# Technische Aspekte: Privacy by Design und Default

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de

# Auszug aus Artikel 25 DSGVO

**Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen**

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z.B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

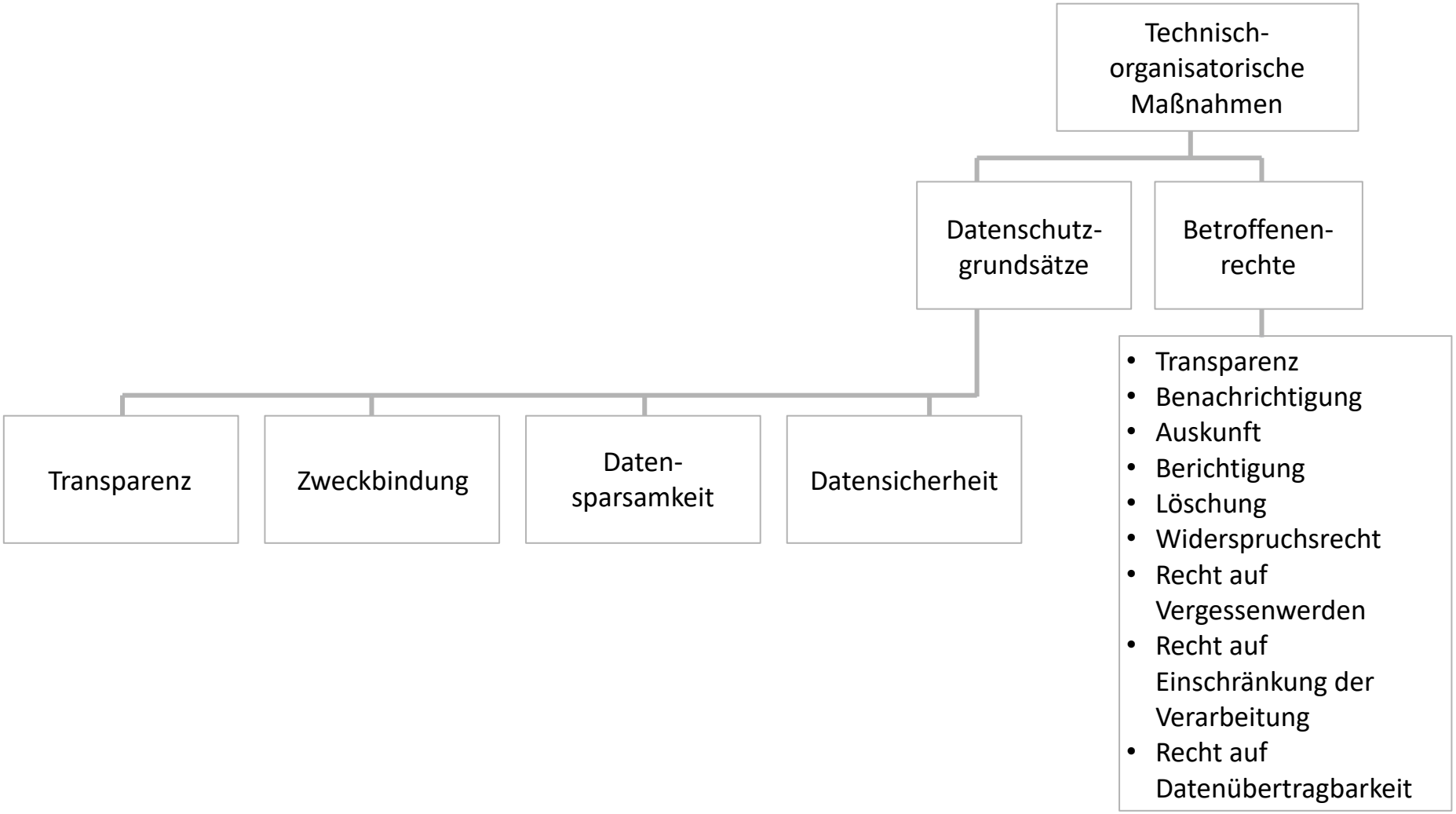
...

# Begriffe

- Art. 25 (1) Privacy by Design – Datenschutz durch Technikgestaltung
  - Berücksichtigung
    - des Stands der Technik
    - der Implementierungskosten
    - der Umstände und Zwecke
    - der Eintrittswahrscheinlichkeiten und … Risiken
  - Geeignete technisch-organisatorische Maßnahmen
    - zur Umsetzung der Datenschutzgrundsätze
      - Rechtmäßigkeit und Transparenz
      - Datenminimierung und Datensparsamkeit
      - Zweckbindung
      - Datensicherheit
    - zur Durchsetzung der Betroffenenrechte

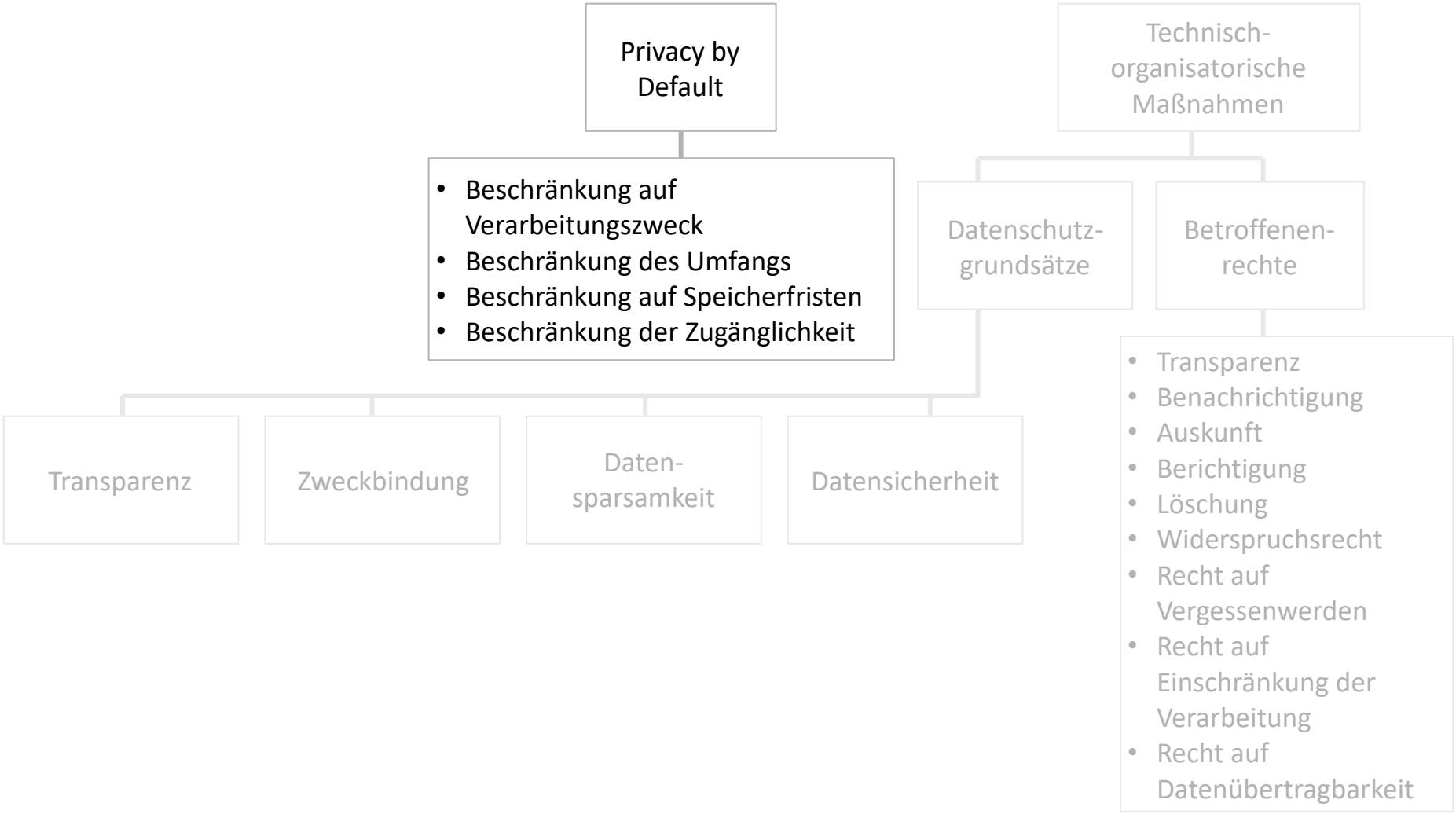
# EU-Datenschutzgrundverordnung (DSGVO)

- Betroffenenrechte
  - Transparenz (Art. 12)
    - einfache, verständliche Sprache; Kosten für Auskunft
  - Benachrichtigung (Art. 13 und 14)
    - Informationspflichten einer verantwortlichen Stelle
  - Recht auf Auskunft (Art. 15)
  - Recht auf Berichtigung (Art. 16)
  - Recht auf Löschung (Art. 17)
    - inklusive Recht auf Vergessenwerden (Art 17. Abs. 2)
  - Recht auf Einschränkung der Verarbeitung (Art. 18)
    - entspricht dem Recht auf Sperrung aus dem BDSG
  - Recht auf Datenübertragbarkeit (Art. 20)
    - Datenmitnahme in strukturierten gängigen elektron. Formaten
  - Widerspruchsrecht (Art. 21)


