**Privacy by Design Documentation for Software Engineers Properties**

|  |  |
| --- | --- |
| **PbD Principle** | **Documentation Properties** |
| 1. Proactive not Reactive; Preventative not Remedial | * Privacy risk model(s) is(are) identifiable
* Privacy risk management documentation includes
	+ System description
	+ Analysis and risk identification
	+ Risk controls
* There is a clear mapping between privacy risks and privacy risk controls
* Personal information is called out as such
* Sensitivity of personal information is indicated
 |
| 2. Privacy by Default | There is traceability between personal data elements and system requirements involving collection, use, disclosure, and retention |
| 3. Privacy Embedded into Design | * Privacy requirements are explicitly articulated/designated
* There is traceability between privacy requirements and system design
* Privacy requirements are associated with other requirements when necessary to support the development life cycle
* There is a privacy-specific architectural view
 |
| 4. Full Functionality: Positive Sum, not Zero-Sum | High-level requirements, including privacy requirements, are design and implementation independent (what, not how) |
| 5. End-to-End Lifecycle Protection | There is a personal information life cycle view of privacy and security* Risk analyses
* Requirements
* Architectures
* Designs
 |
| 6. Visibility and Transparency | Privacy requirements include transparency mechanisms at the point of use and/or elsewhere as applicable |
| 7. Respect for User Privacy | * There is a privacy view of requirements, architecture, and design
* There is an explicit user model that includes privacy
* Validation and operational documentation addresses the user model
 |