Operationalizing Privacy by Design

Ansatz zur praktischen Umsetzung von Privacy by Design

Dirk Rösler

Agenda

- Integrating PbD into the organization
- Using privacy risk models
- Selecting control mechanisms
- Leveraging existing PbD frameworks
- Ensuring accountability

- Integration von PbD in die Organisation
- Modelle zur Risikobewertung
- Geeignete Kontrollmechanismen
- Nutzung existierender PbD-Rahmenwerke
- Nachweisbare Erfüllung

What is ‘Privacy by Design’?

Privacy by Design requires at the time of the determination of the means for processing and the time of the processing itself during the life cycle of a service, product or any other processing activity the controller to ensure the implementation of adequate TOMs in accordance with the data protection principles.

???

Privacy by Design ensures that privacy and data protection is a key consideration in the early stages of any project and then throughout its lifecycle.

“The concept of Privacy by Design and its concrete implementation, whereby data protection compliance would be embedded throughout the entire life cycle of technologies and procedures, from the early design stage to their deployment and use.”

Privacy by Design means applying Privacy by Design.

Elements of ‘Privacy by Design’

- A highly secure system
- Security certification or privacy seal
- Using a lot of PETs (encryption, anonymization etc.)
- Checking or auditing legal compliance, lawfulness
- Performing PIA (or is it?)
- Incorporating functionality to deliver data subject rights

Challenges

- **Data Controllers**: *How to implement?*
  IT architects and solution developers lack concrete models to guide their work

- **Data Protection Authorities**: *How to enforce?*
  Vague, potentially recursive definition, no (technical) standards to audit implementation

Proposal

~~Build~~ Extend your privacy management framework for Privacy by Design

- Risk-based
- Technology-neutral
- Pervasive
- Sustainable
- Demonstrable

Privacy Management Framework[1]

1. **Maintain Governance Structure**
2. Maintain Personal Data Inventory and Data Transfer Mechanisms
3. **Maintain Internal Data Privacy Policy**
4. Embed Data Privacy Into Operations
5. **Maintain Training and Awareness Program**
6. Manage Information Security Risk
7. Manage Third-Party Risk
8. Maintain Notices
9. Respond to Requests and Complaints from Individuals
10. **Monitor for New Operational Practices**
11. Maintain Data Privacy Breach Management Program
12. **Monitor Data Handling Practices**
13. Track External Criteria

[1] Example: Nymity Privacy Management Accountability Framework™

‘Privacy by Design’ Governance

- Set Policy
- Assign Responsibility
- Provide Education
- Implement Framework
- Conduct Checks
- *Document It!*

Set Policy

- **Example Baseline Principles:**
  - "*The Organization* should promote data privacy throughout the organization and at every stage of the development of its products and services."
  - "Privacy protections should be incorporated into business practices at the outset of the planning process."
  - "Comprehensive data privacy management procedures should be maintained throughout the life cycle of products and services."

Assign Responsibility

- Privacy Office
- Business Process Owners
- Product Developers
- Technical Solution Developers / Managers
- Privacy Engineer
- …

Provide Education

- Integrate with Privacy Training and Awareness Program
- Role/job-specific content for all stakeholders
- Inter-disciplinary audience: business process owners, product developers, technical solution developers, project managers…

