Privacy by Design Documentation for Software Engineers Version 1.0

Committee Specification Draft 01

25 June 2014

Specification URIs

This version:

http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/csd01/pbd-se-v1.0-csd01.doc (Authoritative)
http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/csd01/pbd-se-v1.0-csd01.html
http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/csd01/pbd-se-v1.0-csd01.pdf

Previous version:

N/A

Latest version:

http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/pbd-se-v1.0.doc (Authoritative)
http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/pbd-se-v1.0.html
http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/pbd-se-v1.0.pdf

Technical Committee:

OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC

Chairs:

Ann Cavoukian (commissioner.ipc@ipc.on.ca), Office of the Information & Privacy Commissioner of Ontario, Canada
Dawn Jutla (dawn.jutla@gmail.com), Saint Mary's University

Editors:

Ann Cavoukian (commissioner.ipc@ipc.on.ca), Office of the Information & Privacy Commissioner of Ontario, Canada
Fred Carter (fred.carter@ipc.on.ca), Office of the Information & Privacy Commissioner of Ontario, Canada
Dawn Jutla (dawn.jutla@gmail.com), Saint Mary's University
John Sabo (john.annapolis@verizon.net), Individual
Frank Dawson (frank.dawson@nokia.com), Nokia
Jonathan Fox (Jonathan_Fox@McAfee.com), Intel Corporation
Tom Finneran (tfinneran@gmail.com), Individual
Sander Fieten (sander@fieten-it.com), Individual

Related work:

This specification is related to:

- *Annex Guide to Privacy by Design Documentation for Software Engineers Version 1.0*. Edited by Ann Cavoukian, Fred Carter, Dawn Jutla, John Sabo, Frank Dawson, Sander Fieten, Jonathan Fox, and Tom Finneran. Latest version: http://docs.oasis-open.org/pbd-se/pbd-se-annex/v1.0/pbd-se-annex-v1.0.html.
- *Privacy Management Reference Model and Methodology (PMRM) Version 1.0*. Edited by Peter Brown, Gershon Janssen, Dawn N Jutla, John Sabo, and Michael Willett. 03 July 2013. Committee Specification 01. http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs01/PMRM-v1.0-cs01.html.

Abstract:

This specification for software engineers translates the seven *Privacy by Design* (PbD) principles to conformance requirements for documentation, either produced or referenced, that organizations may use to demonstrate that privacy was considered at each stage of the software development life cycle.

Status:

This document was last revised or approved by the OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) 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” button on the Technical Committee’s web page at https://www.oasis-open.org/committees/pbd-se/.

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 (https://www.oasis-open.org/committees/pbd-se/ipr.php).

Citation format:

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

[pbd-se-v1.0]

Privacy by Design Documentation for Software Engineers Version 1.0. Edited by Ann Cavoukian, Fred Carter, Dawn Jutla, John Sabo, Frank Dawson, Jonathan Fox, Tom Finneran, and Sander Fieten. 25 June 2014. Committee Specification Draft 01. http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/csd01/pbd-se-v1.0-csd01.html. Latest version: http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/pbd-se-v1.0.html.

Notices

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

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

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

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

Table of Contents

1 Introduction

The OASIS *Privacy by Design* Documentation for Software Engineers (PbD-SE) Technical Committee provides a specification to operationalize *Privacy by Design* in the context of software engineering. *Privacy by Design*, like security by design, is a normal part of the software development process and a risk reduction strategy for software engineers. Given the savings that come from being proactive rather than trying to retrofit privacy into software, this specification streamlines the process of doing *Privacy by Design* and achieving cost savings.

The PbD-SE specification translates the PbD principles to conformance requirements within software engineering tasks, and helps software development teams to produce artifacts as evidence of PbD-principle adherence. Following the specification facilitates documentation of privacy requirements from software conception to retirement, thereby providing a plan around adherence to or compliance with *Privacy by Design* principles, and other guidance to privacy best practices, such as NIST's 800-53 Appendix J [NIST 800-53] and the Fair Information Practice Principles (FIPPs) [PMRM-1.0]. Software engineers, project managers, privacy officers, data stewards, and auditors, among others, may use the PbD-SE methodology for documenting and auditing such adherence to *Privacy by Design* throughout the entire software development life cycle. Correct application of PbD principles to software engineering helps lower overall risk, and may serve as evidence of compliance with privacy law and regulation.

