Privacy Management Reference Model and Methodology (PMRM) Version 1.0

Committee Specification 02

17 May 2016

Specification URIs

This version:

http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.pdf (Authoritative)
http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.html
http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.doc

Previous version:

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

Latest version:

http://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.pdf (Authoritative)
http://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.html
http://docs.oasis-open.org/pmrm/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. 17 May 2016. OASIS Committee Specification 02. http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.html. Latest version: http://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.html.

Notices

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

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.

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

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

1.2 Major Changes from PMRM V1.0 CS01

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

1.3 Context

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

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

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

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

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

1.4 Objectives and Benefits

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

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

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

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

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

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

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

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

Finally, the PMA can also serve as an important artifact of accountability, in two ways. First, a rigorously developed and documented PMA itself reveals all aspects of privacy management within a Domain or Use Case, making clear the relationship between the Privacy Services, Functionality and Mechanisms in place and their associated Privacy Controls and Policies. Second, in addition to proactively demonstrating that Privacy Controls are in place and implemented via the PMA, the Services may also include functionality that demonstrates accountability at a granular level. Such Functionality implemented in Mechanisms confirms and reports that the Privacy Controls are correctly operating. Thus the privacy office can demonstrate compliance on demand for both design and operational stages.

1.5 Target Audiences

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

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

1.6 Specification Summary

The PMRM consists of:

