Privacy by Design Documentation for Software Engineers Version 1.0

Working Draft 04 – Section 1 with Comments and Notes [at end]

Updated 16 June 2014

Technical Committee:

[OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC](http://www.oasis-open.org/committees/pbd-se/)

Chairs:

Ann Cavoukian (commissioner.ipc@ipc.on.ca), [Office of the Information & Privacy Commissioner of Ontario](http://ipc.on.ca/), Canada

Dawn Jutla (dawn.jutla@gmail.com), [Saint Mary’s University](http://www.smu.ca/)

Editors:

Editor Name(s):

Ann Cavoukian, Office of the Information and Privacy Commissioner of Ontario, Canada, commissioner.ipc@ipc.on.ca

Fred Carter, Office of the Information and Privacy Commissioner of Ontario, Canada, fred.carter@ipc.on.ca

Dawn Jutla, Saint Mary’s University, dawn.jutla@gmail.com

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

Frank Dawson, Nokia, frank.dawson@nokia.com

Jonathan Fox, Intel Corporation, Jonathan\_Fox@McAfee.com

Tom Finneran, Individual, tfinneran@gmail.com

Related work:

This specification is related to:

* 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>

Declared XML namespaces:

* <http://docs.oasis-open.org/pbd-se/ns/pbd>
* <http://docs.oasis-open.org/pbd-se/ns/pbdse>

Abstract:

This specification describes a methodology to help engineers to model and document *Privacy by Design* (PbD) requirements, translate the principles to conformance requirements within software engineering tasks, and produce artifacts as evidence of PbD-principle compliance.

Status:

This [Working Draft](http://www.oasis-open.org/committees/process.php#dWorkingDraft) (WD) has been produced by one or more TC Members; it has not yet been voted on by the TC or [approved](http://www.oasis-open.org/committees/process.php#committeeDraft) as a Committee Draft (Committee Specification Draft or a Committee Note Draft). The OASIS document [Approval Process](http://www.oasis-open.org/committees/process.php#standApprovProcess) begins officially with a TC vote to approve a WD as a Committee Draft. A TC may approve a Working Draft, revise it, and re-approve it any number of times as a Committee Draft.

Initial URI pattern:

<http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/csd01/pbd-se-v1.0-csd01.doc>

**Citation format:**

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

 **[PbDSE-1.0]** *Privacy by Design Documentation for Software Engineers (PbD-SE) Version 1.0*, 11 June 2014, OASIS Working Draft 01, Revision 4, http://docs.oasis-open-org/…/pbd-se-v1 0-wd04.docx

Copyright © OASIS Open 2014. 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.

Table of Contents

1 Introduction 5

1.1 Context and Rationale 5

1.2 Objectives 5

1.3 Intended Audience 6

1.4 Outline of the Specification 6

1.5 Terminology 6

1.6 Normative References 7

1.7 Non-Normative References 7

2 *Privacy by Design* for Software Engineers Error! Bookmark not defined.

