, or system component are compatible with their assigned roles in processing PI and verifies their capability to support required Privacy Controls in compliance with defined policies and assigned roles.	Ensure appropriate privacy management credentials
ENFORCEMENT	Initiates monitoring capabilities to ensure the effective operation of all Services. Initiates response actions, policy execution, and recourse when audit controls and monitoring indicate operational faults and failures. Records and reports evidence of compliance to Stakeholders and/or regulators. Provides evidence necessary for	Monitor proper operation, respond to exception conditions and report on demand

³ See for example the [SOA-RM] and the [SOA-RAF]

	Accountability.	evidence of compliance where required for accountability
SECURITY	Provides the procedural and technical mechanisms necessary to ensure the confidentiality, integrity, and availability of PI; makes possible the trustworthy processing, communication, storage and disposition of PI; safeguards privacy operations	Safeguard privacy information and operations
INTERACTION	Provides generalized interfaces necessary for presentation, communication, and interaction of PI and relevant information associated with PI, encompassing functionality such as user interfaces, system-to-system information exchanges, and agents	Information presentation and communication
ACCESS	Enables Data Subjects, as required and/or allowed by permission, policy, or regulation, to review their PI that is held within a Domain and propose changes, corrections or deletion for their PI	View and propose changes to PI

638 *Table 2*

639 **4.2 Service Details and Function Descriptions**

640 **4.2.1 Core Policy Services**

641 **1. Agreement Service**

- 642 • Defines and documents permissions and rules for the handling of PI based on applicable policies, individual preferences, and other relevant factors. Provides relevant Actors with a mechanism to negotiate or establish new permissions and rules
- 643
- 644
- 645 • Expresses the Agreements for use by other Services

646 **Agreement Service Example**

647 As part of its standard customer service agreement, the Utility requests selected customer PI, with
648 associated permissions for use. Customer negotiates with the Utility (in this case via an electronic
649 interface providing opt-in choices) to modify the permissions. The Customer provides the PI to the
650 Utility, with the modified and agreed-to permissions. This agreement is recorded, stored in an
651 appropriate representation, and the customer provided a copy.

652 **2. Usage Service**

- 653 • Ensures that the use of PI complies with the terms of any applicable permission, policy, law or
654 regulation,
 - 655 ○ Including PI subjected to information minimization, linking, integration, inference, transfer,
656 derivation, aggregation, and anonymization,
 - 657 ○ Over the lifecycle of the PI

658 **Usage Service Example**

659 A third party has acquired specific PI from the Utility, consistent with contractually agreed permissions
660 for use. The third party has implemented technical functionality capable of enforcing the agreement
661 ensuring that the usage of the PI is consistent with these permissions.

662 **4.2.2 Privacy Assurance Services**

663 **3. Validation Service**

- 664 • Evaluates and ensures the information quality of PI in terms of accuracy, completeness,
665 relevance, timeliness and other relevant qualitative factors.

666
667
668

Validation Service Example

The Utility has implemented a system to validate the vehicle's VIN and onboard EV ID to ensure accuracy.

669
670
671
672
673
674

4. Certification Service

- Ensures that the credentials of any Actor, Domain, System, or system component are compatible with their assigned roles in processing PI
- Verifies that an Actor, Domain, System, or system component supports defined policies and conforms with assigned roles

675
676
677
678
679
680
681

Certification Service Example

The Utility operates a data linkage communicating PI and associated policies with the vehicle manufacturer business partner. The Privacy Officers of both companies ensure that their practices and technical implementations are consistent with their agreed privacy management obligations. Additionally, functionality has been implemented which enables the Utility's and the manufacturer's systems to communicate confirmation that updated software versions have been registered and support their agreed upon policies.

682
683
684
685
686
687
688

5. Enforcement Service

- Initiates monitoring capabilities to ensure the effective operation of all Services
- Initiates response actions, policy execution, and recourse when audit controls and monitoring indicate operational faults and failures
- Records and report evidence of compliance to Stakeholders and/or regulators
- Provides data needed to demonstrate accountability

689
690
691
692
693
694
695
696

Enforcement Service Example

The Utility's maintenance department forwards customer PI to a third party not authorized to receive the information. A routine audit by the Utility's privacy auditor reveals this unauthorized disclosure practice, alerting the Privacy Officer, who takes appropriate action. This action includes preparation of a Privacy Violation report, together with requirements for remedial action, as well as an assessment of the privacy risk following the unauthorized disclosure. The Utility's maintenance department keeps records that demonstrate that it only has forwarded customer PI to a third party based upon the agreements with its customers. Such a report may be produced on demand for Stakeholders and regulators.

