OASIS Committee Note

Quick Start Guide for Data Protection to Support Regulatory Compliance Version 9.0

Committee Note Draft 01

14 February 2019

This stage:
https://docs.oasis-open.org/pmrm/PMRM-guide/v9.0/cnd01/PMRM-guide-v9.0-cnd01.docx (Authoritative)
https://docs.oasis-open.org/pmrm/PMRM-guide/v9.0/cnd01/PMRM-guide-v9.0-cnd01.html
https://docs.oasis-open.org/pmrm/PMRM-guide/v9.0/cnd01/PMRM-guide-v9.0-cnd01.pdf

Previous stage:
N/A

Latest stage:
https://docs.oasis-open.org/pmrm/PMRM-guide/v9.0/PMRM-guide-v9.0.docx (Authoritative)
https://docs.oasis-open.org/pmrm/PMRM-guide/v9.0/PMRM-guide-v9.0.html
https://docs.oasis-open.org/pmrm/PMRM-guide/v9.0/PMRM-guide-v9.0.pdf

Technical Committee:
OASIS Privacy Management Reference Model (PMRM) TC

Chair:
John Sabo (john.sabo711@yahoo.com), Individual Member

Editors:
Gail Magnuson (gail.magnuson@gmail.com), Individual Member
John Sabo (john.sabo711@yahoo.com), Individual Member
Beth X. Pumo (beth.pumo@kp.org), Kaiser Permanente

Related work:
This document is related to:

- *Privacy Management Reference Model and Methodology (PMRM) Version 1.0.* Edited by Michele Drgon, Gail Magnuson, and John Sabo. Latest stage: http://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.html.

Abstract:

One of the strengths of the Privacy Management Reference Model and Methodology (PMRM) for practitioners is that it mandates Use Cases as the best way to create a manageable scope. Well-defined and well-bounded Use Cases not only minimize the analytic workload, they also ensure that all data protection elements – from regulations, to control objectives, to technical functionality to risk assessment – can more easily be identified and associated, ensuring a solid, comprehensive analysis usable by multiple stakeholders.

However, even with a tightly defined Use Case, preparing a PMRM-generated Privacy Management Analysis (PMA) can require a large data gathering effort depending on the complexity of a particular Use Case. This also means identifying and working with multiple subject matter experts and stakeholders

within and outside your organization and collecting and cataloguing necessary information from them asynchronously and iteratively.

This Quick Start Guide is a tool to help practitioners get started. It can help organizations capture information to bootstrap the analysis of their applications against the data protection requirements and controls mandated by regulations such as the GDPR as well as their internal data protection policies, and provide a foundation for more detailed analysis.

Status:

This is a Non-Standards Track Work Product. The patent provisions of the OASIS IPR Policy do not apply.

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 stage" 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 document 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/.

Citation format:

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

[PMRM-Guide-v9.0]

Quick Start Guide for Data Protection to Support Regulatory Compliance Version 9.0. Edited by Gail Magnuson, John Sabo, and Beth X. Pumo. 14 February 2019. OASIS Committee Note Draft 01. https://docs.oasis-open.org/pmrm/PMRM-guide/v9.0/cnd01/PMRM-guide-v9.0-cnd01.html. Latest stage: https://docs.oasis-open.org/pmrm/PMRM-guide/v9.0/PMRM-guide-v9.0.html.

Notices

Table of Contents

1 Introduction

A 19-Step Quick Start Guide Based on the Privacy Management Reference Model and Methodology (PMRM) Version 1.0, Committee Specification 2.0

Understanding what privacy controls are required in applications and systems in order to comply with the EU General Data Protection Regulation (GDPR) and other data privacy laws…*and*…how do I engineer technical solutions to implement these controls -- is challenging. We often hear from practitioners: "Where do I begin?"

The PMRM can help – it is a comprehensive tool that identifies and integrates all the complex variables needed to design and engineer privacy-compliant applications and systems, and documents this in a Privacy Management Analysis (PMA) document. In this respect, the PMRM is a methodological tool that supports the privacy engineering discipline (see Appendix 2).

