89998966

Privacy Management Reference Model and Methodology (PMRM) Version 2.0

DRAFT Committee Specification 02

November 2015

Specification URIs

This 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>

Previous version:

<http://docs.oasis-open.org/pmrm/PMRM/v1.0/csprd02/PMRM-v1.0-csprd02.pdf> (Authoritative)

<http://docs.oasis-open.org/pmrm/PMRM/v1.0/csprd02/PMRM-v1.0-csprd02.html>

<http://docs.oasis-open.org/pmrm/PMRM/v1.0/csprd02/PMRM-v1.0-csprd02.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](http://www.oasis-open.org/committees/pmrm/)

Chairs:

John Sabo (john.annapolis@verizon.net), Individual

Michael Willett (mwillett@nc.rr.com), Individual

Editors:

Gail Magnuson (gail.magnuson@gmail.com), Individual

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

Michael Willett (mwillett@nc.rr.com), 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 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.

Technical Committee members should send comments on this specification to the Technical Committee’s email list. Others should send comments to the Technical Committee by using the “[Send A Comment](http://www.oasis-open.org/committees/comments/index.php?wg_abbrev=pmrm)” button on the Technical Committee’s web page at <http://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 Technical Committee web page (<http://www.oasis-open.org/committees/pmrm/ipr.php>).

Citation format:

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

[PMRM-v2.0]

*Privacy Management Reference Model and Methodology (PMRM) Version 1.0*. 03 July 2013. OASIS Committee Specification 01. <http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs01/PMRM-v1.0-cs01.html>.

Notices

Copyright © OASIS Open 2013. 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](http://www.oasis-open.org/policies-guidelines/ipr) 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](http://www.oasis-open.org/), 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 <http://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 6

 1.3 Context 7

 1.4 Objectives 7

 1.5 Target Audiences 8

 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 &Systems, Domains &Domain Owners, Roles &

 Responsibilities, Touch Points & Data Flows 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 20

 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

 Service Details and Function Descriptions 24

 4.1.1 Core Policy Services 24

 1. Agreement Service 24

 2. Usage Service 24

 4.1.2 Privacy Assurance Services 24

 3. Validation Service 24

 4. Certification Service 24

 5. Enforcement Service 25

 6. Security Service 25

 4.1.3 Presentation and Lifecycle Services 25

 7. Interaction Service 25

 8. Access Service 26

4.2 Identify Services satisfying the Privacy Controls 26

Task #17: Identify the Services and Functions necessary to support operation of identified Privacy Controls. 26

5 Define Technical and Procedural Mechanisms Supporting elected Services and Functions 28

5.1 Identify Mechanisms Satisfying the Selected Services and Functions 28

Task #18: Identify the Mechanisms that satisfy the selected Services and Functions 28

6 Perform Operational Risk and/or Compliance Assessment 29

Task #19: Conduct Risk Assessment 29

7 Initiate Iterative Process 30

Task #20: Iterate the analysis and refine. 30

8 Conformance 31

 8.1 Introduction 31

 8.2 Conformance Statement 31

9 Operational Definitions for Privacy Principles and Glossary 32

 9.1 Operational Privacy Principles 32

 9.2 Glossary 33

Appendix A. Acknowledgments 36

Appendix B. Revision History 37

# Introduction

## 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) across legal, regulatory and policy environments in these interconnected Domains. Additionally, in some jurisdictions, there is a distinction between ‘Personal Information’ (PI) and ‘Personally-Identifiable Information’ (PII) and in specific contexts, clear distinctions must be made explicitly between the two; however, for the purposes of this document, the term ‘PI’ will be used and is assumed to cover both. Section 9.2 Glossary addresses the distinctions between PI and PII.

