Grundlagen des Datenschutzes und der IT-Sicherheit (Teil 1c)

Vorlesung im Sommersemester 2013

an der Universität Ulm

von Bernhard C. Witt

1. Grundlagen des Datenschutzes

Grundlagen des Datenschutzes		Grundlagen der IT-Sicherheit	
✓	Geschichte des Datenschutzes		Anforderungen zur IT-Sicherheit
✓	Datenschutzrechtliche Prinzipien		Mehrseitige IT-Sicherheit
➔	Technischer Datenschutz		Risiko-Management
	Kundendatenschutz		Konzeption von IT-Sicherheit

- Begriffsklärung: Daten, personenbezogene Daten & Informationen
- Risikobasierter Ansatz im Datenschutzrecht
- technische & organisatorische Maßnahmen
- Vorabkontrolle zu Datenschutzrisiken
- Datenschutzrisiken bei der Auftragsdatenverarbeitung
- Abgrenzungen zur Datensicherheit
- DSB vs. IT-Sicherheitsbeauftragter
- Datenschutz-Folgenabschätzung nach EU-DSGVO-Entwurf (*)
- Datenschutzfördernde Techniken (*)

(*) = entfällt ggf. aus Zeitmangel

Daten vs. Informationen

Grunddilemma: Uneinheitliche Begriffswelt (vor allem zwischen Informatik & Jura)

→**Lösung**: Festlegung von Definitionen!