697
698
699
700
701

6. Security Service

- Makes possible the trustworthy processing, communication, storage and disposition of privacy operations
- Provides the procedural and technical mechanisms necessary to ensure the confidentiality, integrity, and availability of PI

702
703
704
705
706

Security Service Example

PI is encrypted when communicated between the EV, the Utility's systems and when transmitting PI to its third party to ensure confidentiality.

Strong standards-based, identity, authentication and authorization management systems are implemented to conform to the Utility's data security policies.

707 **4.2.3 Presentation and Lifecycle Services**

708 **7. Interaction Service**

- 709 • Provides generalized interfaces necessary for presentation, communication, and interaction of PI
710 and relevant information associated with PI
- 711 • Encompasses functionality such as user interfaces, system-to-system information exchanges,
712 and agents

713

714 **Interaction Service Example:**

715 The Utility uses a Graphical User Interface (GUI) to communicate with customers, including presenting
716 privacy notices, associated with the EV Charging application, enabling access to PI disclosures, and
717 providing them with options to modify privacy preferences.

718 The Utility utilizes email alerts to notify customers when policies will be changed and uses postal mail to
719 confirm customer-requested changes.

720 **8. Access Service**

- 721 • Enables data-subjects, as required and/or allowed by permission, policy, or regulation, to review
722 their PI held within a Domain and proposes changes, corrections and/or deletions to it

723 **Access Service Example:**

724 The Utility has implemented an online service enabling customers to view the Utility systems that collect
725 and use their PI and to interactively manage their privacy preferences for those systems (such as EV
726 Charging) that they have opted to use. For each system, customers are provided the option to view
727 summaries of the PI collected by the Utility and to dispute and correct questionable information.

728 **4.3 Identify Services satisfying the Privacy Controls**

729 The Services defined in Section 4.1 encompass detailed Functions that are ultimately delivered via
730 Mechanisms (e.g. code, applications, or specific business processes). Such Mechanisms transform the
731 Privacy Controls of section 3.3 into an operational System. Since the detailed Use Case analysis focused
732 on the data flows (Incoming, Internally-Generated, Outgoing) between Systems (and/or Actors), the
733 Service selections should be on the same granular basis.

734 **Task #17: Identify the Services and Functions necessary to support**
735 **operation of identified Privacy Controls**

736 Perform this task for each data flow exchange of PI between Systems and Domains.

737 This detailed mapping of Privacy Controls with Services can then be synthesized into consolidated sets of
738 Service and Functions per Domain, System or business environment as appropriate for the Use Case.

739 On further iteration and refinement, the identified Services and Functions can be further delineated by the
740 appropriate Mechanisms.

741 **Task 17 Examples**

742 **1- “Log EV location” based upon**

- 743 **a) Internally Generated PI** (Current EV location logged by EV On-Board system)
- 744 **b) Outgoing PI** (Current EV location transmitted to Utility Load Scheduler System)

745

746 Convert to operational Services as follows:

747 **Usage** EV On-Board System checks that the reporting of a particular charging location has
748 been opted-in by EV owner per existing **Agreement**

749 **Interaction** Communication of EV Location Information to Utility Metering System
750 **Enforcement** Check that location data has been authorized by EV Owner for reporting and log the
751 action. Notify the Owner for each transaction.
752 **Usage** EV location data is linked to Agreements

753 **2 - "Transmit EV Location to Utility Load Scheduler System"**

754 **Interaction** Communication established between EV Location and ULSS
755 **Security** Authenticate the ULSS site; authorize the communication; encrypt the transmission
756 **Certification** ULSS checks the software version of the EV On-Board System to ensure its most
757 recent firmware update maintains compliance with negotiated information storage
758 privacy controls
759 **Validation** Check the location code and Validate the EV Location against customer- accepted
760 locations

761 **5 Define Technical and Procedural Mechanisms**
762 **Supporting Selected Services and Functions**

763 Each Service is composed of a set of Functions, which are delivered operationally by manual and
764 technical Mechanisms

765 The **Mechanism** step is critical because it requires the identification of specific procedures, applications,
766 technical and vendor solutions, code and other concrete tools that will actually make possible the delivery
767 of required Privacy Controls.

