



Privacy Reference Model

The privacy architecture contained herein provides an approach for capturing privacy requirements and capabilities within an organization's systems and architecture (EA). Specific benefits yielded by incorporating privacy into architecture efforts include

- Ensuring performance objectives, business processes, service-components, technologies, and data each appropriately maps to privacy.
- Describing privacy in the context of a reference model aids in standardizing and consolidating privacy capabilities as appropriate.

Privacy Taxonomy

In order to realize the benefits promised by architectural efforts, organizations must first have a common taxonomy. With the rules governing the handling of personal information slightly different depending on the sector (such as the health sector and the financial services sector in the US) and the jurisdiction (EU rules differ from US rules), a common taxonomy would prove particularly useful for privacy and for those enterprises operating under a complex privacy patchwork. To that end the privacy reference model provides a taxonomy for describing 17 controls that systems and enterprises collecting, storing, and using personal information will need to address.

These privacy control families are as follows:

1. Policies and Procedures – Creating policies and procedures governing the appropriate use of personal information and implementing privacy controls.
2. Privacy as Part of the Development Life Cycle – Implementing privacy reviews and controls throughout the system development life cycle.
3. Assigned Roles, Responsibilities, and Accountability –Identifying general and specific roles and responsibilities for managing and using personal information and ensuring accountability for meeting these responsibilities.
4. Monitoring and Measuring –Monitoring the implementation of privacy controls and measuring their efficacy.
5. Education: Awareness and Role-based Training Programs–Ensuring managers and users of personal information are made aware of the privacy risks associated with their activities and of applicable laws, policies, and procedures related to privacy.
6. Public Disclosure–Publicly disclosing privacy policies and procedures for a program or system.

7. Notice-Providing notice of the information practices to the individual before collecting personal information.
8. Consent-Gaining consent from the individual to use their personal information.
9. Minimum Necessary-Collecting the minimum amount of personal information necessary to accomplish the business purpose.
10. Acceptable Use-Ensuring that personal information is used only in the manner provided on the notice, to which the individual consented, and in accordance with the publicly disclosed practices.
11. Accuracy of Data-Ensuring that personal information is accurate, particularly if harm or denial of benefits may result.
12. Individual Rights-Providing individuals an opportunity to access and correct their personal information and to seek redress for privacy violations.
13. Authorization-Ensuring that the individual authorizes all new and secondary uses of personal information not previously identified on the original collection notice.
14. Chain of Trust-Establishing and monitoring third-party agreements for the handling of personal information.
15. Risk Management-Assessing and managing risks to operations, assets, and individuals resulting from the collection, sharing, storing, transmitting, and use of personal information.
16. Reporting and Response-Providing senior managers and oversight officials the results of the monitoring and measuring of privacy controls and responding to privacy violations.
17. Security Measures-Implementing the appropriate safeguards to assure confidentiality, integrity and availability of personal information.

These privacy controls will vary depending on the other aspects of the enterprise architecture, for privacy cuts across all other reference models. For example, the line of business, the human resources function of a corporation operating in the EU will likely have a very different set of privacy controls than a US corporation that is a Health Insurance Portability and Accountability Act (HIPAA)-covered entity. However, both would need to have controls within the notice and consent family.

Using a Privacy Reference Model

To use the reference model, organizations should follow a three-phased approach:

1. **Step 1: Identification**–Identify privacy requirements and capabilities. For a system or enterprise, all applicable laws and regulations as well enterprise-specific policies and preferences should be analyzed and categorized according to the privacy control families. Similarly, technologies and service components that either directly support or have privacy support components should be captured.
2. **Step 2: Analysis**– Analyze unmet requirements and review current and planned capabilities to identify opportunities to consolidate, re-use, or invest through a trade-off analysis. Map requirements to capabilities and identify unmet requirements that need addressed. Analyze capabilities to identify those that may be re-used to meet a requirement, those capabilities that may be redundant or could be consolidated, and seek opportunities to leverage other non-privacy capabilities to meet a privacy function. Perform a trade-off analysis to identify the cost/benefits of each solution.
3. **Step 3: Selection**–Evaluate proposed solutions and select the solution that best fits in the organization. This stage provides an opportunity to ensure that new solutions or technologies fit into the overall goals of the enterprise and do not introduce new risks. It ensures that privacy is appropriately captured in the individual system as well as privacy solutions support the enterprise.

Across Reference Model Look

Both an enterprise and its systems have multiple objectives. They have performance objectives they meet in the context of a specific business goal and use services and technologies processing data to meet these objectives and goals. The privacy reference model cuts across architectural layers such as

- Business –specific lines of business will require certain unique privacy programmatic requirements (health care versus financial services, for example).
- System – Across an organization’s business lines systems will have to privacy-specific requirements and need privacy controls.
- Technology – an organization will want to both enable technologies to enhance privacy and ensure technological business solutions do not infringe on privacy protections.
- Data – Data may contain personal information data elements and will need to be flagged. These data elements will need to map to the above privacy control families as appropriate given the corresponding business and system models.