One of the strengths of the PMRM methodology for practitioners is that it mandates Use Cases as the best way to create a comprehensive yet manageable scope. Well-defined and well-bounded use-cases not only minimize the analytic workload, they also ensure that all data protection elements – from regulations, to control objectives, to technical functionality to risk assessment – can more easily be identified and associated, ensuring a solid, comprehensive analysis usable by multiple stakeholders.

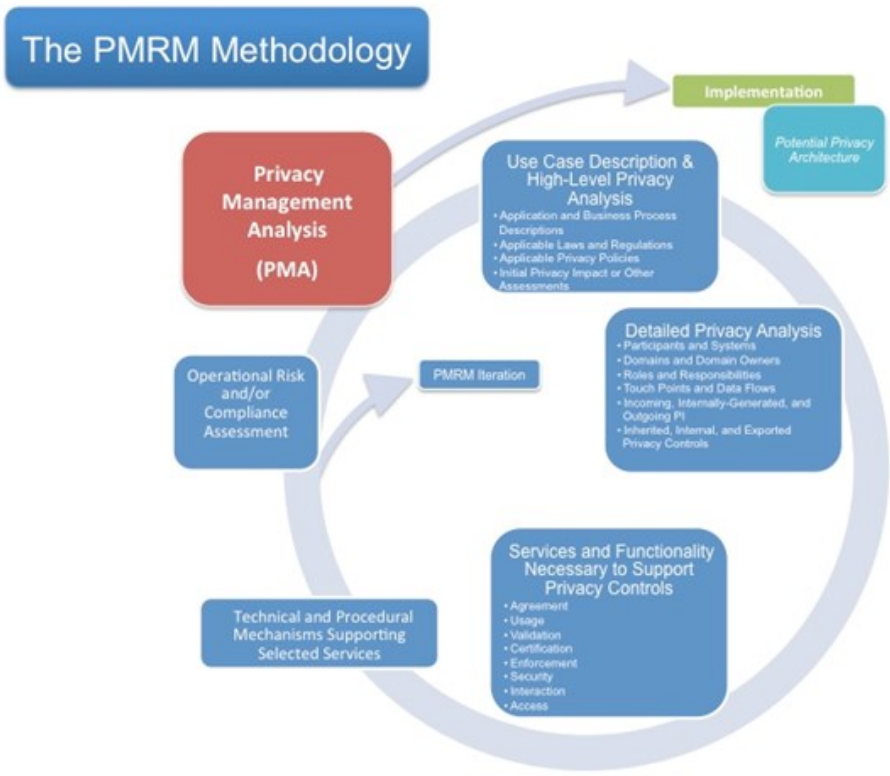
However, even with a tightly bounded Use Case, preparing a PMRM-generated PMA can require a large data gathering effort depending on the complexity of a particular Use Case. This also means identifying and working with multiple subject matter experts and stakeholders within and outside your organization and collecting and cataloguing necessary information from them asynchronously and iteratively.

This *Quick Start Guide* is a tool to help practitioners get started. It can help organizations capture information to bootstrap the analysis of their applications against their internal data protection policies and the data protection requirements and controls mandated by regulations such as the GDPR. The *Quick Start Guide* can provide a foundation for more detailed analysis.

2 Data Protection/Data Privacy – Not Easy, but Achievable!

Organizations need to understand their applications, systems and processes fully to ensure regulatory compliance while attaining their business objectives. Privacy/data protection by design in production systems requires addressing multiple factors: business and application objectives, regulatory and legal policy requirements, customer and client expectations, external service provider environments, system architectures, software, risk assessment and other factors. This is a complex field. Privacy officers, software engineers, business owners and other stakeholders *individually* do not have the knowledge base and experience necessary to produce a reliable and comprehensive analysis and roadmap to compliance.