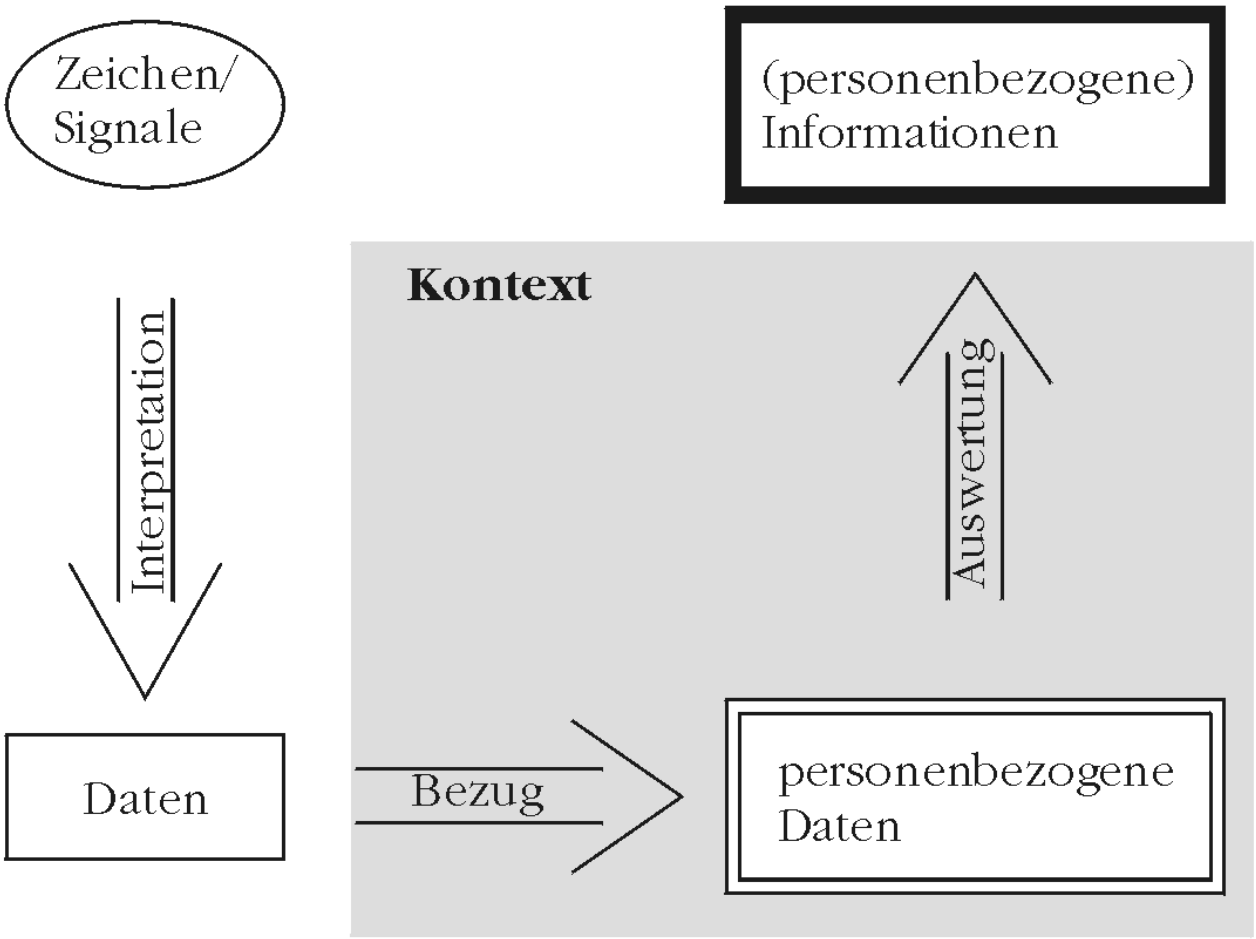
Definition 2: Daten

kontextfreie Angaben, die aus interpretierten Zeichen bzw. Signalen bestehen

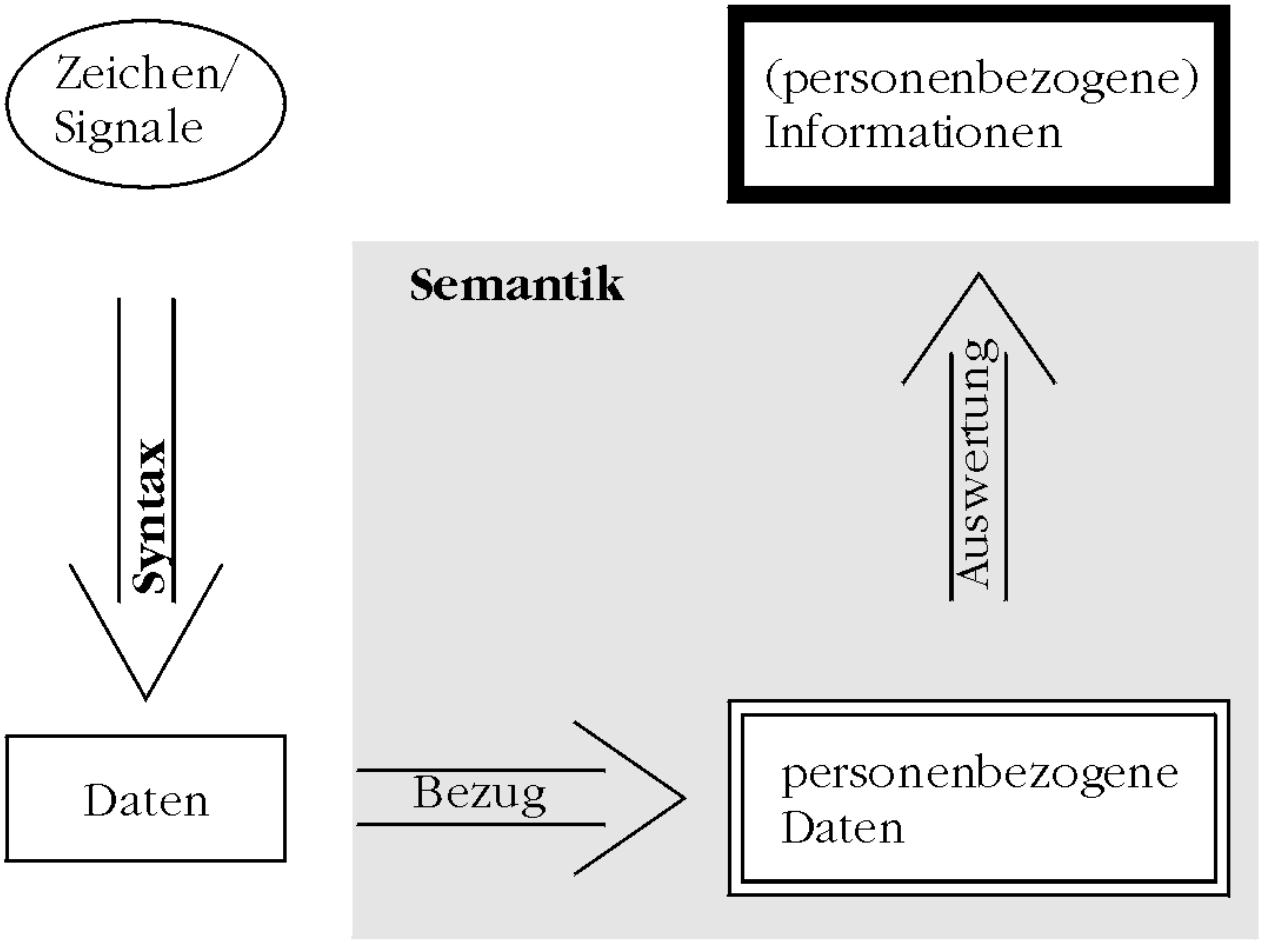
Definition 3: Informationen

Daten, die (durch den Menschen) kontextbezogen interpretiert werden und (prozesshaft) zu Erkenntnisgewinn führen

Vom Datum zur Information (1)



Vom Datum zur Information (2)



Risikobasierter Ansatz im Datenschutzrecht (1)

- Datenschutz betrifft nur Umgang mit **personenbezogenen Daten**
- Unzulässiger Umgang mit eigenem Bußgeldkatalog bestraft bzw. bei Vorsatz strafbar
- **Bußgeldkatalog** in zwei Kategorien unterteilt (vgl. § 43 BDSG):
  ° Verstoß gegen Formvorschriften (§ 43 Abs. 1 BDSG) → max. 50.000 € Strafe
  ° Gravierender Verstoß (§ 43 Abs. 2 BDSG) → max. 300.000 € Strafe + ggf. Gewinnabschöpfung
- Bußgeld wird nur dann fällig, wenn Aufsichtsbehörde dieses verhängt (geschieht selten und i.d.R. nicht unter Ausschöpfung des Maximalbetrags)
  → direkter finanzieller Schaden
- Zudem besteht **Meldepflicht bei Datenpannen**, sofern
  ° Unbefugter Kenntnis über sensible Daten erhalten hat
  ° Schwerwiegende Beeinträchtigungen für die Betroffenen drohen
  → Reputationsverlust! (+ indirekter finanzieller Schaden)
- Meldepflicht gegenüber Aufsichtsbehörde und den Betroffenen

→ **Datenschutzrisiken = Risiken des Datenschutzrechtsverstoßes**

Risikobasierter Ansatz im Datenschutzrecht (2)

- **Risikomanagement im Datenschutz**:
  → **Ziel**: Vermeidung ungewollter (!) Datenschutzrisiken
  → **Vorgaben des Gesetzgebers**:
  1. Durchführung Zulässigkeitsprüfung wg. „Verbot mit Erlaubnisvorbehalt“ für jedes Verfahren
  2. Ergreifung erforderlicher Schutzvorkehrungen
  3. Durchführung einer Erforderlichkeitsprüfung zu Daten
  4. Durchführung der Vorabkontrolle bei riskanten Verfahren
  5. Durchführung der Auftragskontrolle bei Auftragsdatenverarbeitung
- **Verfahren** ist datenschutzrechtlich **zulässig**, wenn es hierzu eine gesetzliche Vorschrift gibt
  ° ausdrücklicher Erlaubnistatbestand (gilt für sehr viele Fälle!)
  ° Abwägung betriebliches Interesse vs. Betroffeneninteresse (für öffentlichen Bereich stark eingeschränkt!)
  ° informierte & freiwillige Einwilligung des Betroffenen
  ° Verwendung öffentlicher Daten (ohne Zugriffsschutz und zulässigerweise veröffentlicht → keine illegal veröffentlichten Daten)

Risikobasierter Ansatz im Datenschutzrecht (3)

- **Technische & organisatorische Maßnahmen** müssen Schutzgrad der Daten entsprechen und angemessen sein (→ Wirtschaftlichkeitsprüfung)
  - ° Gliederung anhand Kontrollbereiche (z.B. gem. BDSG) oder Sicherheitsziele (gem. diverser LDSG)
  - ° Zusammenfassung der Maßnahmen = Datenschutzkonzept
  - ° Stand der Technik im BDSG nur für Verschlüsselung vorgeschrieben
- Bei jeweiligem Verarbeitungsschritt dürfen **nur erforderliche Daten** erhoben, verarbeitet oder genutzt werden
  - → Begründungspflicht für jedes einzelne Datenfeld
  - → Datenfeld muss für Zweckerfüllung benötigt werden
  - → Wenn Zweck auch ohne Datenfeld erfüllbar ist, ist auf dieses Datenfeld im entsprechenden Verarbeitungsschritt zu verzichten (mildester Eingriff in das informationelle Selbstbestimmungsrecht)