Developers are not being blocked from developing solutions, but are required to analyze and succinctly document how they deal with privacy issues. The PbD-SE specification (and its "Annex to the Privacy by Design Documentation for Software Engineers" guide) helps engineers to visualize, model, and document PbD requirements and embed the principles within software engineering tasks. It also helps inform those organizational governance processes that oversee the software engineers.

Visualizing, modeling, and documenting are activities that help software engineers to accelerate their learning and to translate privacy requirements into their software and create a record of it. Software engineers reference documents that others generate as well as produce their own documentation. The PbD-SE specification includes all documentation that supports the software engineer in embedding PbD in software, whether (s)he references the documents (e.g. privacy policies), or generates documentation (e.g. privacy considerations in a user story or system design). Thus this specification includes requiring documentation about privacy governance from the organization in which the software engineer operates.

The PbD-SE specification encourages flexibility of choice of documentation representations for different software engineering methodologies, ranging from waterfall to agile. The PbD-SE TC references the OASIS Privacy Management Reference Model and Methodology v1.0 (PMRM), as a PMRM-derived Privacy Use Case/User Story Template (Privacy Use Template for short) forms part of this specification to assist engineers to understand and document comprehensive privacy requirements in complex environments, and to document the selection of appropriate privacy services and controls. The PbD-SE and its "Annex to the Privacy by Design Documentation for Software Engineers Version 1.0" [PbD-SE-Annex-1.0] use the Privacy Use Template, the OMG software modeling standard UML, data flow diagrams (DFDs) and spreadsheet modeling, to provide visual and textual examples of privacy documentation. Yet it allows for equivalent documentation for conformance to PbD-SE. Thus this specification remains agnostic to choice of visual modeling language or tool for use in generating or referencing documentation in various stages of the software development lifecycle (SDLC).

1.1 Context and Rationale

The management of privacy in the context of software engineering requires normative judgments to be made on the part of software engineers operating within an organization-wide governance framework of privacy protection. It has become increasingly apparent that software systems need to be complemented by a set of governance norms that reflect privacy dimensions. There is a growing demand for provable software privacy claims, systematic methods of privacy due diligence, and greater transparency and accountability in the design and operation of software systems that process personal information, in order to promote wider adoption, gain trust and market success, and demonstrate legal and regulatory compliance.

1.2 Objectives

This specification provides guidance and requirements for engineers to document privacy objectives and associated control measures throughout the software development life cycle. This documentation is the output of the specification's conformance requirements but may be supplemented by artifacts produced from auxiliary privacy processes or services, and procedures for internal independent reviewers to conduct reviews of documentation for explicit adherence to *Privacy by Design* (PbD) guidelines. Artifacts include explicit documentation of functional and non-functional privacy requirements. Examples of artifact representations include, and are not limited to, spreadsheet documentation of compliance tasks and processes, those components of user stories, use cases, misuse cases, interface design, DFD diagrams, class diagrams, data flow diagrams, sequence diagrams or activity diagrams that clearly show embedding of PbD principles and associated requirements, business model diagrams that show personal data flows across technology platforms, and diagrams of privacy architectures. Organizational privacy-related documentation for engineers to reference (e.g. privacy policies, privacy training materials, documentation of go-to personnel for privacy consultations) is expected to be at hand. The documentation specified by this standard may form part of a larger, organization-wide *Privacy by Design* implementation and approach.

1.3 Intended Audience

For *Privacy by Design* to become accessible to mainstream software engineering and software development, the OASIS PbD-SE Technical Committee targets this specification to all software engineers. Software engineers may work in (virtual) organizations and/or on projects of all sizes, including working in distributed platform teams or on solo startup platforms. Software engineers are responsible for implementing, and documenting or referencing documentation to show adherence to or compliance with *Privacy by Design* principles in software deliverables. However, as software engineers operate in larger contexts, this specification is also of interest and use to their project managers, business managers and executives, privacy policy makers and compliance managers, privacy and security consultants, auditors, regulators, and other designers and users of systems that collect, store, process, use, share, transport across borders, exchange, secure, retain or destroy personal data. In larger organizations, where subject matter experts and organizational stakeholders have clear roles in the SDLC, their contributions may be an explicit part of the documentation. In addition, other OASIS TCs and external governing organizations and standards bodies may find the PbD-SE specification useful in producing evidence of adherence to and/or compliance with *Privacy by Design* principles.