2.1 Review of the PbD Principles and their Purposes Error! Bookmark not defined.

2.1.1 Proactive not Reactive; Preventative not Remedial **Error! Bookmark not defined.**

2.1.1.1 Demonstrable Leadership **Error! Bookmark not defined.**

2.1.1.2 Defined Community of Practice **Error! Bookmark not defined.**

2.1.1.3 Proactive and Iterative **Error! Bookmark not defined.**

2.1.2 Privacy as the Default **Error! Bookmark not defined.**

2.1.2.1 Purpose Specificity **Error! Bookmark not defined.**

2.1.2.2 Limiting Collection, Use, and Retention **Error! Bookmark not defined.**

2.1.2.3 Limiting Collection **Error! Bookmark not defined.**

2.1.2.4 Collecting by Fair and Lawful Means **Error! Bookmark not defined.**

2.1.2.5 Collecting from Third Parties **Error! Bookmark not defined.**

2.1.2.6 Uses and Disclosures **Error! Bookmark not defined.**

2.1.2.7 Retention **Error! Bookmark not defined.**

2.1.2.8 Disposal, Destruction and Redaction **Error! Bookmark not defined.**

2.1.3 Privacy Embedded in Design **Error! Bookmark not defined.**

2.1.3.1 Holistic and Integrative **Error! Bookmark not defined.**

2.1.3.2 Systematic and Auditable **Error! Bookmark not defined.**

2.1.3.3 Reviewed and Assessed **Error! Bookmark not defined.**

2.1.3.4 Human-Proof **Error! Bookmark not defined.**

2.1.4 Full Functionality — Positive-sum, Not Zero-sum **Error! Bookmark not defined.**

2.1.4.1 No Loss of Functionality **Error! Bookmark not defined.**

2.1.4.2 Accommodate Legitimate Objectives **Error! Bookmark not defined.**

2.1.4.3 Practical and Demonstrable Results **Error! Bookmark not defined.**

2.1.5 End to End Security – Lifecycle Protection **Error! Bookmark not defined.**

2.1.5.1 Protect Continuously **Error! Bookmark not defined.**

2.1.5.2 Control Access **Error! Bookmark not defined.**

2.1.5.3 Use Metrics **Error! Bookmark not defined.**

2.1.6 Visibility and Transparency – Keep it Open **Error! Bookmark not defined.**

2.1.6.1 Open Collaboration **Error! Bookmark not defined.**

2.1.6.2 Open to Review **Error! Bookmark not defined.**

2.1.6.3 Open to Emulation **Error! Bookmark not defined.**

2.1.7 Respect for User\* Privacy – Keep it User-Centric **Error! Bookmark not defined.**

2.1.7.1 Anticipate and Inform **Error! Bookmark not defined.**

2.1.7.2 Support Data Subject Input and Direction **Error! Bookmark not defined.**

2.1.7.3 Encourage Direct User/Subject Access **Error! Bookmark not defined.**

3 Operationalizing the PbD Principles in Software Engineering Error! Bookmark not defined.

3.1 Organizational Privacy Readiness Error! Bookmark not defined.

3.2 Scope and Document Privacy Requirements Error! Bookmark not defined.

3.3 Conduct Privacy Risk Analysis and Privacy Property Analysis Error! Bookmark not defined.

3.4 Identify privacy resource(s) to support the Solution Development Team Error! Bookmark not defined.

3.5 Assign Responsibility for PbD-SE Operationalization and Artifacts Output Error! Bookmark not defined.

3.6 Design Error! Bookmark not defined.

3.7 Review Code Error! Bookmark not defined.

3.8 Plan for Retirement of Software Product/Service/Solution Error! Bookmark not defined.

3.9 Review Artifacts throughout the PDLC Error! Bookmark not defined.

3.10 Sign off with PbD-SE methodology check list Error! Bookmark not defined.

4 Mapping of Privacy by Design Principles to Documentation Error! Bookmark not defined.

5 Software Development Life Cycle Documentation for Privacy by Design Error! Bookmark not defined.

5.1 *Privacy by Design* Use Case Template for Privacy Requirements Error! Bookmark not defined.

5.2 Modeling Representations for Privacy Requirements Analysis & Design Error! Bookmark not defined.

5.2.1 Spreadsheet Modeling **Error! Bookmark not defined.**

5.2.2 Modeling Languages **Error! Bookmark not defined.**

5.2.2.1 Privacy by Design and Use Case Diagrams **Error! Bookmark not defined.**

5.2.2.2 Privacy by Design and Misuse Case Diagrams **Error! Bookmark not defined.**

5.2.2.3 *Privacy by Design* and Activity Diagrams **Error! Bookmark not defined.**

5.2.2.4 *Privacy by Design* and Sequence Diagrams **Error! Bookmark not defined.**

5.3 Privacy by Design and Privacy Reference Architecture Error! Bookmark not defined.

5.3.1 Privacy Properties **Error! Bookmark not defined.**

5.4 Privacy by Design and Design Patterns Error! Bookmark not defined.

5.5 Coding / Development Error! Bookmark not defined.

5.6 Testing / Validation Error! Bookmark not defined.

5.6.1 *Privacy by Design* Structured Argumentation **Error! Bookmark not defined.**

5.7 Deployment Phase Considerations Error! Bookmark not defined.

5.7.1 Fielding **Error! Bookmark not defined.**

5.7.2 Maintenance **Error! Bookmark not defined.**

5.7.3 Retirement **Error! Bookmark not defined.**

5.8 Privacy Checklists Error! Bookmark not defined.

Appendix A. Acknowledgements Error! Bookmark not defined.