768 **5.1 Identify Mechanisms Satisfying the Selected Services and**
769 **Functions**

770 Up to this point in the PMRM methodology, the primary focus of the Use Case analysis has been on the
771 “what:” PI, policies, Privacy Controls, Services and their associated Functions. However, the PMRM
772 methodology also focuses on the “how” – the Mechanisms necessary to deliver the required functionality.

773 **Task #18: Identify the Mechanisms that Implement the Identified Services**
774 **and Functions**

775 **Examples**

776 **“Log EV Location”**

777 **Mechanism: Software Vendor’s DBMS is used as the logging mechanism, and includes active**
778 **data encryption and key management for security.**

779 **“Securely Transmit EV Location to Utility Load Scheduler System (ULSS)”**

780 Establish a TLS/SSL communication between EV Location and ULSS, including Mechanisms for
781 authentication of the source/destination and authorization of the access.

6 Perform Operational Risk and/or Compliance Assessment

Task #19: Conduct Risk Assessment

Objective Once the requirements in the Use Case have been converted into operational Services, Functions and Mechanisms, an overall risk assessment should be performed from an operational perspective.

Note *This risk assessment is operational – distinct from other risk assessments, such as the initial assessments leading to choice of privacy policies and selection of privacy controls. Additional controls may be necessary to mitigate risks within and across Services. The level of granularity is determined by the Use Case scope and should generally include operational risk assessments for the selected Services within the Use Case.*

Examples

“Log EV location”:

Validation EV On-Board System checks that location is not previously rejected by EV owner

Risk: On-board System has been corrupted

Enforcement If location is previously rejected, then notify the Owner and/or the Utility

Risk: On-board System not current

EV On-Board System logs the occurrence of the Validation for later reporting on request.

Risk: On-board System has inadequate storage for recording the data

Interaction Communicate EV Location to EV On-Board System

Risk: Communication link not available

Usage EV On-Board System records EV Location in secure storage, together with agreements

Risk: Security controls for On-Board System are compromised

“Transmit EV Location to Utility Load Scheduler System (ULSS)”:

Interaction Communication established between EV Location and ULSS

Risk: Communication link down

Security Authenticate the ULSS site; secure the transmission

Risk: ULSS site credentials are not current

Certification ULSS checks the credentials of the EV On-Board System

Risk: EV On-Board System credentials do not check

Validation Validate the EV Location against accepted locations

Risk: System cannot access accepted locations

Usage ULSS records the EV Location, together with agreements

Risk: Security controls for the ULSS are compromised

820

7 Initiate Iterative Process

821 **Goal** A 'first pass' through the Tasks above can be used to identify the scope of the Use Case
822 and the underlying privacy policies. Additional iterative passes would serve to refine the
823 Privacy Controls, Services and Functions, and Mechanisms. Later passes could serve to
824 resolve "TBD" sections that are important, but were not previously developed.

825 **Note** *Iterative passes through the analysis will almost certainly reveal additional, finer-grain*
826 *details. Keep in mind that the ultimate objective is to develop sufficient insight into the*
827 *Use Case to provide an operational, Service-based, solution.*

828 Task #20: **Iterate the analysis and refine**

829 Iterate the analysis in the previous sections, seeking further refinement and detail. Continually-iterate the
830 process, as desired, to further refine and detail.

831 8 Conformance

832 8.1 Introduction

833 The PMRM as a “model” is abstract. However, as a Methodology it is through the process of developing
834 a detailed Use Case and a PMA that important levels of detail emerge, enabling a complete picture of
835 how privacy risks and privacy requirements are being managed. As a Methodology the PMRM – richly
836 detailed and having multiple, iterative task levels - is intentionally open-ended and can help users build
837 PMAs at whatever level of complexity they require.

838 Using the PMRM, detailed privacy service profiles, sector-specific implementation criteria, and
839 interoperability testing, implemented through explicit, executable, and verifiable methods, can emerge
840 and may lead to the development of detailed compliance and conformance criteria.

841 In the meantime, the following statements indicate whether, and if so to what extent, each of the Tasks
842 outlined in Sections 2 to 7 above, are to be used in a target work product (such as a privacy analysis,
843 privacy impact assessment, privacy management framework, etc.) in order to claim conformance to the
844 PMRM, as currently-documented.

