**Data Protection - More “Art” than “Science”? Not with the New OASIS PMRM Privacy Analysis Methodology**

**by John Sabo, Michele Drgon, Michael Willet and Gail Magnuson**

We have worked on data privacy policy and practices issues since the 1980’s, when virtually all PI was created from manual paper collection processes and key punched into mainframe systems. How times have changed! Over the past four decades, we have seen global technological innovation and disruptive business models. But from a privacy perspective, this disruption has outstripped the ability of business owners, government agencies and IT engineers/developers to confidently deliver the data protection obligations expected by regulators, consumers and citizens in online and backend systems.

Obviously, some of this was inevitable given the speed of change and the frenetic adoption of disruptive technologies (initially networked computing, then the Web, mobile devices, networked apps, the cloud, big data…). But a huge factor suppressing the deployment of strong privacy compliant systems has also been the lack of standardization among inconsistent privacy practices/principles contained in scores of international laws, regulations and codes of practice and the flows of PI across applications, systems and geo boundaries.

Of course, in the abstract, data protection seems so clear and universal: Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, Accountability (OECD, 1980). But an examination of international privacy instruments carried out from 2007 until now illustrates some of the challenges that flow from inconsistent policies and definitions.

Now the EU General Data Protection [Regulation](http://ec.europa.eu/justice/data-protection) (“GDPR”) - with its enhanced focus on processing roles (such as Controller, Processor) and expanded principles (such as Right to be Forgotten, Erasure and Accountability) establishes additional definitions and terminology, coupled with a strengthened data protection regulatory regime. However, the new GDPR operates on the existing global data environment rife with incredible technical and application complexity.

So how can we approach this problem of delivering privacy-compliant, accountable systems and applications in the global data sphere? Can data protection become less a practice of “art” and more a practice of “science, ” truly enabling the GDPR and other regulatory and business policy mandates to have a genuine impact on operational data privacy delivery?

One piece of the solution is to have models, methodologies and tools that enable the analysis of policy/privacy control expectations against the actual systems that carry the PI and PII; that is, models, methodologies and tools that are usable across the privacy stakeholder community, empowering regulators, privacy officers, business owners, system engineers, and individuals/data subjects to understand and manage privacy in defined systems and applications.

The OASIS Privacy Management Reference Model and Methodology (PMRM - <http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.html> is a specification that can make explicit the linkages between policy and privacy control requirements and the actual PI, data flows and implementing-functionality in defined system and application use cases or user stories.

As noted in the PMRM abstract:

*The PMRM provides a model and a methodology to*

* *understand and analyze privacy policies and their privacy management requirements in defined Use Cases; and*
* *select the technical Services, Functions and Mechanisms that must be implemented to support requisite Privacy Controls.*

*It is particularly valuable for Use Cases in which Personal Information (PI) flows across regulatory, policy, jurisdictional, and system boundaries.*

The power and the value of the PMRM to each stakeholder, whether privacy officer, business owner, developer, regulator or data subject, lies in executing a series of specific tasks that move from initially establishing high-level descriptions (and boundaries) of a particular use case, to exposing greater levels of specificity, including the PI, data flows, domains and domain owners, privacy controls and their supporting services, functionality and mechanisms. The PMRM incorporates iterative risk analysis that focuses on the expected/actual operation of the functionality put in place to make privacy delivery a reality. The outcome of this final step is a Privacy Management Analysis (PMA) that links together the policies, PI, controls, and procedural/technical service delivery functionality.

The product is an artifact that can make clear just what data protection controls are expected – and what is delivered – in any system or application.

Notably, the PMRM can be a key enabler to achieve privacy and data protection by design and default. It can be used by privacy officers to certify the operational readiness of a system to meet their data protection mandates, by system and privacy engineers to understand their development requirements, and by regulatory authorities who require accountable privacy systems. And it can be used to ensure that individual users and data subjects have confidence that their privacy agreements and expectations are being honored.

We encourage you to download the PMRM, read it through, and apply it to your use case or user story in which data protection is a requirement.