1.4 Outline of the Specification

This specification provides:

- An expression and explanation of the *Privacy by Design* principles in the context of software engineering. In effect, it closes a communications, requirements, and operations gap among policymakers, business stakeholders, and software engineers.
- A mapping of the *Privacy by Design* principles to engineering-related sub-principles, and to documentation, and thus PbD-SE conformance criteria.
- Privacy considerations for the entire software development life cycle from software conception to software retirement.
- Software engineering Documentation Checklists

Accompanying this specification is an Annex Guide [PbD-SE-Annex-1.0] that further provides:

- a process to ensure that privacy requirements are considered throughout the entire software development life cycle from software conception to software retirement.
- a methodology for an organization and its software engineers to produce and reference privacy-embedded documentation to demonstrate conformance to this PbD-SE Version 1.0 specification.
- a Privacy Use Template that helps software engineers document privacy requirements and integrate them with core functional requirements.
- *Privacy by Design* Reference Architecture for software engineers to customize to their context, and Privacy Properties that software solutions should exhibit.
- *Privacy by Design* Patterns
- *Privacy by Design* for Maintenance and Retirement

1.5 Terminology

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]**.

Architectural Principle: A qualitative statement of intent that should be met by the architecture (adapted from The Open Group Architecture Framework (TOGAF), http://pubs.opengroup.org/architecture/togaf8-doc/arch/).

Informational Privacy: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve.", see page 7 of Westin, A, *Privacy and Freedom*, 1967) Information Privacy, then is the discipline of applying privacy principles to any processing of personally identifiable information or personal data, including those that involve digital technology, such as the product of software development.

Personal Data/Personal Information: any data/information about an individual including (1) any data/information that can be used to distinguish or trace an individual‘s identity, and (2) any other data/information that is linked or linkable to an individual or an individual’s device. Adapted from NIST, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) Special Publication 800-122 (April 2010)

Principle: A fundamental truth or proposition that serves as the foundation for a system of belief or behaviour or for a chain of reasoning (Oxford Dictionary); a comprehensive and fundamental law, doctrine, or assumption (Merriam-Webster)

Privacy Control: A process designed to provide reasonable assurance regarding the achievement of stated privacy properties or objectives

Privacy Service: A service-based software implementation of one or more privacy controls.

Software Engineer: A person that adopts engineering approaches, such as established methodologies, processes, architectures, measurement tools, standards, organization methods, management methods, quality assurance systems and the like in the development of software (adapted from Wang, 2011).

Software Organization: Any organization or department or unit within an organization that engages in the development of software products and services either directly or indirectly.

1.6 Normative References

[Cavoukian 2011]

Seven Foundational Principles, available at www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

[PMRM-1.0]

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

[RFC2119]

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

1.7 Non-Normative References

[PbD-SE-Annex-1.0]

OASIS Annex to the Privacy by Design Documentation for Software Engineers Version 1.0, 25 June 2014. http://docs.oasis-open.org/pbd-se/pbd-se-annex/v1.0/pbd-se-annex-v1.0.doc.

[NIST 800-53]

Security and Privacy Controls for Federal Information Systems and Organizations Revision 4, Appendix J: Privacy Controls Catalog

2 Mapping of *Privacy by Design* Principles to Documentation

Table 2.1 provides a mapping between the seven PbD principles and the documentation that software engineers SHALL produce or reference throughout the software development lifecycle from software conception to retirement. A checklist column may be added to the table.

Please note spreadsheets, modeling languages, and other tools or representations may be used on their own or in combination for documentation, as long as they are sufficiently powerful to capture the essence of the software engineering translation of the PbD principles as provided in Table 2.1.

An "Annex to the Privacy by Design Documentation for Software Engineers Version 1.0" [PbD-SE-Annex-1.0] accompanies this specification and provides further information, process thinking, explanation of techniques and pedagogical material. It is intended to be helpful to software organizations and engineers implementing the specification.