Implement Framework

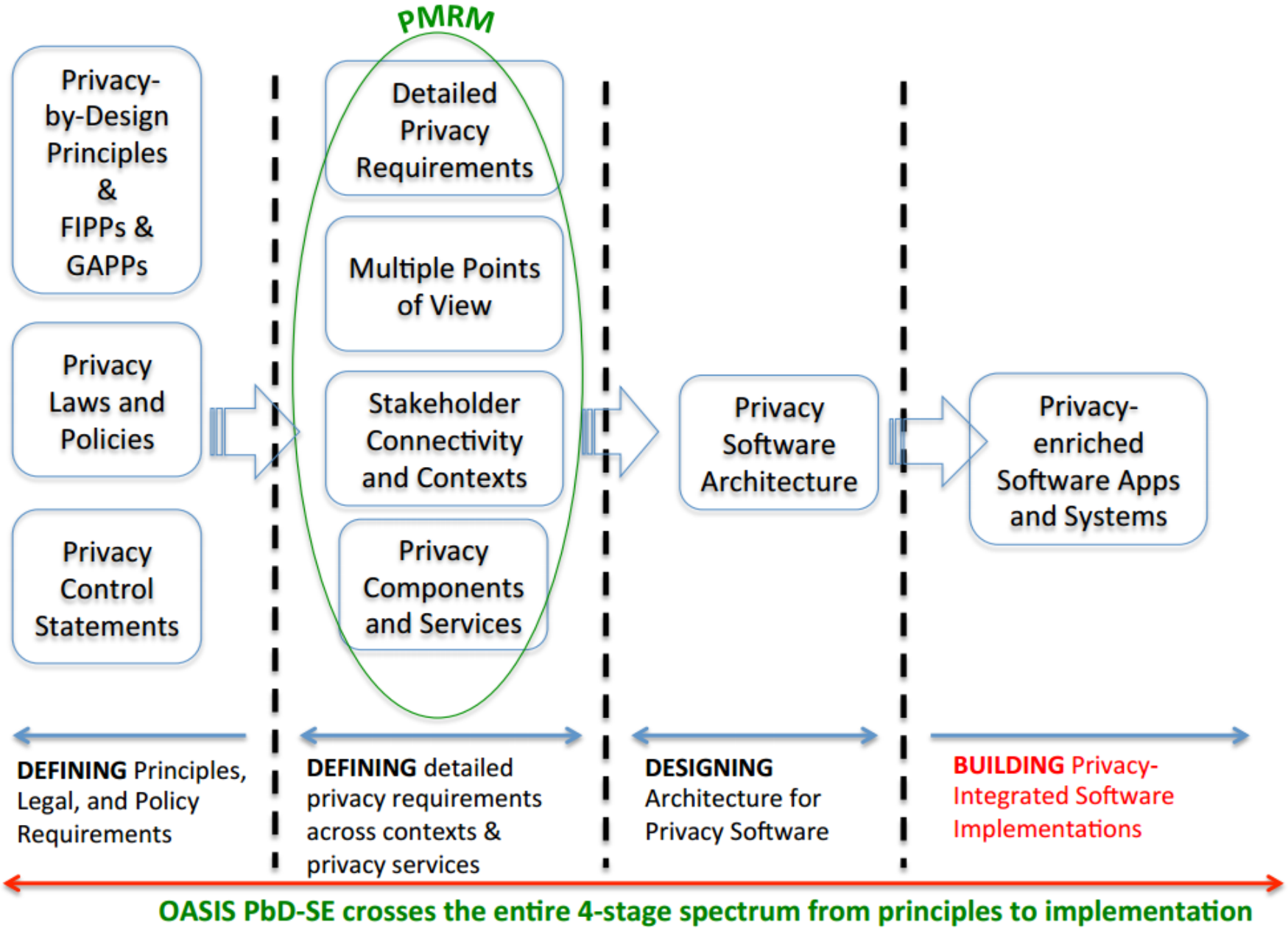
- **OASIS Privacy Management Reference Model and Methodology (PMRM)**
  The Reference Model is intended to serve as a guideline or template for developing operational solutions to privacy issues, as an analytical tool for assessing the completeness of proposed solutions, and as the basis for establishing categories and groupings of privacy management controls.

  https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pmrm

- **PRIPARE PR**eparing **I**ndustry to **P**rivacy-by-design by supporting its **A**pplication in **Re**search
  PRIPARE's methodology covers the whole lifecycle of both, the system (previous to its inception and until its decommission) and of the personal data (from the planning for its collection and up to its disposal). The structure of PRIPARE's methodology has been designed to provide an easy match and merge with prevalent engineering practices, dividing its 24 processes in 8 meaningful and recognizable phases (e.g. analysis, design, and implementation)