Organizations differ in size, availability of in-house and consultant expertise, and privacy engineering maturity. As a result, discovering and documenting all of the elements needed to complete even a minimally adequate data protection solution may be daunting to the internal champions who would like to use a tool such as the PMRM methodology. To help address these challenges, the OASIS PMRM Technical Committee has prepared this PMRM Quick Start Guide ("Guide"). It is intended to provide an informal approach to help address the "where do I begin" and "how do I move forward" questions. The Guide is a set of 19 essential action steps derived from the PMRM's methodological tasks. From an initial data gathering study produced using this Guide, enough core information can be collected to help the organization identify the additional information and stakeholders needed to produce a more comprehensive and robust analytic study and to understand its risk management and compliance responsibilities.



3 The Quick Start Guide - a Starting Point and Baseline for Further Action

The Guide provides a starting point - a tool to define a Use Case and gather an essential set of information needed for more detailed analysis and action. It helps ease the challenge of using the PMRM methodology and undertaking a more robust PMRM-based PMA.

One additional point: using the Guide and the more detailed PMRM methodology supports risk analysis by providing a structured and re-usable knowledge base – what data protection controls are necessary to meet business objectives as well as regulatory expectations, how are the controls implemented, how do they interact with one another and other systems, and how must they change when the application and its interfaces with other applications and systems change.

Recommendations for this quick start process are to:

- Define a manageable Use Case
- Create an initial inventory of the internal and external stakeholders who have the knowledge, resources or expertise needed to address each step in the Guide
- Start with the quick start process steps you know the most about and then tackle the others
- Move quickly through each of these steps
- Establish short timelines for these steps in order to see results and create a foundation for iterative analysis
- Summarize the results of each step by grouping like items and as much detail as possible into higher-level sets or categories
- Create a uniform, structured template that captures the data you are collecting and that can be used by all stakeholders to add content to the data set
- Look backwards to previously completed steps and update them as needed.
- Keep a rolling list of questions, issues, potential controls, risks, and subject matter experts that will be needed further along in the analysis.
- Consider not only applications and systems, but also business processes and the end user experience
- Keep the findings summarized so that they remain easy to understand in order to reduce confusion and to enhance the usability of the analysis.
- Create matrices to make the documentation for each step easier to access and to correlate with other related steps
- Consider branching new, associated Use Cases to minimize complexity and maximize manageability of the current Use Case.

PMRM PRIVACY MANAGEMENT ANALYSIS (PMA)
QUICK START PROCESS STEPS

Process Steps	***Action Items***
Step 1: **Define your application and its business processes, and describe a manageable Use Case - what is your System or Application designed to do?** (PMRM Task #1)	• Set tight boundaries around the Use Case • Additional Use Cases can be appended to expand if needed. • Begin at the core and expand as necessary to include other applications or systems and processes linked to your Use Case.
Step 2: **Produce an Initial Use Case Inventory – a set of facts that you are aware of from your business environment, your technical systems, and your policy requirements that likely will have an impact on privacy in the Use Case** (PMRM Task #2)	• Complete this step at a high level to establish important reference points for consideration as the subsequent tasks are completed. • Update the inventory as new information becomes available. • Update the inventory information as additional elements of the inventory are discovered.
Step 3: **List the Privacy Policy Conformance Criteria you are aware of – internal privacy and security policies -- regulatory mandates applicable to the Use Case --**	• Collect commitments and privacy controls already made by your organization in the form of any existing privacy and security policies and public privacy statements. • Include any inherited privacy commitments and controls from other organizations and exported privacy commitments and controls that you require other organizations to implement. • Highlight the commitments and controls that seem applicable to this Use Case.