The PMRM is a valuable tool that helps improve privacy management, compliance and accountability in IoT, Big Data, cloud computing, health and finance IT, smart grid, social networking, federated identity and similarly complex environments where the use of personal information is governed by laws, regulations, business contracts and operational policies, but where traditional enterprise-focused tools are inadequate. The PMRM is a valuable tool for those seeking to improve privacy management, compliance and accountability in their information systems and solutions - such as health IT, financial services, federated identity, social networks, mobile apps, cloud computing, Big Data, IoT etc. - where the use of Personal Information across the entire ecosystem is governed by laws, regulations, business contracts and operational policies, It also can be of particular value to business and program managers who need to understand the implications of privacy policies for specific business systems and to assess privacy management risks.

The PMRM is neither a static model nor a purely prescriptive set of rules (although it includes characteristics of both). 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 corporation. Using a comprehensive approach, the privacy office could establish broad Privacy Controls, design their Services and implement their underlying functionality in manual and technical Mechanisms – and these, in turn, would produce a high level Privacy Management Analysis (PMA) and could also inform a high-level Privacy Architecture. Both the Privacy Management Analysis 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 using the PMRM at the broadest level first is to inform the more-granular initiatives with guidance from a corporate perspective, potentially reducing the amount of work for the privacy office and engineers.

Even if the development of an overarching Privacy Management Analysis is not appropriate for an organization, the PMRM may also 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 which use PI.

## Major Changes from PMRM V1.0

This V 2.0 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, and improve the graphical figures used to illustrate the PMRM. 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.

## Context

Predictable and trusted privacy management must function within a complex, inter-connected set of networks, processes, systems, applications, devices, data, and associated governing policies. Such a privacy management capability is needed both 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 personal information (“PI”) and associated privacy policies. The PMRM supports this by producing a Privacy Management Analysis: mapping Policy to Privacy Controls to Services and Functions, which in turn are implemented via Mechanisms, both technical and procedural, .The Privacy Management Analysis 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 reuse the works from other applications of the PMRM 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 Privacy Management Analysis (PMA) for the particular Use Case.

## Objectives

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 policy, Domains, systems, and ownership boundaries. A PMRM-derived Privacy Management Analysis 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.

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 can also aid the design of a Privacy Architecture (PA) in response to Use Cases and, as appropriate, for a particular operational environment. It can also be used to help in the selection of integrated Services, their underlying functionality and implemented in 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.

In addition, multiple jurisdictions, inconsistent and often-conflicting laws, regulations, business practices, and consumer preferences, together create 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 important to note that 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 so 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.

The Privacy Management Reference Model and Methodology 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 Privacy Management Analysis (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 the PIA.

While other privacy instruments, such as privacy impact assessments (“PIAs”), also serve multiple Stakeholders, the PMRM does so in a way that is somewhat 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 from it their own meanings, 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.

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.

## 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 created and managed in accordance with requisite privacy provisions.
* **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.

## 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.



Figure – The PMRM Model - Achieving Comprehensive Operational Privacy

In Figure 1, 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.

**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 general reliance by the privacy policy community on non-uniform definitions of so-called “Privacy Principles”, a non-normative, working set of *operational* privacy policy definitions (see section 9.1) 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 and to abstract their operational features.

**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 Privacy Management Analysis 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.

The core of this specification is expressed in two normative sections: the High Level Privacy Analysis and the Detailed Privacy Management Reference Model Description. The Detailed PMRM Description section is informed by the general findings associated with the High Level Privacy Analysis. However, it is much more detail-focused 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, communicated, processed, stored, and 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.

Use of the PMRM, by and within a particular business Use Case, will lead to the production of a Privacy Management Analysis (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.

 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 Privacy Management Analysis, and determining how and when implementation will be carried out, may be started at any stage during the overall process.



Figure - The PMRM Methodology

## 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 operational definitions for sample Fair Information Practices/Principles (“FIPPs”) are included in Section 8 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..

## 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.

## 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>

[NIST 800-53] “Security and Privacy Controls for Federal Information Systems and Organizations – Appendix J: Privacy Controls Catalog”, NIST Special Publication 800-53 Draft Appendix J, July 2011.

# 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 the second phase, covered in Section 3, “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.

