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

forum <privatheit> selbstbestimmtes_leben_in_der_digitalen_welt | ABC4TRUST | FutureID | ipen | ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Setting of ULD

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

Schleswig-Holstein	
State of Germany	
Flag / Coat of arms	
Coordinates: 54°28'12"N 9°30'50"E	
Country	Germany
Capital	Kiel
Government	
• Minister-President	Torsten Albig (SPD)
• Governing parties	SPD / Greens / SSW
• Votes in Bundesrat	4 (of 69)
Area	
• Total	15,763.18 km² (6,086.20 sq mi)
Population (2013-12-31)[1]	
• Total	2,815,955
• Density	180/km² (460/sq mi)

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

Source: www.maps-for-free.com

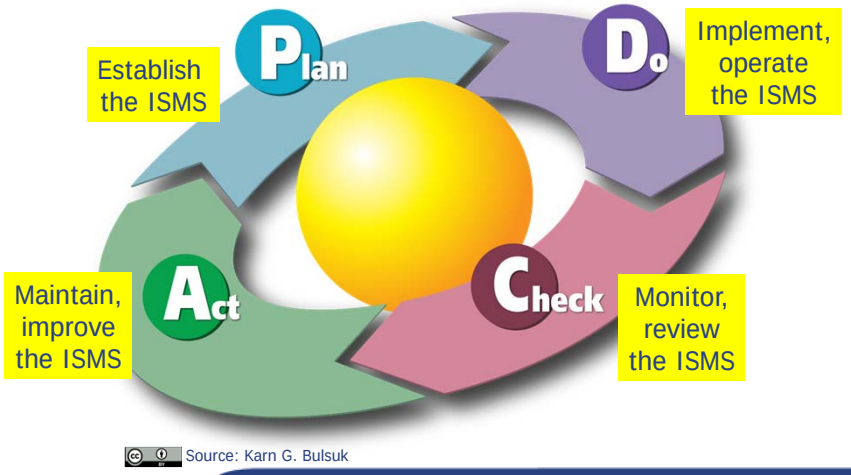
Overview

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

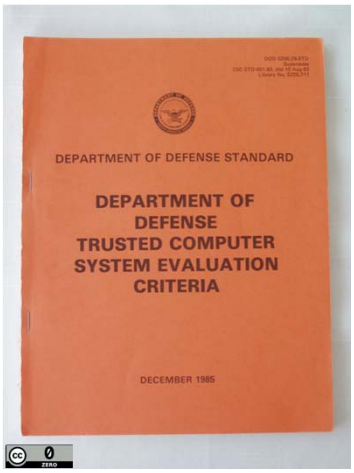
Same for Information Security Management Systems (ISMS) [cf. ISO 27001]



Source: Karn G. Bulsuk

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

ISO/IEC 27001:2005

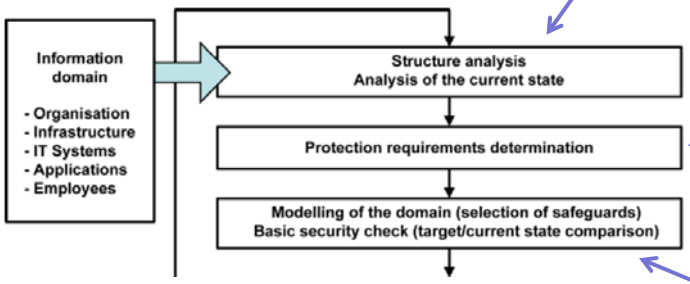
- Established procedure
  - Analysis of risks
  - Dealing with risks
    → selecting the appropriate safeguards
  - Considering the lifecycle of development

