IEEE P7002

Data Privacy Process

ITU Workshop on "Machine Learning for 5G and beyond”

San Jose, California, USA August 7th, 2018

JOHN WUNDERLICH & ASSOCIATES

PRIVACY AND SECURITY

Disclaimer

The IEEE p7002 Data Privacy Process standard has not yet been finalized. The views and information contained in this presentation are the personal views of the presenter and are not meant to represent the IEEE or the P7002 Working Group.

IEEE P7002 Data Privacy Process

Scope

This standard defines requirements for a systems/software engineering process for privacy oriented considerations regarding products, services, and systems utilizing employee, customer or other external user's personal data. It extends across the life cycle from policy through development, quality assurance, and value realization. It includes a use case and data model (including metadata). It applies to organizations and projects that are developing and deploying products, systems, processes, and applications that involve personal information. By providing specific procedures, diagrams, and checklists, users of this standard will be able to perform a conformity assessment on their specific privacy practices. **Privacy impact assessments (PIAs)** are described as a tool for both identifying where privacy controls and measures are needed and for confirming they are in place.

Additional information can be found on the approved PAR.

Managing Privacy and Security Risk

Assumptions:

- Systems are built with flaws
- Good privacy and security today is better than perfect privacy and security tomorrow
- Good privacy and security today may not be good tomorrow
- Bad guys do NOT think rationally
- Whatever can go wrong probably already has.

The intersection of 5G, ML, and Privacy

A bigger, faster network with more sensors in more devices communicating more information about more things. Many of those things will implicate personal data directly or by inference.

Larger data sets from more diverse sources enabling deeper analytics about more things – including individuals' behaviour, interactions, habits, and more.

Retrofitting for inappropriate collection, use, or disclosure of personal data will vary from impractical to impossible.

Will 5G become the backbone of the Internet of Things?

By **Alexander Hellemans**

Photo: iStockphoto https://spectrum.ieee.org/tech-talk/computing/networks/5g-taking-stock

Is accountability possible without an explained decision process?

"We are building systems that govern healthcare and mediate our civic dialogue. We would influence elections. I would like to live in a society whose systems are built on top of verifiable, rigorous, thorough knowledge, and not on alchemy."