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

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

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

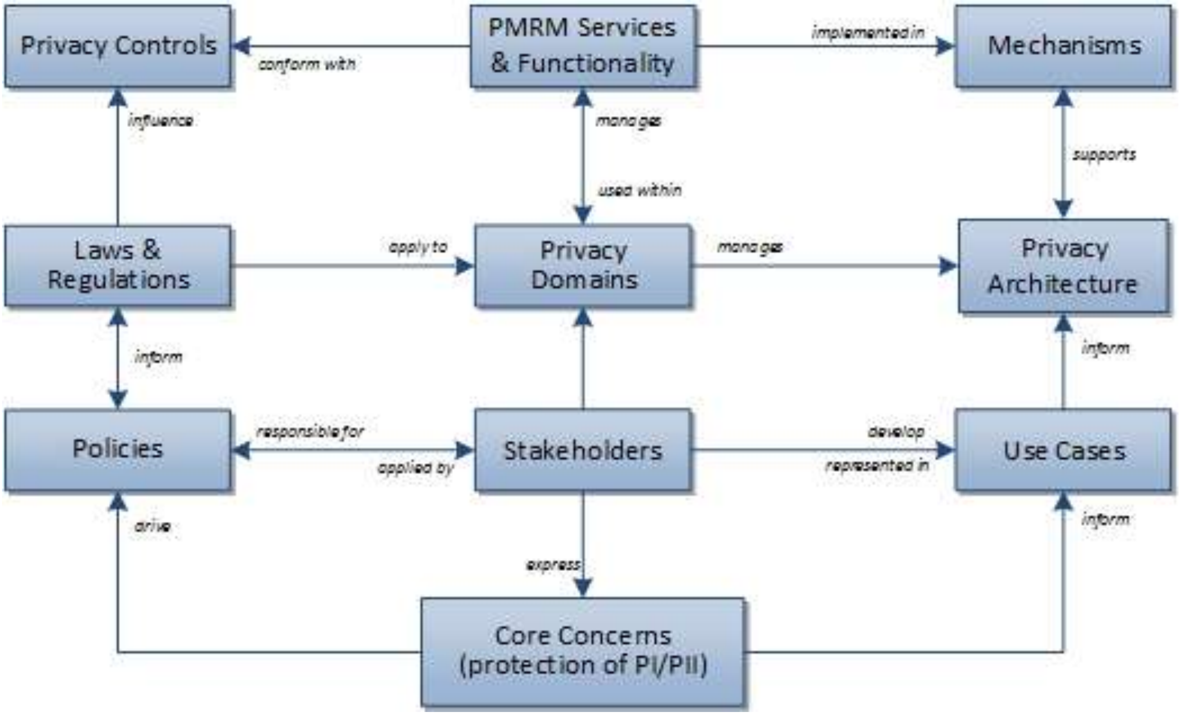

Figure 1 – The PMRM Model - Achieving Comprehensive Operational Privacy

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

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

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

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

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

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

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

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

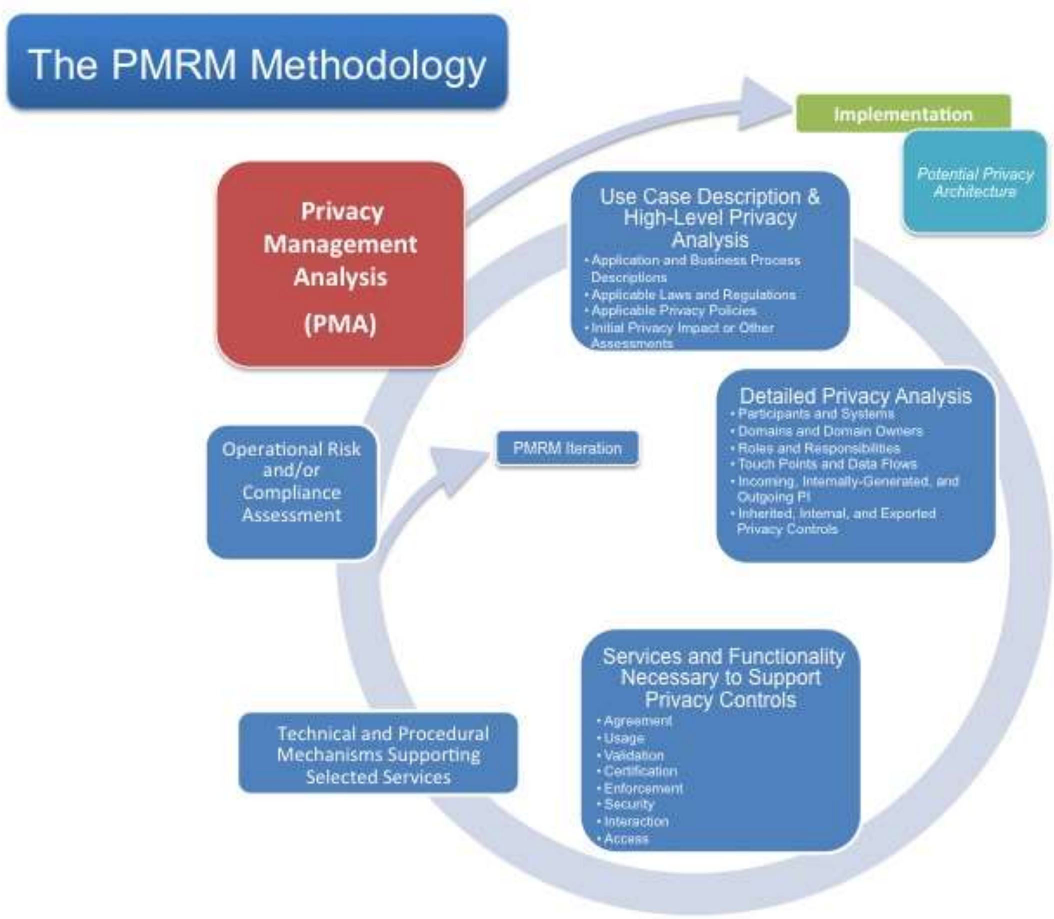
The PMRM Methodology
Implementation
Potential Privacy Architecture
Privacy Management Analysis (PMA)
Use Case Description & High-Level Privacy Analysis
• Application and Business Process Descriptions
• Applicable Laws and Regulations
• Applicable Privacy Policies
• Initial Privacy Impact or Other Assessments
Detailed Privacy Analysis
• Participants and Systems
• Domains and Domain Owners
• Roles and Responsibilities
• Touch Points and Data Flows
• Incoming, Internally-Generated, and Outgoing PI
• Inherited, Internal, and Exported Privacy Controls
PMRM Iteration
Operational Risk and/or Compliance Assessment
Services and Functionality Necessary to Support Privacy Controls
• Agreement
• Usage
• Validation
• Certification
• Enforcement
• Security
• Interaction
• Access
Technical and Procedural Mechanisms Supporting Selected Services