Process Steps	***Action Items***
existing privacy statements – existing controls (PMRM Task; #3)	• State whether your initial review indicates that this Use Case is/is not/or may be governed by the GDPR and/or other laws and regulations. • If *yes or may be*, note the particular regulations and related references material. If *no,* state why not or what you have done to find out. • Identify any known risks associated with these privacy controls (PMRM Task #19)
Step 4: **Document previous relevant studies or analysis, if available.** (PMRM Task #4)	• Collect and organize relevant previous Use Case privacy management analyses • Collect and reference high level depictions of the overall environment (ecosystem) the Use Case may be a part of • Collect and organize previous studies or Data Protection/Data Privacy Impact Assessments DPIA/PIAs that are relevant to the Use Case to assist the completion of the previous and following steps. • Add the findings of the previous studies DPIA/PIA to the relevant steps.
Step 5: **Identify the Stakeholders – organizations and individuals – whose expertise is needed for the Privacy Analysis** (PMRM Task #5)	• Identify any stakeholder associated with the Use Case who is responsible for managing, creating policy, collecting, storing, using, sharing, transmitting, transferring across-borders, retaining or disposing of personal data. • Keep the Core Use Case stakeholder inventory tight initially to reduce complexity. • Organize the stakeholder list, using categories such as privacy officer, privacy consultant, security consultant, software development team, cloud provider, business owner, citizen/user, etc. • Prioritize the stakeholder list to help move the analysis forward more quickly. ***Note: Review the results of Steps #1-4 to confirm that these first steps are accurate and complete and update as needed with your Stakeholders***

Process Steps	*Action Items*
Step 6: **List the Participants, Business Processes, Applications and Systems where data is collected, stored, used, shared, transmitted, transferred across-borders, retained or disposed** (PMRM Task # 6)	• Make an initial list of the relevant participants in this Use Case. Include customers, clients and participants within core of the Use Case and among the various third parties involved in the Use Case • Make an initial list of the relevant business processes and associated business entities and systems contained in the Use Case. • Determine and annotate which internal systems or external third parties or cloud providers are integral to the application of the Use Case. • Annotate the country locations of their business operations and systems/data bases. • Group each participant, business process, system or application into categories (for example group all systems that provide back up and recovery services for the Use Case).
Step 7: **Annotate the Business Processes, Applications and Systems listed in Task 6 where Personal Data (PD) is collected, stored, used, shared, transmitted, transferred across borders, retained or disposed, including third party systems** (PMRM Task #6)	• Label data that you identify as PD. • Consult references to determine what constitutes PD under the GDPR and/or other regulations relevant to the Use Case. • Group like PD into categories. • Update as needed the previous steps as necessary, based on this additional information.
Step 8: **Identify Domain and Domain Owners associated with the Participants, Business Processes,**	• Understand these definitions: ○ *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

Process Steps	***Action Items***
Applications and Systems identified in Steps 6 and 7, above, together with their respective owners (PMRM Task #7)	environment) that are subject to the control of a particular Domain owner. ○ *A Domain Owner* is the stakeholder responsible for ensuring that Privacy Controls are implemented in within a given Domain. • List the Domains and associated Domain Owners that support the collection, storage, usage, sharing, transmitting, transferring across borders, retention and disposition of the PD included in the Use Case under Step 7. Often the identification of the Domains will require revising the previous steps as this step will often broaden the definition of the Use Case. • Include all Domains that provide PD to the Use Case, participate in the Use Case or are recipients of the PD from the Use Case • Identify the country location of these domains. • Group this information into like categories.
Step 9: **Identify relevant Roles and Responsibilities for each Domain–** (PMRM Task #8)	• List the key managers/contacts for a Domain –the individual or team responsible for the business processes, applications and systems interfacing with your Use Case and ensuring data protection is properly managed. • Label the key contacts characterizing their responsibilities.
Step 10: **Identify Touch Points – Identify the Business Processes and Application/System Touch Points through which the data flows** (PMRM Task #9)	• List the connection points such as sub-systems in your Use Case and the Domains. • Touch Points are the intersection of PD and Privacy Controls. This is the place where the Roles take responsibility for incoming PD and inherited Privacy Controls for their operations and ensures that the outgoing PD and exported Privacy Controls are passed on. • Annotate the business processes, applications and systems. • Annotate the touch points that cross international borders. • Annotate the touch points that cross organizational boundaries.