Technisch-organisatorische Maßnahmen
Datenschutz-grundsätze
Betroffenen-rechte
Transparenz
Zweckbindung
Daten-sparsamkeit
Datensicherheit
• Transparenz
• Benachrichtigung
• Auskunft
• Berichtigung
• Löschung
• Widerspruchsrecht
• Recht auf Vergessenwerden
• Recht auf Einschränkung der Verarbeitung
• Recht auf Datenübertragbarkeit

# Begriffe

- Art. 25 (2) Privacy by Default – datenschutzfreundliche Voreinstellungen
  - Beschränkung durch fest eingebaute Funktionalität
    - Beschränkung auf Verarbeitungszweck
    - Beschränkung des Umfangs
    - Beschränkung auf Speicherfristen
    - Beschränkung der Zugänglichkeit


Privacy by Default
• Beschränkung auf Verarbeitungszweck
• Beschränkung des Umfangs
• Beschränkung auf Speicherfristen
• Beschränkung der Zugänglichkeit
Technisch-organisatorische Maßnahmen
Datenschutz-grundsätze
Betroffenen-rechte
Transparenz
Zweckbindung
Daten-sparsamkeit
Datensicherheit
• Transparenz
• Benachrichtigung
• Auskunft
• Berichtigung
• Löschung
• Widerspruchsrecht
• Recht auf Vergessenwerden
• Recht auf Einschränkung der Verarbeitung
• Recht auf Datenübertragbarkeit

# Auszug aus Artikel 32 DSGVO

**Art. 32 Sicherheit der Verarbeitung**

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

...

# Begriffe

- Art. 32 (1) Sicherheit der Verarbeitung
  - Geeignete technisch-organisatorische Maßnahmen
    - zur Pseudonymisierung und Verschlüsselung
    - zur Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit
    - zur Wiederherstellung der Verfügbarkeit nach Zwischenfällen
    - zur Überprüfung, Bewertung und Evaluierung der technisch-organisatorischen Maßnahmen


Privacy by Default
Technisch-organisatorische Maßnahmen
• Beschränkung auf Verarbeitungszweck
• Beschränkung des Umfangs
• Beschränkung auf Speicherfristen
• Beschränkung der Zugänglichkeit
Datenschutz-grundsätze
Betroffenen-rechte
Transparenz
Zweckbindung
Daten-sparsamkeit
Datensicherheit
• Transparenz
• Benachrichtigung
• Auskunft
• Berichtigung
• Löschung
• Widerspruchsrecht
• Recht auf Vergessenwerden
• Recht auf Einschränkung der Verarbeitung
• Recht auf Datenübertragbarkeit
• Pseudonymisierung
• Verschlüsselung
• Vertraulichkeit
• Integrität
• Verfügbarkeit
• Belastbarkeit
• Wiederherstellbarkeit
• Notfallmanagement
• Überprüfbarkeit
• Bewertung
• Evaluierung

# Unter Berücksichtigung …

**Art. 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen**

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z.B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck e… enge der erhobenen personenbezogene… Zugänglichkeit. Solche Maßnahme… durch Voreinstellungen nicht ohne… sonen zugänglich gemacht werden.

- Stand der Technik
- Implementierungskosten
- Art, Umfang, Umstände, Zwecke
- Risiko
- Technisch-organisatorische Maßnahmen

…

# Unter Berücksichtigung …

**Art. 32 Sicherheit der Verarbeitung**

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

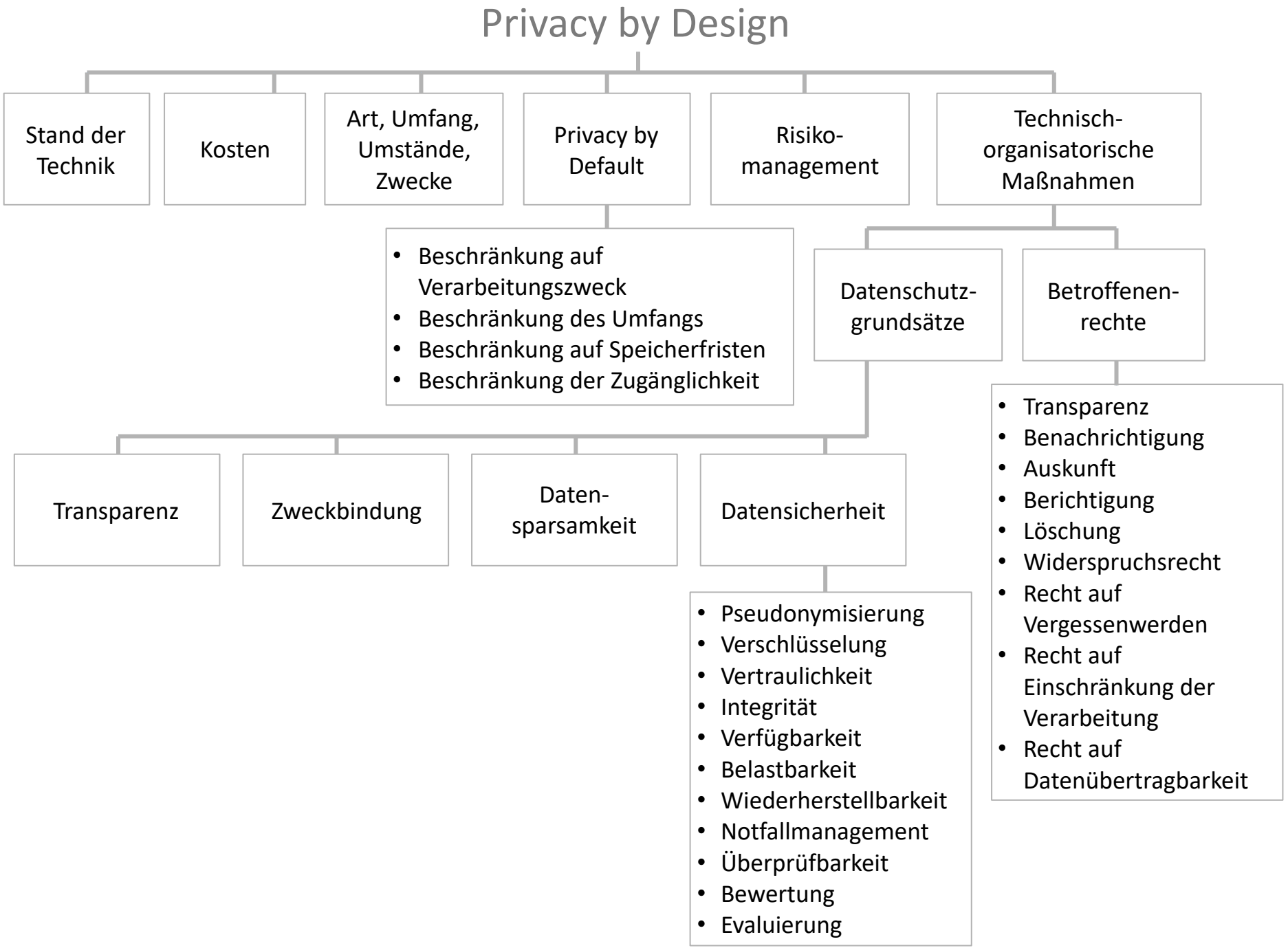
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

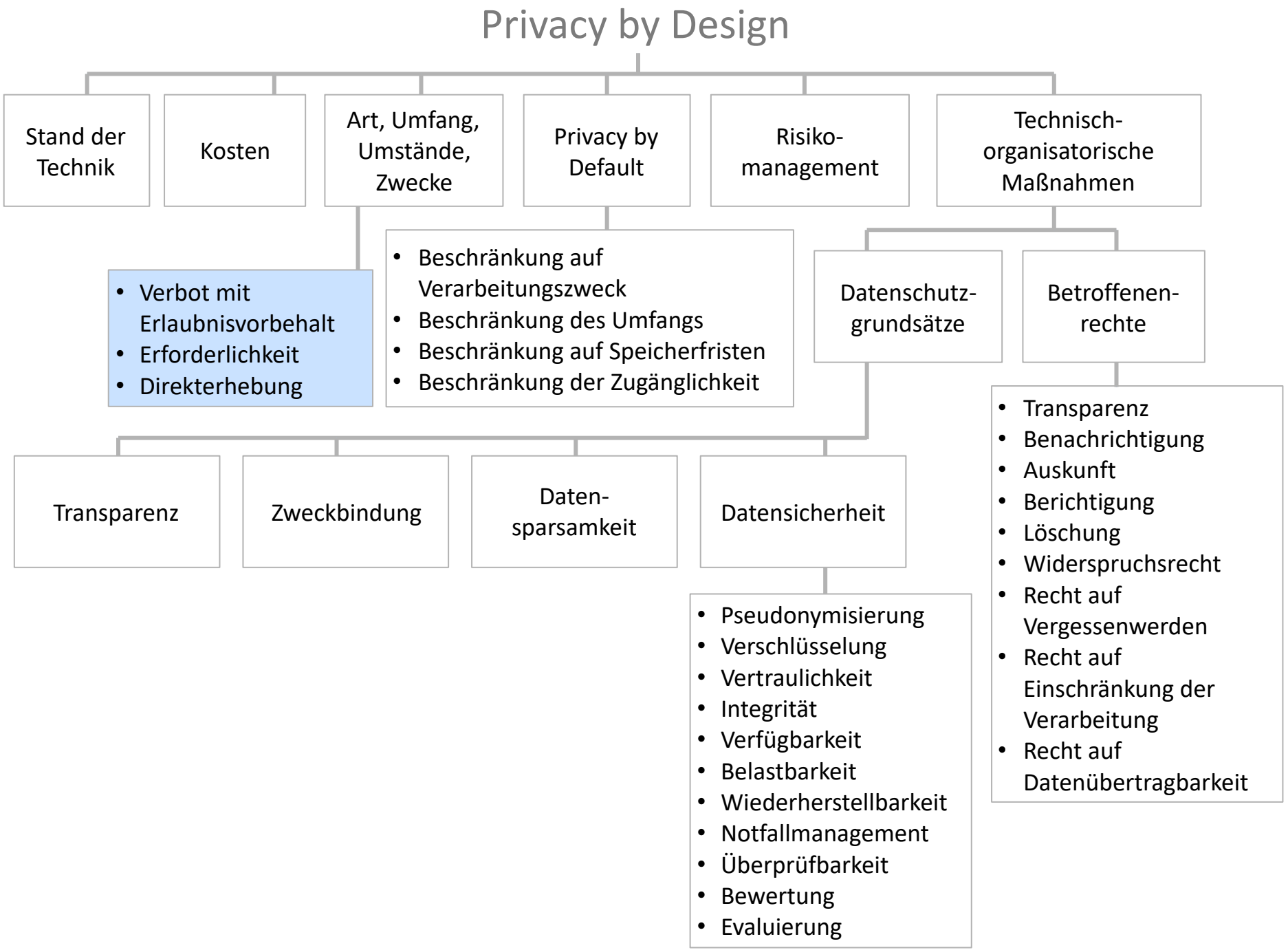
d) ein Verfahren zur regelmäßigen
technischen und organisatorischer