Ali Rahimi, NIPS 17

The Guardian

US edition

Magical thinking about machine learning won't bring the reality of AI any closer

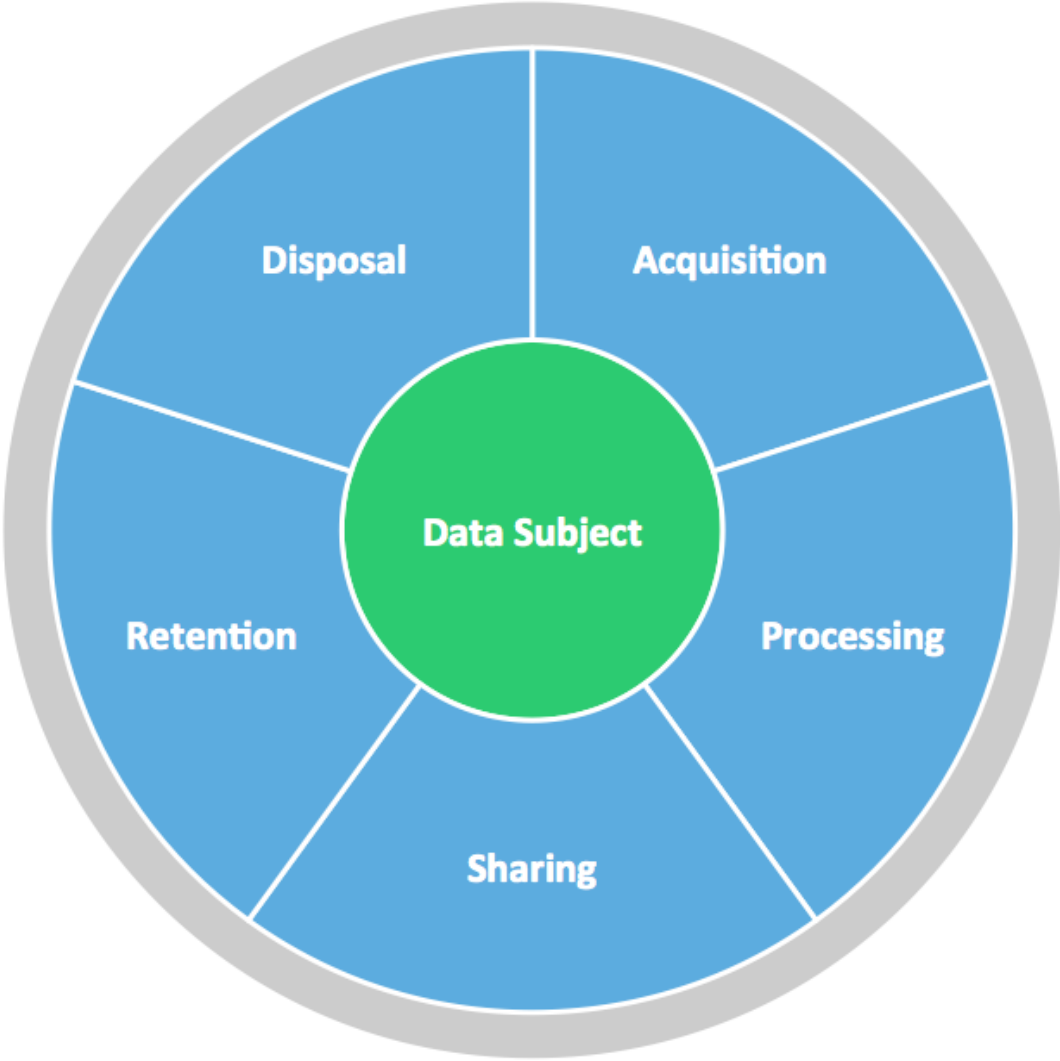
John Naughton

Unchecked flaws in algorithms, and even the technology itself, should put a brake on the escalating use of big data

https://www.theguardian.com/commentisfree/2018/aug/05/magical-thinking-about-machine-learning-will-not-bring-artificial-intelligence-any-closer

Data Privacy Life Cycle

A product, service or system that processes data about an identifiable individual has to account for, or be accountable to, the data subject at every stage of the life cycle of the data.



Data Privacy Process in Projects

1. Initiation

   Does this project implicate personal data? Are we allowed to do what we are thinking about?

2. Planning

   How can we respect the user while using data about them?

   Functional & Non-functional requirements

3. Execution

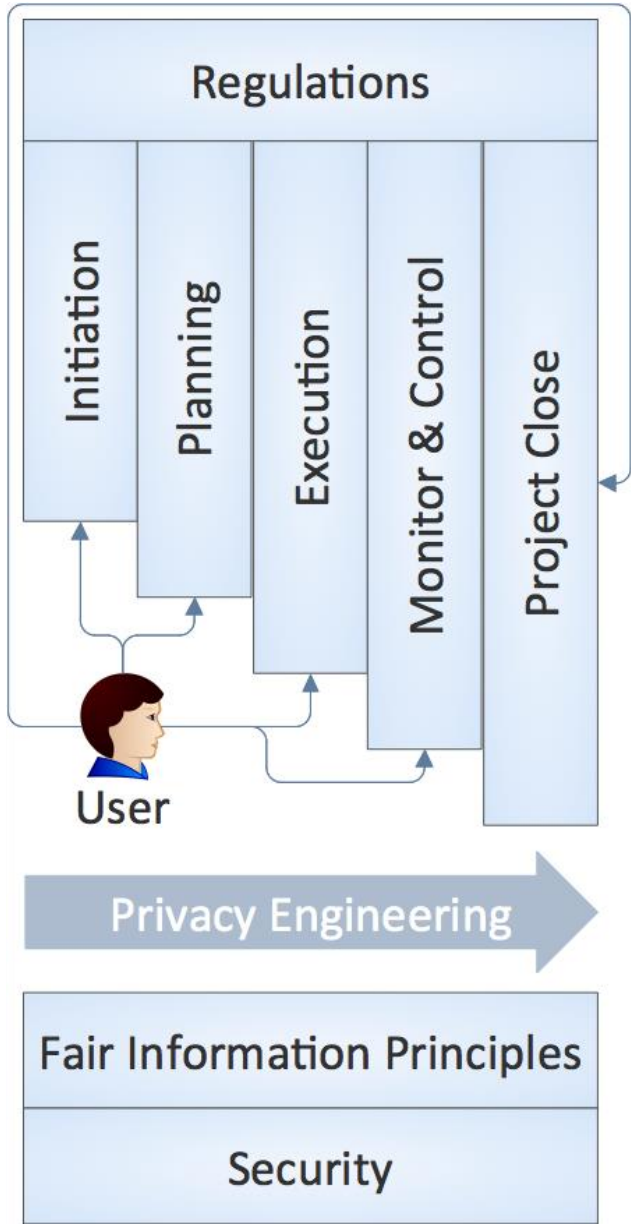
   Are there data protection checkpoints and/or gates?