Figure 2 - The PMRM Methodology

1.7 Terminology

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

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

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

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

1.8 Normative References

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

1.9 Non-Normative References

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

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

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

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

[ISTPA-OPER] International Security Trust and Privacy Alliance (ISTPA) publication**,** "Analysis of Privacy Principles: Making Privacy Operational," v2.0 (2007). https://www.oasis-open.org/committees/download.php/55945/ISTPAAnalysisofPrivacyPrinciplesV2.pdf

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 Example[2]

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.

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

Task #2: Use Case Inventory

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

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

Task 2 Example

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

Legal and Regulatory Jurisdictions:

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

Office of Privacy Protection - California Government Code section 11549.5.

Automobile Black Boxes" - Vehicle Code section 9951.

…

Personal Information Collected on Internet:

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

The California Public Utilities Commission, which “serves the public interest by protecting consumers and ensuring the provision of safe, reliable utility service and infrastructure at reasonable rates, with a commitment to environmental enhancement and a healthy California economy”…

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

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

2.2 Applicable Privacy Policies

Task #3: Privacy Policy Conformance Criteria

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

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

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…

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

Task #4: Assessment Preparation

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.

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.

3 Develop Detailed Privacy Analysis

Goal Prepare and document a detailed PMA of the Use Case, which corresponds with the High Level Privacy Analysis and the High Level Use Case Description.

The Detailed Use Case must be clearly bounded and must include the components in the following sections.

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

Task #5: Identify Participants

Objective Identify Participants having operational privacy responsibilities.

A Participant is any Stakeholder responsible for collecting, storing, using, sharing, transmitting, transferring across-borders, retaining or disposing PI, or is involved in the lifecycle of PI managed by a Domain, or a System or Business Process within a Domain.

Task 5 Example

Participants Located at the Customer Site:

Registered Customers (Customers One and Two)

Participants Located at the EV's Location:

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

Participants Located within the Utility's Domain:

Service Provider (Utility)

Contractors and Suppliers to the Utility

Task #6: Identify Systems and Business Processes

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

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

Task 6 Example

System Located at the Customer Site(s):

Customer Communication Portal

EV Physical Re-Charging and Metering System

System Located in the EV(s):

EV: Device

EV On-Board System

System Located within the EV Manufacturer's Domain:

EV Charging Data Storage and Analysis System

System Located within the Utility's Domain:

EV Program Information System (includes Rates, Customer Charge Orders, Customers enrolled in the program, Usage Info etc.)

EV Load Scheduler System

Utility Billing System

Remote Charge Monitoring System

Selection System for selecting and transferring PI to the third party

Task #7: Identify Domains and Owners

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

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

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

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

Domain Owner identification is important for purposes of establishing accountability.

Task 7 Example

Utility Domain:

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

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

Customer Domain:

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

Vehicle Domain:

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

Ownership

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

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

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

Task #8: Identify Roles and Responsibilities within a Domain

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

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

Task 8 Example

Role: EV Manufacturer Privacy Officer

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

Role: Utility Privacy Officer

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

Task #9: Identify Touch Points

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

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

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

Task 9 Example

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

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

Task #10: Identify Data Flows

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

Data flows may be multidirectional or unidirectional.