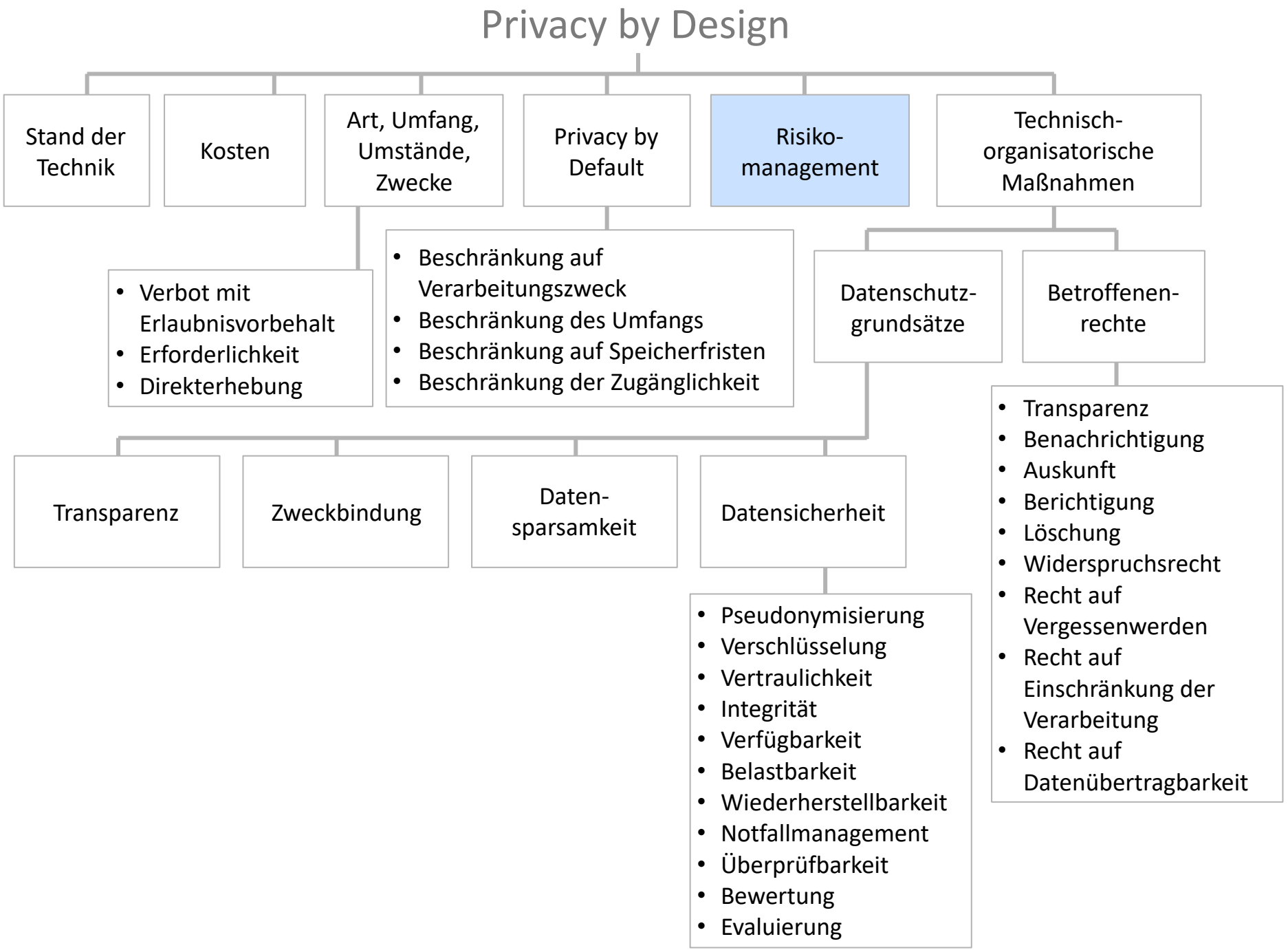
(2) Bei der Beurteilung des angem
die mit der Verarbeitung verbunde
Vernichtung, Verlust, Veränderung
personenbezogenen Daten, die üb

- Stand der Technik
- Implementierungskosten
- Art, Umfang, Umstände, Zwecke
- Risiko
- Technisch-organisatorische Maßnahmen

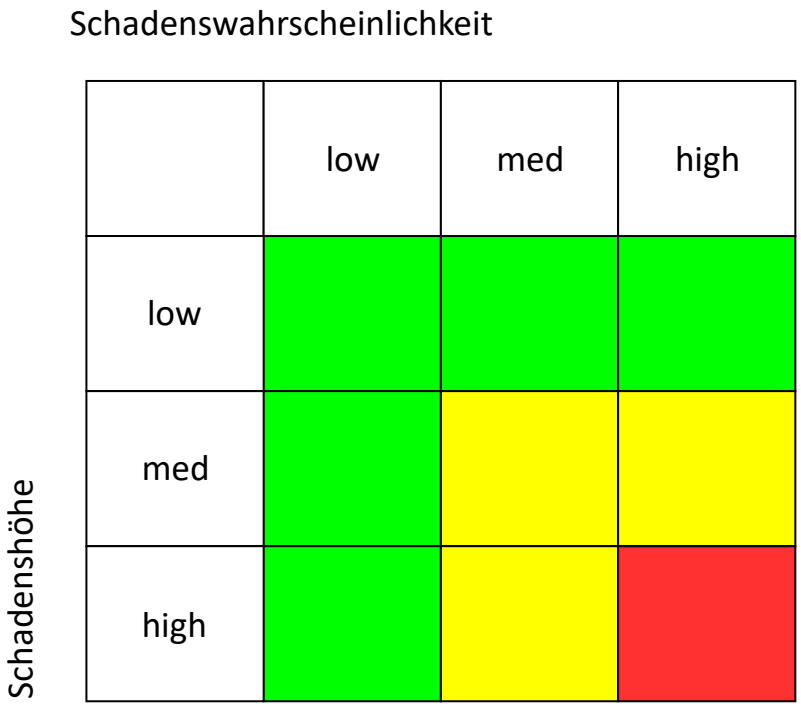
…


Privacy by Design
Stand der Technik
Kosten
Art, Umfang, Umstände, Zwecke
Privacy by Default
Risiko-management
Technisch-organisatorische Maßnahmen
Beschränkung auf Verarbeitungszweck
Beschränkung des Umfangs
Beschränkung auf Speicherfristen
Beschränkung der Zugänglichkeit
Datenschutz-grundsätze
Betroffenen-rechte
Transparenz
Benachrichtigung
Auskunft
Berichtigung
Löschung
Widerspruchsrecht
Recht auf Vergessenwerden
Recht auf Einschränkung der Verarbeitung
Recht auf Datenübertragbarkeit
Transparenz
Zweckbindung
Daten-sparsamkeit
Datensicherheit
Pseudonymisierung
Verschlüsselung
Vertraulichkeit
Integrität
Verfügbarkeit
Belastbarkeit
Wiederherstellbarkeit
Notfallmanagement
Überprüfbarkeit
Bewertung
Evaluierung

