**A review of the Conformance Chapter 3 of Privacy by Design Documentation for Software Engineers Version 1.0 by Gail Magnuson using the NYMITY Privacy Management Accountability Framework available at** [**http://www.nymity.com/Whitepapers.aspx**](http://www.nymity.com/Whitepapers.aspx)

Introduction:

* First and foremost, congratulations on developing such a thorough and thoughtful document. It is truly impressive.
* Second, I apologize for not using track change. I have made gray the changes I made to the existing text and made my additions in italic.
* Third, when John and Gershon encouraged us to review the work in the latest PMRM meeting, I decided to compare Chapter 3 to the Nymity Privacy Management Accountability Framework with its 13 Privacy Management Processes (PMPs) and its 150+ Privacy Management Activities (PMAs). Needless to say, it took a few more hours than I expected ☺
* My findings or observations include:
	+ Overall observations
	+ Recommendations for small changes
	+ Recommendations for additions
* While the two works are written in different voices/perspectives for different audiences, I attempted to map each of the SHALL statements to the corollary NYMITY PMP and or specific PMA. When I referenced an entire PMP I said so. Where I referred to a PMA I just listed it. The process reminds me just how complex, dynamic and illusive.
* Finally, I do hope, that as I explain each recommendation, you receive them as suggestions to be used/or not.

Observations:

* Overall observations
	+ This is an important work, along with the PMRM work and naturally others in **helping to codify/standardize/translate privacy (and security), especially for those that develop systems, applications, technologies and processes.**
	+ **In the overall comparison**, my observation was that:
		- The **consistent references to terminology** of strategies (corporate directives); objectives; policies (corporate internal commitment); notices (external corporate commitment); guidelines (enabling direction to engineers); controls; services; requirements (engineer specifications) is key. I where I saw places where one or more terms might be missing I added them (but not thoroughly) I eliminated the term ‘principles’, only because this was a term I never used in my corporate life relating to privacy. In reading the definition I would suggest that a principle comes before a policy.
			* It might be good to define the terms you would like to use in section 1.5 along with their relationship and order. I have listed them in the order I used them. Then, naturally edit the document accordingly.
		- I would recommend **establishing the same set of terminology regarding the collection, storage, use, sharing, transborder flows, securing and retirement of personal** data and editing the document accordingly
		- I would love to see a **definition for “Privacy Architecture”**. I have always thought that privacy was integrated into systems and process/operations architectures. I would be interested in knowing what a privacy architecture is.
		- **Security** was rarely referenced. While I appreciate that privacy includes security, it might be beneficial to strengthen the security references throughout.
		- **Transborder flows and working with Data Protection Authorities and establishing data transfer mechanisms** were not specifically referenced. It might be beneficial to add references to reinforce the flows of information between jurisdictions and the required work with DPAs and legal contracts.
		- **The treatment of flows of data to third parties**, required contractual language, risk assessing, auditing/monitoring such external flows might be added as well. I recommended additions in the Privacy Embedded into Design section. There may be other places as well
		- **Consider removing duplication**. As I made my correlations, I noticed that I was repeating Nymity references for many of the PbD sections and statements. Some of these repetitions were due to the fact that the details where inside the Nymity references. Others however might indicate a need to streamline the PbD document requirements. I defer to the editing team on this matter.
		- Finally, while this document is targeted to software engineers, **it applies to any and all product developers of systems, applications, technology and processes**. As the mother of two very brilliant engineers and a mother-in-law to a bio-informatics/genomics PhD candidate, all who hold various patents, I would strongly encourage you to broaden the audience, in name, for this work. In so many situations, software is but a minor tool (much like word, excel, wiring, et. al.) in the development of breakthrough inventions such as a low cost ventilator developed by a small team in a premier west coast university or the monitoring of each battery performance and quality in an electronic car company. While we focus on software engineers at major companies, you might consider producing a summary version of this work (once it is ready for publication) that might reach those that are inventing technologies for the 21st century.
* Recommendation for small changes (see my comments)
* Recommendation for additions (see my comments)
* Enjoy!