## Application and Business Process Descriptions

### Use Case Description

**Objective** Provide a general description of the Use Case

**Example[[1]](#footnote-1)**

A California utility, with a residential customer base with smart meters installed, wants to promote the increased use of electric vehicles in its service area by offering significantly-reduced electricity rates for evening recharging of vehicle battery. The system 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.

This Use Case involves utility customers who have registered with the utility to enable EV charging (EV customer). An EV customer plugs in the car at her residence and requests “charge at cheapest rates”. The utility is notified of the car’s presence, its ID number and the approximate charge required (provided by the car’s onboard computer). The utility schedules the recharge to take place during the evening hours and at times determined by the utility (thus putting diversity into the load).

The billing department calculates the amount of money to charge the EV customer, based on EV rates and the measured time period.

The same EV customer drives to a friend’s home (also a registered EV customer) and requests a quick charge to make sure that she can get back home. When she plugs her EV into her friend’s EV charger, the utility identifies the fact that the EV is linked to a different customer account than that of the site resident, and places the charging bill on the correct customer’s invoice.

The billing department now calculates the amount of money to invoice the customer who owns the EV, based on EV rates and for the measured time period.

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

### 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 4, the components of the inventory should align as closely as possible with the components that will be analyzed in the corresponding detailed Section 4 analysis.

**Context** The inventory can include organizational structures, applications and business processes; products; policy environment; legal and regulatory jurisdictions; systems supporting the capabilities and applications; data; time; and other factors impacting the collection, communication, processing, storage and disposition 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.

**Example**

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

Legal and Regulatory Jurisdictions:

 [California Constitution, Article 1, section 1](http://www.leginfo.ca.gov/.const/.article_1) gives each citizen an "inalienable right" to pursue and obtain "privacy."

 [Office of Privacy Protection - California Government Code section 11549.5](http://www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=11001-12000&file=11549.5-11549.10).

 [Automobile "Black Boxes" - Vehicle Code section 9951](http://www.leginfo.ca.gov/cgi-bin/displaycode?section=veh&group=09001-10000&file=9950-9955).

 …

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”…

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.

## Applicable Privacy Policies

### 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 Privacy Principles and expressed as Privacy Constraints.

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

**Example**

Privacy Policy Conformance Criteria:

(1) Ensure that the utility does not share data with third parties without the consumer’s consent…etc.

(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 personal data is deleted on expiration of retention periods…

…

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

### 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 within the scope of analysis carried out in sections 2.1 and 2.2 above. Such an assessment can be deferred until a later iteration step (see Section 4.3) or inherited from a previous exercise.

**Example**

Since the Electric Vehicle (EV) has a unique ID, it can be linked to a specific customer. As such, customer’s whereabouts may be tracked through utility transaction visibility.

The EV charging and vehicle management system may retain data, which can be used to identify charging and location patterns that can constitute PI.

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 wishes to capture behavioral and movement patterns and sell this information to potential advertisers or other information brokers to generate additional revenue. This information constitutes PII. The collection and use of this information requires the explicit, informed consent of the customer.

# Develop Detailed Privacy Analysis

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

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

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

### Identify Participants

**Objective** Identify Participants having operational privacy responsibilities.

**Definition** A “Participant” is any Stakeholder creating, managing, interacting with, or otherwise subject to, PI managed by a Domain or System within a Domain.

**Example**

*Participants Located at the Customer Site:*

 Registered Customer

*Participants Located at the EV’s Location:*

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

*Participants Located within the Utility’s Domain:*

 Service Provider (Utility)

 Contractors and Suppliers to the Utility

### Identify Systems and Business Processes

**Objective** Identify the Systems and Business Processes where PI is collected, communicated, processed, stored or disposed within a Privacy.

**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.

**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

*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

 Partner Marketing System for transferring usage pattern and location information

### Identify Domains and Owners

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

**Definition** A “Domain” covers both physical areas (such as a customer site or home) 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 and PMRM Services and Functions are managed in business processes and technical systems Mechanisms within a given Domain.

