

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



ULD  www.datenschutzzentrum.de

Setting of ULD

Schleswig-Holstein
State of Germany




Coordinates: 54°28'12"N 9°30'50"E

Country	Germany
Capital	Kiel
Government	
• Minister	Torsten Albig (SPD)
• President	
• Governing parties	SPD / Greens / SSW
• Votes in Bundesrat	4 (of 69)
Area	
• Total	15,763.18 km ² (6,086.20 sq mi)
Population (2013-12-31) ^[1]	
• Total	2,815,955
• Density	180/km ² (460/sq mi)

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



Source: www.maps-for-free.com

Source: en.wikipedia.org/wiki/Schleswig-Holstein

Protection Goals for Privacy Auditing

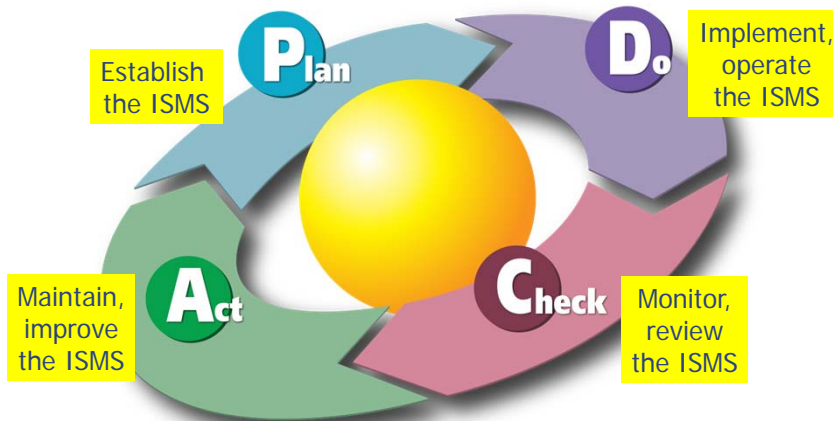
Overview

1. Working with Protection Goals
2. Protection Goals for Privacy Engineering
3. Dependencies between Protection Goals
4. Privacy Auditing
5. Conclusion

1. WORKING WITH PROTECTION GOALS

Successful engineering needs iteration: The PDCA Cycle

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

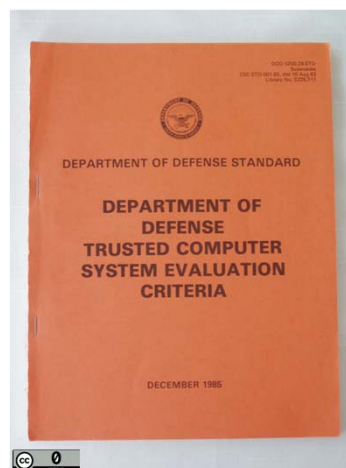


 Source: Karn G. Bulsuk

Protection Goals for Privacy Auditing and Privacy Engineering

Information security protection goals

- Confidentiality
- Integrity
- Availability





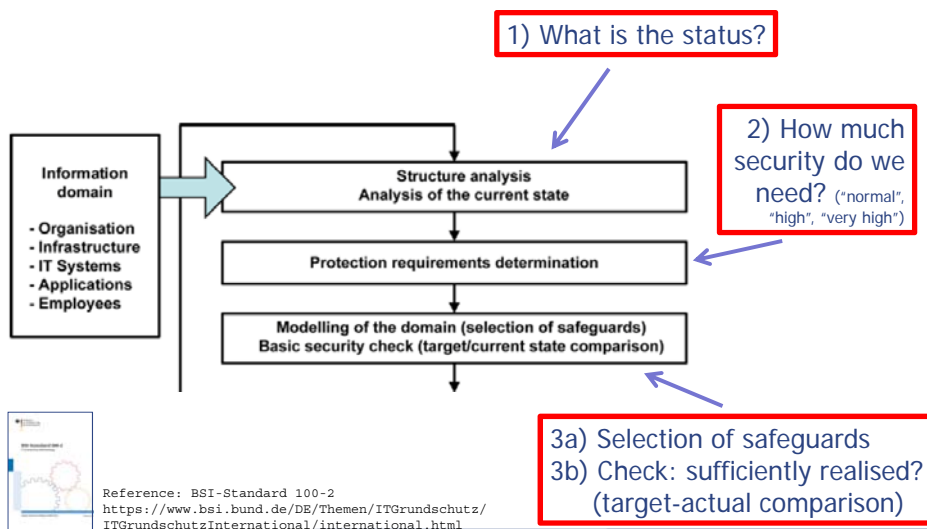
Protection Goals for Privacy Auditing and Privacy Engineering