4. Monitor & Control

   Q/A tests for data protection?

5. Project Close

   Release to production with data protection instrumentation (metrics and controls)



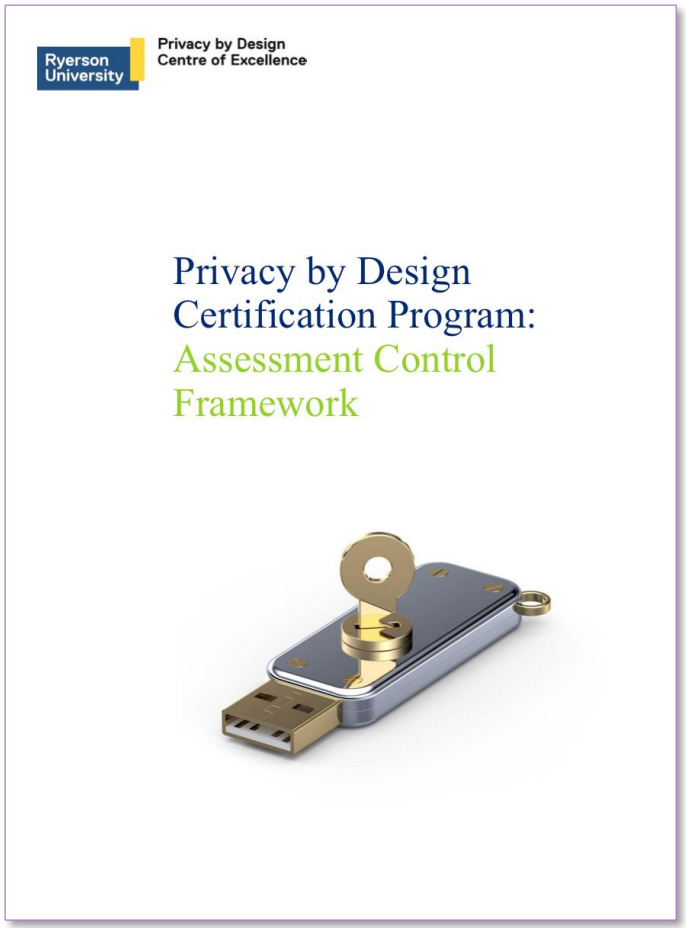
Input

Already existing frameworks and approaches to consider in a data privacy process

Privacy by Design

1. Proactive not reactive; preventative not remedial
2. Privacy as the default
3. Privacy embedded into design
4. Full functionality – positive-sum, not zero-sum
5. End-to-end security – full lifecycle protection
6. Visibility and transparency – keep it open
7. Respect for user privacy – keep it user-centric

