Operationalizing ***Privacy by Design*** Principles in Software Engineering

|  |  |  |
| --- | --- | --- |
| *PbD “Sub-Principles”* | *Compliance Criteria* | *Requirement(s)* |
| **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. | * Commitment to apply OASIS Specification to software engineering project | * Documentation MUST normatively reference PdD-se specification * Documentation MUST reference the applicable privacy policy |
| **1.2–Defined Community of Practice**: Demonstrable privacy commitment shared by organization members, user communities and stakeholders. | * Relevant stakeholders and team assembled for project | * Project plan MUST describe *privacy champ/lead/…* * All [categories of] data subjects SHOULD be listed as a stakeholder * Project plan MUST include RACI matrix for privacy resources |
| **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. | * OASIS Specification applied at earliest stages of software engineering and at critical points thereafter. | * Project plan MUST include privacy section * Other documents SHOULD include privacy section *(might be limited to saying not applicable)* * Documentation MUST define privacy metrics * Documentation MUST include privacy review reports *(either in reviewed documents or in separate report)* |
| **2. Privacy as the *Default* Setting (Data Minimization)** | |  |
| **2.1–Purpose Specificity:** Purposes must be specific and limited, and be amenable to engineering controls | * *See separate Appendix for illustrative list of methods, techniques and tools* * OASIS PbD-SE methodology and OASIS PMRM specifications applied   For each functional use case/user story, integrated privacy requirements with the ***EQUIVALENT*** to the unified modeling language (UML) used in software engineering: Use Case Template or User Story BoardsUse Case DiagramMisuse Case DiagramClass DiagramActivity DiagramSequence Diagram Identified privacy controls and services e.g. the PMRM-type Services:  e.g. Agreement, Validation, Usage, Interaction, Certification, Security, Enforcement, and Access  AND other  e.g. Minimization, De-Identification, Monitoring, Data classification services. | * Documentation MUST describe functional and privacy requirements. * Documentation MUST relate technical components to functional and privacy requirements. |
| **2.2–Adherence to Purposes:** methods must be in place to ensure that personal data is collected, used and disclosed:   * 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; * Uses and Disclosures; * Retention; * Disposal, Destruction; and Redaction * Transparancy and visibility | * Documentation MUST describe data and behavioural requirements for each use case/user story, and possible misuses of data. * Documentation MUST describe selection of privacy controls/services and where they apply to functional requirements. |
| **3. Privacy *Embedded* into Design** | |  |
| **3.1–Holistic and Integrative**: Privacy commitments must be embedded in holistic and integrative ways | * Widest possible project scope adopted * Documentation MUST describe data and behavioural requirements for each use case/user story, and possible misuses of data. * Documentation MUST describe selection of privacy controls/services and where they apply to functional requirements. | * Scope MUST include “privacy functionality” *(relates to PMRM functions/services)* * The OASIS PMRM Privacy Use Case Template is RECOMMENDED for describing privacy requirements. * Documentation MUST include identification of privacy architectural design principles * Documentation MUST contain a Privacy Architecture * Documentation MUST contain description of the Business Model showing personal data flows for software services |
| **3.2–Systematic and Auditable:** A systematic, principled approach should be adopted that relies upon accepted standards and process frameworks, and is amenable to external review. | * Acknowledged software engineering process/methodology adopted * Metrics applied * Privacy Metrics, e.g. effectiveness, monitored | * Architecture documents SHOULD include privacy view (this does not apply only to software engineering do * Documentation MUST identify the software engineering process/methodology used * Documentation SHOULD contain evidence of monitoring of privacy metrics |
| **3.3–Review and Assess:** Detailed privacy impact and risk assessments should be used as a basis for design decisions. | * Completed PIA and/or TRA * Completed Priority Matrix of Privacy Controls/Threats from Risk Analysis | * Documentation MUST contain a PIA * Documentation SHOULD contain TRA for privacy |
| **3.4–Human-Proof:** The privacy risks should be demonstrably minimized and not increase through use, misconfiguration, or error. | * Appropriate privacy failsafe mechanisms adopted | * Documentation SHOULD describe configuration parameters and their impact on privacy risks * Software SHOULD warn about events that increase privacy risks (including misconfiguration, errors or misuse). These warnings MUST be documented * Documentation MUST contain identification and description of privacy controls. |
| **4. Full Functionality — *Positive-sum*, Not Zero-sum** | |  |
| **4.1–No Loss of Functionality:** Embedding privacy should not impair functionality of a given technology, process or network architecture. | * Functional objectives achieved | * Documentation MUST limitative describe all functional objectives |
| **4.2–Accommodate Legitimate Objectives**: All interests and objectives must be documented, desired functions articulated, metrics agreed, and trade-offs rejected, when seeking a solution that enables multi-functionality | * Outcomes mapped/matched to requirements | * Documentation SHOULD describe rationale for objectives |
| **4.3–Practical and Demonstrable Results**: Optimized outcomes should be published for others to emulate and become best practice. | * Outcomes replicable/reusable in other systems | * It is RECOMMENDED that [generic] solutions are made publicly available |
| **5. End to End Security – 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 | * Encrypt by Default:Whether at rest, in transit, or in use, data should be protected, by default. * Authenticate Privileges, Not Identities:Seek privacy enhanced identity, authentication and access controls. * Trust, But Verify:Activity monitoring, logging and auditing are credible deterrents but should not introduce new privacy risks. |  |
| **5.2–Control Access:** Access to personal data should be commensurate with its degree of sensitivity, and be consistent with recognized standards and critieria. |  |
| **5.3–Use Metrics:** Applied security standards must assure the confidentiality, integrity and availability of personal data and be amenable to verification. |  |
| **6. Visibility and Transparency – Keep it Open** | |  |
| **6.1–Open Collaboration:** Privacy requirements, risks, implementation methods and outcomes should be documented throughout the development lifecycle and communicated to project members and stakeholders. | * Records retained of key project consultations and decisions |  |
| **6.2–Open to Review:** The design and operation of software systems should demonstrably satisfy the strongest privacy laws, contracts, policies and norms (as required). | * Where relevant, documentation should support compliance and other reporting/diligence/validation requirements |  |
| **6.3–Open to Emulation:** The design and operation of privacy-enhanced information technologies and systems should be open to scrutiny, praise and emulation by all. | * Where the software product is to be used by other systems, relevant documentation should be available |  |
| **7. Respect for User\* Privacy – Keep it User-Centric** \*User = Data Subject | |  |
| **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. | * Attention to effective UI/UX Design |  |
| **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. | * Privacy options and controls are available, prominent, clear and effective |  |
| **7.3–Encourage Direct User/Subject Access:** Software systems should be designed to provide data subjects direct access to data held about them, and an account of uses and disclosures. | * Record of personal data uses is available to data subjects |  |