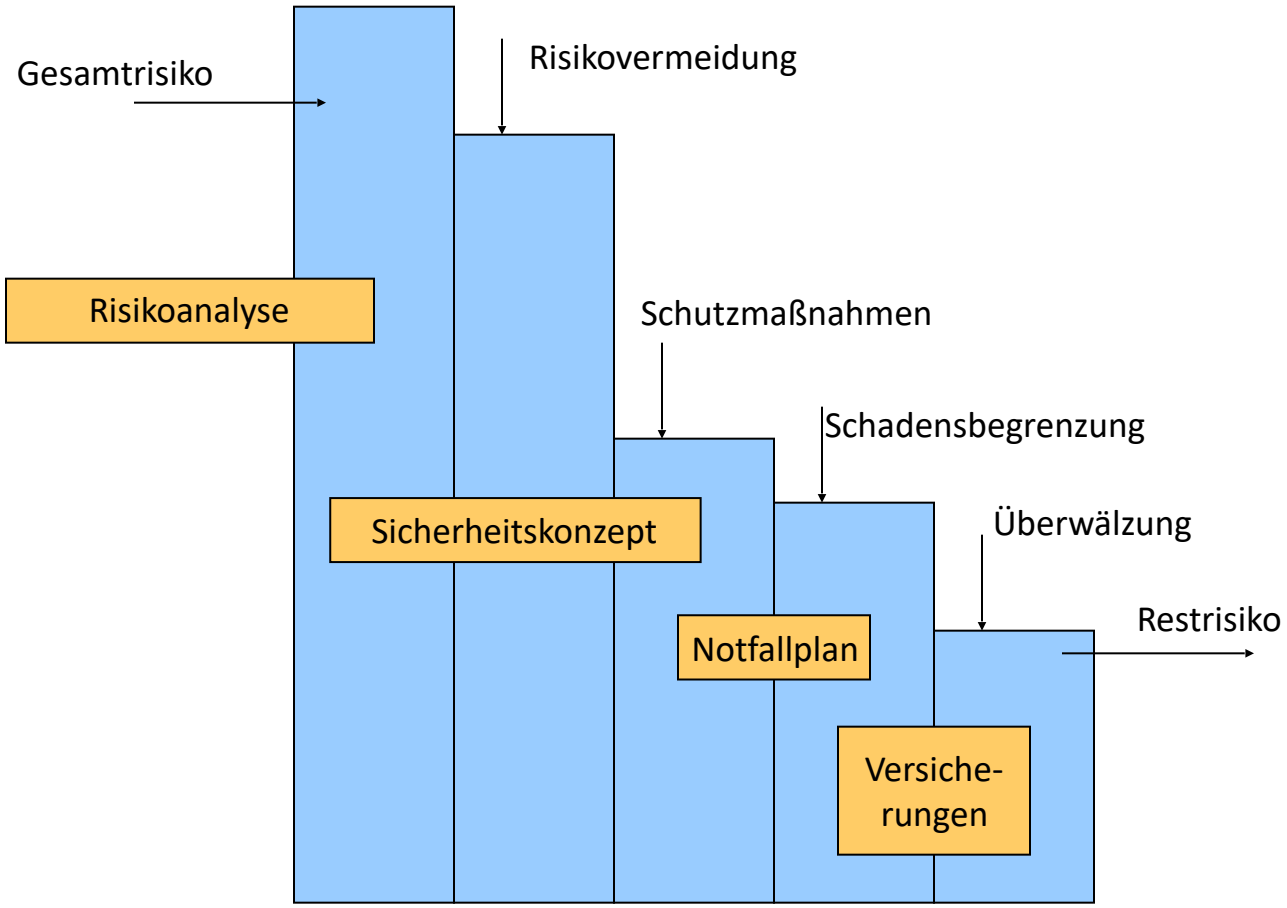

Privacy by Design
Stand der Technik
Kosten
Art, Umfang, Umstände, Zwecke
Privacy by Default
Risiko-management
Technisch-organisatorische Maßnahmen
Verbot mit Erlaubnisvorbehalt
Erforderlichkeit
Direkterhebung
Beschränkung auf Verarbeitungszweck
Beschränkung des Umfangs
Beschränkung auf Speicherfristen
Beschränkung der Zugänglichkeit
Datenschutz-grundsätze
Betroffenen-rechte
Transparenz
Zweckbindung
Daten-sparsamkeit
Datensicherheit
Transparenz
Benachrichtigung
Auskunft
Berichtigung
Löschung
Widerspruchsrecht
Recht auf Vergessenwerden
Recht auf Einschränkung der Verarbeitung
Recht auf Datenübertragbarkeit
Pseudonymisierung
Verschlüsselung
Vertraulichkeit
Integrität
Verfügbarkeit
Belastbarkeit
Wiederherstellbarkeit
Notfallmanagement
Überprüfbarkeit
Bewertung
Evaluierung


Privacy by Design
Stand der Technik
Kosten
Art, Umfang, Umstände, Zwecke
Privacy by Default
Risiko-management
Technisch-organisatorische Maßnahmen
• Verbot mit Erlaubnisvorbehalt
• Erforderlichkeit
• Direkterhebung
• Beschränkung auf Verarbeitungszweck
• Beschränkung des Umfangs
• Beschränkung auf Speicherfristen
• Beschränkung der Zugänglichkeit
Datenschutz-grundsätze
Betroffenen-rechte
Transparenz
Zweckbindung
Daten-sparsamkeit
Datensicherheit
• Transparenz
• Benachrichtigung
• Auskunft
• Berichtigung
• Löschung
• Widerspruchsrecht
• Recht auf Vergessenwerden
• Recht auf Einschränkung der Verarbeitung
• Recht auf Datenübertragbarkeit
• Pseudonymisierung
• Verschlüsselung
• Vertraulichkeit
• Integrität
• Verfügbarkeit
• Belastbarkeit
• Wiederherstellbarkeit
• Notfallmanagement
• Überprüfbarkeit
• Bewertung
• Evaluierung

# Risiko-Management für IT-Systeme



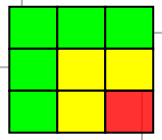
# Risiko-Management für IT-Systeme



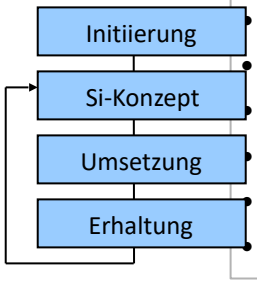

nach: Schaumüller-Bichl 1992

# Privacy by Design

- Stand der Technik
- Kosten
- Art, Umfang, Umstände, Zwecke
  - Verbot mit Erlaubnisvorbehalt
  - Erforderlichkeit
  - Direkterhebung
- Privacy by Default
  - Beschränkung auf Verarbeitungszweck
  - Beschränkung des Umfangs
  - Beschränkung auf Speicherfristen
  - Beschränkung der Zugänglichkeit
- Risiko-management



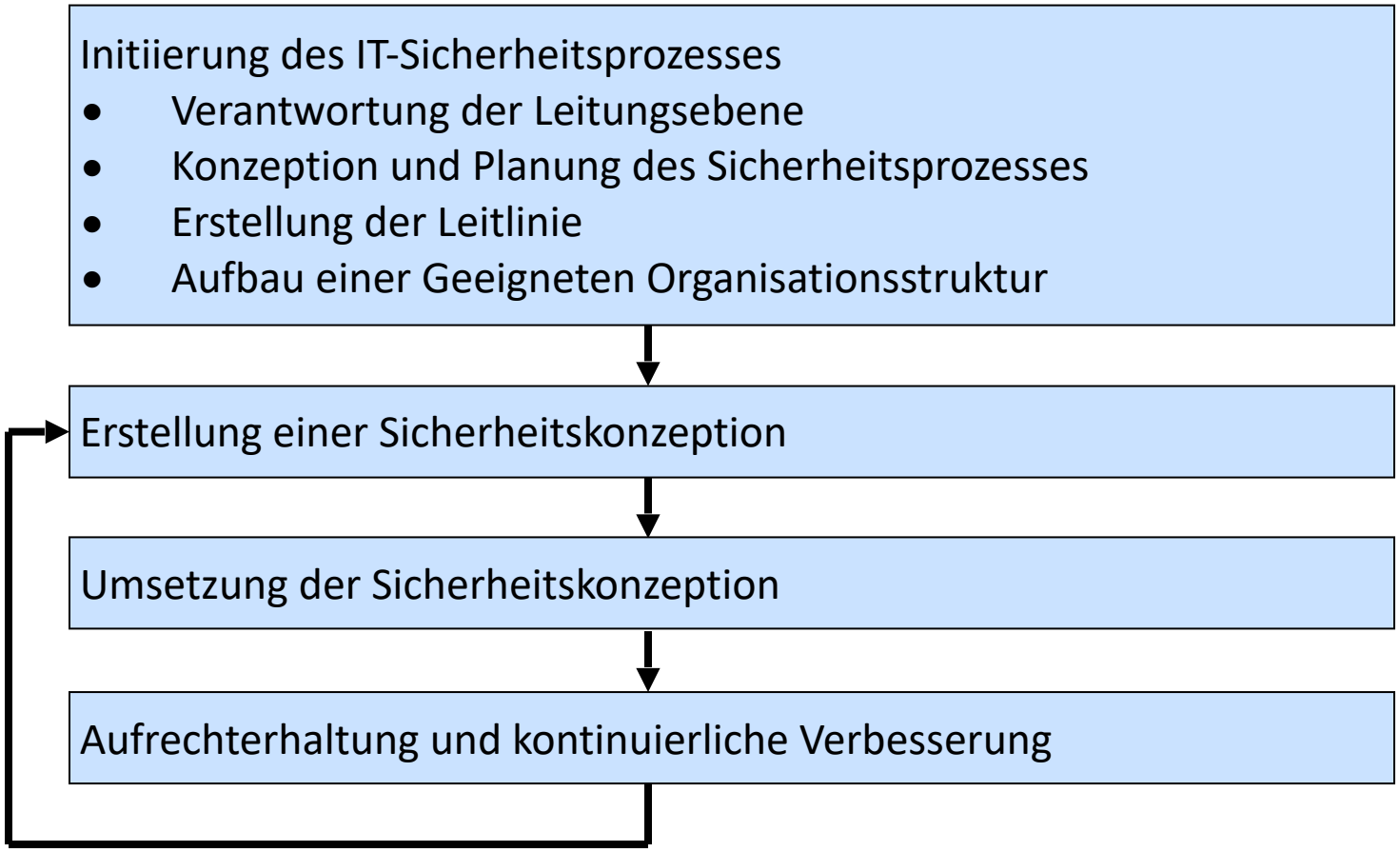
- Technisch-organisatorische Maßnahmen
  - Datenschutz-grundsätze
    - Transparenz
    - Zweckbindung
    - Daten-sparsamkeit
    - Datensicherheit
      - Pseudonymisierung
      - Verschlüsselung
      - Vertraulichkeit
      - Integrität
      - Verfügbarkeit
      - Belastbarkeit
      - Wiederherstellbarkeit
      - Notfallmanagement
      - Überprüfbarkeit
      - Bewertung
      - Evaluierung