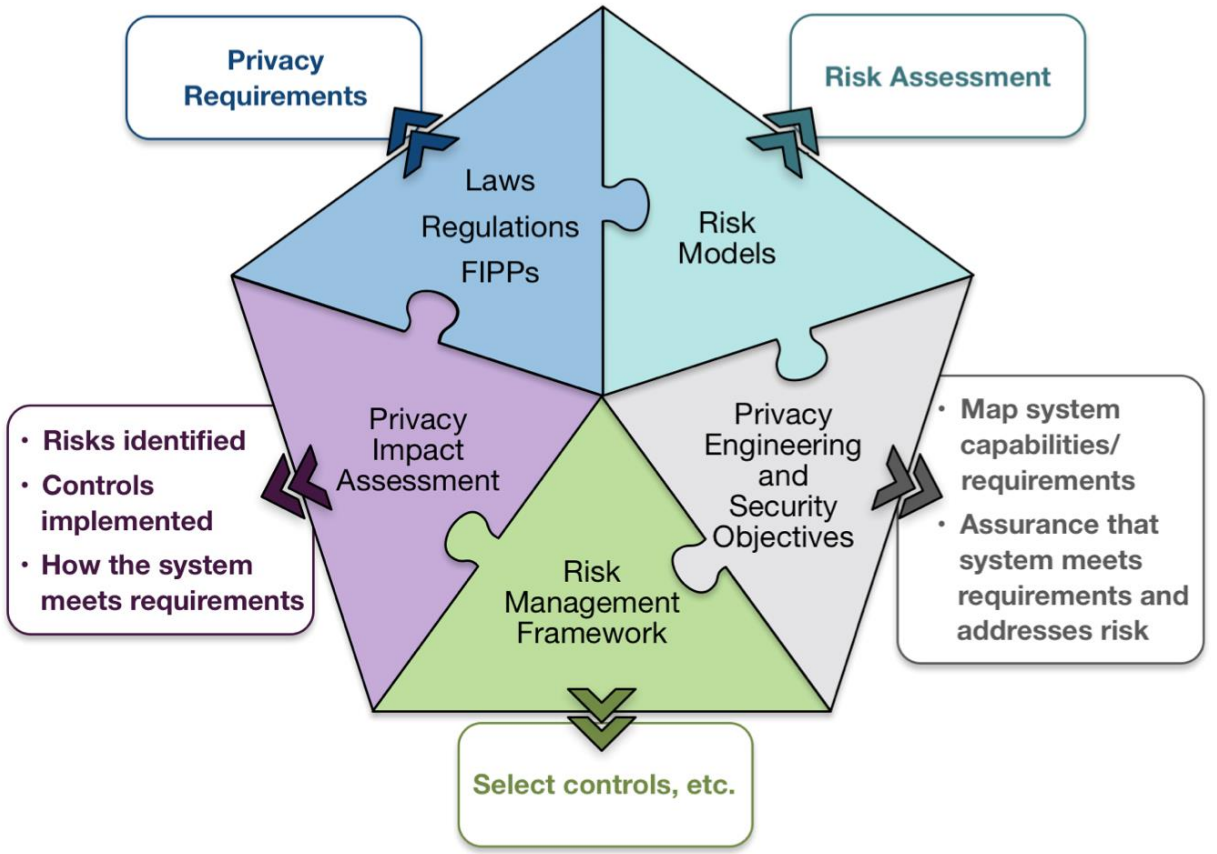
ISO/PC 317: Consumer protection: privacy by design for consumer goods and services



NIST Privacy Engineering

Privacy engineering is a specialty discipline of systems engineering focused on removing conditions that can create problems for people when system operations process their information.

- Predictability
- Manageablity
- Dissassociability



https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering

NIST Privacy Engineering Objectives

Predictability

- enabling reliable assumptions by individuals, owners, and operators about PII and its processing by an information system

Manageability

- providing the capability for granular administration of PII including alteration, deletion, and selective disclosure