Revision History Error! Bookmark not defined.

# Introduction

The OASIS *Privacy by Design* Documentation for Software Engineers Technical Committee provides a specification of a methodology to help engineers model and document *Privacy by Design* (PbD) goals and requirements, translate the PbD principles to conformance requirements within software engineering tasks, and produce artifacts as evidence of PbD-principle compliance. Outputs of the methodology document privacy requirements from software conception to retirement, thereby providing a plan around compliance to *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 such compliance to PbD 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.

The PbD-SE specification 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. It tackles 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). Software engineers reference documents that others in a software organization generate as well as produce their own documentation. Thus this specification further addresses the documenting of the organizational context 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 uses the Privacy Use Template, the OMG software modeling standard UML, and other popular representation languages and tools, including and not limited to, 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 SDLC.

## 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 privacy-respecting software systems, in order to promote wider adoption, gain trust and market success, and demonstrate legal and regulatory compliance.

## Objectives

This specification provides guidance and requirements for engineers to document privacy-enhancing objectives and associated control measures throughout the software development life cycle. This documentation is the output of the specification’s methodology 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.

## Intended Audience

The intended audience is primarily software engineers tasked with implementing and documenting functional privacy requirements and/or to show compliance to *Privacy by Design* principles. However, as software engineers operate in larger contexts, this specification should also be 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 organizations and standards bodies may find the PbD-SE useful in producing evidence of compliance to *Privacy by Design* principles.

## 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 process to insure 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 compliance to *Privacy by Design* principles.
* A mapping of the *Privacy by Design* principles to engineering-related sub-principles, and to documentation, and thus PbD-SE compliance criteria.
* Privacy considerations for the entire software development life cycle from software conception to software retirement.
* A Privacy Use Case Template that helps software engineers document privacy requirements and integrate them with core functional requirements.
* A *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 (developed in a future version of specification)
* *Privacy by Design* for Maintenance and Retirement (developed in a future version of specification)
* Software engineering Documentation Checklists

## 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].

**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**: any data about an individual including (1) any data that can be used to distinguish or trace an individual‘s identity, and (2) any other data 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)

**Personally Identifiable Information (PII)**: any information about an individual including (1) any information that can be used to distinguish or trace an individual‘s identity, and (2) any other information that is linked or linkable to an individual. 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.

## 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.

## Non-Normative References

**[BIRO 2009]**

The BIRO Project, Cross-border flow of health information: is 'privacy by design' enough? Privacy performance assessment in EUBIROD. Available at <http://www.ncbi.nlm.nih.gov/pubmed/22562711>.

[**Cavoukian 1995]**

Privacy-Enhancing Technologies: The Path to Anonymity, Volume II, available at <http://www.privacybydesign.ca/content/uploads/1995/03/anoni-v2.pdf>

[**Cavoukian 2011]**

*Privacy by Design*: *The 7 Foundational Principles Implementation and Mapping of Fair Information Practices* at [www.ipc.on.ca/images/Resources/pbd-implement-7found-principles.pdf](http://www.ipc.on.ca/images/Resources/pbd-implement-7found-principles.pdf) [**Cavoukian 2012]**

*Privacy by Design*: Leadership, Methods, and Results, Chapter 8: [http://link.springer.com/chapter/10.1007%2F978-94-007-5170-5\_8](http://link.springer.com/chapter/10.1007/978-94-007-5170-5_8), *5th Int. Conference on Computers, Privacy & Data Protection European Data Protection: Coming of Age,* Springer, Brussels, Belgium.

[**CICA 2014]**

CICA/AICPA Privacy Maturity Model, available at http://www.cica.ca/resources-and-member-benefits/privacy-resources-for-firms-and-organizations/docs/item48094.pdf

**[Dennedy et al 2014]**

[Michelle Finneran Dennedy](http://www.apress.com/author/author/view/id/7426), [Jonathan Fox](http://www.apress.com/author/author/view/id/7427), [Thomas Finneran](http://www.apress.com/author/author/view/id/7428) (2014). *The Privacy Engineer’s Manifesto: Getting from Policy to Code to QA and Value*, Apress, Jan. 2014, 400 pages.