Task 10 Example

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

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

3.2 Identify PI in Use Case Domains and Systems

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

Task #11: Identify Incoming PI

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

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

Task #12: Identify Internally Generated PI

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

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

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

Task #13: Identify Outgoing PI

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

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

Tasks 11, 12, 13 Example

Incoming PI:

Customer ID received by Customer Communications Portal

Internally Generated PI:

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

Outgoing PI:

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

3.3 Specify Required Privacy Controls Associated with PI

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

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

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

Task #14: Specify Inherited Privacy Controls

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

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.

Task #15: Specify Internal Privacy Controls

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

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.

Task #16: Specify Exported Privacy Controls

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

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.

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.

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

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.

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

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

As used here,

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

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

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

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

Table 2

4.2 Service Details and Function Descriptions

4.2.1 Core Policy Services

1. Agreement Service

- 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
- Expresses the Agreements for use by other Services

Agreement Service Example

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

2. Usage Service

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

Usage Service Example

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

4.2.2 Privacy Assurance Services

3. Validation Service

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

Validation Service Example

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

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

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.

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

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.

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

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.

4.2.3 Presentation and Lifecycle Services

7. Interaction Service

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

Interaction Service Example:

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

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

8. Access Service

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

Access Service Example:

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

4.3 Identify Services satisfying the Privacy Controls

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

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

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

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

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

Task 17 Examples

1- “Log EV location” based upon

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

Convert to operational Services as follows:

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

Interaction Communication of EV Location Information to Utility Metering System

Enforcement Check that location data has been authorized by EV Owner for reporting and log the action. Notify the Owner for each transaction.

Usage EV location data is linked to Agreements

2 - “Transmit EV Location to Utility Load Scheduler System”

Interaction Communication established between EV Location and ULSS

Security Authenticate the ULSS site; authorize the communication; encrypt the transmission

Certification ULSS checks the software version of the EV On-Board System to ensure its most recent firmware update maintains compliance with negotiated information storage privacy controls

Validation Check the location code and Validate the EV Location against customer- accepted locations

5 Define Technical and Procedural Mechanisms Supporting Selected Services and Functions

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

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

5.1 Identify Mechanisms Satisfying the Selected Services and Functions

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

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

Examples

"Log EV Location"

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

"Securely Transmit EV Location to Utility Load Scheduler System (ULSS)"

Establish a TLS/SSL communication between EV Location and ULSS, including Mechanisms for 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

7 Initiate Iterative Process

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

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

Task #20: Iterate the analysis and refine

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

8 Conformance

8.1 Introduction

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

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

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

8.2 Conformance Statement

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

Any work product claiming conformance with PMRM v2.0

1. **MUST** result from the documented performance of the Tasks outlined in Sections 2 to 7 above

and where,

2. Tasks #1-3, 5-18 are **REQUIRED**;
3. Tasks # 19 and 20 are **RECOMMENDED**;
4. Task #4 is **OPTIONAL**.

9 Operational Definitions for Privacy Principles and Glossary

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

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

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

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

9.1 Operational Privacy Principles

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

Accountability

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

Notice

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

Consent and Choice

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

Collection Limitation and Information Minimization

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

Use Limitation

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

Disclosure

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

Access, Correction and Deletion

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

Security/Safeguards

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

Information Quality

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

Enforcement

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

Openness

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

Anonymity

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

Information Flow

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

Sensitivity

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

9.2 Glossary

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

Access Service

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

Accountability

Privacy principle intended to ensure that controllers and processors are more generally in control and in the position to **ensure and demonstrate** compliance with privacy principles in practice. This may require the inclusion of business processes and/or technical controls in order to ensure compliance and provide evidence (such as audit reports) to demonstrate compliance to the various Domain Owners, Stakeholders, regulators and data subjects.

Agreement Service

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

Actor

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

Audit Controls

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

Business Process

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

Certification Service

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

Control

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

Data Subject

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

Domain

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

Domain Owner

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

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 reports evidence of compliance to Stakeholders and/or regulators. Provides evidence necessary for Accountability.

Exported Privacy Controls

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

Function

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

Incoming PI

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

Inherited Privacy Controls

Privacy Controls which are inherited from Domains, or Systems or Business Processes.