Federal Office for Information Security

Creation of a security policy

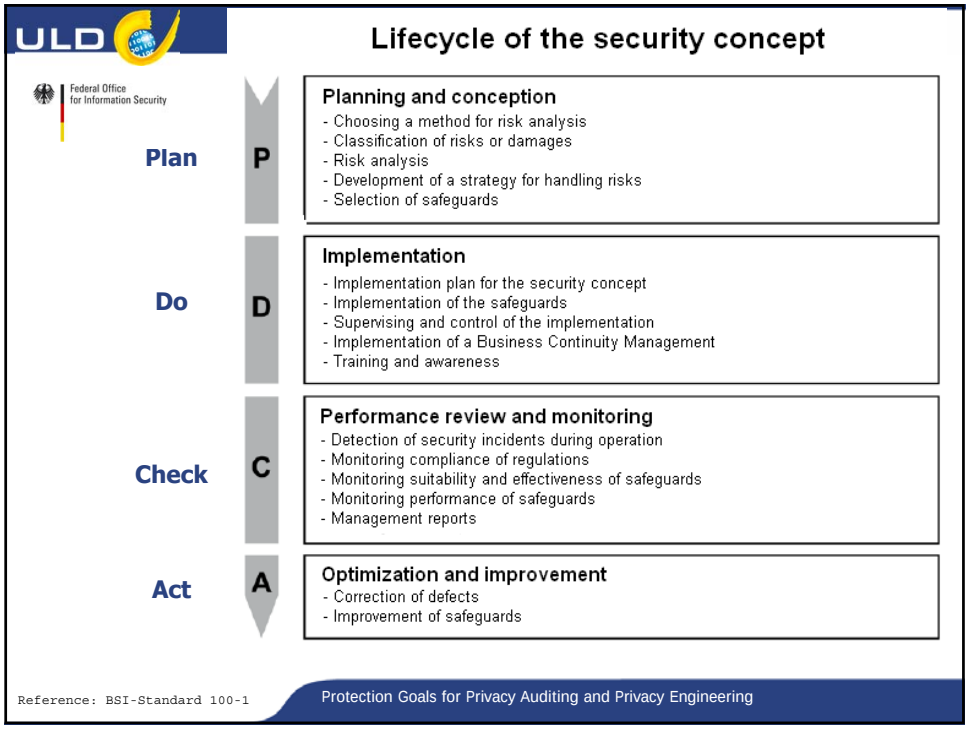
1) What is the status?

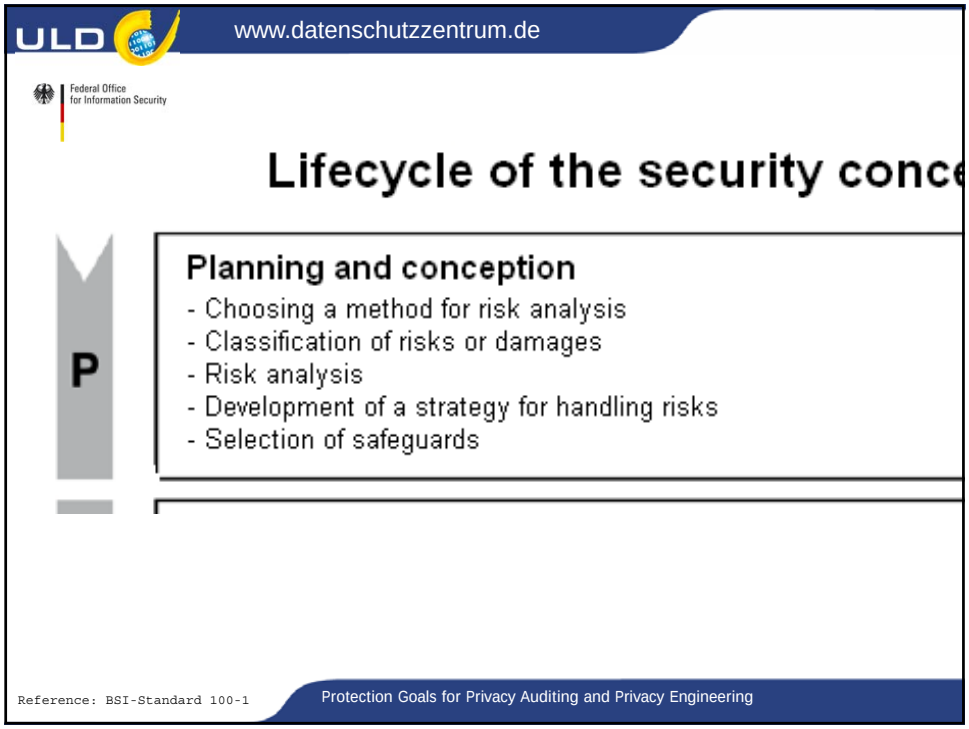
2) How much security do we need? ("normal", "high", "very high")



3a) Selection of safeguards
3b) Check: sufficiently realised? (target-actual comparison)

Reference: BSI-Standard 100-2
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzInternational/international.html


ULD
Federal Office for Information Security
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
Protection Goals for Privacy Auditing and Privacy Engineering


ULD
www.datenschutzzentrum.de
Federal Office for Information Security
Lifecycle of the security conce
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
Reference: BSI-Standard 100-1
Protection Goals for Privacy Auditing and Privacy Engineering

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.