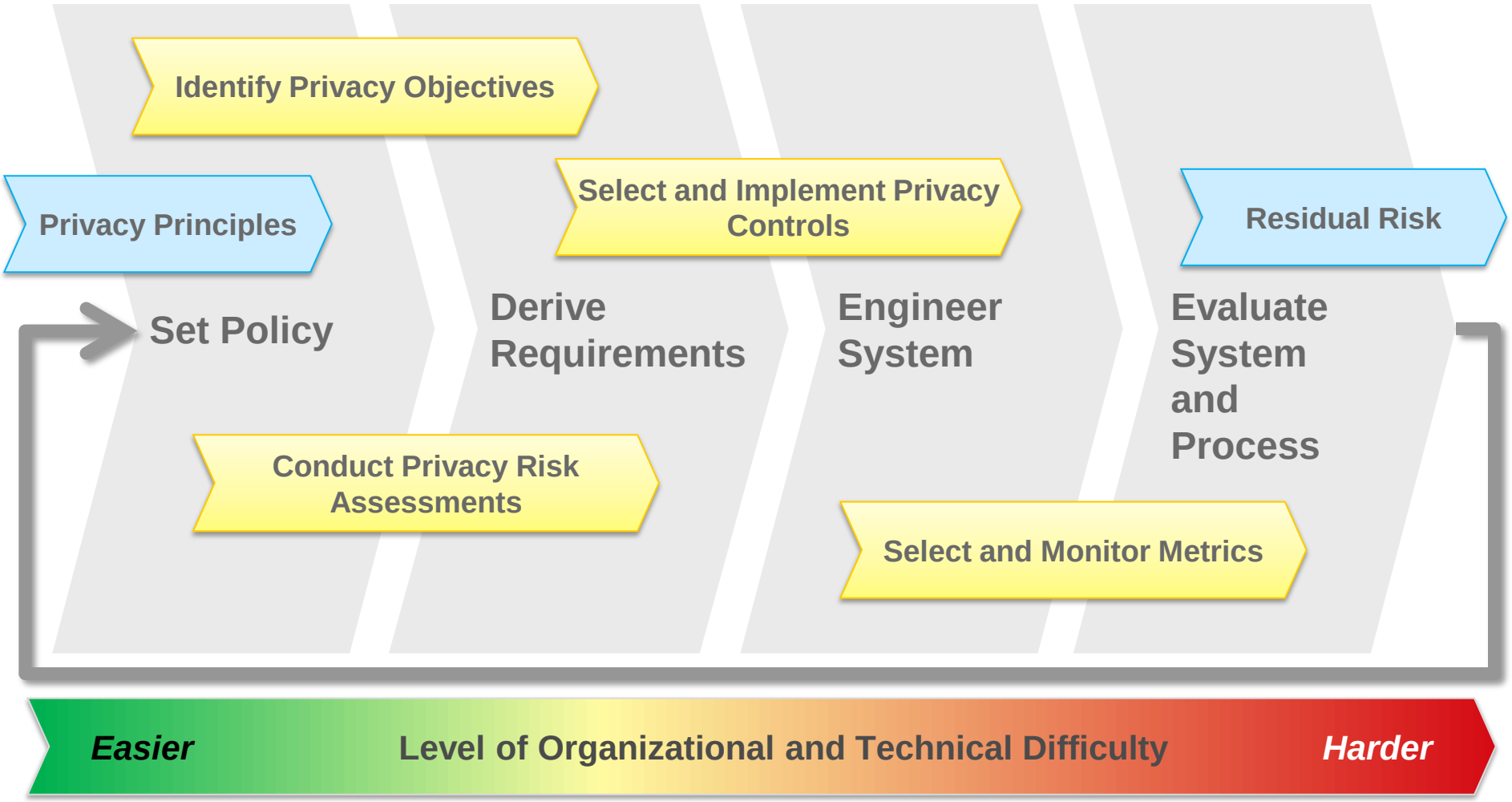
  http://pripareproject.eu/research/

Scope of the OASIS PbD-SE and OASIS PMRM Standard-Track Work Products



Source: OASIS

Privacy Risk Lifecycle Model

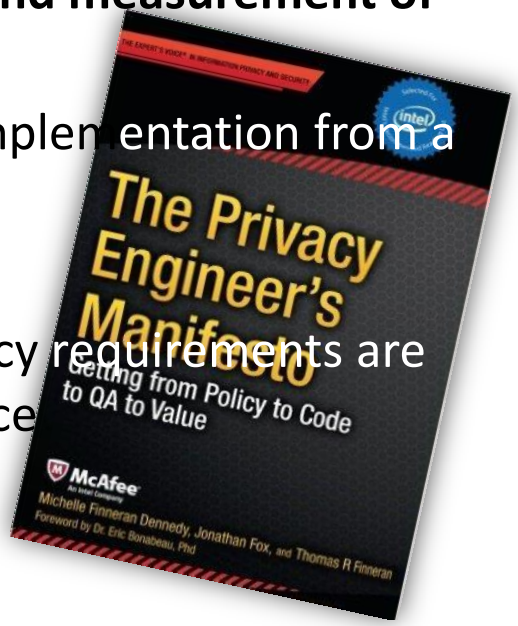


Conduct Checks

- Do you maintain a **data privacy policy** which includes Privacy by Design? (3)
- Have you **assigned accountability and responsibility** to implement Privacy by Design? (1)
- Do you include Privacy by Design when conducting **privacy training** reflecting job-specific content? (5)
- Do you maintain a **Privacy by Design framework** for all system and product development? (10)
- Do you **conduct PIAs** that include Privacy by Design for new programs, systems, processes? (10)
- Do you maintain a **product life-cycle process** that includes Privacy by Design to address privacy impacts of changes to existing programs, systems, or processes? (10)