Interaction Service

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.

Internally-Generated PI

PI created within the Domain, Business Process or System itself.

Internal Privacy Controls

Privacy Controls which are created within the Domain, Business Process or System itself.

Mechanism

The packaging and implementation of Services and Functions into manual or automated solutions called Mechanisms.

Monitor

To observe the operation of processes and to indicate when exception conditions occur.

Operational Privacy Principles

A non-normative composite set of Privacy Principle definitions derived from a review of a number of relevant international legislative and regulatory instruments. They are intended to illustrate the operational and technical implications of the principles.

Outgoing PI

PI flowing out of one system or business process to another system or business process within a Doman or to another Domain.

Participant

A Stakeholder creating, managing, interacting with, or otherwise subject to, PI managed by a System or business process within a Domain or Domains.

PI

Personal Information – any data that describes some attribute of, or that is uniquely associated with, a natural person.

> ***Note:*** *The PMRM uses this term throughout the document as a proxy for other terminology, such a PII, personal data, non-public personal financial information, protected health information, sensitive personal information*

PII

Personally-Identifiable Information – any (set of) data that can be used to uniquely identify a natural person.

Policy

Laws, regulations, contractual terms and conditions, or operational rules or guidance associated with the collection, use, transmission, storage or destruction of personal information or personally identifiable information

Privacy Architecture (PA)

An integrated set of policies, Controls, Services and Functions implemented in Mechanisms appropriate not only for a given Use Case resulting from use of the PMRM but applicable more broadly for future Use Cases

Privacy by Design (PbD)

Privacy by Design is an approach to systems engineering which takes privacy into account throughout the whole engineering process. The concept is an example of value sensitive design, i.e., to take human values into account in a well-defined matter throughout the whole process and may have been derived from this. The concept originates in a joint report on "Privacy-enhancing technologies" by a joint team of the Information and Privacy Commissioner of Ontario, Canada, the Dutch Data Protection Authority and the Netherlands Organisation for Applied Scientific Research in 1995. (Wikipedia)

Privacy Control

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

Privacy Impact Assessment (PIA)

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

Privacy Management

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

Privacy Management Analysis (PMA)

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

Privacy Management Reference Model and Methodology (PMRM)

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

Privacy Policy

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

Privacy Principles

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

Service

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

Requirement

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

Security Service

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.

Stakeholder

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

System

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

Touch Point

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

Use Case

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

Usage Service

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.

Validation Service

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

9.3 PMRM Acronyms

CPUC	California Public Utility Commission
DBMS	Data Base Management System
EU	European Union
EV	Electric Vehicle
GUI	Graphical User Interface
IoT	Internet of Things
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
PA	Privacy Architecture
PbD	Privacy by Design
PbD-SE	Privacy by Design Documentation for Software Engineers
PI	Personal Information
PII	Personally Identifiable Information
PIA	Privacy Impact Assessment
PMA	Privacy Management Analysis
PMRM	Privacy Management Reference Model and Methodology
PMRM TC	Privacy Management Reference Model Technical Committee
RFC	Request for Comment
SOA	Service Oriented Architecture
TC	Technical Committee
ULSS	Utility Load Scheduler System

Appendix A. Acknowledgments

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

PMRM V1.0 CS01 Participants:

Peter F Brown, Individual Member
Gershon Janssen, Individual Member
Dawn Jutla, Saint Mary’s University
Gail Magnuson, Individual Member
Joanne McNabb, California Office of Privacy Protection
John Sabo, Individual Member
Stuart Shapiro, MITRE Corporation
Michael Willett, Individual Member

PMRM V1.0 CS02 Participants:

Michele Drgon, Individual Member
Gershon Janssen, Individual Member
Dawn Jutla, Saint Mary’s University
Gail Magnuson, Individual Member
Nicolas Notario O’Donnell
John Sabo, Individual Member
Michael Willett, Individual Member