Table 2.1. Mapping of *Privacy by Design* Principles to Software Engineering Referenced and Generated Documentation

PbD Principle	PbD Sub-Principle	Documentation
1. Proactive not Reactive; Preventative not Remedial	**1.1–Demonstrable Leadership**: A clear commitment, at the highest levels, to prescribe and enforce high standards of privacy protection, generally higher than prevailing legal requirements. **1.2–Defined Community of Practice**: Demonstrable privacy commitment shared by organization members, user/data subject communities and relevant stakeholders. **1.3–Proactive and Iterative**: Continuous processes to identify privacy and data protection risks arising from poor designs, practices and outcomes, and to mitigate unintended or negative impacts in proactive and systematic ways.	**SHALL** normatively reference the PbD-SE specification **SHALL** reference assignment of responsibility and accountability for privacy in the organization, and privacy training program(s). **SHALL** include assignment of resources to the software project, recording who are responsible, accountable, consulted, or informed for various privacy-related tasks **SHALL** reference all external sources of privacy requirements, including policies, principles, and regulations. **SHALL** include privacy requirements specific to the service/product being engineered, and anticipated deployment environments **SHALL** include privacy risk/threat model(s) including analysis and risk identification, risk prioritization, and controls clearly mapped to risks
2. Privacy by Default	**2.1–Purpose Specificity:** Purposes must be specific and limited, and be amenable to engineering controls **2.2–Adherence to Purposes:** methods must be in place to ensure that personal data is collected, used and disclosed:	**SHALL** list all [categories of] data subjects as a stakeholder **SHALL** clearly record the purposes for collection and processing, including retention of personal data **SHALL** document expressive models of detailed data flows, processes, and behaviors for use cases or user

	in conformity with specific, limited purposes;
	in agreement with data subject consent; and
	in compliance with applicable laws and regulations
	2.3–Engineering Controls: Strict limits should be placed on each phase of data processing lifecycle engaged by the software under development, including:
	Limiting Collection;
	Collecting by Fair and Lawful Means;
	Collecting from Third Parties;
	Limiting Uses and Disclosures;
	Limiting Retention;
	Disposal, Destruction; and Redaction
		stories associated with internal software project and all data/process interaction with external platforms, systems, APIs, and/or imported code.
		SHALL describe selection of privacy controls and privacy services/APIs and where they apply to privacy functional requirements and risks.
		SHALL include software retirement plan from a privacy viewpoint

3. Privacy Embedded into Design	**3.1–Holistic and Integrative**: Privacy commitments must be embedded in holistic and integrative ways. **3.2–Systematic and Auditable:** A systematic approach should be adopted that relies upon accepted standards and process frameworks, and is amenable to external review. **3.3–Review and Assess:** Detailed privacy impact and risk assessments should be used as a basis for design decisions. **3.4–Human-Proof:** The privacy risks should be demonstrably minimized and not increase through operation, misconfiguration, or error.	**SHALL** use the OASIS PbD-SE Privacy Use Template (see PbD-SE Annex Section 5 [PbD-SE-Annex-1.0]) or the more comprehensive OASIS PMRM methodology [PMRM 1.0] or equivalent for identifying and documenting privacy requirements. **SHALL** contain description of its business model showing traceability of personal data flows for any data collected through new software services under development. **SHALL** include identification of privacy design principles **SHALL** contain a privacy architecture **SHALL** describe privacy UI/UX design **SHALL** define privacy and security metrics **SHALL** include human sign-offs/privacy checklists for software engineering artifacts **SHALL** include privacy review reports *(either in reviewed documents or in separate report)*