Technische & organisatorische Maßnahmen zum Datenschutz

- **Zutrittskontrolle**: Einrichtung physischer Schutzzonen
- **Zugangskontrolle**: Nutzung von IT-Systemen erst nach Authentifizierung
- **Zugriffskontrolle**: Zugriff gemäß begründetem Berechtigungs-konzept
- **Weitergabekontrolle**: Einrichtung von Perimeterschutz
- **Eingabekontrolle**: Zuordnung von Verantwortung
- **Auftragskontrolle**: Aufgabenerfüllung gemäß Weisungskette
- **Verfügbarkeitskontrolle**: Schutz der Daten vor Zerstörung oder Verlust
- **Datentrennungskontrolle**: Zweckgebundene & -getrennte Da-tenverarbeitung

→ **Angemessenheit nach <u>Schutzgrad</u> & <u>Verletzlichkeit</u>**

Beispiel für technische & organisatorische Maßnahmen (1)

- **Zutrittskontrolle**:
  - Gebäude nur mittels Chipkartenfreischaltung betretbar
  - Datenserver in besonders geschütztem Server-raum gespeichert, zu dem nur EDV-Personal Zutritt hat
- **Zugangskontrolle**:
  - System nur mittels Eingabe von Benutzerkennung und (regelmäßig zu änderndem) Passwort nutzbar
  - Sicherungsbänder werden im Tresor aufbewahrt (anderer Brandabschnitt)

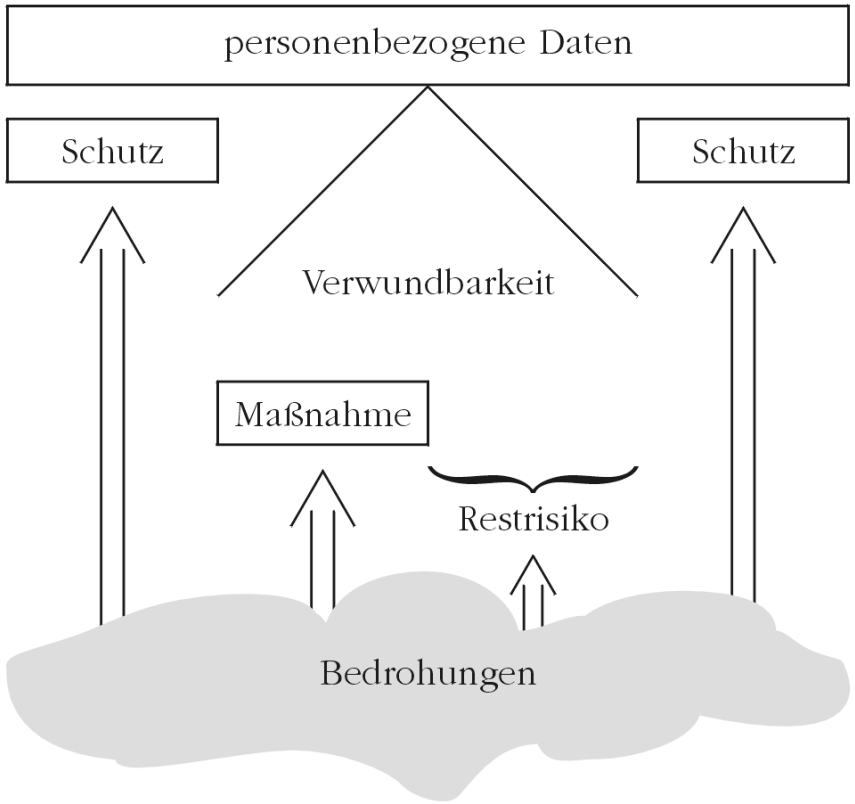
Beispiel für technische & organisatorische Maßnahmen (2)