- Do you **conduct audits**, assessments, self-assessments, benchmarks or ad-hoc walk-throughs that include Privacy by Design? (12)

Privacy Engineering

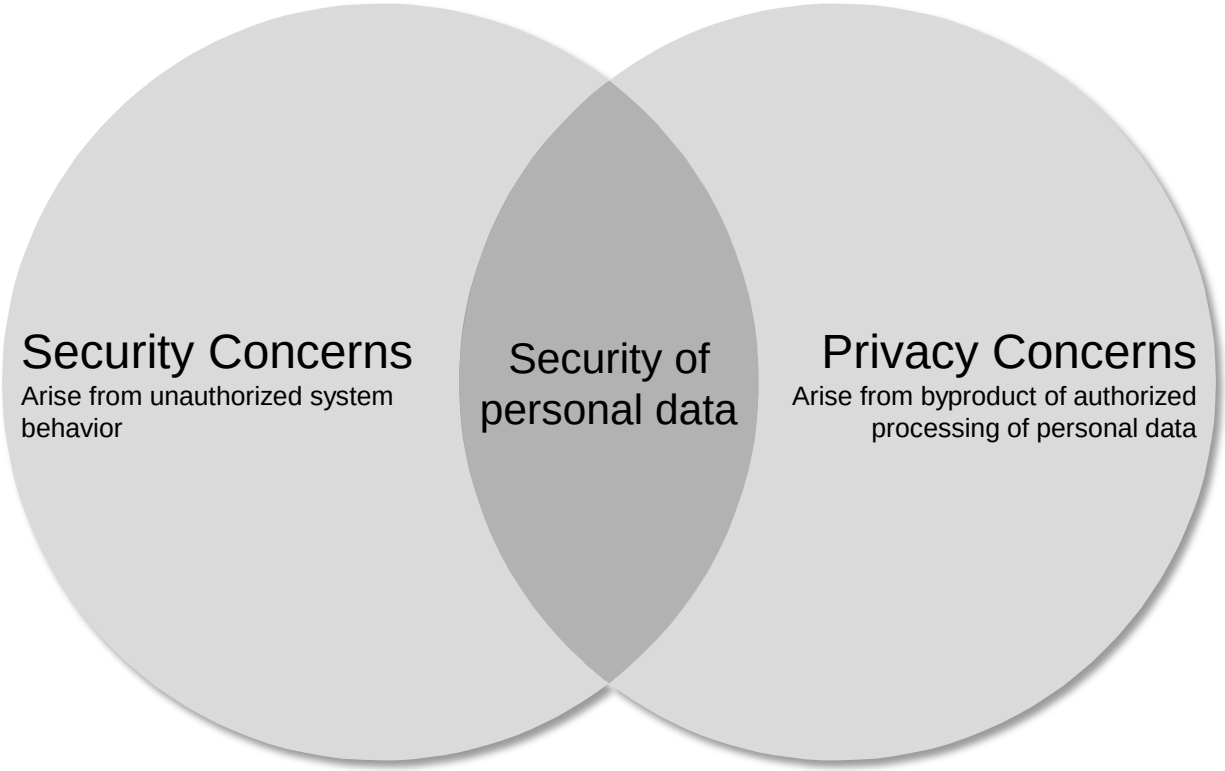
- *Privacy Engineering* is the emerging engineering discipline for implementing Privacy by Design operationally.
- Privacy Engineers take responsibility for:
  - **Designing and constructing processes, products, and systems** with privacy in mind that appropriately collect or use personal information
  - **Supporting the development, implementation, and measurement of privacy policies**, standards, guidelines and rules
  - **Analysing software and hardware designs** and implementation from a privacy and user experience perspective
  - **Supporting privacy audits**
  - **Working with other stakeholders** to ensure privacy requirements are met outside as well as inside the engineering space