  - Betroffenen-rechte
    - Transparenz
    - Benachrichtigung
    - Auskunft
    - Berichtigung
    - Löschung
    - Widerspruchsrecht
    - Recht auf Vergessenwerden
    - Recht auf Einschränkung der Verarbeitung
    - Recht auf Datenübertragbarkeit

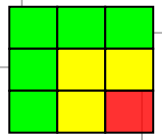
# IT-Sicherheitsprozess in der Standard-Absicherung

nach BSI 200-2, S. 26

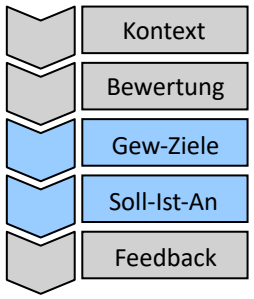


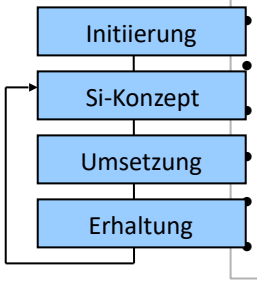
# Privacy by Design

- Stand der Technik
- Kosten
  - ROSI
- Art, Umfang, Umstände, Zwecke
- Privacy by Default
  - Beschränkung auf Verarbeitungszweck
  - Beschränkung des Umfangs
  - Beschränkung auf Speicherfristen
  - Beschränkung der Zugänglichkeit
- Risiko-management

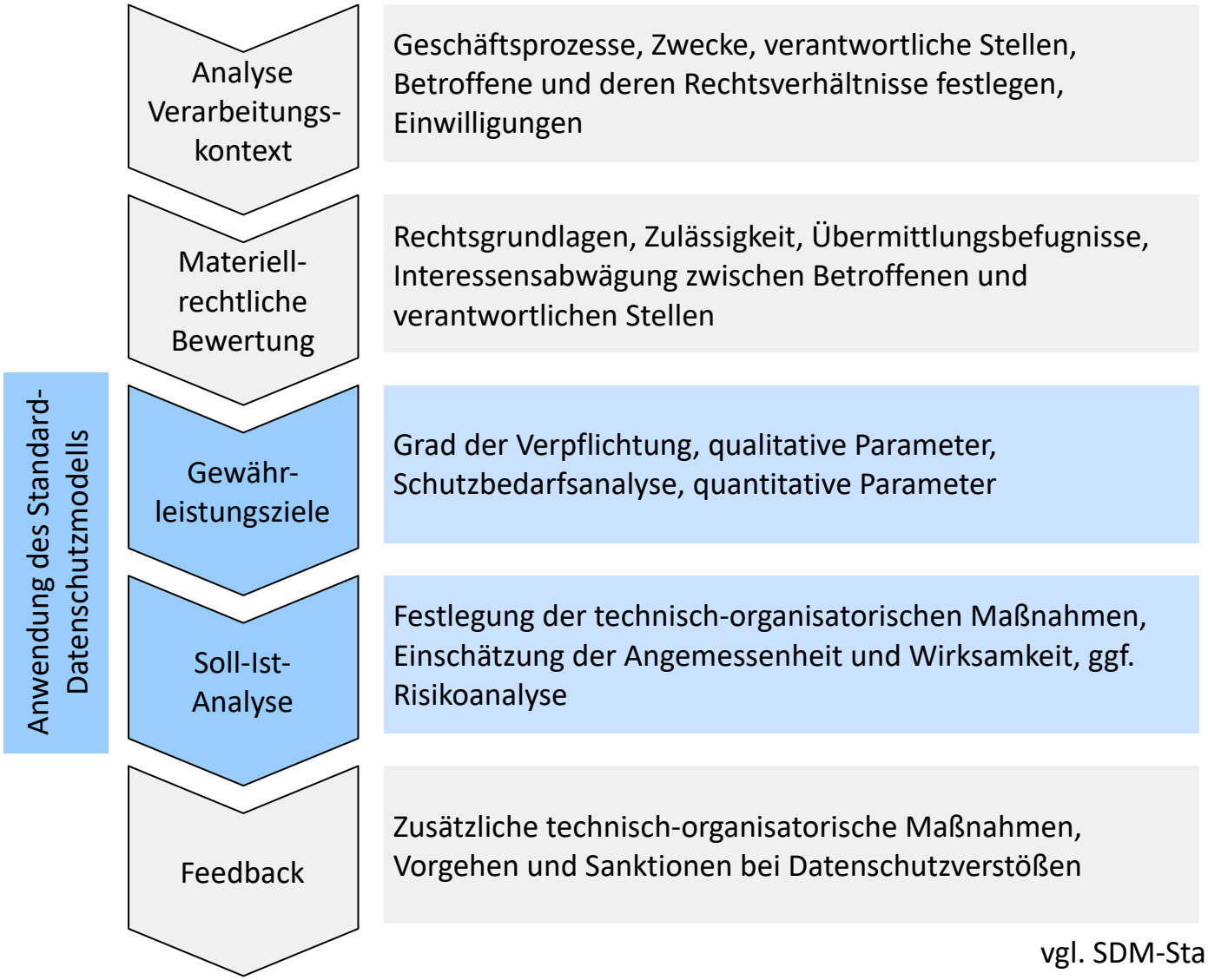


- Technisch-organisatorische Maßnahmen
  - Datenschutz-grundsätze
    - Transparenz
    - Zweckbindung
    - Daten-sparsamkeit
    - Datensicherheit
      - Pseudonymisierung
      - Verschlüsselung
      - Vertraulichkeit
      - Integrität
      - Verfügbarkeit
      - Belastbarkeit
      - Wiederherstellbarkeit
      - Notfallmanagement
      - Überprüfbarkeit
      - Bewertung
      - Evaluierung
  - Betroffenen-rechte
    - Transparenz
    - Benachrichtigung
    - Auskunft
    - Berichtigung
    - Löschung
    - Widerspruchsrecht
    - Recht auf Vergessenwerden
    - Recht auf Einschränkung der Verarbeitung
    - Recht auf Datenübertragbarkeit



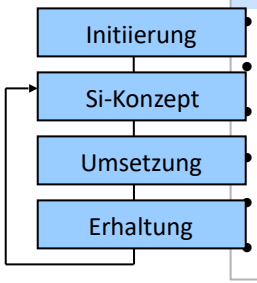
# Standard-Datenschutzmodell




vgl. SDM-Standard 1.0, 2016

# Privacy by Design

- Stand der Technik
- Kosten
- Art, Umfang, Umstände, Zwecke
  - Verbot mit Erlaubnisvorbehalt
  - Erforderlichkeit
  - Direkterhebung
- Privacy by Default
  - Beschränkung auf Verarbeitungszweck
  - Beschränkung des Umfangs
  - Beschränkung auf Speicherfristen
  - Beschränkung der Zugänglichkeit
- Risiko-management
- Technisch-organisatorische Maßnahmen
  - Datenschutz-grundsätze
    - Transparenz
    - Zweckbindung
    - Daten-sparsamkeit
    - Datensicherheit
      - Pseudonymisierung
      - Verschlüsselung
      - Vertraulichkeit
      - Integrität
      - Verfügbarkeit
      - Belastbarkeit
      - Wiederherstellbarkeit
      - Notfallmanagement
      - Überprüfbarkeit
      - Bewertung
      - Evaluierung


  - Betroffenen-rechte
    - Transparenz
    - Benachrichtigung
    - Auskunft
    - Berichtigung
    - Löschung
    - Widerspruchsrecht
    - Recht auf Vergessenwerden
    - Recht auf Einschränkung der Verarbeitung
    - Recht auf Datenübertragbarkeit

