Protection Goals for Privacy Auditing and Privacy Engineering

Marit Hansen
Privacy and Information Commissioner
Schleswig-Holstein, Germany

marit.hansen@datenschutzzentrum.de

NordSec 2015
Stockholm, 20 October, 2015

Setting of ULD

- Data Protection Authority (DPA) for both the public and private sector
- Also responsible for freedom of information

Source: en.wikipedia.org/wiki/Schleswig-Holstein
1. Working with Protection Goals

2. Protection Goals for Privacy Engineering

3. Dependencies between Protection Goals

4. Privacy Auditing

5. Conclusion
Successful engineering needs iteration: The PDCA Cycle

Same for Information Security Management Systems (ISMS) [cf. ISO 27001]

Establish the ISMS

Implement, operate the ISMS

Maintain, improve the ISMS

Monitor, review the ISMS

Information security protection goals

- Confidentiality
- Integrity
- Availability
How to make use of the notion of protection goals?

- (Skilled) engineers know how to deal with the traditional security protection goals
- Security protection goals are part of Information Security Information Systems (ISMS) – cf. ISO 27001
- Established procedure
  - Analysis of risks
  - Dealing with risks → selecting the appropriate safeguards
  - Considering the lifecycle of development

Creation of a security policy

1) What is the status?
2) How much security do we need? ("normal", "high", "very high")
3a) Selection of safeguards
3b) Check: sufficiently realised? (target-actual comparison)
Lifecycle of the security concept

**Plan (P)**
- Planning and conception
  - Choosing a method for risk analysis
  - Classification of risks or damages
  - Risk analysis
  - Development of a strategy for handling risks
  - Selection of safeguards

**Do (D)**
- Implementation
  - Implementation plan for the security concept
  - Implementation of the safeguards
  - Supervising and control of the implementation
  - Implementation of a Business Continuity Management
  - Training and awareness

**Check (C)**
- Performance review and monitoring
  - Detection of security incidents during operation
  - Monitoring compliance of regulations
  - Monitoring suitability and effectiveness of safeguards
  - Monitoring performance of safeguards
  - Management reports

**Act (A)**
- Optimization and improvement
  - Correction of defects
  - Improvement of safeguards

Reference: BSI-Standard 100-1
4 possibilities of risk treatment *(Dorfman*)

- **Avoidance** (eliminate, withdraw from)
- **Reduction** (optimize, mitigate)
- **Sharing** (transfer, outsource or insure)
- **Acceptance** (accept and budget)

Violation of privacy as a basic right?  
Risk-based approach can be problematic!


---

2. PROTECTION GOALS FOR PRIVACY


Slides: Meiko Jensen
"The protection goal of Confidentiality is defined as the property that (privacy-relevant) data and services that process such data cannot be accessed by unauthorized entities."
Confidentiality

... in other words:

- Secrecy
- Non-Disclosure
- Access Restrictions
- Security Clearances
- Data Minimization
- Steganography
- Unobservability

Implementation Techniques:

- Data Encryption
  - in transit (TLS, HTTPS, SSH, ...)
  - at rest (PGP, S/MIME, TrueCrypt, ...)
  - ...
- Data Segregation
  - Secret Sharing, Secure Multiparty Computations
  - Onion Routing
- Access Control Enforcement
"The protection goal of **Integrity** is defined as the property that (privacy-relevant) data and services that process such data cannot be modified in an unauthorized or undetected manner."