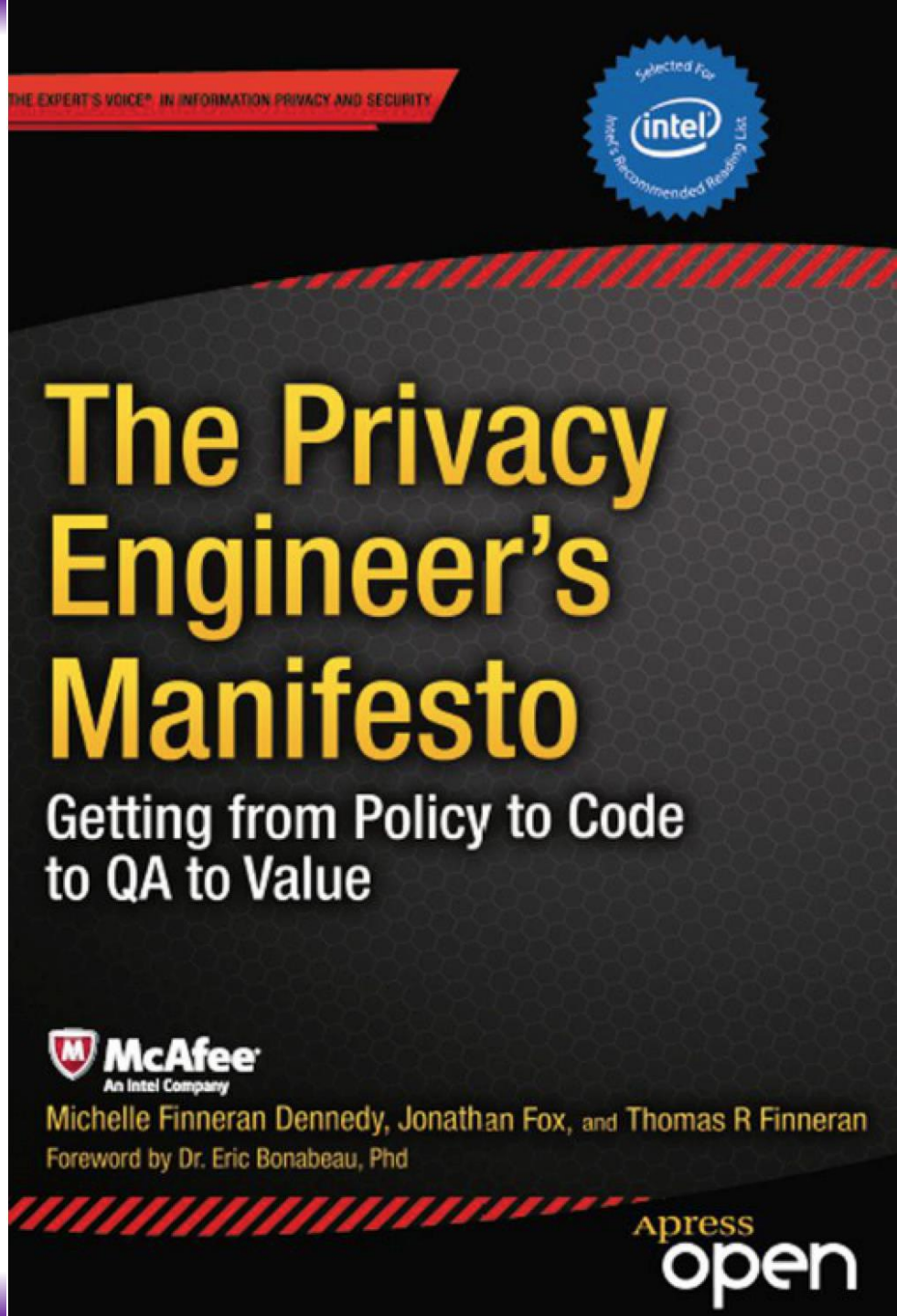
Disassociability

- enabling the processing of PII or events without association to individuals or devices beyond the operational requirement of the system