Protection Goals for Privacy Engineering

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.

Slides: Meiko Jensen

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

ULD www.datenschutzzentrum.de

Availability

Implementation Techniques:

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

Protection Goals for Privacy Auditing and Privacy Engineering

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

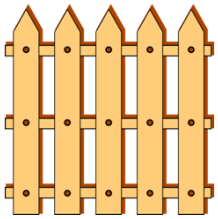
Unlinkability

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

ULD www.datenschutzzentrum.de

Intervenability

Implementation Techniques:

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

Protection Goals for Privacy Auditing and Privacy Engineering

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

ULD www.datenschutzzentrum.de

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

Protection Goals for Privacy Auditing and Privacy Engineering

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

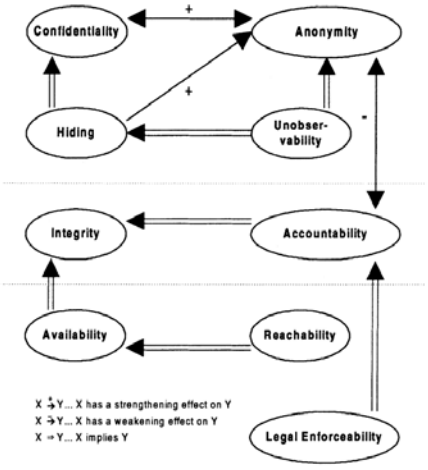


Fig. 3. Synergies and interferences of protection goals.

Frequent effect: adding or deriving numerous protection goals

*) 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.

Confidentiality ↔ Availability

No access to data	Full access to data
No access to services	Full access to services
Authorized entities only	Everybody

Confidentiality **Availability**

Integrity ↔ Intervenability

No changes to data	All types of changes
No changes to process	Full process flexibility
Defined by processor	Defined by individual

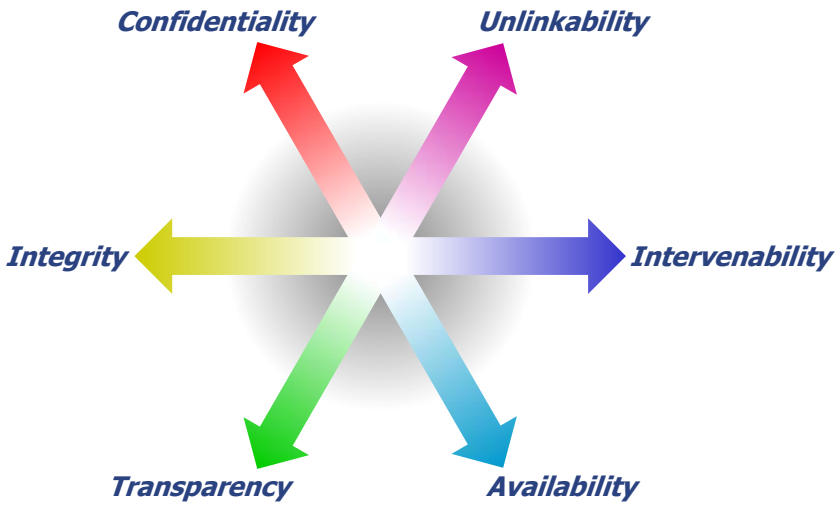
Integrity ***Intervenability***

Unlinkability ↔ Transparency

No linkable data	Full linkability of data
No disclosure of process	Full disclosure of process
Need-to-know	Want-to-know