# Schutzziele

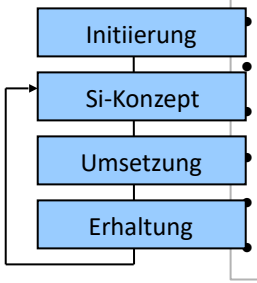
Voydock, Kent, 1983

- Klassische IT-Sicherheit berücksichtigt im Wesentlichen Risiken, die durch *regelwidriges Verhalten* in IT-Systemen entstehen.

| | |
|---|---|
| Vertraulichkeit | unbefugter Informationsgewinn |
| Integrität | unbefugte Modifikation |
| Verfügbarkeit | unbefugte Beeinträchtigung der Funktionalität |

# Privacy by Design

- Stand der Technik
- Kosten
- Art, Umfang, Umstände, Zwecke
  - Verbot mit Erlaubnisvorbehalt
  - Erforderlichkeit
  - Direkterhebung
- Privacy by Default
  - Beschränkung auf Verarbeitungszweck
  - Beschränkung des Umfangs
  - Beschränkung auf Speicherfristen
  - Beschränkung der Zugänglichkeit
- Risiko-management
- Technisch-organisatorische Maßnahmen
  - Datenschutz-grundsätze
    - Transparenz
    - Zweckbindung
    - Daten-sparsamkeit
    - Datensicherheit
      - Pseudonymisierung
      - Verschlüsselung
      - Vertraulichkeit
      - Integrität
      - Verfügbarkeit
      - Belastbarkeit
      - Wiederherstellbarkeit
      - Notfallmanagement
      - Überprüfbarkeit
      - Bewertung
      - Evaluierung
  - Betroffenen-rechte
    - Transparenz
    - Benachrichtigung
    - Auskunft
    - Berichtigung
    - Löschung
    - Widerspruchsrecht
    - Recht auf Vergessenwerden
    - Recht auf Einschränkung der Verarbeitung
    - Recht auf Datenübertragbarkeit

# Anwendungsfall x Schlüsselbeziehung

| | Konzelation (Verschlüsselung) | Authentikation |
|---|---|---|
| symmetrische | *One-time-pad, DES, Triple-DES, AES, IDEA, A5/1 (GSM), A5/2 (GSM) …*<br>GnuPG/PGP, WPA2, IPSec, SSL/TLS | *Symmetrische Authentikationscodes, CCM, A3 (GSM), …*<br>SecurID, WPA2, IPSec, SSL/TLS |
| asymmetrische | *RSA, ElGamal, McEliece, …*<br>GnuPG/PGP, HBCI, SSL/TLS | *RSA, ElGamal, DSA, GMR, …*<br>GnuPG/PGP, HBCI, SSL/TLS |

*Algorithmus*

Anwendung

# Welche Schlüssellängen und Kryptoalgorithmen sind sicher?

## Jährlicher Algorithmenkatalog nach § 17 (1) SigG des Bundesamts für die Sicherheit in der Informationstechnik (BSI)

**Tabelle 3: Geeignete Schlüssellängen für DSA**

| Parameter \ Zeitraum | bis Ende **2015** | bis Ende **2021** |
|---|---|---|
| $p$ | 2048 | 2048 |
| $q$ | 224 | 256 |

**Tabelle 8: Nicht mehr geeignete RSA-Schlüssellängen**

| Modullänge $n$ | geeignet bis |
|---|---|
| 768 | Ende 2000 |
| 1024 | Ende März 2008* |
| 1280 | Ende 2008 |
| 1536 | Ende 2009 |
| 1728 | Ende 2010 |

* Januar – März 2008: Übergangsfrist

**Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen**

**Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung**

**(Übersicht über geeignete Algorithmen)**

**Vom 15. 12. 2014**

Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen als zuständige Behörde gemäß § 3 Signaturgesetz (SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091), veröffentlicht gemäß Anlage 1 Abschnitt 1 Nr. 2 Signaturverordnung (SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 15. November 2010 (BGBl. I S. 1542), im Bundesanzeiger eine Übersicht über die Algorithmen und zugehörigen Parameter, die zur Erzeugung von Signaturschlüsseln, zum Hashen zu signierender Daten oder zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen als geeignet anzusehen sind, sowie den Zeitpunkt, bis zu dem die Eignung jeweils gilt.

**Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG vom 16. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 16. November 2001**

**Vorbemerkung:** Wie in den Vorjahren werden im Folgenden geeignete Algorithmen und Schlüssellängen für den Zeitraum der kommenden sieben Jahre anstatt des in der SigV vorgesehenen Mindestzeitraums von sechs Jahren aufgeführt. Das heißt konkret, dass geeignete Algorithmen und Schlüssellängen bis Ende 2021 statt bis Ende 2020 aufgeführt sind. Im Allgemeinen sind solche längerfristigen Prognosen schwer möglich. Die vorliegende Übersicht über geeignete Algorithmen unterscheidet sich von der zuletzt veröffentlichten Übersicht vom 20. Februar 2014 (BAnz AT 20.02.2013 B4) im Wesentlichen in folgenden Punkten:

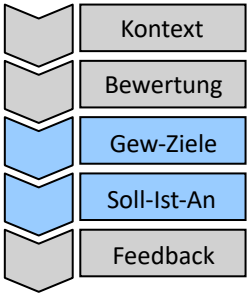
1. Die Eignung von Nyberg-Rueppel-Signaturen wird nicht über das Jahr 2020 hinaus verlängert. Dies hat keine Sicherheitsgründe, sondern dient der Vereinfachung der Pflege des Algorithmenkatalogs. Nachdem die Streichung von Nyberg-Rueppel-Signaturen in den letzten beiden Versionen der vorliegenden Bekanntmachung angekündigt und in den entsprechenden Expertenanhörungen diskutiert wurde, sind bei den zuständigen Stellen im Bundesamt für Sicherheit in der Informationstechnik und in der Bundesnetzagentur keine Einsprüche gegen die Streichung dieses Verfahrens eingegangen. Es wird daher davon ausgegangen, dass es keine praktische Verwendung findet im Bereich der qualifizierten elektronischen Signatur.

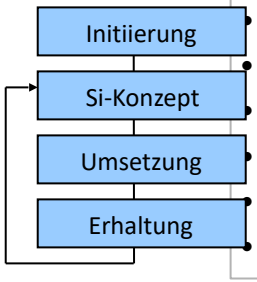
2. Wie bereits im vorigen Algorithmenkatalog angekündigt wurde, wird die Eignung von Zufallsgeneratoren, die entsprechend der Funktionalitätsklassen nach [31] zertifiziert wurden, von wenigen Ausnahmefällen abgesehen nicht über das Jahr 2020 hinaus verlängert.

https://www.bsi.bund.de/Algorithmenkatalog

# Privacy by Design

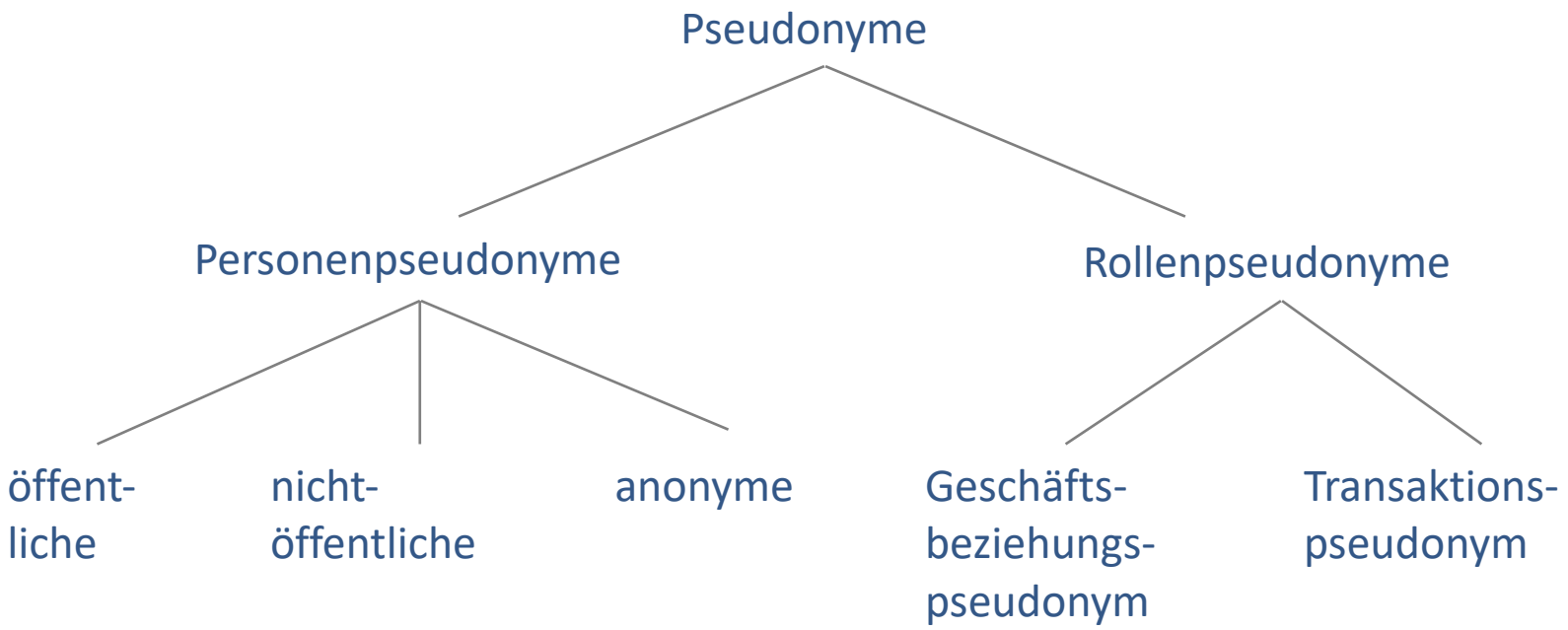
- Stand der Technik
- Kosten
- Art, Umfang, Umstände, Zwecke
  - Verbot mit Erlaubnisvorbehalt
  - Erforderlichkeit
  - Direkterhebung
- Privacy by Default
  - Beschränkung auf Verarbeitungszweck
  - Beschränkung des Umfangs
  - Beschränkung auf Speicherfristen
  - Beschränkung der Zugänglichkeit
- Risiko-management
- Technisch-organisatorische Maßnahmen
  - Datenschutz-grundsätze
    - Transparenz
    - Zweckbindung
    - Daten-sparsamkeit
      - Anonymität
      - Unbeobachtbarkeit
    - Datensicherheit
      - Pseudonymisierung
      - Verschlüsselung
      - Vertraulichkeit
      - Integrität
      - Verfügbarkeit
      - Belastbarkeit
      - Wiederherstellbarkeit
      - Notfallmanagement
      - Überprüfbarkeit
      - Bewertung
      - Evaluierung
  - Betroffenen-rechte
    - Transparenz
    - Benachrichtigung
    - Auskunft
    - Berichtigung
    - Löschung
    - Widerspruchsrecht
    - Recht auf Vergessenwerden
    - Recht auf Einschränkung der Verarbeitung
    - Recht auf Datenübertragbarkeit