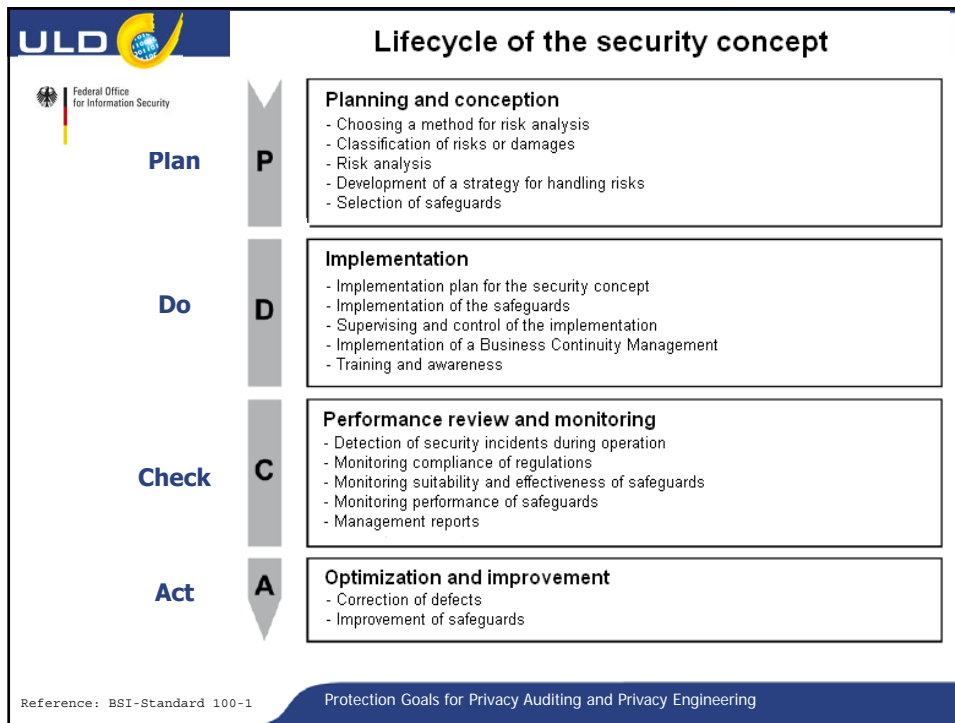
How to make use of the notion of protection goals?

- (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





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!

*) Reference: Dorfman, Mark S. (2007): Introduction to Risk Management and Insurance (9 ed.). Englewood Cliffs, N.J: Prentice Hall.



2. PROTECTION GOALS FOR PRIVACY

Reference: Hansen, Marit / Jensen, Meiko / Rost, Martin (2015): Protection Goals for Privacy Engineering. International Workshop on Privacy Engineering – IWPE'15, IEEE.

Classic Protection Goals

Confidentiality



“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

Confidentiality



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



Integrity

**“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.”**

Integrity

... in other words:

- Authenticity
- Detection of Data Changes
- Non-Repudiation
- Reliability

Integrity

Implementation Techniques:

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



Availability

“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.”

Availability



... in other words:

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

Availability



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

Unlinkability



Implementation Techniques:

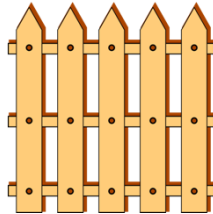
- Data Avoidance / Reduction
- Access Control Enforcement
- Generalization
 - Anonymization / Pseudonymization
 - Abstraction
 - Derivation
- Separation / Isolation
- Avoidance of Identifiers



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

Transparency



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 ...



