**PbD-SE Privacy Use Case Template**

**Purpose:**

The Privacy Use Case Template is a foundational tool that provides a structured format for describing Use Cases relevant to the objectives of the PbD-SE Technical Committee. The Use Case Template provides a “first step” in addressing several objectives outlined in the “Scope” section of the PbD-SE Charter:

* Ensure that software developers integrate privacy requirements (e.g. need for notice, disclosure, obtaining user consent, user access, data minimization, data security, and others as determined by the PbD principles) into functional use cases for software products and services.
* Ensure that privacy interface design guidelines, such as the 7 Cs (Comprehension, Consciousness, Choice, Consent, Context, Confinement, and Consistency) are incorporated into interface designs and are well documented.
* Ensure that attention is paid to the distribution and linkage of personal data between entities in class diagrams. When design-level classes are created, an intermediate level of "Privacy by Design" classes may be layered into the class mappings.
* A misuse case should be developed for each use case that deals with the handling of personally identifiable data.

As Use Cases are collected, they can be organized into both “application” categories (such as “mobile banking”) and also “model” categories or sub-categories (such as “three domain model”) usable for the TC to begin further work in addressing its scope and its deliverables. The template may also be helpful in developing a second template for the “misuse”cases.

The PbD-SE Privacy Use Case Template is built on the Privacy Management Reference Model and Methodology (PMRM) “Develop Use Case Description and High Level Privacy Analysis” and “Develop Detailed Privacy Analysis” specifications. However, for purposes of the TC’s initial work, the template does not require the level of detail anticipated by the PMRM.

The template includes two components: a “High Level Use Case Description” and a “Detailed Use Case Description.”

**HIGH LEVEL USE CASE DESCRIPTION**

1. Use Case Title

2. Category of Use Case [To be established as Used Cases are submitted - may be Application categories or Model categories]

3. Provide a general description of the Use Case

4. Provide a summary inventory for the Use Case, including:

* Application(s) associated with Use Case
* Data subject(s) associated with Use Case
* Parties and Business processes associated with Use Case
* Systems supporting the Use Case applications;
* Products Created in Use Case;
* PI and PII covered by the Use Case
* Legal, regulatory and /or business policies governing the Use Case

5. Provide or include link to a PIA if available

**DETAILED USE CASE DESCRIPTION**

1. Identify Participants having operational privacy responsibilities.

2. Identify the Systems where PI /PII is collected, communicated, processed, stored or disposed within a Privacy Domain.

**3.** Identify the Privacy Domains included in the Use Case together with the respective Domain Owners.

* A “Domain” covers both physical areas (such as a customer site or home) and logical areas (such as a wide-area network or cloud computing environment) that are subject to the control of a particular domain owner. Privacy Domains may be under the control of data subjects as well as other Participants
* A “Domain Owner” is the Participant responsible for ensuring that privacy controls and PMRM services are managed in business processes and technical systems within a given Domain.

4. Identify the roles and responsibilities assigned to specific Participants and Systems in each Privacy Domain in the Use Case

5. Identify the touch points at which the data flows intersect with Privacy Domains or Systems within Privacy Domains.

* Touch Points are the intersections of data flows with Privacy Domains or Systems

6. Specify the PI/PII collected, created, communicated, processed or stored within Privacy Domains or Systems in the Use Case, in three categories:

* Incoming PI/PII
* Internally generated PI/PII
* Outgoing PI/PII

7. For Incoming, Internally Generated and Outgoing PI, specify the privacy controls required/implemented to enforce the privacy policy associated with the PI/PII.

* Privacy controls are typically associated with specific Fair Information Practices Principles (FIP/Ps) that apply to the PI/PII.

8. For each category of PI/PII, specify the controls in three Control Categories:

* Inherited Privacy Controls
  + For example, controls defined by Data Subject consent
* Internal Privacy Controls
  + For example, controls defined by the business system or embedded I the application
* Exported Privacy Controls
  + For example, controls that must be implemented by a third or any external domain, system, application with which PI/PII is shared