|  |  |
| --- | --- |
| **1. Proactive, Not Reactive:** | **Nymity Privacy Management Activities** |
| **Documentation:** 1. **SHALL** normatively reference the PbD-SE specification
2. **SHALL** reference assignment of responsibility and accountability for privacy in the organization, its allocation of funds and privacy training program(s), including. the employees’ commitment to policy and metrics of participation, completion and comprehension
3. **SHALL** include assignment of privacy resources to the software project, recording who are responsible, accountable, consulted, or informed for various privacy-related tasks
4. **SHALL** reference all external sources of privacy requirements, including strategies, policies, notices, ~~principles~~, guidelines and regulations.
5. **SHALL** include privacy requirements specific to the service/product being engineered, anticipated deployment environments and all service providers
6. **SHALL** include privacy risk/threat model(s) including analysis and risk identification, risk prioritization, and controls clearly mapped to risks
7. ***SHALL*** *include reporting the status of the privacy program to designated stakeholders*
 | **Documentation:** 1. **SHALL** normatively reference the PbD-SE specification
2. Assign responsibility for data privacy; Maintain job descriptions for individuals responsible for data privacy; Assign accountability for data privacy at a senior level; Allocate resources to adequately implement and support the privacy program; Appoint a representative in member states where the organization does not maintain a physical presence; Require employees to acknowledge and agree to adhere to the data privacy policies; Conduct data privacy training needs analysis by position/job responsibilities; Maintain a core training program for all employees; Conduct training for newly appointed for newly appointed employees upon assignment to privacy sensitive positions; Maintain a second level training program reflecting job specific content; Conduct regular refresher training to reflect new developments; Integrate data privacy into other training programs such as HR, security, call center, retail operations training; Measure participation in data privacy training in data privacy training activities (e.g. numbers of participants, scoring); Require completion of data privacy training as part of performance reviews; Measure comprehension if data privacy comprehension; Conduct one-off, one –time tactical training and communication dealing with specific , highly-relevant issues/topics; Provide ongoing education and training for the privacy office (e.g. conferences, webinars, guest speakers);
3. Assign responsibility for data privacy;
4. Maintain a Privacy Strategy; Maintain a privacy program charter; Maintain a data privacy policy; Maintain a Code of Conduct; Maintain ethics guidelines; PMP 8 Maintain Notices (10 PMAs); PMP 9 Maintain Procedures for Inquiries and Complaints (10 PMAs); Document legal basis for processing personal data; Document guiding principles for consent; Conduct ongoing research on developments in law; Record/report on the tracking of new Rule Source or amendments to Rule Sources; Seek legal opinions regarding recent developments in laws; Document that new requirements have been implemented (also document where a decision is made to not implement changes, including reason); .
5. Applicable PMP 4 Embed Data Privacy into Operations (31 PMAs); Maintain a Privacy by Design framework for all system and product development; Conduct PIAs for new programs, systems, processes; Maintain a procedure to address data protection issues identified during PIAs;
6. Conduct a Privacy Risk Assessment; Integrate data privacy into business risk assessment/reporting; PMP 12 (7 PMAs)
7. Report, on a scheduled basis, on the status of the privacy program (e.g. board of directors, management board); Report periodically on the status of the privacy program, as appropriate (e.g. annual reports, third parties, clients)
 |
| **2. Privacy as the Default** |  |
| **Documentation:** 1. **SHALL** list all [categories of] data subjects as a stakeholder
2. **SHALL** clearly document the purposes for collection and processing, including retention of personal data
3. **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, operations, systems, jurisdictions, APIs, and/or imported code.
4. **SHALL** describe selection of privacy controls and privacy services/APIs and where they apply to privacy functional requirements and risks.
5. **SHALL** include software retirement plan from a privacy viewpoint
 | 1. Maintain a Privacy by Design framework for all system and product development;
2. Conduct PIAs for new programs, systems and processes
3. Maintain an inventory of key personal data holdings (what personal data is held where); Classify personal data holdings by type (e.g. sensitive, confidential, public); Maintain flow charts for key data flows (e.g. between systems, between processes, between countries); Maintain documentation for all cross-border data flows (e.g. country, mechanism used as a basis for the transfer such as Safe Harbor, model clause, binding corporate rules, or approvals from data protection authorities);
4. Applicable PMP 4 Embed Data Privacy into Operations (31 PMAs)
5. Applicable PMP 4 Embed Data Privacy into Operations (31 PMAs)
 |
| **3. Privacy Embedded into Design** |  |
| **Documentation:** 1. **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
2. **SHALL** contain description of business model showing traceability of personal data flows for any data collected through new software services under development.
3. **SHALL** include identification of privacy design ~~principles~~ guidelines
4. **SHALL** contain a privacy architecture
5. **SHALL** describe privacy UI/UX design
6. **SHALL** define privacy metrics
7. **SHALL** include human sign-offs/privacy checklists for software engineering artifacts
8. **SHALL** include privacy review reports *(either in reviewed documents or in separate report)*
9. **SHALL** treat *privacy-as-a-functional requirement* i.e. functional software requirements and privacy requirements should be considered together, with no loss of functionality.
10. **SHALL** show tests for meeting privacy requirements ~~objectives,~~ in terms of the operation and effectiveness of implemented privacy controls or services
11. **SHALL** be produced for all stages of the software development lifecycle from referencing applicable strategies, policies, guidelines principles, and regulations to defining privacy requirements, to design, implementation, maintenance, and retirement.