Intervenability



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

Intervenability



... in other words:

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

Intervenability



Implementation Techniques:

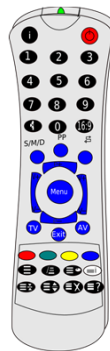
- Configuration Menu
- Help Desks
- Stop-Button for Processes
- Break-Glass / Alert Procedures
- Manual Override of Automated Decisions
- External Supervisory Authorities (DPAs)



Intervenability



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](#)

Side remark 2:
Related concept: (Notice &) Choice

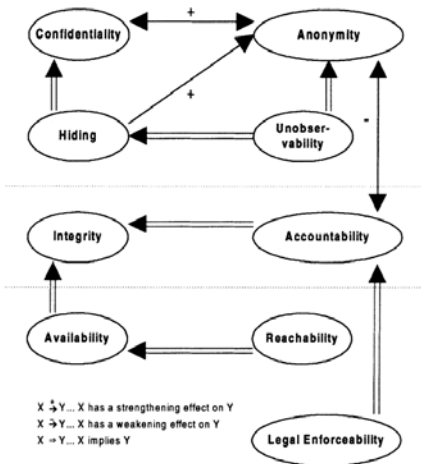
- Hasn't worked well in reality:
 - Lack of transparency
 - **Choices are usually very limited**
(and at the same time **maybe too complex**)
 - A "take it or leave it" choice is usually no appropriate intervention
- **Not sufficient**

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**

3. DEPENDENCIES BETWEEN PROTECTION GOALS

Dependencies between protection goals: being researched for a long time



Frequent effect: adding or deriving numerous protection goals

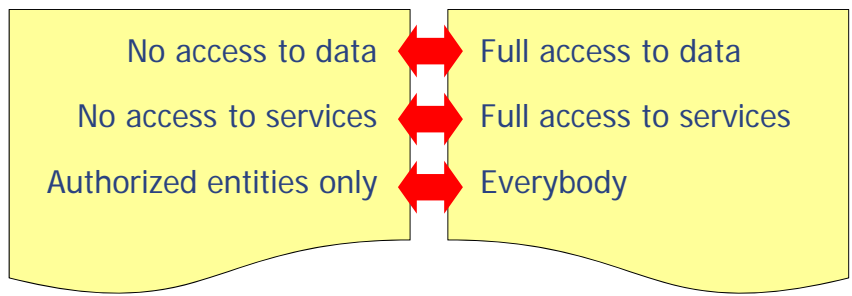


X ⇌ Y... X has a strengthening effect on Y
 X → Y... X has a weakening effect on Y
 X → Y... X implies Y

*) Reference: Wolf, Gritta / Pfitzmann, Andreas (2000): Properties of protection goals and their integration into a user interface. Computer Networks Vol. 32, Issue 6, pp. 685-699.

Fig. 3. Synergies and interferences of protection goals.