**Context** 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.

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

**Example**

*Utility Domain:*

 The physical premises, located at…. which includes the Utility’s program information system, load scheduling system, billing system, and remote monitoring 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 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 adjacent land 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).

*Ownership*

 The EV On-Board System belongs to the utility Privacy Domain Owner.

 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.

### Identify Roles and Responsibilities within a Domain

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

**Rationale** 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.

**Example**

Role: EV Manufacturer Privacy Officer

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

### Identify Touch Points

**Objective** Identify the touch points at which the data flows intersect with Domains or Systems or Processes within Domains.

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

**Rationale** 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 Processes in which PI is used.

**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 the customer 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.

### Identify Data Flows

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

**Constraint** Data flows may be multidirectional or unidirectional.

**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 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.

## Identify PI in Use Case Domains and Systems

**Objective** Specify the PI collected, created, communicated, processed or stored within Domains or Systems or Processes in three categories, (Incoming, Internally-Generated and Outgoing)

### Identify Incoming PI

**Definition** Incoming PI is PI flowing into a Domain, or a system or process within a Domain.

**Constraint** Incoming PI may be defined at whatever level of granularity appropriate for the scope of analysis of the Use Case and the Privacy Policies established in Section 2.

### Identify Internally Generated PI

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

**Constraint** Internally Generated PI may be defined at whatever level of granularity appropriate for the scope of analysis of the Use Case and the Privacy Policies established in Section 2.

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

### Identify Outgoing PI

**Definition** Outgoing PI is PI flowing from one system to another, or from one process to another, either within a Domain or to another Domain.

**Constraint** Outgoing PI may be defined at whatever level of granularity appropriate for the scope of analysis of the Use Case and the Privacy Policies established in Section 2.

**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

## 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. In either case, Privacy Controls are typically associated with specific Privacy Principles that apply to the PI.

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

**Definition** Privacy Controls are administrative, technical and physical ~~Mechanisms requirements~~ employed within an organization or Domain in order to protect and manage PI. They are the means by which privacy policies are satisfied in an operational setting.

### Specify Inherited Privacy Controls

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

**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 the customer’s Operational Privacy Control Requirements, expressed as privacy preferences, via a link with the customer communications portal when she plugs her EV into friend Rick’s charging station.

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

### Specify Internal Privacy Controls

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

**Example**

**Use Limitation Internal Privacy Controls**

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

It 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 PII with third parties to assess whether they are authorized and whether additional or new public notice is required.

### Specify Exported Privacy Controls

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

**Example**

The Utility exports Jane’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 with marketing aggregators or advertisers.

# 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 operational procedures and digital world,“system-level”, concerns. “Services” and their associated Functions provide the bridge between those Privacy Controls and a privacy management implementation by providing Privacy Constraints on system-level actions governing the flow of PI between touch points.

## Services and Functions Needed to Implement the Privacy Controls

A set of operational Services and their associated Functions comprise the organizing structure which will be used to link the required Privacy Controls specified in Section 4.3 to operational Mechanisms, (both manual and automated), that are necessary to implement those requirements.

PMRM identifies eight Privacy Services, based on the mandate to support a set of privacy policies and Controls, but 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

Security

Enforcement

Access

*Table 1*

A privacy engineer, system architect or technical manager should be able to define these privacy Services and Functions, and package them into Mechanisms that will implement them.~~selected to implement these Functions.~~ In fact, a key purpose of 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 is an analytic tool.

The PMRM Services and Functions identify various system and process capabilities that are not typically described in privacy practices and principles. For example, a policy management (or “usage and control”) Function is essential to manage the PI usage parameters established by a data subject , information processor or by regulation, but such a Function is not explicitly named in privacy principles/practices. Likewise, interfaces (and agents) are not explicit in the privacy principles/practices, but are necessary to represent other essential operational capabilities.