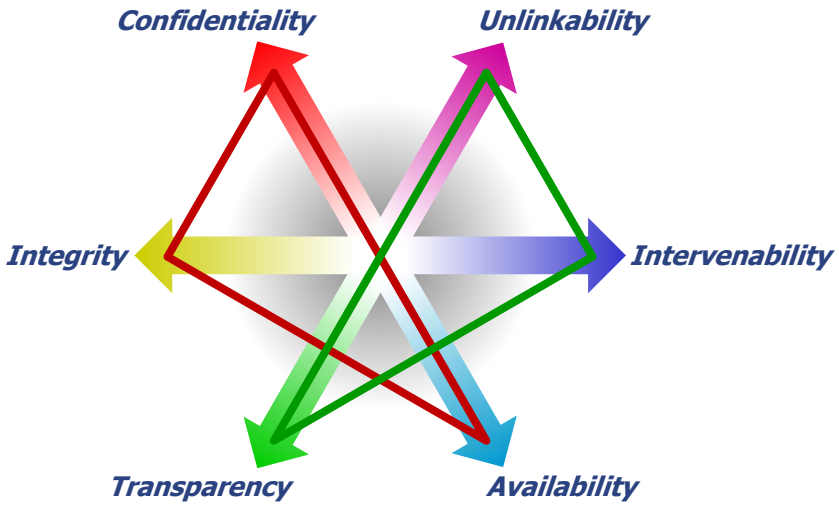
Unlinkability ***Transparency***

The Six-Pointed Star



ULD www.datenschutzzentrum.de

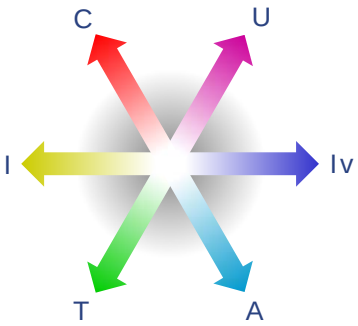
The Six-Pointed Star



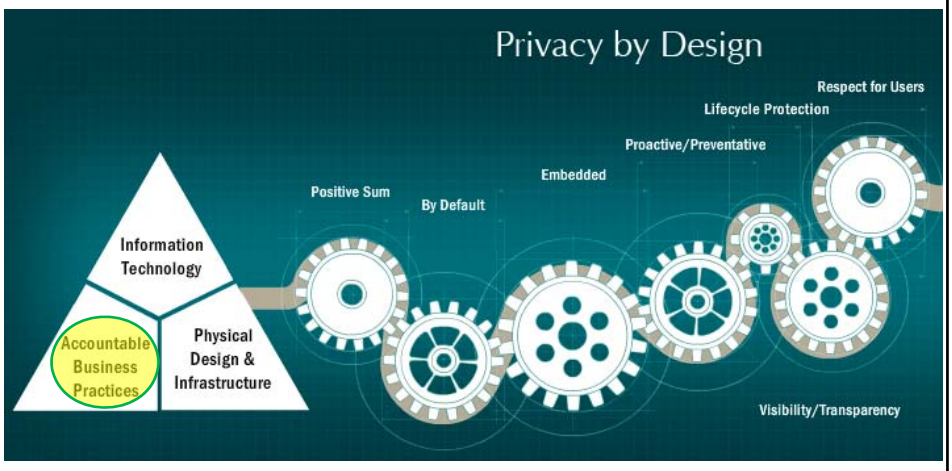
Protection Goals for Privacy Auditing and Privacy Engineering

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



http://privacybydesign.ca/

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***
	Amendment 118		
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.
	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 33, the results shall be taken into account when developing those measures and procedures.		

In short:

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

ULD www.datenschutzzentrum.de

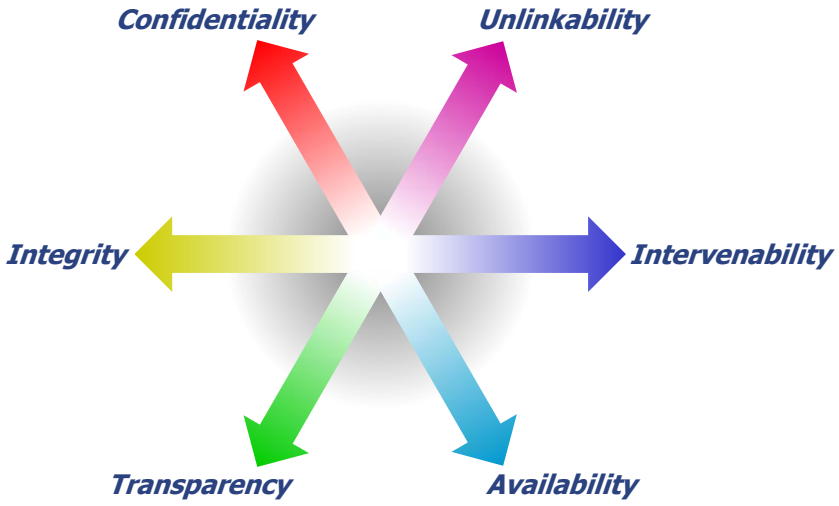
Our approach for "Data Protection by Design" in Art. 23 of the General Data Protection Regulation