- **Zugriffskontrolle**:
  - Zugriffsberechtigt sind nur befugte Benutzer
  - Applikationspasswort weist ausreichende Komplexität auf (8 Stellen, Angabe von Buchstaben, Zeichen und Sonderzeichen obligatorisch)
- **Weitergabekontrolle**:
  - Datentransfer via Internet erfolgt mittels SSLv3
  - LAN durch DMZ vom Internet separiert
  - USB-Port nur für Befugte freigegeben
- **Eingabekontrolle**:
  - Protokollierung von Eingaben, Änderungen und Löschungen

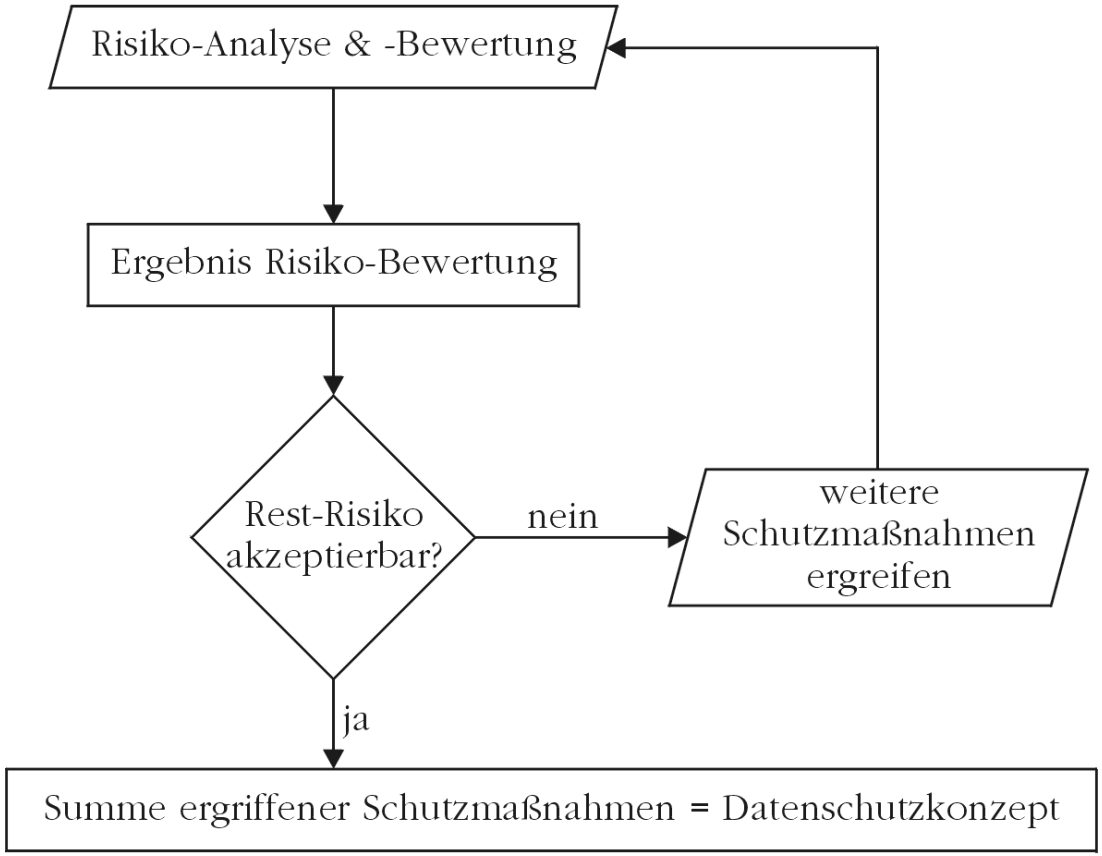
Beispiel für technische & organisatorische Maßnahmen (3)

- **Auftragskontrolle**:
  - Auftragnehmer darf keine Subunternehmer einsetzen
  - Auftraggeber darf jederzeit ergriffene Maßnahmen des Auftragnehmers kontrollieren
- **Verfügbarkeitskontrolle**:
  - Datensätze werden täglich auf Band gesichert
  - Rückeinspielung von Bandsicherungen auch im Notfall erprobt
- **Datentrennungskontrolle**:
  - Applikation mehrmandantenfähig
  - logische Trennung der Datensätze realisiert

Ziel der technischen & organisatorischen Maßnahmen (1)