845 8.2 Conformance Statement

846 The terms “**MUST**”, “**REQUIRED**”, “**RECOMMENDED**”, and “**OPTIONAL**” are used below in conformance
847 with [RFC 2119].

848 Any work product claiming conformance with PMRM v2.0

- 849 1. **MUST** result from the documented performance of the Tasks outlined in Sections 2 to 7 above
850 and where,
851 2. Tasks #1-3, 5-18 are **REQUIRED**;
852 3. Tasks # 19 and 20 are **RECOMMENDED**;
853 4. Task #4 is **OPTIONAL**.

854 9 Operational Definitions for Privacy Principles and 855 Glossary

856 **Note: This section is for information and reference only. It is not part of the normative text of the**
857 **document**

858 As explained in the introduction, every specialized Domain is likely to create and use a Domain-specific
859 vocabulary of concepts and terms that should be used and understood in the specific context of that
860 Domain. PMRM is no different and this section contains such terms.

861 In addition, a number of “operational definitions” are included in the PMRM as an aid to support
862 development of the “Detailed Privacy Use Case Analysis” described in Section 4. Their use is completely
863 optional, but may be helpful in organizing privacy policies and controls where there are inconsistencies in
864 definitions across policy boundaries or where existing definitions do not adequately express the
865 operational characteristics associated with the Privacy Principles below.

866

867 These Operational Privacy Principles are intended support the Principles in the OASIS PbD-SE
868 Specification and may be useful in understanding the operational implications of Privacy Principles
869 embodied in international laws and regulations and adopted by international organizations

870 9.1 Operational Privacy Principles

871 The following 14 Operational Privacy Principles are composite definitions, intended to illustrate the
872 operational and technical implications of commonly accepted Privacy Principles. They were derived from
873 a review of international legislative and regulatory instruments (such as the U.S. Privacy Act of 1974 and
874 the EU Data Protection Directive) in the ISTPA document, “Analysis of Privacy Principles: Making Privacy
875 Operational,” v2.0 (2007). They have been updated slightly for use in the PMRM. These operational
876 Privacy Principles can serve as a sample set to assist privacy practitioners. They are “composite”
877 definitions because there is no single and globally accepted set of Privacy Principles and so each
878 definition includes the policy expressions associated with each term as found in all 14 instruments.

879 **Accountability**

880 Functionality enabling the ability to ensure and demonstrate compliance with privacy policies to the
881 various Domain Owners, Stakeholders, regulators and data subjects by the privacy program,
882 business processes and technical systems.

883 **Notice**

884 Functionality providing Information, in the context of a specified use and in an open and transparent
885 manner, regarding policies and practices exercised within a Domain including: definition of the
886 Personal Information collected; its use (purpose specification); its disclosure to parties within or
887 external to the Domain; practices associated with the maintenance and protection of the information;
888 options available to the data subject regarding the processor’s privacy practices; retention and
889 deletion; changes made to policies or practices; and other information provided to the data subject at
890 designated times and under designated circumstances.

891 **Consent and Choice**

892 Functionality enabling data subjects to agree to the collection and/or specific uses of some or all of
893 their PI either through an opt-in affirmative process, opt-out, or implied (not choosing to opt-out when
894 this option is provided). Such functionality may include the capability to support sensitive Information,
895 informed consent, choices and options, change of use consent, and consequences of consent denial.

896 **Collection Limitation and Information Minimization**

897 Functionality, exercised by the information processor, that limits the personal information collected,
898 processed, communicated and stored to the minimum necessary to achieve a stated purpose and,
899 when required, demonstrably collected by fair and lawful means.

900 **Use Limitation**

901 Functionality, exercised by the information processor, that ensures that Personal Information will not
902 be used for purposes other than those specified and accepted by the data subject or provided by law,
903 and not maintained longer than necessary for the stated purposes.

904 **Disclosure**

905 Functionality that enables the transfer, provision of access to, use for new purposes, or release in any
906 manner, of Personal Information managed within a Domain in accordance with notice and consent
907 permissions and/or applicable laws and functionality making known the information processor's
908 policies to external parties receiving the information.