Components

- **System objectives** (e.g., confidentiality, integrity, availability) to map and evaluate system capabilities in order to provide assurance that the system meets the requirements and addresses risk appropriately
- **Risk model** to produce a risk assessment
- **Risk management framework** to provide a process for selecting and assessing controls to manage identified risks and meet the requirements

Privacy Concerns

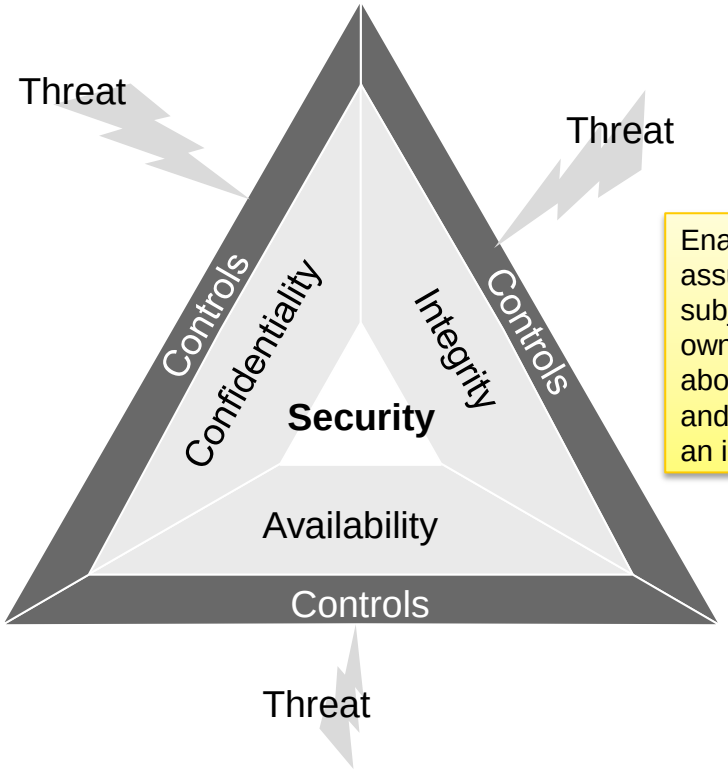


"While some privacy concerns arise from unauthorized activity, privacy concerns also can arise from authorized processing of personal data." – NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems

Security vs. Privacy Objectives

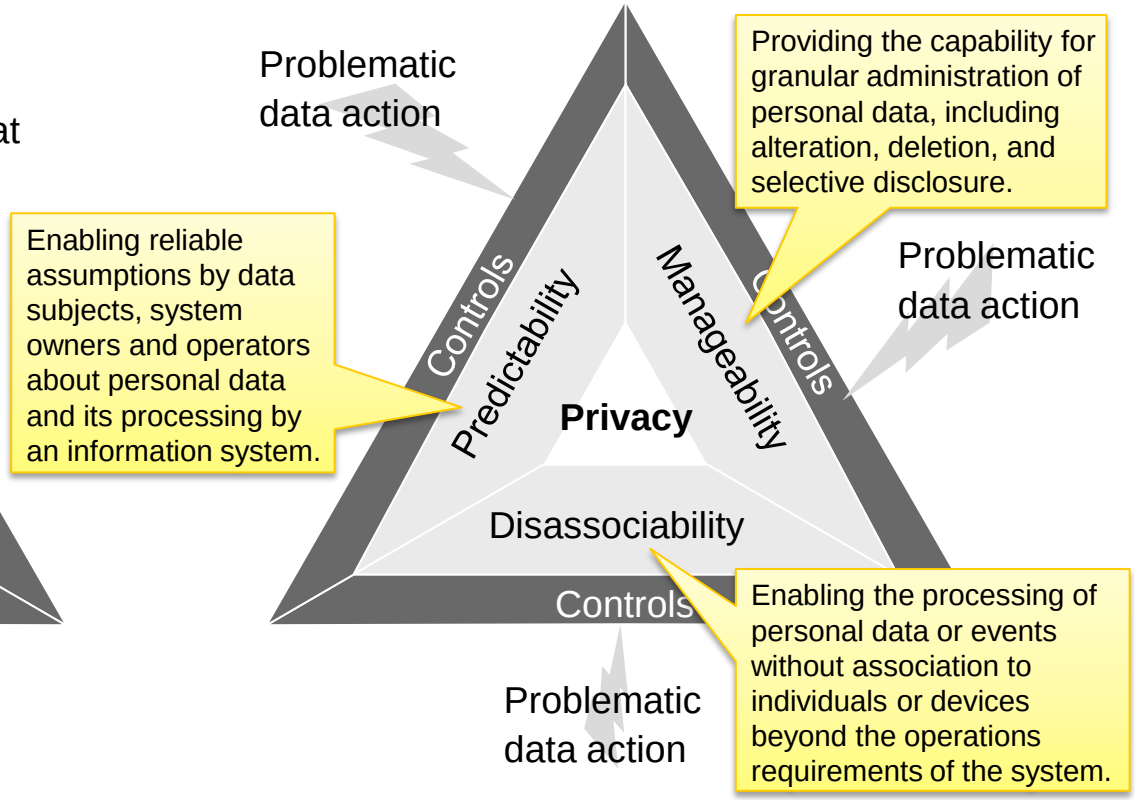
CIA model of information security

"Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)."



NIST *privacy engineering* objectives

Designed to enable system designers and engineers to build information systems that are capable of implementing privacy goals and support the management of privacy risk.



Privacy Risk Model

Privacy risk is the result of likelihood and impact (privacy harm) of a problematic data action. It can be expressed as:

Parameters can be expressed on a High/Medium/Low scale

[1] Note: only individuals—not system owners or operators —can directly experience a privacy problem is especially challenging for assessing impact.

Problematic Data Actions

Problematic data actions occur when the data actions of an information system contravene the objectives of **Predictability**, **Manageability** and **Disassociability**

Unanticipated Revelation: Non-contextual use of data reveals or exposes an individual or facets of an individual in unexpected ways

Distortion: The use or dissemination of inaccurate or misleadingly incomplete personal information

Unwarranted Restriction: The improper denial of access or loss of privilege to personal information

Surveillance: Tracking or monitoring of personal information that is disproportionate to the purpose or outcome of the service

Appropriation: Personal information is used in ways that exceed an individual's expectation or authorization

Induced Disclosure: Pressure to divulge personal information

Insecurity: Lapses in data security

Privacy Harms

Harms to individuals (not system owner) that result from problematic data actions can be grouped into four categories:

Economic Loss

Economic loss can include direct financial losses as the result of identity theft, as well as the failure to receive fair value in a transaction involving personal information.

Loss of Trust

The breach of implicit or explicit expectations or agreements about the handling of personal information.

Discrimination

The unfair or unequal treatment of individuals. This includes the harms of Stigmatization and Power Imbalance.

Loss of Self-Determination

The loss of an individual's personal sovereignty or ability to freely make choices. This includes the harms of Loss of Autonomy, Exclusion, Loss of Liberty and Physical Harm.