Ziel der technischen & organisatorischen Maßnahmen (2)



Vorabkontrolle (1)

- Sofern automatisierte Verarbeitungen u.U. **besondere Risiken** für die Rechte und Freiheiten der Betroffenen erzeugen können, ist nach § 4d Abs. 5 BDSG eine Vorabkontrolle durchzuführen
- Vorabkontrolle ausdrücklich vorgeschrieben bei
  ° Umgang mit „**besonderen Arten personenbezogener Daten**“
  ° Zweck der **Persönlichkeitsbewertung** (zu Fähigkeiten, Leistung oder Verhalten)
  sofern nicht ausdrücklich gesetzlich vorgeschrieben, basierend auf Einwilligung des Betroffenen oder erforderlich zur Begründung bzw. Durchführung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses (= Vertrag + Vertragsanbahnung)
  → Ausnahmeregel führt in der Praxis dazu, dass Vorabkontrolle zu selten durchgeführt wird (Folge: trügerische Sicherheit)

Vorabkontrolle (2)

- In erster Linie wird bei der Vorabkontrolle die **Rechtmäßigkeit** der geplanten automatisierten Verarbeitung überprüft
- Ein besonderer Augenmerk gilt den vorgesehenen **technischen und organisatorischen Maßnahmen**, die wirksam ein besonderes Risiko vermeiden helfen

→ Vorabkontrolle = Instrument präventiver Compliance

- Vorabkontrolle ist durch den Datenschutzbeauftragten durchzuführen
- Nichtdurchführung selbst ist nicht strafbewährt, sondern nur die potenziellen Folgen (i.d.R. gravierender Verstoß im Sinne von § 43 Abs. 2 Nr. 1 oder 2 BDSG)

Anlässe für Vorabkontrolle

Checkliste für Vorabkontrolle

- ☐ besondere Arten personenbezogener Daten?
- ☐ Leistungs- / Verhaltens- / Fähigkeitsbewertung?
- ☐ Erstellung Persönlichkeitsprofil?
- ☐ neu entwickelte bzw. hochkomplexe IuK-Technik?
- ☐ Medienwechsel bei vertraulichem Verfahren?
- ☐ gravierende Wirkung auf Betroffenen?
- ☐ verschiedene Zwecke mit einem IT-System?
- ☐ Daten verschiedener Auftraggeber auf einem IT-System?
- ☐ Daten mit Amtsgeheimnis?
- ☐ Personalplanungs-/-informationssystem?
- ☐ CRM-System mit ERP-System vernetzt?

Bestimmung des Datenschutzrisikos

Schutzgrad

Schutzgrad 1 (kein Schutzbedarf):
Daten weisen keinen Personenbezug auf

Schutzgrad 2 (niedriger Schutzbedarf):
ein Personenbezug kann nur mit erheblichem Aufwand hergestellt werden

Schutzgrad 3 (mittlerer Schutzbedarf):
Daten sind mit vertretbarem Aufwand repersonalisierbar oder stammen aus allgemein zugänglichen Quellen

Schutzgrad 4 (hoher Schutzbedarf):
ein Vertraulichkeitsverlust der Daten erzeugt bereits einen Schaden für den Betroffenen, z.B. aufgrund von Zusatzwissen

Schutzgrad 5 (sehr hoher Schutzbedarf):
besonders sensible bzw. aufgrund einer besonderen Schutzverpflichtung geschützte Daten

Eintrittsstufe

Eintrittsstufe 1 (keine Kompromittierung):
mit einer an Sicherheit grenzenden Wahrscheinlichkeit erfolgt keine Kompromittierung