Process Steps	***Action Items***
Step 11: **Identify Data Flows – Identify the data flows carrying PD among Domains within the Use Case** (PMRM Task #10)	• List the *sets or categories* of data which flow within the Use Case from Domain to Domain, Sub Domain to Sub Domain overseen by Roles and which can be characterized as PD. • Ensure that the various Domains and Sub Domains are identified as part of various organizational entities, including Sub Domains within an organizational entity and Domains that include all entities involved in the Use Case (the user, the third parties, et.al.)
Step 12: **What Personal Data (PD) will be collected - used – communicated – stored – disposed of by the application or system?** (PMRM Tasks # 11-13)	• Use the definition of PD that defined in the GDPR or whatever regulation primarily applies. • Learn what constitutes PD under the GDPR or other applicable regulation. Expand on Task #2 • Know what and where PD is collected, stored, used, shared, transmitted, transferred across-borders, retained or disposed as part of the application(s) and processes. • Categorize and group this PD – for example, individual PD (names, addresses, IP addresses, other unique personal identifiers, location data) financial PD, et.al. into like categories to simplify the overall process. Often the treatment of a category of PD is the same for each individual PD data element. • Using the categories identified above, prepare matrices that correlate the relationship between, for example the PD used by within the Use Case Business Processes, Applications. Systems, Participants and Domains. • Use information from the previous steps for this consolidation step
Step 13: **Identify where the PD comes from and where it is communicated** (PMRM Tasks # 11-13)	• *Identify Incoming PD* - PD flowing into the Business Process, Application, System or Domain. • *Identify Internally Generated PD* - PD created *within* the Business Process, Application, System or Domain itself. • *Identify Outgoing PD* - PD flowing from one Business Process, Application, System or Domain

Process Steps	***Action Items***
	to another within the Use Case. • Update Step 12 with this information.
Step 14: **Specify the Required Data Protection Controls Associated with PD** (PMRM Tasks # 14-16)	• Identify an initial list of data protection controls associated with PD in the Use Case. • Segment three types of controls, as determined by the scope of your Use Case: ○ *Inherited controls:* controls mandated by external parties. ○ *Internal controls:* your organization's controls. ○ *Exported controls:* controls that you require associated applications systems or domains to implement. • Associate these controls with the PD.
Step 15: **Identify the risks associated with these privacy controls if they are not implemented or if there are control failures** (PMRM Task #19)	• Using a risk management process of your choice, assess the risk of implementing or not the identified privacy controls. • Select the privacy controls to be further defined and potentially implemented. • Consider the their implementation based upon the results of the follow-on design initiatives.
Step 16: **Identify the Services and Functions necessary to support the Privacy Controls** (PMRM Task #17)	• Prioritize the Privacy Controls that are core to the Use Case and/or might have been identified as a high level risk • Define each Privacy Control by using the services as a checklist to ensure the control is fully defined. ○ For example the Enforcement service addresses the need for demonstrating accountability which is a requirement of the GDPR • Update the risks associated with these privacy controls (Task #19)

Process Steps	*Action Items*
Step 17: **Identify the Technical and Procedural Mechanisms to support the services and functions defined for the Data Protection Controls** (PMRM Task 18)	• Identify which business processes, applications, systems or processes will need to implement the Privacy Controls. • Identify existing implemented Privacy Controls and reuse as much of the implementation design as possible. • Consider grouping the Privacy Control requirements into implementable units. ○ For example, the services and functions associated with demonstrating accountability might be packaged into one mechanism that might be shared (or is already developed) with other Use Cases • Update the risks associated with these privacy controls (Task #19)
Step 18: **Perform a Risk and/or Compliance Assessment** (PMRM Task #19)	• Review all identified risks. • Prioritize risks. Do so through out the Use Case project to ensure that the organization is maximizing its resources. • Ensure that GDPR and/or other legal and regulatory requirements identified in Step #3 have been addressed. • Catalogue the Controls and associated Mechanisms that are available to manage the identified Risks. • Make recommendations for implementation.
Step 19: **Iterate the Analysis and Refine** (PMRM Tasks #20)	• Identify further iterations of the PMA as is necessary. • Include all elements of the Quick Start Guide that your team is capable of. ○ There may elements that might need to be reviewed. • Determine if you need to conduct a more thorough iteration of the full or portion of the Use Case.

Appendix A. PMRM GLOSSARY

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.