Such inferred capabilities are necessary if information systems and process design are to be made “privacy-configurable and compliant.” 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, Security, Validation, Certification, Enforcement, Interaction,** and **Access.** ~~Specific operational behavior of these Services is governed by the privacy policy and Constraints and Privacy Controls that are configured in a particular implementation and jurisdictional context.~~ These will be identified as part of the Use Case analysis. Practice with Use Cases has shown that the Services listed above can, together, operationally encompass any arbitrary set of privacy policy and Control requirements.

The functions of one Service may invoke another Service and its 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)[[2]](#footnote-2), 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 solve a particular Privacy Control. By examining and by solving multiple Use Cases, the PMRM can be tested for applicability and robustness.

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

|  |  |  |
| --- | --- | --- |
| **SERVICE** | **FUNCTIONALITY** | **PURPOSE** |
| **AGREEMENT** | Define and document permissions and rules for the handling of PI based on applicable policies, data subject preferences, and other relevant factors; provide relevant Actors with a mechanism to negotiate or establish new permissions and rules; express the agreements for use by other Services | Manage and negotiate permissions and rules  |
| **USAGE** | Ensure that the use of PI complies with the terms of any applicable permission, policy, law or regulation, ncluding PI subjected to information minimization, linking, integration, inference, transfer, derivation, aggregation, and anonymization over the lifecycle of the PI | Control PI use |
| **VALIDATION** | Evaluate and ensure the information quality of PI in terms of Accuracy, Completeness, Relevance, Timeliness and other relevant qualitative factors | Check PI quality |
| **CERTIFICATION** | Ensure that the credentials of any Actor, Domain, System, or system component are compatible with their assigned roles in processing PI; and verify their compliance and trustworthiness against defined policies and assigned roles. | Check credentials |
| **ENFORCEMENT** | Initiate monitoring capabilities to ensure the effective operation of all Services. Initiate response actions, policy execution, and recourse when audit controls and monitoring indicate operational faults and failures. Record and report evidence of compliance to Stakeholders and/or regulators. | Monitor proper operation, respond to exception conditionsand report on demand evidence of compliance where required for accountability |
|  |   |  |
| **SECURITY** | Provide the procedural and technical mechanisms necessary to ensure the confidentiality, integrity, and availability of PI; make possible the trustworthy processing, communication, storage and disposition of privacy operations | Safeguard privacy information and operations |
| **INTERACTION** | Provide 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 | Information presentation and communication |
| **ACCESS** | Enable 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 stored PI  |

*Table 2*

## Service Details and Function Descriptions

### Core Policy Services

1. Agreement Service
* Define and document 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
* Express the Agreements for use by other Services

**Example**

As part of its standard customer service agreement, a bank requests selected customer PI, with associated permissions for use. Customer negotiates with the bank (whether via an electronic interface, by telephone or in person) to modify the permissions. Customer provides the PI to the bank, with the modified and agreed-to permissions. This agreement is signed by both parties, stored in an appropriate representation and the customer is provided a copy.

1. Usage Service
* Ensure 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.

**Example**

A third party has acquired specific PI, consistent with agreed permissions for use. Before using the PI, the third party has implemented functionality ensuring that the usage of the PI is consistent with these permissions.

### Privacy Assurance Services

1. Validation Service
* Evaluate and ensure the information quality of PI in terms of Accuracy, Completeness, Relevance, Timeliness and other relevant qualitative factors.

**Example**

PI is received from an authorized third party for a particular purpose. Specific characteristics of the PI, such as date the information was originally provided, are checked to ensure the PI meets specified use requirements.

1. Certification Service
* Ensure that the credentials of any Actor, Domain, System, or system component are compatible with their assigned roles in processing PI
* Verify that an Actor, Domain, System, or system component supports defined policies and conforms with assigned roles

**Example**

A patient enters an emergency room, presenting identifying credentials. Functionality has been implemented which enables hospital personnel to check those credentials against a patient database information exchange. Additionally, the certification service’s authentication processes ensure that the information exchange is authorized to receive the request.