# Arten von Pseudonymen

Pfitzmann, Waidner, Pfitzmann, 1990



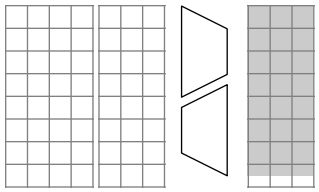

Beispiele für Pseudonyme:

**Telefon-nummer** | **Konto-nummer** | **Biometrische Merkmale (solange kein Register)** | **Künstlername** | **Kennwort**

Gute Skalierbarkeit bezüglich der Anonymität

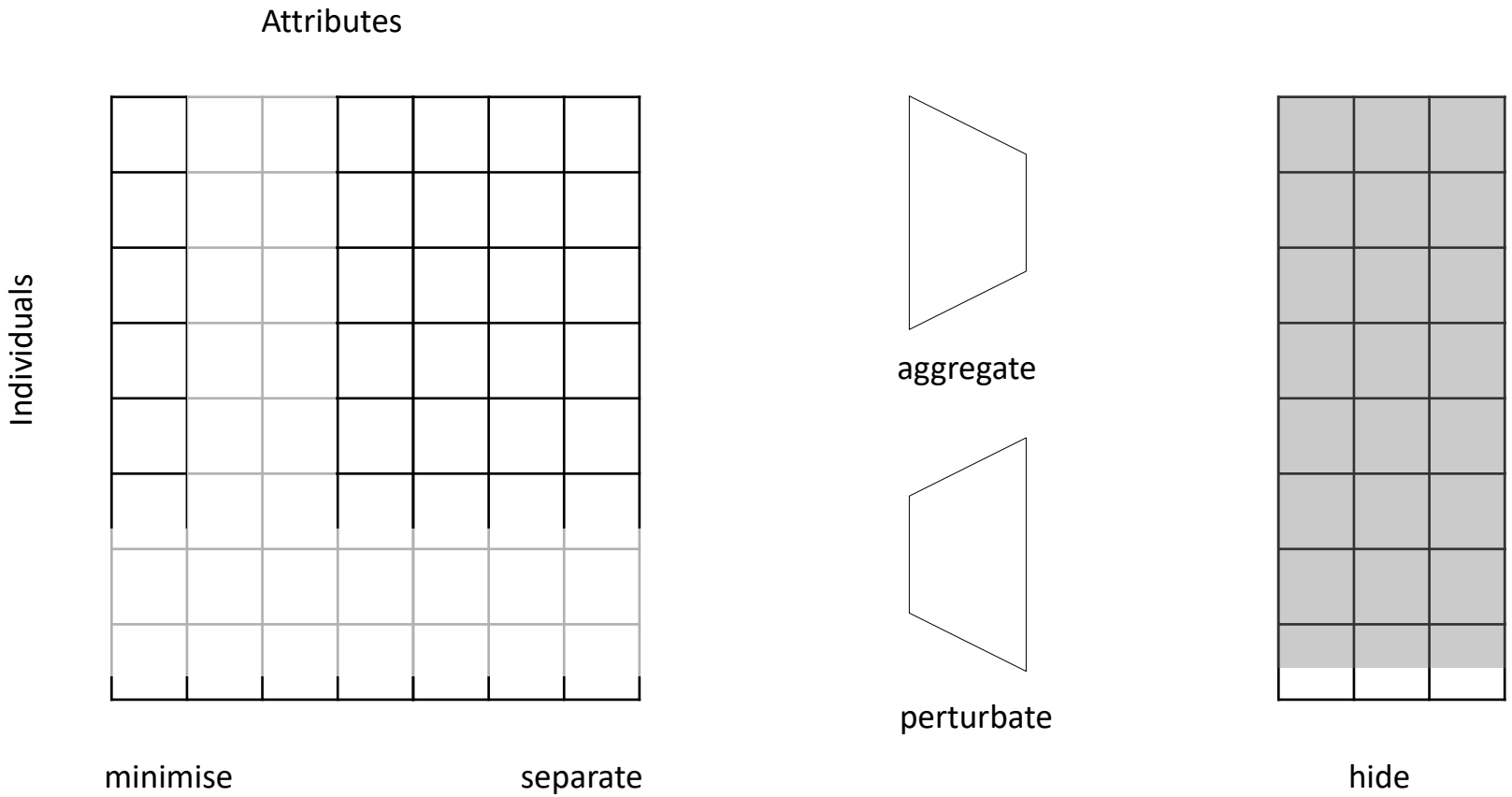
# Privacy by Design

- Stand der Technik
- Kosten
- Art, Umfang, Umstände, Zwecke
  - Verbot mit Erlaubnisvorbehalt
  - Erforderlichkeit
  - Direkterhebung
- Privacy by Default
  - Beschränkung auf Verarbeitungszweck
  - Beschränkung des Umfangs
  - Beschränkung auf Speicherfristen
  - Beschränkung der Zugänglichkeit
- Risiko-management
- Technisch-organisatorische Maßnahmen
  - Datenschutz-grundsätze
    - Transparenz
      - Enforce
      - Inform
      - Control
      - Demonstrate
    - Zweckbindung
    - Daten-sparsamkeit
      - Anonymität
      - Unbeobachtbarkeit
      - Minimise
      - Separate
      - Aggregate
      - Perturbate
      - Hide
    - Datensicherheit
      - Pseudonymisierung
      - Verschlüsselung
      - Vertraulichkeit
      - Integrität
      - Verfügbarkeit
      - Belastbarkeit
      - Wiederherstellbarkeit
      - Notfallmanagement
      - Überprüfbarkeit
      - Bewertung
      - Evaluierung
  - Betroffenen-rechte
    - Transparenz
    - Benachrichtigung
    - Auskunft
    - Berichtigung
    - Löschung
    - Widerspruchsrecht
    - Recht auf Vergessenwerden
    - Recht auf Einschränkung der Verarbeitung
    - Recht auf Datenübertragbarkeit



# Privacy design strategies

in Anlehnung an Hoepmann, 2013



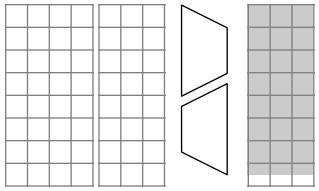
# Privacy design strategies

in Anlehnung an Hoepmann, 2013

- Technisch
  - Minimise: Nur notwendige Daten speichern und verarbeiten
  - Separate: Daten verteilt verarbeiten und speichern
  - Aggregate: Daten auf das notwendige Maß zusammenfassen
  - Perturbate: Daten durch zufällige Störungen ungenau machen
  - Hide: Daten nicht in offener Form speichern

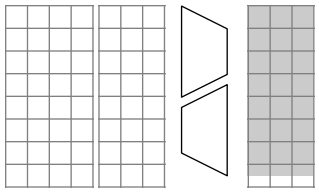
- Organisatorisch
  - Enforce: Durchsetzung einer Datenschutz-Policy (access control)
  - Inform: Betroffene über Datenverwendung informieren (P3P)
  - Control: Eingriffsmöglichkeit der Betroffenen (informed consent)
  - Demonstrate: Überprüfbarkeit (privacy management, logging)