909 **Access, Correction and Deletion**

910 Functionality that allows an adequately identified data subject to discover, correct or delete, Personal
911 Information managed within a Privacy Domain; functionality providing notice of denial of access;
912 options for challenging denial when specified; and "right to be forgotten" implementation.

913 **Security/Safeguards**

914 Functionality that ensures the confidentiality, availability and integrity of Personal Information
915 collected, used, communicated, maintained, and stored; and that ensures specified Personal
916 Information will be de-identified and/or destroyed as required.

917 **Information Quality**

918 Functionality that ensures that information collected and used is adequate for purpose, relevant for
919 purpose, accurate at time of use, and, where specified, kept up to date, corrected or destroyed.

920 **Enforcement**

921 Functionality that ensures compliance with privacy policies, agreements and legal requirements and
922 to give data subjects a means of filing complaints of compliance violations and having them
923 addressed, including recourse for violations of law, agreements and policies, with optional linkages to
924 redress and sanctions. Such Functionality includes alerts, audits and security breach management.

925 **Openness**

926 Functionality, available to data subjects, that allows access to an information processor's notice and
927 practices relating to the management of their Personal Information and that establishes the existence,
928 nature, and purpose of use of Personal Information held about the data subject.

929 **Anonymity**

930 Functionality that prevents data being collected or used in a manner that can identify a specific
931 natural person.

932 **Information Flow**

933 Functionality that enables the communication of personal information across geo-political jurisdictions
934 by private or public entities involved in governmental, economic, social or other activities in
935 accordance with privacy policies, agreements and legal requirements.

936 **Sensitivity**

937 Functionality that provides special handling, processing, security treatment or other treatment of
938 specified information, as defined by law, regulation or policy.

939 **9.2 Glossary**

940 *Note: This Glossary does not include the Operational Privacy Principles listed in Section 9.1 above. They*
941 *are defined separately given their composite formulation from disparate privacy laws and regulations*

942 **Access Service**

943 Enables Data Subjects, as required and/or allowed by permission, policy, or regulation, to review their
944 PI that is held within a Domain and propose changes, corrections or deletion for their PI

945 **Accountability**

946 Privacy principle intended to ensure that controllers and processors are more generally in control and

947 in the position to **ensure and demonstrate** compliance with privacy principles in practice. This may
948 require the inclusion of business processes and/or technical controls in order to ensure compliance
949 and provide evidence (such as audit reports) to demonstrate compliance to the various Domain
950 Owners, Stakeholders, regulators and data subjects.

951 **Agreement Service**

952 Defines and documents permissions and rules for the handling of PI based on applicable policies,
953 individual preferences, and other relevant factors Provide relevant Actors with a mechanism to
954 negotiate or establish new permissions and rules. Expresses the Agreements for use by other
955 Services.

956 **Actor**

957 A human or a system-level, digital 'proxy' for either a (human) Participant (or their delegate)
958 interacting with a system or a (non-human) in-system process or other agent.

959 **Audit Controls**

960 Processes designed to provide reasonable assurance regarding the effectiveness and efficiency of
961 operations and compliance with applicable policies, laws, and regulations..

962 **Business Process**

963 A business process is a collection of related, structured activities or **tasks** that produce a specific
964 service or product (serve a particular goal) for a particular customer or customers within a Use Case.
965 It may often be visualized as a **flowchart** of a sequence of activities with interleaving decision points
966 or as a process matrix of a sequence of activities with relevance rules based on data in the process.

967 **Certification Service**

968 Ensures that the credentials of any Actor, Domain, System, or system component are compatible with
969 their assigned roles in processing PI and verify their capability to support required Privacy Controls in
970 compliance with defined policies and assigned roles.

971 **Control**

972 A process designed to provide reasonable assurance regarding the achievement of stated policies,
973 requirements or objectives.

974 **Data Subject**

975 An identified or identifiable person to who the personal data relate.

976 **Domain**

977 A physical or logical area within the business environment or the Use Case that is subject to the
978 control of a Domain Owner(s).

979 **Domain Owner**

980 A Participant having responsibility for ensuring that Privacy Controls are implemented and managed
981 in business processes and technical systems in accordance with policy and requirements.

982 **Enforcement Service**

983 Initiates monitoring capabilities to ensure the effective operation of all Services. Initiates response
984 actions, policy execution, and recourse when audit controls and monitoring indicate operational faults
985 and failures. Records and reports evidence of compliance to Stakeholders and/or regulators.
986 Provides evidence necessary for Accountability.