1. Enforcement Service
* Initiate monitoring capabilities to ensure the effective operation of all Services
* Initiate response actions, policy execution, and recourse when audit controls and monitoring indicate operational faults and failures
* Record and report evidence of compliance to Stakeholders and/or regulators
* Provide data needed to demonstrate accountability

**Example**

A magazine’s subscription service provider forwards customer PI to a third party not authorized to receive the information. A routine audit of the service provider’s system reveals this unauthorized disclosure practice, alerting the relevant official (the organization’s privacy officer), who takes appropriate action. This action includes preparation of a Privacy Violation report submitted to the subscription service provider, together with a series of recommendations for remedial action, as well as an assessment of the privacy risk following the unauthorized disclosure.

The same magazine subscription service provider has established a Privacy Control that commits to educating its employees, contractors and service providers about its Privacy Policy annually and asking for a signed commitment to such policy. Each employee and contractor must take the online computer-based training and electronically sign his/her commitment to the policy. Training records are reported regularly to the privacy office and management to ensure full compliance.. The contracts with all service providers include language requiring the same actions. The privacy office receives evidence of compliance from each service provider.

1. Security Service
* Make possible the trustworthy processing, communication, storage and disposition of privacy operations
* Provide the procedural and technical mechanisms necessary to ensure the confidentiality, integrity, and availability of PI

**Example**

PI is transferred between authorized recipients, using transmission encryption, to ensure confidentiality.

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

### Presentation and Lifecycle Services

1. Interaction Service
* Provide 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

**Example:**

A home banking application uses a Graphical User Interface (GUI) to communicate with customers, including presenting any relevant privacy notices, enabling access to PI disclosures, and providing them with options to modify privacy preferences.

The banking application utilizes email alerts to notify customers when policies have changed and uses postal mail to confirm customer-requested changes.

1. Access Service
* Enable data-subjects, as required and/or allowed by permission, policy, or regulation, to review their PI held within a Domain and propose changes, corrections and/or deletions to it.

**Example:**

A national credit bureau has implemented an online service enabling customers to request their credit score details and to report discrepancies in their credit histories.

## 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) that are needed to transform the Privacy Controls of section 3.3 into an operational system design for the Domains or Use Case. Since the detailed Use Case analysis focused on the data flows (Iincoming, Internally-Generated, Outgoing ) between Systems (and Actors), the Service selections should be on the same granular basis.

### 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, actors and Domains.

This detailed conversion of Privacy Controls into Service operations can then be synthesized into consolidated sets of Service and Functions per System or business environment involved in the Domain(s) or Use Case.

On further iteration and refinement, the identified Services can be further delineated by the appropriate Functions and made operational by Mechanisms for the relevant Privacy Controls.

**Examples:**

Based upon

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

Convert to operational Services as follows:

**“Log EV location”:**

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

**Enforcement** If location has not been authorized by EV Owner for reporting and the location data has been transmitted, then notify the Owner and/or the Utility or positively log the authorized action

**Interaction** Communicate EV Location to EV On-Board System

**Usage** EV On-Board System records EV Location in secure storage; EV location data is linked to Agreements

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

**Interaction** Communication established between EV Location and ULSS

**Security** Authenticate the ULSS site; secure the transmission

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

**Validation** Validate the EV Location against customer-approved accepted locations

**Usage** ULSS records the EV Location, together with Agreements

# Define the Technical and Procedural Mechanisms Supporting the Selected Services and Functions

Each Service is comprised of a set of operational Functions, which in turn are delivered operationally by manual and technical Mechanisms

The **Mechanism** step is critical because it necessitates selecting the specific Services and Functions to be packaged into manual or technical Mechanisms.

A subset of these Mechanisms can then be selected to inform a recommended Privacy Architecture (PA) for other applications of the PMRM.

## 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, Controls, Privacy Constraints, Services and their Functions are needed to manage privacy. Here the PMRM requires a statement of the “how” – what Mechanisms are needed to be implemented.