Confidentiality ↔ Availability

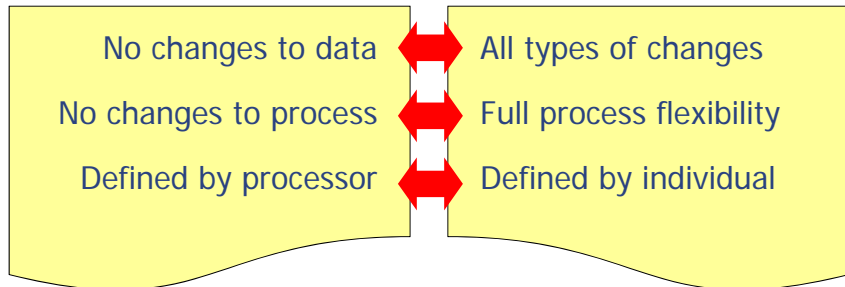


Confidentiality

Availability



Integrity ↔ Intervenability

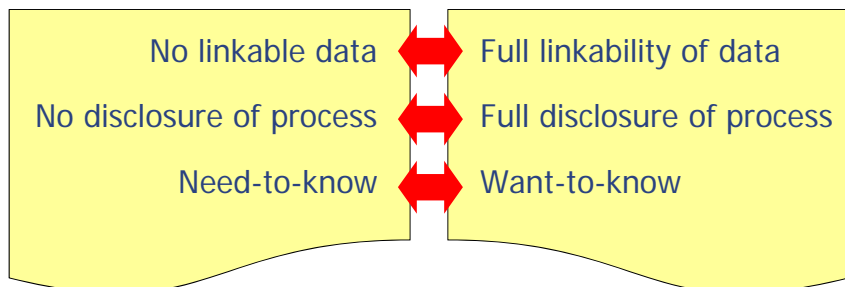


Integrity

Intervenability



Unlinkability ↔ Transparency

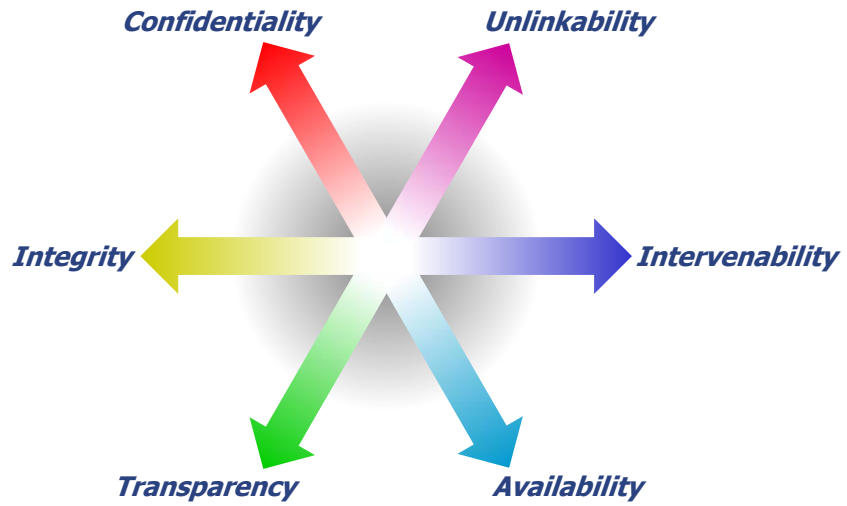


Unlinkability

Transparency

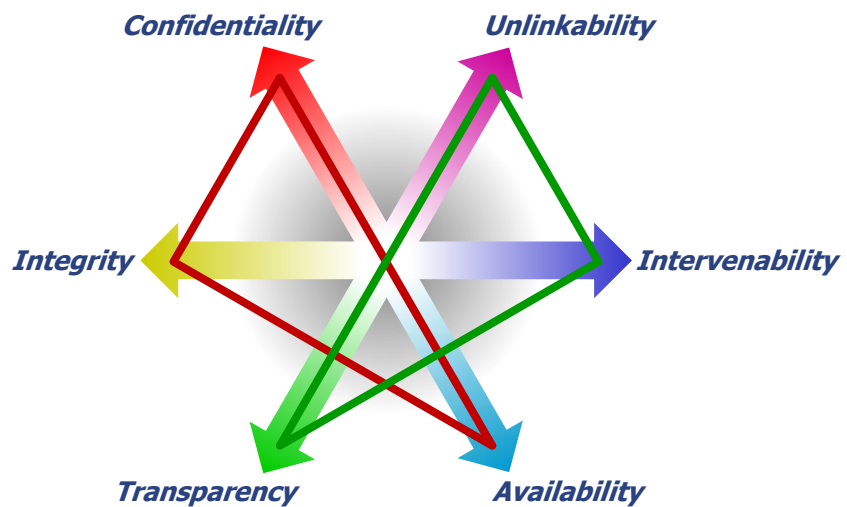


The Six-Pointed Star



Protection Goals for Privacy Auditing and Privacy Engineering

The Six-Pointed Star

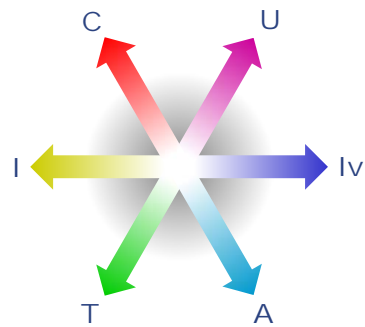


Protection Goals for Privacy Auditing and Privacy Engineering

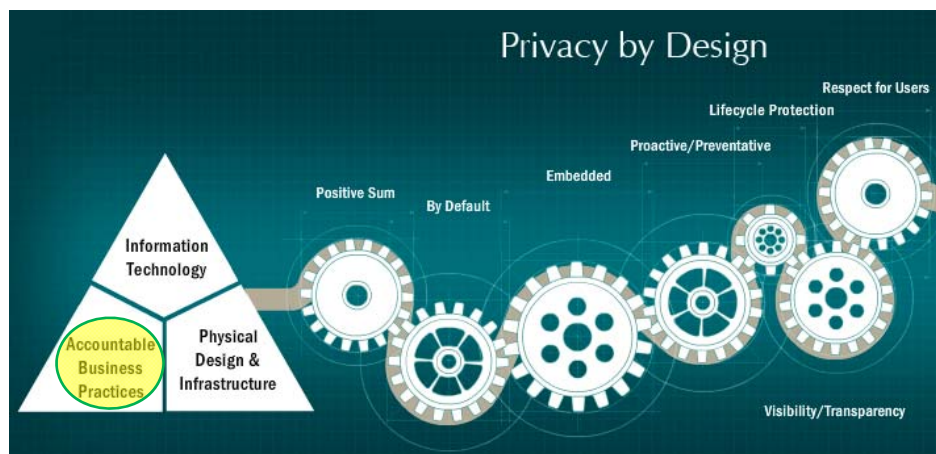
Protection goals in the application context



- 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




Our approach for "Data Protection by Design" in Art. 23 of the General Data Protection Regulation

Article 23	Article 23	Article 23	Article 23
Data protection by design and by default	Data protection by design and by default	Data protection by design and by default	Data protection by design and by default
<i>Amendment 118</i>			
1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.	1. Having regard to the state of the art and the cost of implementation, current technical knowledge, international best practices and the risks represented by the data processing, the controller and the processor, if any, shall, both at the time of the determination of the purposes and means for processing and at the time of the processing itself, implement appropriate and proportionate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular with regard to the principles laid down in Article 5. Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to	1. Having regard to available technology the state-of-the-art and the cost of implementation, and taking account of the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for rights and freedoms of individuals posed by the processing, the controllers shall, both at the time of the determination of the means for processing and at the time of the processing itself; implement appropriate technical and organisational measures appropriate to the processing activity being carried out and its objectives, such as data minimisation and pseudonymisation, and procedures in such a way that the processing will meet the requirements of this Regulation and ensure protect the protection of the rights of the data subjects.	1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the purposes and means for processing and at the time of the processing itself, adopt appropriate technical and organisational solutions designed to implement data protection principles in an effective way and to integrate the necessary safeguards into the processing tools.
	<i>deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. Where the controller has carried out a data protection impact assessment pursuant to Article 35, the results shall be taken into account when developing those measures and procedures.</i>		

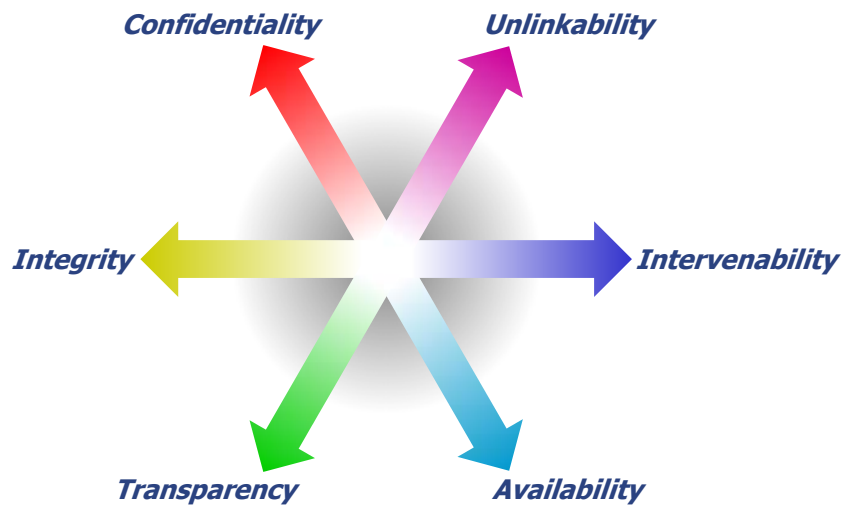
- In short:
- "... by design" = built-in
 - "Data protection" = reqs from the GDPR, esp. rights of the data subject
 - Differences: who, when, how, how much?