987 **Exported Privacy Controls**

988 Privacy Controls which must be exported to other Domains or to Systems or Processes within
989 Domains

990 **Function**

991 Activities or processes within each Service intended to satisfy the Privacy Control

992 **Incoming PI**

993 PI flowing into a Domain, or a System or Business Process within a Domain.

- 994 **Inherited Privacy Controls**
- 995 Privacy Controls which are inherited from Domains, or Systems or Business Processes.
- 996 **Interaction Service**
- 997 Provides generalized interfaces necessary for presentation, communication, and interaction of PI and
- 998 relevant information associated with PI, encompassing functionality such as user interfaces, system-
- 999 to-system information exchanges, and agents.
- 1000 **Internally-Generated PI**
- 1001 PI created within the Domain, Business Process or System itself.
- 1002 **Internal Privacy Controls**
- 1003 Privacy Controls which are created within the Domain, Business Process or System itself.
- 1004 **Mechanism**
- 1005 The packaging and implementation of Services and Functions into manual or automated solutions
- 1006 called Mechanisms.
- 1007 **Monitor**
- 1008 To observe the operation of processes and to indicate when exception conditions occur.
- 1009 **Operational Privacy Principles**
- 1010 A non-normative composite set of Privacy Principle definitions derived from a review of a number of
- 1011 relevant international legislative and regulatory instruments. They are intended to illustrate the
- 1012 operational and technical implications of the principles.
- 1013 **Outgoing PI**
- 1014 PI flowing out of one system or business process to another system or business process within a
- 1015 Doman or to another Domain.
- 1016 **Participant**
- 1017 A Stakeholder creating, managing, interacting with, or otherwise subject to, PI managed by a System
- 1018 or business process within a Domain or Domains.
- 1019 **PI**
- 1020 Personal Information – any data that describes some attribute of, or that is uniquely associated with,
- 1021 a natural person.
- 1022 ***Note:** The PMRM uses this term throughout the document as a proxy for other terminology, such*
- 1023 *a PII, personal data, non-public personal financial information, protected health information,*
- 1024 *sensitive personal information*
- 1025 **PII**
- 1026 Personally-Identifiable Information – any (set of) data that can be used to uniquely identify a natural
- 1027 person.
- 1028 **Policy**
- 1029 Laws, regulations, contractual terms and conditions, or operational rules or guidance associated with
- 1030 the collection, use, transmission, storage or destruction of personal information or personally
- 1031 identifiable information
- 1032 **Privacy Architecture (PA)**
- 1033 An integrated set of policies, Controls, Services and Functions implemented in Mechanisms
- 1034 appropriate not only for a given Use Case resulting from use of the PMRM but applicable more
- 1035 broadly for future Use Cases
- 1036 **Privacy by Design (PbD)**
- 1037 Privacy by Design is an approach to [systems engineering](#) which takes [privacy](#) into account
- 1038 throughout the whole engineering process. The concept is an example of [value sensitive design](#), i.e.,
- 1039 to take human values into account in a well-defined matter throughout the whole process and may
- 1040 have been derived from this. The concept originates in a joint report on “[Privacy-enhancing](#)

1041 [technologies](#)” by a joint team of the Information and Privacy Commissioner of Ontario, Canada, the
1042 Dutch Data Protection Authority and the [Netherlands Organisation for Applied Scientific Research](#) in
1043 1995. (Wikipedia)

1044 **Privacy Control**

1045 An administrative, technical or physical safeguard employed within an organization or Domain in
1046 order to protect and manage PI.

1047 **Privacy Impact Assessment (PIA)**

1048 A Privacy Impact Assessment is a tool for identifying and assessing privacy risks throughout the
1049 development life cycle of a program or System.

1050 **Privacy Management**

1051 The collection of policies, processes and methods used to protect and manage PI.

1052 **Privacy Management Analysis (PMA)**

1053 Documentation resulting from use of the PMRM and that serves multiple Stakeholders, including
1054 privacy officers, engineers and managers, general compliance managers, and system developers

1055 **Privacy Management Reference Model and Methodology (PMRM)**

1056 A model and methodology for understanding and analyzing privacy policies and their management
1057 requirements in defined Use Cases; and for selecting the Services and Functions and packaging
1058 them into Mechanisms which must be implemented to support Privacy Controls.