... in other words:

- Authenticity
- Detection of Data Changes
- Non-Repudiation
- Reliability
Implementation Techniques:

- Digital Signatures
  - RSA, ElGamal
  - Message Authentication Codes
  - ...
- Hash Values
- Access Control Enforcement
- Watchdogs / Canaries
- Two-Man Rules

The protection goal of **Availability** is defined as the property that access to (privacy-relevant) data and to services that process such data is always granted in a comprehensible, processable, timely manner.
Protection Goals for Privacy Auditing and Privacy Engineering

Availability

... in other words:

- Redundancy
- Monitoring of Availability
- Responsiveness
- Accessibility
- Uptime

Implementation Techniques:

- Backups
- Load Balancers
- Failovers
- Redundant Components
- Avoidance of Single-Points-of-Failure
- Watchdogs / Canaries
Privacy Protection Goals

Unlinkability

“The protection goal of Unlinkability is defined as the property that privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context.”
Unlinkability

... in other words:

- Data Minimization
- Necessity / Need-to-Know
- Purpose Binding
- Separation of Power
- Unobservability
- Undetectability

Implementation Techniques:

- Data Avoidance / Reduction
- Access Control Enforcement
- Generalization
  - Anonymization / Pseudonymization
  - Abstraction
  - Derivation
- Separation / Isolation
- Avoidance of Identifiers
Unlinkability

Think of it as ...

Transparency

"The protection goal of

Transparency

is defined as the property that
all privacy-relevant data processing
—including the legal, technical,
and organizational setting–
can be understood and reconstructed at any time."
Transparency

... in other words:

- Openness
- Accountability
- Documentation
- Reproducibility
- Notice (and Choice)
- Auditability
- Full-Disclosure

Implementation Techniques:

- Logging and Reporting
- User Notifications
- Documentation
- Status Dashboards
- Privacy Policies
- Transparency Services for Personal Data
- Data Breach Notifications
Transparency

Think of it as ...

Protection Goals for Privacy Auditing and Privacy Engineering

Intervenability

"The protection goal of Intervenability is defined as the property that intervention is possible concerning all ongoing or planned privacy-relevant data processing."

Protection Goals for Privacy Auditing and Privacy Engineering
Intervenability

... in other words:

- Self-Determination
- User Controls
- Rectification or Erasure of Data
- (Notice and) Choice
- Consent Withdrawal
- Claim Lodging / Dispute Raising
- Process Interruption

Implementation Techniques:

- Configuration Menu
- Help Desks
- Stop-Button for Processes
- Break-Glass / Alert Procedures
- Manual Override of Automated Decisions
- External Supervisory Authorities (DPAs)
Think of it as ...

Side remark 1:

*Intervenability* ↔ *transparency*

- At best, intervenability bases on sufficient transparency
- But: lack of transparency may be a reason to intervene
- At least transparency about possibilities to intervene required
  - Potentially outside the IT system
  - If not provided by the data controller: legal options
  - Proof of point at issue required
Side remark 2:

Related concept: (Notice &) Choice

- Based on Fair Information Practice Principles (FIPPs)
- Sind the mid-1990s encouraged by the Federal Trade Commission (FTC)

“Simplified Choice for Businesses and Consumers - companies should give consumers the option to decide what information is shared about them, and with whom. This should include a Do-Not-Track mechanism that would provide a simple, easy way for consumers to control the tracking of their online activities.”

FTC Report “Protecting Consumers Privacy in an Era of Rapid Change”, 2012

保护隐私权的审计和隐私工程

Side remark 2:

Related concept: (Notice &) Choice

- Hasn’t worked well in reality:
  - Lack of transparency
  - Choices are usually very limited
    (and at the same time maybe too complex)
  - A “take it or leave it” choice is usually no appropriate intervention

- Not sufficient
Side remark 3: intervenability and privacy engineering research

- Intervenability is not prominent in privacy engineering literature

- Reasons for that:
  - Hard to formalise and to measure
  - Compared with data minimisation research
    far less proposed techniques and technologies
  - Can often not be solved within the IT system alone
  - Needs a running system with clear responsibilities (operator, users)
    - not on prototype level
  - Not one fixed solution, but process-oriented, taking into account
    the full lifecycle of system evolution
Dependencies between protection goals: being researched for a long time