Privacy Risks Illustrated

Predictability	Manageability	Disassociability
Enabling reliable assumptions by data subjects, system owners and operators about personal data and its processing by an information system.	*Providing the capability for granular administration of personal data, including alteration, deletion, and selective disclosure.*	*Enabling the processing of personal data or events without association to individuals or devices beyond the operations requirements of the system.*
Example Problematic Data Action		
Unanticipated Revelation: behavioural or consumer data is analysed and a previously unknown or private health condition becomes apparent	Unwarranted Restriction: a customer has her information deleted and can no longer carry out transactions	Appropriation: a customer provides date of birth to prove that she is over 18. The information is stored alongside the customer profile and later used for age-oriented advertising
Example Potential Harm		
Stigmatization: Personal information is linked to an actual identity in such a way as to cause embarrassment, emotional distress or discrimination	Loss of Self-Determination (Exclusion): lack of knowledge about or access to personal information can lead to inability to participate in decision-making	Power Imbalance: unfair advantage or abuse of a power imbalance between data acquirer and the data subject

Privacy Risk Mitigation Plan

Data Class	Data Objects	• Problematic data action • Likelihood	• Problematic data action • Impact	Privacy Risk (L/M/H)	Mitigating Privacy Control
Consignee Data	• Name • Address • Contact email/phone				
Job Application (Employee Data)	• Name • Address • DoB • CV/Education • Photo • References				
Invoice Data	• Name • Address • Bank account • …				
System Logs	• User ID (employee data)				
CCTV/video surveillance	• Imagery of persons (employees, customers)				

Multi-level Privacy Controls[1]

Policy

- Formulate organizational or system-wide policy on how personal data is to be treated
- Assign roles and responsibilities
- Ensure transparency and awareness of business and technological practices

Architecture

- Data/business models that minimize the processing of personal data
- Apply anonymization wherever possible
- Decentralized or compartmentalized processing
- Apply Privacy Enhancing Technologies (PET)

Point Controls

- Data minimization on technical level
- Randomization and obfuscation to reduce linkability hide original meaning
- Technical security (identity and access management, auditing and logging, data loss prevention etc.)

[1] Control: measure that is modifying risk. Controls include any process , policy , device, practice, or other actions which modify risk. Controls may not always exert the intended or assumed modifying effect. (ISO/IEC 27000:2016)

Privacy Enhancing Technologies (PET)

"A system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without loss of functionality of the information system."

Examples:

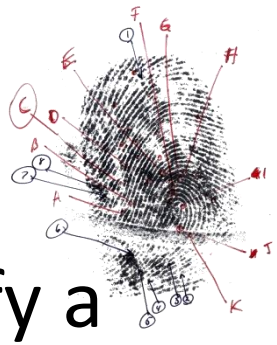
- Anonymization
- Identity Management
- Database Privacy
- Encryption/Access Control

Inhibitors:

- Often limited purpose
- No control for accountable business practices
- Limitations in networked infrastructures
- Complex to develop
- Slowly maturing
- Lack of incentive for deployment

"Some feel that just by using PETs, they are protecting privacy. Although this can be partially true, it is not completely true. […] Even if the design is full of PETs, privacy may not be fully protected. PETs are enablers, but they are not substitutes for privacy engineering. PETs can be just one of many design components but alone are not a privacy solution." – **The Privacy Engineer's Manifesto**

Re-Identification



- 12 points are needed to uniquely identify a person's fingerprint
- Four spatio-temporal points of mobile phones are enough to uniquely identify 95% of individuals
- Even location data traces most difficult to identify can be uniquely identified knowing only 11 locations

Summary

- Privacy by Design is an approach to projects that promotes privacy and data protection compliance from the start
- Privacy by Design minimises privacy risks, builds trust and supports legal compliance
- Privacy Engineering is the emerging engineering discipline for implementing Privacy by Design operationally
- Privacy risk is the product of problematic data actions and their associated privacy harms
- Existing frameworks can be leveraged to implement Privacy by Design operationally
- Privacy Enhancing Technologies (PET) can be used as controls to counter some of these risks
- Privacy by Design may not address all privacy risks