12. **SHALL** reference requirements, risk analyses, architectures, design, implementation mechanisms, retirement plan, and sign-offs with respect to privacy and security.
13. **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.
14. **SHALL** demonstrate designs and implementations that satisfy state-of-the-art privacy *~~properties~~* techniques
15. ***SHALL*** *demonstrate designs and implementations that deliver state-of-the-art security techniques;*
16. ***SHALL*** *demonstrate designs and implementations that deliver state-of-the-art Third Party risk Management*
17. ***SHALL*** *demonstrate designs and implementations that are supported by the appropriate legal requirements*
18. ***SHALL*** *demonstrate designs and implementations that are integrated into the organizations data breach management program*
 | 1. Maintain a Privacy by Design framework for all system and product development;
2. Maintain an inventory of key personal data holdings (what personal data is held where); Classify personal data holdings by type (e.g. sensitive, confidential, public); Maintain flow charts for key data flows (e.g. between systems, between processes, between countries); Maintain documentation for all cross-border data flows (e.g. country, mechanism used as a basis for the transfer such as Safe Harbor, model clause, binding corporate rules, or approvals from data protection authorities);
3. Maintain a Privacy by Design framework for all system and product development; PMP 4 Embed Data Privacy into Operations (31 PMAs)
4. Maintain a Privacy by Design framework for all system and product development
5. Maintain a Privacy by Design framework for all system and product development
6. Maintain privacy program metrics
7. Maintain a product sign-off procedure that involves the privacy office
8. Maintain a product sign-off procedure that involves the privacy office
9. Maintain a Privacy by Design framework for all system and product development
10. Maintain a Privacy by Design framework for all system and product development; PMA Monitor Data Handling Practices (7 PMAs)
11. Maintain a Privacy by Design framework for all system and product development; PMA Monitor Data Handling Practices (7 PMAs)
12. Maintain a Privacy by Design framework for all system and product development; PMA Monitor Data Handling Practices (7 PMAs); Conduct a Privacy Risk Assessment
13. Maintain privacy program metrics
14. Maintain a Privacy by Design framework for all system and product development;
15. PMP 6 Manage Information Security Risk (13 PMAs)
16. PMP 7 Manage Third Party Risk (8 PMAs)
17. Obtain approval for data processing (where prior approval is required); Register data bases with data protection authority (where prior approval is required); Use BCRs, Standard Contractual Clauses, CBPR, SH, Data Protection Authority approval and/or adequacy as a data transfer mechanism; Maintain a strategy to align Activities with legal requirements; Consult with stakeholders throughout the organization on data privacy matters; Maintain procedures to execute contracts or agreements
18. PMP 11 Maintain Data Privacy Breach Management Program
 |
| **4. Full Functionality: Positive Sum, not Zero-Sum** |  |
| **Documentation:**1. **SHALL** treat *privacy-as-a-functional requirement,* i.e. functional software requirements and privacy requirements should be considered together, with no loss of functionality.
2. **SHALL** show tests for meeting privacy objectives, in terms of the operation and effectiveness of implemented privacy controls or services
 | 1. PMP 4 Embed Data Privacy into Operations (31 PMAs)
2. PMP 12 Monitor Data Handling Practices (7 PMAs)
 |
| **5. End to End Safeguards: Full Lifecycle Protection** |  |
| **Documentation:**1. **SHALL** be produced for all stages of the software development lifecycle from referencing applicable strategies, ~~principles~~, policies, guidelines and regulations to defining privacy requirements, to design, implementation, maintenance, and retirement.
2. **SHALL** reference requirements, risk analyses, architectures, design, implementation mechanisms, retirement plan, and sign-offs with respect to privacy and security.
3. **SHALL** include security and privacy metrics and monitoring practices designed in and/or deployed in the software, or monitoring software, or otherwise in the organization, and across partnering software systems or organizations.
4. **SHALL** demonstrate designs and implementations that satisfy state-of-the-art privacy *properties*.
 | 1. Maintain a Privacy by Design framework for all system and product development; Maintain a product life cycle process to address privacy impacts of changes to existing programs, systems or processes
2. Maintain a Privacy by Design framework; Maintain a product sign-off procedure that involves the privacy office
3. PMP 12 Monitor Data Handling Practices (7 PMAs)
4. PMP 4 Embed Data Privacy into Operations (31 PMAs)
 |
| **6. Visibility and Transparency: Keep It Open** |  |
| **Documentation:**1. **SHALL** *reference*the privacy policies and documentation of all other collaborating stakeholders
2. **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, transborder flows, retirement and/or elsewhere as applicable
3. **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.
4. **SHALL** describe placement of privacy settings, privacy controls, privacy notices ~~policy(ies),~~ and accessibility, prominence, clarity, and intended effectiveness
 | 1. Maintain data privacy requirements for third parties (e.g. vendors, processors, affiliates); Maintain a policy governing use of cloud providers; Applicable PMP 4 Embed Data Privacy into Operations (31 PMAs);
2. Integrate data privacy into customer/patient/citizen facing practices (e.g. retail sales, provision of healthcare, tax processing);
3. Maintain privacy program metrics;
4. PMP 12 Monitor Data Handling Practices (7 PMAs);
 |
| **7. Keep it User-Centric** |  |
| **Documentation:**1. **SHALL** describe user/data subject privacy options (including access), controls, user privacy preferences/settings, UI/UX supports, and user/data subject-centric privacy model.
2. **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).
 | 1. Maintain policies for collecting consent preferences; Integrate data privacy into customer/patient/citizen facing practices (e.g. retail sales, provision of healthcare, tax processing); PMP 9 Maintain Procedures for Inquiries and Complaints (9 PMAs)
2. PMP 8 Maintain Notices (8 PMAs)
 |