A Manifesto

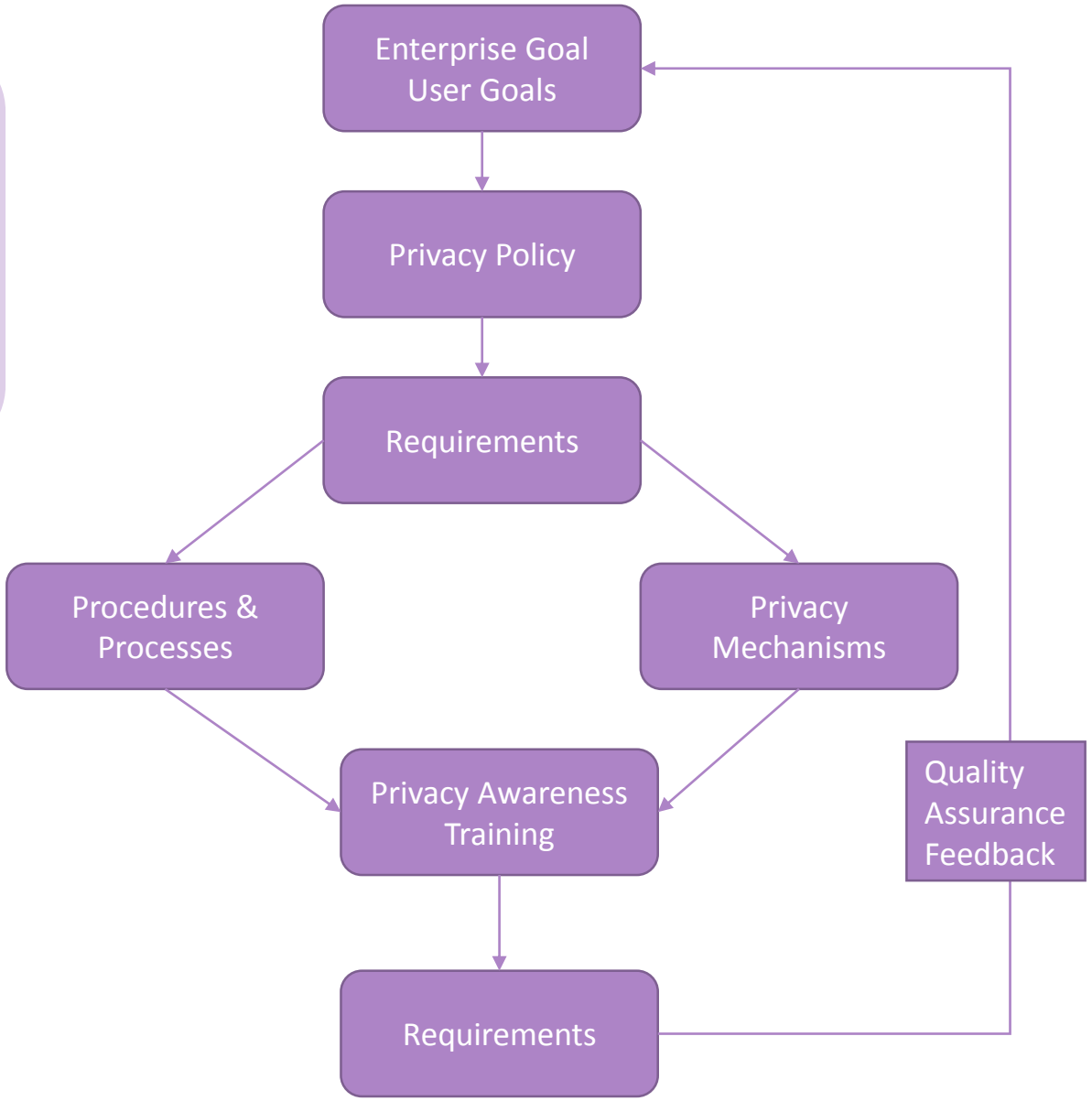
The purpose of this book is to provide, for data and privacy practitioners (and their management and support personnel), a systematic engineering approach to develop privacy policies based on enterprise goals and appropriate government regulations. Privacy procedures, standards, guidelines, best practices, privacy rules, and privacy mechanisms can then be designed and implemented according to a system's engineering set of methodologies, models, and patterns that are well known and well regarded but are also presented in a creative way. A proposed quality assurance checklist methodology and possible value models are described.

Michelle Finneran Dennedy, Jonathan Fox, Thomas R. Finneran. The Privacy Engineer's Manifesto Apress Open



Touchpoints for a privacy engineering development process

- Organizational Structure
- Enterprise Architecture
- Project Management
- Enterprise Risk Management
- Change Management
- Stakeholder Relations



Privacy engineering development process, Privacy Engineer's Manifesto

Examples

Functional Requirements

- The system must provide a privacy notice to users
- The system must collect an opt-in consent from users
- The system must encrypt all PII at rest and in motion
- Unattended patch management
- All non-required ports closed by default

Non-functional Requirements

- Where there are user configurable choices, the default choices should be privacy protective
- Identifying and contacting the system privacy office should be built into the UX
- Mandatory breach notification
- Unique default password per device (no “admin”/”admin”)

Questions?

The most basic systems failure regarding privacy is to not ask the question, “Does this system impact people and their data?”