4. Full Functionality: Positive Sum, not Zero-Sum	**4.1–No Loss of Functionality:** Embedding privacy adds to the desired functionality of a given technology, process or network architecture. **4.2-Accommodate Legitimate Objectives**: All interests and objectives must be documented, desired functions articulated, metrics agreed, and trade-offs rejected, when engineering software solutions. **4.3–Practical and Demonstrable Results**: Optimized outcomes should be published for others to emulate and become best practices.	**SHALL** treat *privacy-as-a-functional requirement (see section 2.1.4 of the PbD-SE Annex Guide* [PbD-SE-Annex-1.0]*),* i.e. functional software requirements and privacy requirements should be considered together, with no loss of functionality. **SHALL** show tests for meeting privacy objectives, in terms of the operation and effectiveness of implemented privacy controls or services.
5. End-to-End Lifecycle Protection	**5.1–Protect Continuously:** Personal data must be continuously protected across the entire domain and throughout the data life-cycle from creation to destruction. **5.2–Control Access:** Controls on access to personal data should be commensurate with its degree of sensitivity, and be consistent with recognized standards and practices. **5.3–Use Security and Privacy Metrics:** Applied security standards must assure the confidentiality, integrity and availability of personal data and be amenable to verification **5.4 Satisfy Privacy Properties:** Wherever possible, software must satisfy properties such as user/data subject comprehension, choice, consent, consciousness, consistency, confinement (setting limits to collection, use, disclosure, retention, purpose), and context(s) around personal data at a functional level; minimized identifiability, linkability, and observability; and maximized traceability, audibility and accountability at a systems level, and be amenable to verification.	**SHALL** be produced for all stages of the software development lifecycle from referencing applicable principles, policies, and regulations to defining privacy requirements, to design, implementation, maintenance, and retirement. **SHALL** reference requirements, risk analyses, controls selection, architectures, design, implementation mechanisms, retirement plan, and sign-offs with respect to privacy and security. **SHALL** include security and privacy metrics designed in and/or deployed in the software, or monitoring software, or otherwise in the organization, and across partnering software systems or organizations. **SHALL** demonstrate designs and implementations that satisfy state-of-the-art privacy *properties*.
6. Visibility and Transparency	**6.1–Open Collaboration:** Privacy requirements, risks, implementation methods and	**SHALL** *reference* the privacy policies and documentation of all other collaborating stakeholders

	outcomes should be documented throughout the development lifecycle and communicated to project members and relevant stakeholders. **6.2–Open to Review:** The design and operation of software systems should demonstrably satisfy the strongest privacy laws, contracts, policies and industry norms (as required). **6.3–Open to Emulation:** The design and operation of privacy-enhanced information technologies and systems should be open to scrutiny, improvement, praise, and emulation by others.	**SHALL** include description of contextual visibility and transparency mechanisms at the point of contextual interaction with the user/data subject and other stakeholders for data collection, use, disclosure, and/or elsewhere as applicable **SHALL** describe any measurements incorporated in the software, or monitoring software, or otherwise to measure the usage and effectiveness of provided privacy options and controls, and to ensure continuous improvement. **SHALL** describe placement of privacy settings, privacy controls, privacy policy(ies), and accessibility, prominence, clarity, and intended effectiveness.
7. Respect for User Privacy	**7.1–Anticipate and Inform:** Software should be designed with user/data subject privacy interests in mind, and convey privacy attributes (where relevant) in a timely, useful, and effective way. **7.2–Support Data Subject Input and Direction:** Technologies, operations and networks should allow users/data subjects to express privacy preferences and controls in a persistent and effective way. **7.3–Encourage Direct User/Data Subject Access:** Software systems should be designed to provide data subjects direct access to data held about them, wherever feasible, and an account of uses and disclosures.	**SHALL** describe user/data subject privacy options, including (access) controls, privacy preferences/settings, UI/UX supports, and user/data subject- centric privacy model. **SHALL** describe notice, consent, and other privacy interactions at the EARLIEST possible point in a data transaction exchange with a user/data subject or her/his automated agent(s) or device(s).

3 Conformance

This section summarizes the requirements for meeting the PbD "Conformance Targets" of this specification.

1. Proactive, Not Reactive:

Documentation:

a) **SHALL** normatively reference the PbD-SE specification

b) **SHALL** reference assignment of responsibility and accountability for privacy in the organization, and privacy training program(s).

c) **SHALL** include assignment of privacy resources to the software project, recording who are responsible, accountable, consulted, or informed for various privacy-related tasks

d) **SHALL** reference all external sources of privacy requirements, including policies, principles, and regulations.

e) **SHALL** include privacy requirements specific to the service/product being engineered, and anticipated deployment environments

f) **SHALL** include privacy risk/threat model(s) including analysis and risk identification, risk prioritization, and controls clearly mapped to risks

2. Privacy as the Default

Documentation:

a) **SHALL** list all [categories of] data subjects as a stakeholder

b) **SHALL** clearly document the purposes for collection and processing, including retention of personal data

c) **SHALL** document expressive models of detailed data flows, processes, and behaviors for use cases or user stories associated with internal software project and all data/process interaction with external platforms, systems, APIs, and/or imported code.