1059 **Privacy Policy**

1060 Laws, regulations, contractual terms and conditions, or operational rules or guidance associated with
1061 the collection, use, transmission, trans-boarder flows, storage, retention or destruction of Personal
1062 Information or personally identifiable information.

1063 **Privacy Principles**

1064 Foundational terms which represent expectations, or high level requirements, for protecting personal
1065 information and privacy, and which are organized and defined in multiple laws and regulations, and in
1066 publications by audit and advocacy organizations, and in the work of standards organizations.

1067 **Service**

1068 A defined collection of related Functions that operate for a specified purpose. For the PMRM, the
1069 eight Services and their Functions, when selected, satisfy Privacy Controls.

1070 **Requirement**

1071 A requirement is some quality or performance demanded of an entity in accordance with certain fixed
1072 regulations, policies, controls or specified Services, Functions, Mechanisms or Architecture.

1073 **Security Service**

1074 Provides the procedural and technical mechanisms necessary to ensure the confidentiality, integrity,
1075 and availability of PI; makes possible the trustworthy processing, communication, storage and
1076 disposition of PI; safeguards privacy operations.

1077 **Stakeholder**

1078 An individual or organization having an interest in the privacy policies, privacy controls, or operational
1079 privacy implementation of a particular Use Case.

1080 **System**

1081 A collection of components organized to accomplish a specific function or set of functions having a
1082 relationship to operational privacy management.

1083 **Touch Point**

1084 The intersection of data flows with Actors, Systems or Processes within Domains.

1085 **Use Case**

1086 In software and systems engineering, a use case is a list of actions or event steps, typically
1087 defining the interactions between a role (known in the Unified Modeling Language as an *actor*)
1088 and a system, to achieve a goal. The actor can be a human, an external system, or time.

1089 **Usage Service**

1090 Ensures that the use of PI complies with the terms of permissions, policies, laws, and regulations,
1091 including PI subjected to information minimization, linking, integration, inference, transfer, derivation,
1092 aggregation, anonymization and disposal over the lifecycle of the PI.

1093 **Validation Service**

1094 Evaluates and ensures the information quality of PI in terms of accuracy, completeness, relevance,
1095 timeliness, provenance, appropriateness for use and other relevant qualitative factors.

1096

1097 **9.3 PMRM Acronyms**

1098	CPUC	California Public Utility Commission
1099	DBMS	Data Base Management System
1100	EU	European Union
1101	EV	Electric Vehicle
1102	GUI	Graphical User Interface
1103	IoT	Internet of Things
1104	NIST	National Institute of Standards and Technology
1105	OASIS	Organization for the Advancement of Structured Information Standards
1106	PA	Privacy Architecture
1107	PbD	Privacy by Design
1108	PbD-SE	Privacy by Design Documentation for Software Engineers
1109	PI	Personal Information
1110	PII	Personally Identifiable Information
1111	PIA	Privacy Impact Assessment
1112	PMA	Privacy Management Analysis
1113	PMRM	Privacy Management Reference Model and Methodology
1114	PMRM TC	Privacy Management Reference Model Technical Committee
1115	RFC	Request for Comment
1116	SOA	Service Oriented Architecture
1117	TC	Technical Committee
1118	ULSS	Utility Load Scheduler System
1119		

1120

Appendix A. Acknowledgments

1121 The following individuals have participated in the creation of this specification and are gratefully
1122 acknowledged:

1123 **PMRM V1.0 CS01 Participants:**

1124

1125 Peter F Brown, Individual Member
1126 Gershon Janssen, Individual Member
1127 Dawn Jutla, Saint Mary's University
1128 Gail Magnuson, Individual Member
1129 Joanne McNabb, California Office of Privacy Protection
1130 John Sabo, Individual Member
1131 Stuart Shapiro, MITRE Corporation
1132 Michael Willett, Individual Member

1133

1134 **PMRM V1.0 CS02 Participants:**

1135 Michele Drgon, Individual Member
1136 Gershon Janssen, Individual Member
1137 Dawn Jutla, Saint Mary's University
1138 Gail Magnuson, Individual Member
1139 Nicolas Notario O'Donnell
1140 John Sabo, Individual Member
1141 Michael Willett, Individual Member

1142