# Privacy by Design

- Stand der Technik
- Kosten
- Art, Umfang, Umstände, Zwecke
  - Verbot mit Erlaubnisvorbehalt
  - Erforderlichkeit
  - Direkterhebung
- Privacy by Default
  - Beschränkung auf Verarbeitungszweck
  - Beschränkung des Umfangs
  - Beschränkung auf Speicherfristen
  - Beschränkung der Zugänglichkeit
- Risiko-management
- Technisch-organisatorische Maßnahmen
  - Datenschutz-grundsätze
    - Transparenz
      - 
      - Bereitschaft und gute Dokumentation
        - Enforce
        - Inform
        - Control
        - Demonstrate
    - Zweckbindung
    - Daten-sparsamkeit
      - Anonymität
      - Unbeobachtbarkeit
      - 
        - Minimise
        - Separate
        - Aggregate
        - Perturbate
        - Hide
    - Datensicherheit
      - Pseudonymisierung
      - Verschlüsselung
      - Vertraulichkeit
      - Integrität
      - Verfügbarkeit
      - Belastbarkeit
      - Wiederherstellbarkeit
      - Notfallmanagement
      - Überprüfbarkeit
      - Bewertung
      - Evaluierung
      - 
      - 
  - Betroffenen-rechte
    - Transparenz
    - Benachrichtigung
    - Auskunft
    - Berichtigung
    - Löschung
    - Widerspruchsrecht
    - Recht auf Vergessenwerden
    - Recht auf Einschränkung der Verarbeitung
    - Recht auf Datenübertragbarkeit
    - 
    - Bereitschaft

# Privacy by Design

- Stand der Technik
- Kosten
- Art, Umfang, Umstände, Zwecke
  - Verbot mit Erlaubnisvorbehalt
  - Erforderlichkeit
  - Direkterhebung
- Privacy by Default
  - Beschränkung auf Verarbeitungszweck
  - Beschränkung des Umfangs
  - Beschränkung auf Speicherfristen
  - Beschränkung der Zugänglichkeit
- Risiko-management
- Technisch-organisatorische Maßnahmen
  - Datenschutz-grundsätze
    - Transparenz
      - Big Data
      - Bereitschaft und gute Dokumentation
      - Algorithmen
        - Enforce
        - Inform
        - Control
        - Demonstrate
    - Zweckbindung
    - Daten-sparsamkeit
      - Anonymität
      - Unbeobachtbarkeit
      - Minimise
      - Separate
      - Aggregate
      - Perturbate
      - Hide
    - Datensicherheit
      - Pseudonymisierung
      - Verschlüsselung
      - Vertraulichkeit
      - Integrität
      - Verfügbarkeit
      - Belastbarkeit
      - Wiederherstellbarkeit
      - Notfallmanagement
      - Überprüfbarkeit
      - Bewertung
      - Evaluierung
  - Betroffenen-rechte
    - Transparenz
    - Benachrichtigung
    - Auskunft
    - Berichtigung
    - Löschung
    - Widerspruchsrecht
    - Recht auf Vergessenwerden
    - Recht auf Einschränkung der Verarbeitung
    - Recht auf Datenübertragbarkeit



Bereitschaft

# Prädiktive Big-Data-Analytik: Stecknadeln im Heuhaufen

# Der Fall Cambridge Analytica

heise.de

## Facebook-Datenskandal

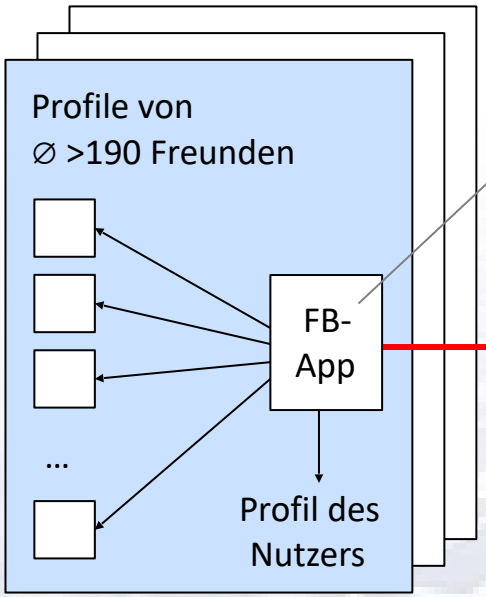
Die englische Datenanalyse-Firma Cambridge Analytica hat sich während des US-Wahlkampfes unerlaubt Zugang zu Daten von mehr als 50 Millionen Facebook-Nutzern verschafft. Mit den Informationen soll die Firma geholfen haben, Anhänger des heutigen US-Präsidenten Donald Trump zu mobilisieren und zugleich potenzielle Wähler der Gegenkandidaten Hillary Clinton vom Urnengang abzuhalten. Mithilfe der Nutzerprofile wurden im sozialen Netzwerk gezielt Botschaften als Werbung ausgespielt.

Der im März 2018 bekannt gewordene Datenskandal ist aber offfenbar nur die Spitze eines Eisbergs. Laut einem ehemaligen Facebook-Manager habe das Social Network keinerlei Kontrolle über abgeflossene Nutzerdaten.

# Der Fall Cambridge Analytica

nach: ct 2018, Heft 8, S. 20

>270.000 Facebook-Nutzer



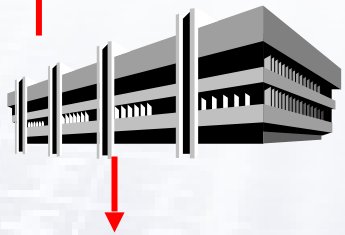

Facebook-App »thisisyourdigitallife« des Psychologen Alexander Kogan greift (mit Einwilligung der Facebook-Nutzer auf Basis der damaligen Privacy-Einstellungen) »zu wiss. Zwecken« auf Profile und Daten von Freunden zu

>50 Mio. Facebook-Profile

Unerlaubte Datenweitergabe

Auswertung nach Persönlichkeitsprofilen gem. OCEAN-Modell:

- Openness
- Conscientiousness
- Extraversion
- Agreeableness
- Neuroticism



Cambridge Analytica: Weiterverwendung zur gezielten Anzeige von (Wahl)-Werbung: Brexit, Trump, …

# Auszug aus Artikel 22 DSGVO

## Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

…

## Auszug aus Erwägungsgrund 71:

Die betroffene Person sollte das Recht haben, keiner Entscheidung […] unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wie die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen. Zu einer derartigen Verarbeitung zählt auch das „Profiling“, das in jeglicher Form automatisierter Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte in Bezug auf eine natürliche Person besteht, insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person, soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

# Automatisierte Entscheidungen im Einzelfall einschl. Profiling

- DSGVO Art. 22 (1) Automatisierte Entscheidungen
  - automatisierte Entscheidungen verletzen das Persönlichkeitsrecht
  - Profiling verletzt das Persönlichkeitsrecht
  - Erwägungsgrund 71 nennt Beispiele:
    - Online-Kreditantrag
    - Online-Einstellungsverfahren
    - Analyse oder Prognose von
      - Arbeitsleistung
      - wirtschaftlicher Lage
      - Gesundheit
      - persönlichen Vorlieben oder Interessen
      - Zuverlässigkeit oder Verhalten
      - Aufenthaltsort oder Ortswechsel

# Privacy by Design

Stand der Technik

Kosten

ROSI

Art, Umfang, Umstände, Zwecke

- Verbot mit Erlaubnisvorbehalt
- Erforderlichkeit
- Direkterhebung

Privacy by Default

- Beschränkung auf Verarbeitungszweck
- Beschränkung des Umfangs
- Beschränkung auf Speicherfristen
- Beschränkung der Zugänglichkeit

Risiko-management

Technisch-organisatorische Maßnahmen

Datenschutz-grundsätze

Betroffenen-rechte

- Transparenz
- Benachrichtigung
- Auskunft
- Berichtigung
- Löschung
- Widerspruchsrecht
- Recht auf Vergessenwerden
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit

Transparenz

Policy

Big Data

Bereitschaft und gute Dokumentation

Algorithmen

- Enforce
- Inform
- Control
- Demonstrate

Zweckbindung

Daten-sparsamkeit

- Anonymität
- Unbeobachtbarkeit

- Minimise
- Separate
- Aggregate
- Perturbate
- Hide

Datensicherheit

- Pseudonymisierung
- Verschlüsselung
- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit
- Wiederherstellbarkeit
- Notfallmanagement
- Überprüfbarkeit
- Bewertung
- Evaluierung

Bereitschaft

inf.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

DEPARTMENT OF INFORMATICS
SECURITY AND PRIVACY

HOME COURSES THESES RESEARCH PEOPLE SERVICE


UHH → MIN-Fakultät → Fachbereich Informatik → Einrichtungen → Arbeitsbereiche → Security and Privacy → **Home**

# WORKING GROUP ON «SECURITY AND PRIVACY»

## Security and Privacy

Information systems become more and more important in critical infrastructures, while the Internet has evolved to a critical infrastructure itself. The secure operation of these infrastructures is vital and their failure can have severe impacts up to the loss of human lives.
Security refers to the fact that protection goals are achieved in the presence of malicious attacks and system failures. Typical security goals can be confidentiality, integrity, accountability, and availability. Security and privacy in information systems addresses both technical and organizational aspects, such as building and establishing security concepts and security infrastructures as well as risk analysis and risk management.
Privacy can be a conflicting goal to security, but they can also benefit from each other. Hence, it is necessary to balance both when developing secure information systems.

Prof. Dr. Hannes Federrath
Fachbereich Informatik
Universität Hamburg
Vogt-Kölln-Straße 30
D-22527 Hamburg

Telefon +49 40 42883 2358

federrath@informatik.uni-hamburg.de

https://svs.informatik.uni-hamburg.de