d) **SHALL** describe selection of privacy controls and privacy services/APIs and where they apply to privacy functional requirements and risks.

e) **SHALL** include software retirement plan from a privacy viewpoint

3. Privacy Embedded into Design

Documentation:

a) **SHALL** use the Privacy Use Template (see PbD-SE Annex Section 5 [PbD-SE-Annex-1.0]) or the more comprehensive OASIS PMRM methodology [PMRM 1.0] or equivalent for identifying and documenting privacy requirements

b) **SHALL** contain description of business model showing traceability of personal data flows for any data collected through new software services under development.

c) **SHALL** include identification of privacy design principles

d) **SHALL** contain a privacy architecture

e) **SHALL** describe privacy UI/UX design

f) **SHALL** define privacy metrics

g) **SHALL** include human sign-offs/privacy checklists for software engineering artifacts

h) **SHALL** include privacy review reports *(either in reviewed documents or in separate report)*

i) **SHALL** treat *privacy-as-a-functional requirement* i.e. functional software requirements and privacy requirements should be considered together, with no loss of functionality.

j) **SHALL** show tests for meeting privacy objectives, in terms of the operation and effectiveness of implemented privacy controls or services

k) **SHALL** be produced for all stages of the software development lifecycle from referencing applicable principles, policies, and regulations to defining privacy requirements, to design, implementation, maintenance, and retirement.

l) **SHALL** reference requirements, risk analyses, architectures, design, implementation mechanisms, retirement plan, and sign-offs with respect to privacy and security.

m) **SHALL** include security and privacy metrics designed in and/or deployed in the software, or monitoring software, or otherwise in the organization, and across partnering software systems or organizations.

n) **SHALL** demonstrate designs and implementations that satisfy state-of-the-art privacy *properties*.

4. Full Functionality: Positive Sum, not Zero-Sum

Documentation:

a) **SHALL** treat *privacy-as-a-functional requirement,* i.e. functional software requirements and privacy requirements should be considered together, with no loss of functionality.

b) **SHALL** show tests for meeting privacy objectives, in terms of the operation and effectiveness of implemented privacy controls or services

5. End to End Safeguards: Full Lifecycle Protection

Documentation:

a) **SHALL** be produced for all stages of the software development lifecycle from referencing applicable principles, policies, and regulations to defining privacy requirements, to design, implementation, maintenance, and retirement.

b) **SHALL** reference requirements, risk analyses, architectures, design, implementation mechanisms, retirement plan, and sign-offs with respect to privacy and security.

c) **SHALL** include security and privacy metrics designed in and/or deployed in the software, or monitoring software, or otherwise in the organization, and across partnering software systems or organizations.

d) **SHALL** demonstrate designs and implementations that satisfy state-of-the-art privacy *properties*.

6. Visibility and Transparency: Keep It Open

Documentation:

a) **SHALL** *reference* the privacy policies and documentation of all other collaborating stakeholders

b) **SHALL** include description of contextual visibility and transparency mechanisms at the point of contextual interaction with the user/data subject and other stakeholders for data collection, use, disclosure, and/or elsewhere as applicable

c) **SHALL** describe any measurements incorporated in the software, or monitoring software, or otherwise to measure the usage and effectiveness of provided privacy options and controls, and to ensure continuous improvement.

d) **SHALL** describe placement of privacy settings, privacy controls, privacy policy(ies), and accessibility, prominence, clarity, and intended effectiveness

7. Keep it User-Centric

Documentation:

a) **SHALL** describe user/data subject privacy options (including access), controls, user privacy preferences/settings, UI/UX supports, and user/data subject-centric privacy model.

b) **SHALL** describe notice, consent, and other privacy interactions at the earliest possible point in a data transaction exchange with a user/data subject or her/his automated agent(s) or device(s).