Confidentiality ↔ Availability

Frequent effect: adding or deriving numerous protection goals

**Integrity ↔ Intervenability**

- **Integrity**
  - No changes to data
  - No changes to process
  - Defined by processor

- **Intervenability**
  - All types of changes
  - Full process flexibility
  - Defined by individual

**Unlinkability ↔ Transparency**

- **Unlinkability**
  - No linkable data
  - No disclosure of process
  - Need-to-know

- **Transparency**
  - Full linkability of data
  - Full disclosure of process
  - Want-to-know
The Six-Pointed Star

- Confidentiality
- Unlinkability
- Integrity
- Intervenability
- Transparency
- Availability

Protection Goals for Privacy Auditing and Privacy Engineering
Protection goals in the application context

• Protection Goals have proven very useful:
  - for Implementers
  - for Lawyers
  - for Data Protection Authorities
  - for Users

• Privacy Protection Goals:
  - Unlinkability
  - Transparency
  - Intervenability

As a method for Cavoukian’s Privacy by Design Principles

http://privacybydesign.ca/
Important: perspective of the individual!

Confidentiality  Unlinkability

Integrity    Intervenability

Transparency Availability

Protection Goals for Privacy Auditing and Privacy Engineering

4. PRIVACY AUDITING

(English translation available soon: "Standard Data Protection Model")
Analysis of the context of processing

Substantive assessment

Specification of the protection goals to be considered

Target performance comparison

Feedback

Privacy auditing

- Controller, data subjects and their legal relationships
- Consent: content and collection procedure
- Business processes
- Purposes pursued
- Data, data flow, data processing steps

- Applicable law, legal basis for processing
- Balancing of interests of controller and data subjects
- Legitimacy of purposes
- Admissible data sets and transfers
- Special requirements

- Level of legal obligation (binding requirements vs. recommendation for privacy-friendly design)
- Qualitative parameters
  (e.g. circle of persons authorised to access the data)
- Analysis of protection requirements
- Quantitative parameters
  (e.g. quantified availability requirements)

- Institutional context (responsibilities, data protection management)
- Ascertainment of technical and organisational measures in the scope of the proceedings, where necessary including auxiliary processes and technical infrastructure, comparison with reference catalogue
- Determination of the effectiveness, verification of risk analysis
- Determination of shortcomings, applicable additional measures and their appropriateness

- Request to take additional measures
- Sanctions, provided serious violations of the protection goals due to missing measures have been found

- Involvement context (responsibilities, data protection management)
- Ascertainment of technical and organisational measures in the scope of the proceedings, where necessary including auxiliary processes and technical infrastructure, comparison with reference catalogue
- Determination of the effectiveness, verification of risk analysis
- Determination of shortcomings, applicable additional measures and their appropriateness

- Request to take additional measures
- Sanctions, provided serious violations of the protection goals due to missing measures have been found
Putting the pieces together

Protection Goals for Privacy Auditing and Privacy Engineering

Abstract protection goal

Applicable law

Conditions

Objective conditions

Level of obligation

Legal relationships

Specified protection goal

Qualitative parameters

Protection requirement

(English translation available soon: “Standard Data Protection Model”)

5. CONCLUSION
Conclusion

- Privacy and data protection by design
  - Will be demanded in the General Data Protection Regulation (but how exactly?)
  - Can be achieved by applying protection goals (all six)
  - With focus on the perspective of the individuals (not the controller)

- Useful for
  - Privacy engineering (not only IT systems, but business models, laws, standards, …)
  - Privacy auditing (and Data Protection Impact Assessment)

- In other privacy engineering approaches not much on transparency and intervenability, yet: tasks for cross-disciplinary research

Thank you for your attention!

Marit Hansen
marit.hansen@datenschutzzentrum.de
Funding Notice

Shaping the Future of Electronic Identity partly funded by EU FP7, GA n° 318424

Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt (Privacy Forum) partly funded by the German Federal Ministry of Education and Research

www.futureid.eu www.forum-privatheit.de