Our approach for "Data Protection by Design" in Art. 23 of the General Data Protection Regulation

European Commission	1st reading position of the European Parliament	General Approach of the Council	EDPS recommendations
2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.	2. The controller shall implement mechanisms for ensuring ensure that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained or disseminated beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals and that data subjects are able to control the distribution of their personal data.	2. The controller shall implement mechanisms appropriate measures for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of are processed; this applies to the amount of the data collected, the extent of their processing, and the time-period of their storage and their accessibility. Where the purpose of the processing is not intended to provide the public with information in particular, those mechanisms shall ensure that by default personal data are not made accessible without human intervention to an indefinite number of individuals.	2. The controller shall implement appropriate solutions for ensuring that, by default, <u>personal data are processed in the least intrusive manner possible</u> without prejudice to the choice of the data subject to allow the processing of personal data in a broader sense.
			<p>In short:</p> <ul style="list-style-type: none"> • "... by default" = configuration should be privacy-friendly • Related to necessity for purpose

ULD  www.datenschutzzentrum.de

Important: perspective of the individual!





Confidentiality Unlinkability

Integrity Intervenableity

Transparency Availability

Protection Goals for Privacy Auditing and Privacy Engineering

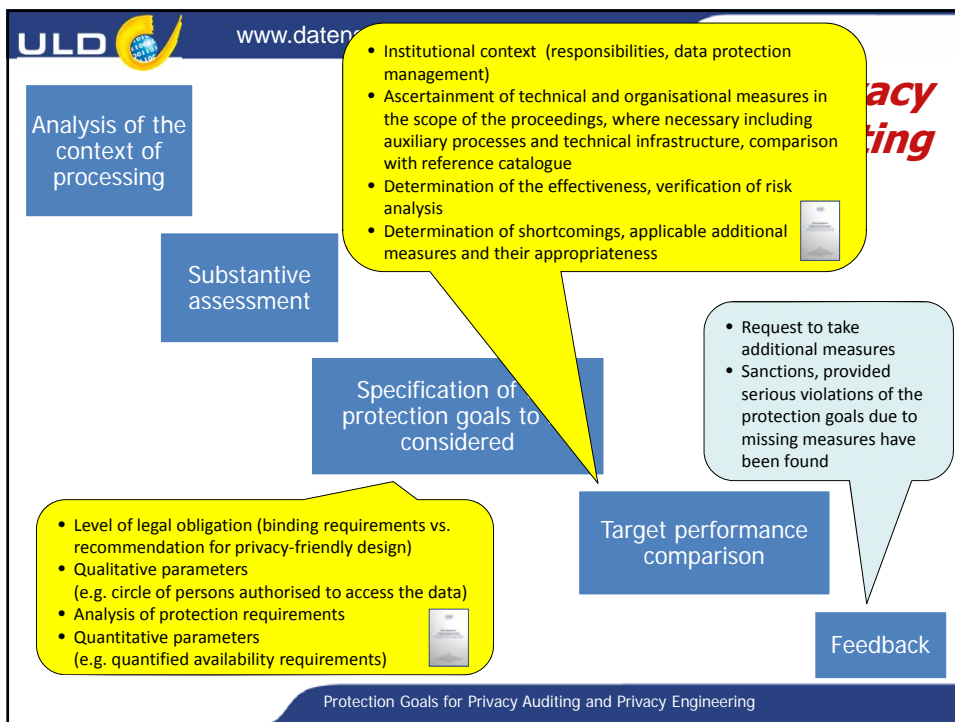
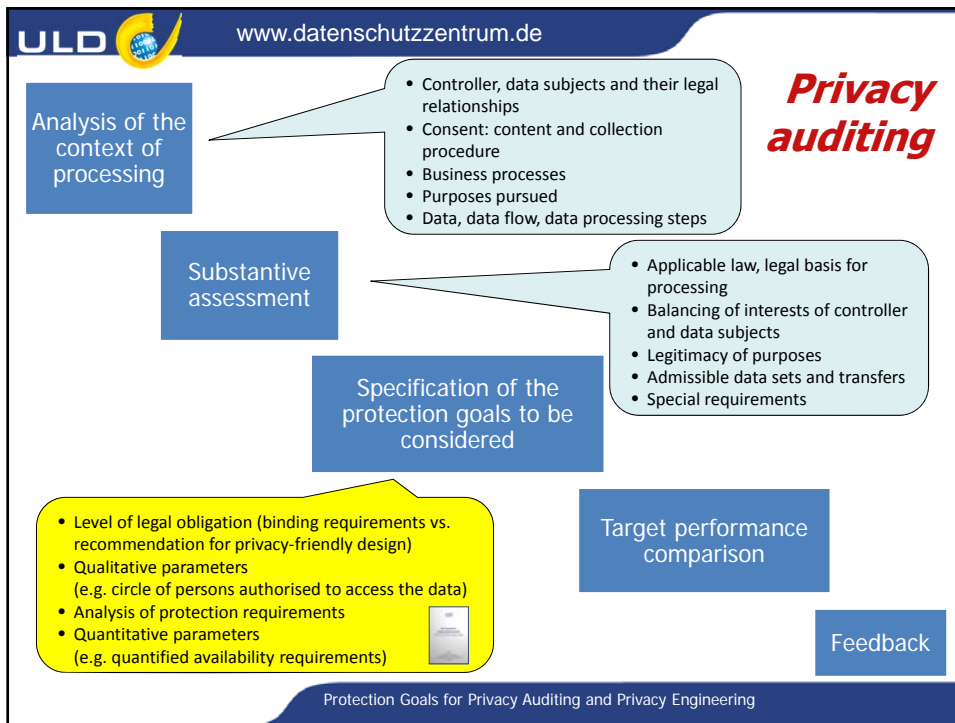
ULD  www.datenschutzzentrum.de



4. PRIVACY AUDITING

Reference: <https://www.datenschutzzentrum.de/uploads/sdm/SDM-Handbuch.pdf>
 (English translation available soon: "Standard Data Protection Model")

Protection Goals for Privacy Auditing and Privacy Engineering

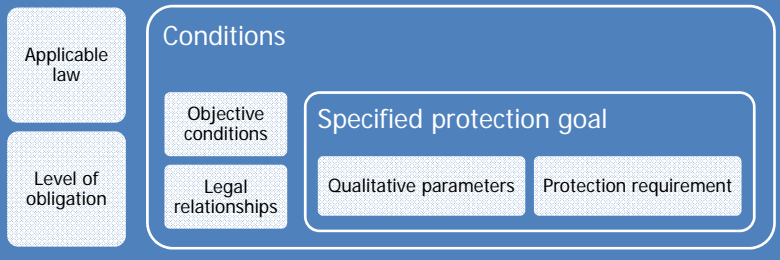




Putting the pieces together

 Source: Karn G. Bulsuk

Abstract protection goal



<https://www.datenschutzzentrum.de/uploads/sdm/SDM-Handbuch.pdf>
(English translation available soon: "Standard Data Protection Model")

Protection Goals for Privacy Auditing and Privacy Engineering

5. CONCLUSION

Protection Goals for Privacy Auditing and Privacy Engineering

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



Protection Goals for Privacy Auditing and Privacy Engineering

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



www.futureid.eu



Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt (Privacy Forum)



partly funded by the
German Federal Ministry
of Education and Research

www.forum-privatheit.de