Appendix A. Acknowledgements

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

Participants:

Peter Brown, Individual
Kim Cameron, Microsoft
Fred Carter, Office of the Information & Privacy Commissioner of Ontario, Canada
Ann Cavoukian, Office of the Information & Privacy Commissioner of Ontario, Canada
Les Chasen, Neustar
Michelle Chibba, Office of the Information & Privacy Commissioner of Ontario, Canada
Frank Dawson, Nokia
Mike Davis, Individual
Eli Erlikhman, SecureKey technologies, Inc.
Ken Gan, Ontario Canada Lottery and Gaming Corporation
Sander Fieten, Individual Member
Jonathan Fox, Intel Corporation
Frederick Hirsch, Nokia
Gershon Janssen, Individual Member
Dawn Jutla, Saint Mary's University
Antonio Kung, Trialog
Kevin MacDonald, Individual
Drummond Reed, XDI.org
John Sabo, Individual
Stuart Shapiro, MITRE Corporation
Aaron Temin, MITRE Corporation
Colin Wallis, New Zealand Government
David Weinkauf, Office of the Information & Privacy Commissioner of Ontario, Canada
Michael Willett, Individual

Appendix B. Revision History

Revision	Date	Editor	Changes Made
01	10 July 2013	Ann Cavoukian Fred Carter	Initial Draft Outline
02	20 Aug 2013	Ann Cavoukian Fred Carter	Revisions to document structure, content added to sections 1 and 2
03	07 Oct 2013	Ann Cavoukian Fred Carter	Incorporate TC member comments and suggested revisions to v02; modify document structure, add new PbD content. Revisions accepted by Committee 30 October 2013 as basis for next revision of working draft.
04	6 Mar 2014	Dawn Jutla	Introductory paragraphs added. Revised Section 3 as a methodology to produce *Privacy by Design* documentation for software engineers; steps refined and re-ordered Created and added new Section 4 (now section 2). Created and added new mapping of PbD principles to sub-principles, privacy services, and documentation. This new section links Sections 3 and 5. Restructuring of Section 5. Insertion of new materials
04	07/08 Mar 2014	Dawn Jutla	Refinement of Sections 3 and 4 with TC at March 7 and 8 face to face meetings.
04	07/08 Mar 2014 15 June 2014	Sander Fieten	Suggest use of conformance verbs for Table 4.1. (now Table 2.1) Suggested edits for Table 2.1; minor edits elsewhere.
04	10 Mar 2014	Dawn Jutla	Addition of further steps in methodology
04	7 Jan 2014 8 Mar 2014	Frank Dawson	Provided Spreadsheet modeling for Section 5. Contributions to methodology in Section 3.
04	21 Mar 2014 19 Apr 2014 10 May 2014 31 May 2014	Dawn Jutla	Filled in initial text for all 10 methodological steps, and created sample RACI table (Fig. 3.1) for the methodology in Section 3. Substantially revised and completed mapping of PbD-principles to documentation in Section 4 –Table 4.1 (now Table 2.1). Removed Privacy services mapping from this version. Added sections 5.2, 5.2.2, 5.2.2.1, 5.2.2.2, 5.2.2.4 and Architecture section 5.3 and 5.3.1. Substantial edits throughout sections 3, 4, & 5. Filled in section 1.4, and multiple edits throughout sections 1, 3, 4, 5, & 6 of document.

04	24 Apr 2014	Ann Cavoukian Fred Carter	Completion of Section 2 with 7 PbD principles and sub-principles. Substituted new descriptions of sub-principles into Table 4.1 (now Table 2.1)
04	29 Apr 2014	John Sabo	Added Privacy Use Template in Section 5.1.
	3 June 2014		Feedback and edits throughout
04	9 May 2014	Jonathan Fox	Added bulleted points in Sections 3.1 and 3.5.
04	9 May 2014	Tom Finneran	Created and added Section 5.2.2.3
04	15 Jun 2014	Fred Carter	Minor revisions to sections 2 and 4 + new conformance section 6
04	5 Jun 2014	Dawn Jutla	Processed John's edits and added conformance requirements to Section 3 for discussion.
	10 Jun 2014		Added Fred's edits to John's.
	17 Jun 2014		Combined TC edits (Jonathan, Stuart, Sander, John, Fred, Colin) and minor edits for sections 1, 3, 4, and 5
05	18 Jun 2014	Dawn Jutla	Processed Kim Cameron's suggestion for re-organization of document into (1) specification (former Section 4 becomes Section 2 in this document and former Section 6 becomes Section 3 in this document) and (2) an Annex How-to Guide to address specification elaboration and adoption.
06	21 Jun 2014	Dawn Jutla	Completed TC edits (from documents and emails), minor edits for alignment, and updated Master edits table compiled by the IPC