**[Jutla and Bodorik 2005]**

Dawn N. Jutla, Peter Bodorik (2005), Sociotechnical Architecture for Online Privacy, *IEEE Security and Privacy*, vol. 3, no. 2, pp. 29-39, March-April 2005, doi:10.1109/MSP.2005.50.

**[Jutla et al 2013]**

Dawn N. Jutla, [Peter Bodorik](http://www.informatik.uni-trier.de/~ley/pers/hd/b/Bodorik%3APeter.html), [Sohail Ali](http://www.informatik.uni-trier.de/~ley/pers/hd/a/Ali%3ASohail.html) (2013). [Engineering Privacy for Big Data Apps with the Unified Modeling Language](http://www.smu.ca/commonresources/webfiles/Jutla-Extending_Use_Case_Diagrams_with_Privacy_Services.pdf). *IEEE* [*Big Data Congress 2013*](http://www.informatik.uni-trier.de/~ley/db/conf/bigdata/bigdata2013.html#JutlaBA13): 38-45. Santa Clara.

**[Jutla 2014]**

Evolving OASIS *Privacy by Design* Standards, April 9, 2014, available at <http://csrc.nist.gov/news_events/privacy_workshop_040914/nist_pew_2014dawn_jutla.pdf>

**[Jutla 2014a**]

M2M Vehicle Telematics and the OASIS Privacy by Design Documentation for Software Engineers (PbD-SE), *European Identity and Cloud Conference*, Munich, April 15 2014, slide deck available to attendees.

**[Jutla 2014b]** Overview of the OASIS PbD-SE and PMRM emerging privacy standards, *PRIPARE workshop*, Cyber Security and Privacy Forum, Athens, May 22, 2014.

Evolving OASIS Privacy by Design Standards, April 9, 2014, available at <http://csrc.nist.gov/news_events/privacy_workshop_040914/nist_pew_2014dawn_jutla.pdf>

 **[Jutla et al 2014]**

Dawn N. Jutla, Ann Cavoukian, John T. Sabo, Michael Willett, Fred Carter, Michelle Chibba, *Operationalizing Privacy by Design Documentation for Software Engineers and Business: From Principles to Software Architecture*, submitted for journal review, April 21, 2014.

**[PbD-FIPPS]**

Cavoukian, A., *The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices*, <http://bit.ly/vjvrPE> January 2011

[NIST 800-53] [Security and Privacy Controls for Federal Information Systems and Organizations Revision 4, Appendix J: Privacy Controls Catalog]

**[Shostack 2014]**

Adam Shostack (2014), *Threat Modeling: Designing for Security*, Wiley, Feb 2014.624 pages.

 **[Zachmann 1987]**

J. Zachmann. [A framework for information systems architecture.](http://zachman.com/images/ZI_PIcs/ibmsj2603e.pdf) IBM Systems Journal, Vol. 26. No. 3, 1987.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Notes: Accepted the great majority of edits from John, Stuart, Jonathan, Sander, Colin, Gail, and Fred.

Further requests for clarification and comments to address TC’s edits and comments

Stuart: Page 5, please can you explain why we may need to clarify “ beyond user/data subject preferences”?

Jonathan: I intend to add text and an edited diagram to illustrate how the Privacy by Design Use Case Template can be adapted for agile methodology and user stories. So the “however” is not needed. I have suggested to John that we can rename it to the Privacy Use Template so that agile methodologists do not feel that the PbD-SE spec is not applicable to them.

John: We may leave a few further details about the PMRM to Section 5 without loss to the PbD-SE introduction. I left in the PMRM reference as normative as you correctly stated that the PbD-SE WD asserts that Privacy Use Template is RECOMMENDED for embedding privacy requirements in a Privacy Use Case or User Story, then the Normative designation for PMRM is appropriate as the accessible Privacy Use Template is based on the PMRM.

Fred: I added goals in section 1 but also left in requirements as software engineers interests in this document are for privacy requirements and the documentation required by PbD.

Sander and Colin: There are normative references to section 5 in Table 4.1. e.g. to the Privacy Use Template that provides documentation in itself. There will be more explicit linking of software engineering documentation, or spec asks for “equivalent” documentation across Sections 3, 4, and 5.

Text formatting edits will be re-applied to full document.