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	2. The controller shall implement appropriate solutions for ensuring that, by default, personal data are processed in the least intrusive manner possible without prejudice to the choice of the data subject to allow the processing of personal data in a broader sense.
		mechanisms shall ensure that by default personal data are not made accessible *without human intervention* to an indefinite number of individuals.	

In short:

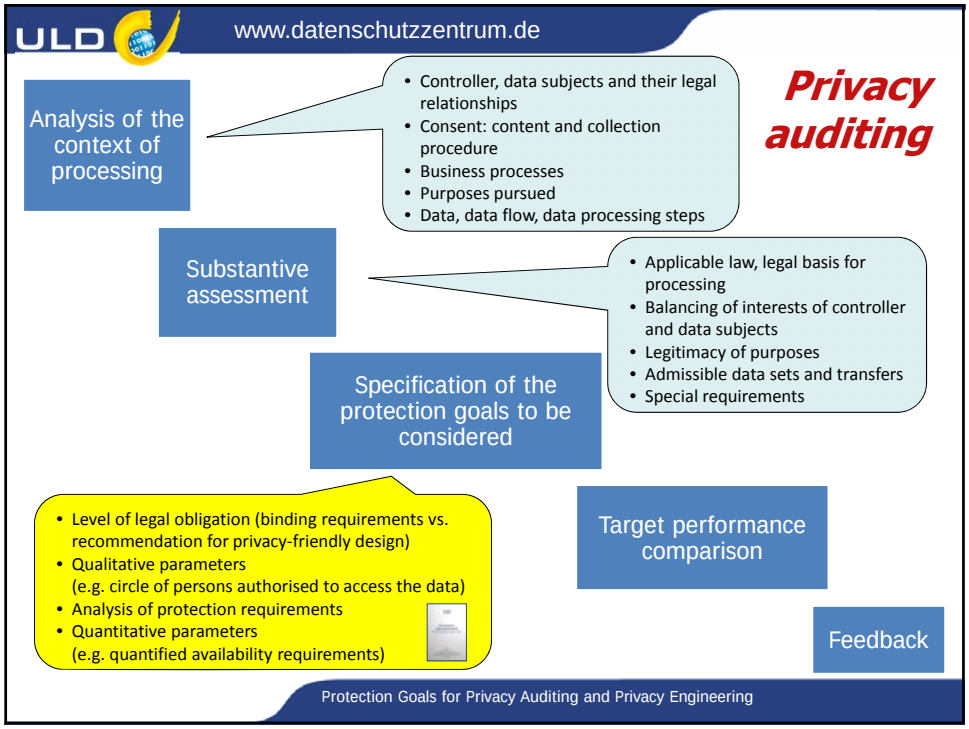
- "... by default" = configuration should be privacy-friendly
- Related to necessity for purpose