###  Identify the Mechanisms that satisfy the selected Services and Functions

**Examples**

**“Log EV Location”** (uses **Validation**, **Enforcement**, **Interaction**, and **Usage** Services**):**

 **Mechanism:** Encrypt the EV location information and Agreements and store in on-board solid-state drive

**“Transmit EV Location to Utility Load Scheduler System (ULSS)”** (uses **Interaction**, **Security**, **Mechanism:** Establish a TLS/SSL communication between EV Location and ULSS, including Mechanisms for authentication of the source/destination

# Perform Operational Risk and/or Compliance Assessment

### 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*

**Constraint** Additional controls may be necessary to mitigate risks within Services. The level of granularity is determined by the Use Case scope. Provide 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**: Accepted locations are back-level

**Usage** ULSS records the EV Location, together with agreements

 **Risk**: Security controls for the ULSS are compromised

# 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 & Functions, Mechanisms and Privacy Architecture, producing the various refined versions of the Privacy Management Analysis. Later passes could serve to resolve “TBD” sections that are important, but were not previously developed.

Note that a ‘single pass’ analysis might mislead the PMRM user into thinking that the Use Case was fully-developed and well-understood. 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.

### 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.?

# Conformance

## Introduction

The PMRM as a “model” is abstract - and appropriately- so because Use Cases will cause the required level of detail to emerge. It is also a Methodology that is ery richly-detailed and multi-step but intentionally open-ended..

The emergence over time of profiles, sector-specific implementation criteria, and interoperability testing, implemented through explicit, executable, and verifiable methods, will lead to the development of detailed compliance and conformance criteria and may be included as part of a separate implementation guide.

In the meantime, the following statements indicate whether, and if so to what extent, each of the Tasks outlined in Sections 3 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.

## Conformance Statement

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

Any work product claiming conformance with PMRM v1.0

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

and where,

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

# 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..

## Operational Privacy Principles

The following 14 Operational Privacy Principles are composite definitions derived from a review of a number of relevant international legislative instruments. These operational Privacy Principles can serve as a sample set, as needed. Note however that there is no single and globally accepted set of Privacy Principles and the PMRM does not require use of these composite definitions.

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, including support for Sensitive Information, Informed Consent, Choices and Options, Change of Use Consent, and Consequences of Consent Denial, enabling data subjects to agree to the collection and/or specific uses of some or all of their Personal Information either through an affirmative process (opt-in) or implied (not choosing to opt-out when this option is provided).

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; and options for challenging denial when specified.

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.

## Glossary

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.

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.

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 Owner

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

Externally-Generated 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 Processes.

Internally-Generated PI

PI created within the Domain, business process or System itself.

Internally Generated 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.

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.

PI

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

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)

A collection of proposed 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 Constraint

An operational Mechanism that controls the extent to which PII may flow between touch points.

Privacy Control

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

Privacy Management

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

Privacy Management Analysis

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.

(PMRM) Service

A defined collection of related Functions that operate for a specified purpose. The eight Services and their Functions when selected ~~to~~ satisfy a Privacy Control.

Requirements

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

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.

1. Acknowledgments

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

PMRM V1.0 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 V2.0 Participants:**

Gershon Janssen, Individual Member

Dawn Jutla, Saint Mary’s University

Gail Magnusson, Individual Member

Nicolas Notario O’Donnell

John Sabo, Individual Member

Michael Willett, Individual Member

1. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Editor** | **Changes Made** |
| CSPRD02 | 2012-12-13 | John Sabo | Incorporate agreed dispositions to issues raised during Second Public Review |
| WD06 | 2013-03-12 | Peter F Brown | Non-Material changes |
| WD07 | 2013-04-03 | Peter F Brown | Addition of conformance section |

1. **Note**: The boxed examples are not to be considered as part of the normative text of this document. [↑](#footnote-ref-1)
2. See for example the **[SOA-RM]** and the **[SOA-RAF]** [↑](#footnote-ref-2)