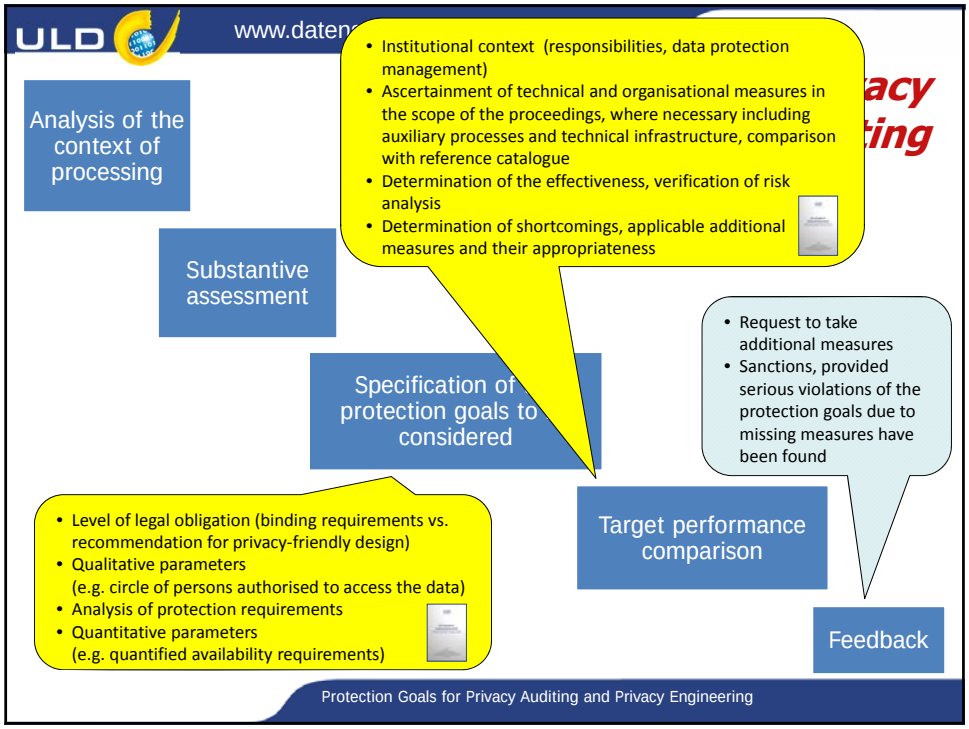
Important: perspective of the individual!



4. PRIVACY AUDITING

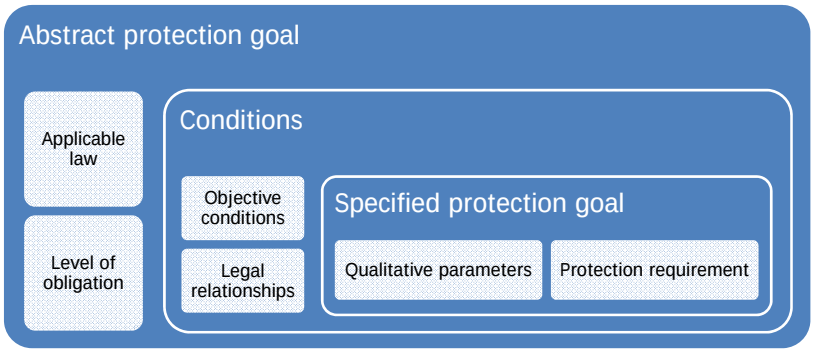
Reference: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Handbuch.pdf
(English translation available soon: “Standard Data Protection Model”)


ULD
www.datenschutzzentrum.de
Privacy auditing
Analysis of the context of processing
• Controller, data subjects and their legal relationships
• Consent: content and collection procedure
• Business processes
• Purposes pursued
• Data, data flow, data processing steps
Substantive assessment
• Applicable law, legal basis for processing
• Balancing of interests of controller and data subjects
• Legitimacy of purposes
• Admissible data sets and transfers
• Special requirements
Specification of the protection goals to be considered
• 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)
Target performance comparison
Feedback
Protection Goals for Privacy Auditing and Privacy Engineering


ULD
www.daten
Analysis of the context of processing
• 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
Substantive assessment
Specification of protection goals to considered
• Request to take additional measures
• Sanctions, provided serious violations of the protection goals due to missing measures have been found
• 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)
Target performance comparison
Feedback
Protection Goals for Privacy Auditing and Privacy Engineering

Source: Karn G. Bulsuk

Putting the pieces together



https://www.datenschutzzentrum.de/uploads/sdm/SDM-Handbuch.pdf
(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

forum <privatheit> selbstbestimmtes_leben_in_der_digitalen_welt
ABC4TRUST
FutureID
ipen
ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Funding Notice

Shaping the Future of Electronic Identity

partly funded by EU FP7, GA n° 318424

SEVENTH FRAMEWORK PROGRAMME

www.futureid.eu

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

GEFÖRDERT VOM Bundesministerium für Bildung und Forschung

partly funded by the German Federal Ministry of Education and Research

www.forum-privatheit.de