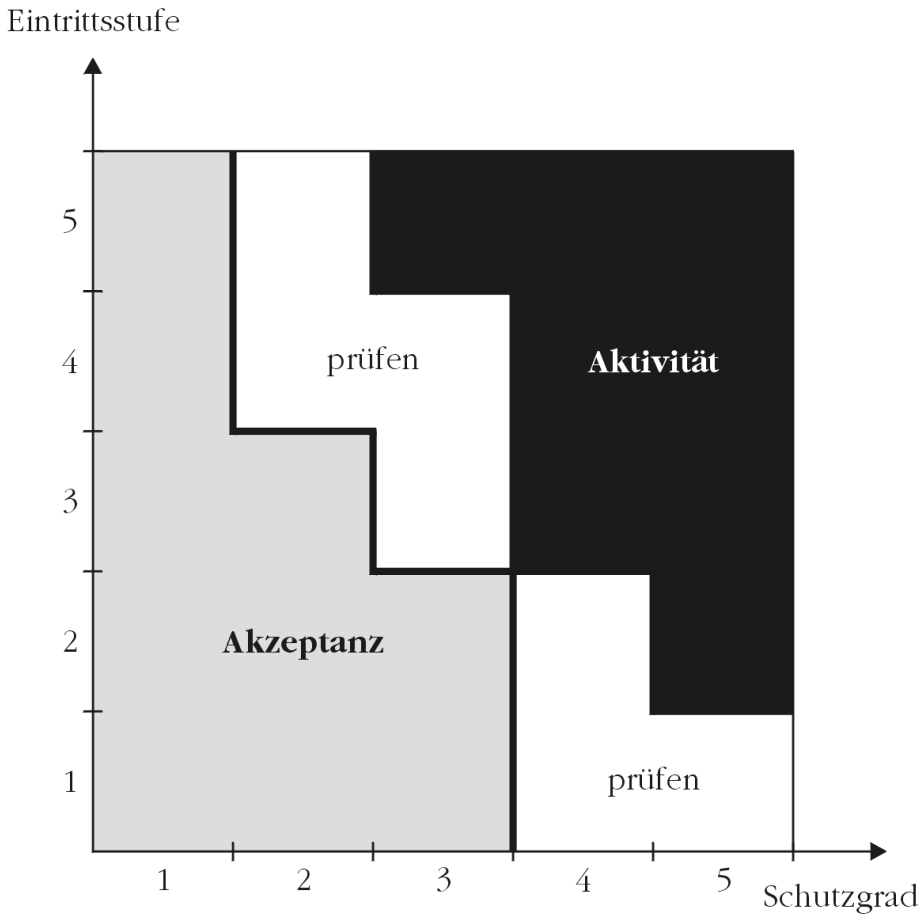
Eintrittsstufe 2 (unwahrscheinliche Komprom.):
ein Störer oder Angreifer muss über erhebliche Ressourcen oder Kenntnisse verfügen, um eine Kompromittierung erreichen zu können

Eintrittsstufe 3 (mögliche Kompromittierung):
ein Störer oder Angreifer muss über begrenzte Ressourcen oder Kenntnisse verfügen, um eine Kompromittierung erreichen zu können

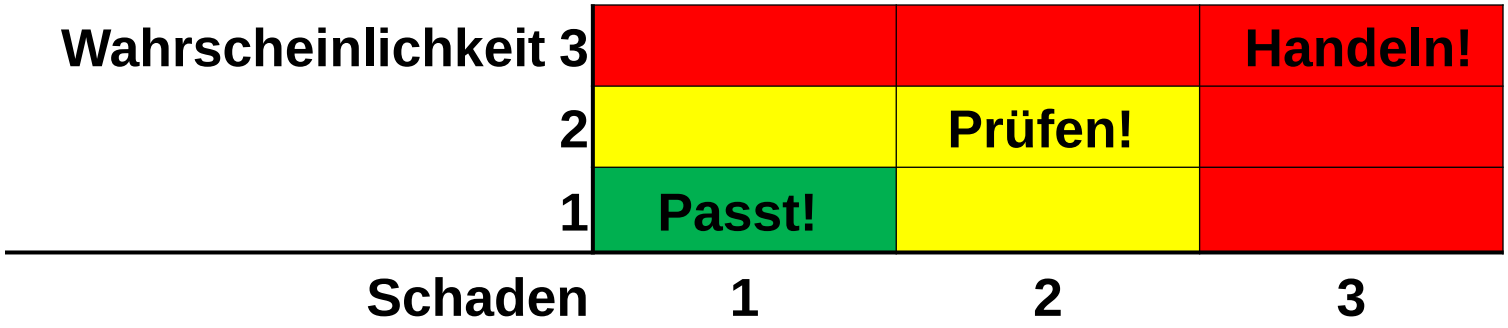
Eintrittsstufe 4 (wahrscheinliche Komprom.):
für eine Kompromittierung sind keine Ressourcen oder Kenntnisse erforderlich, die nicht leicht zu beschaffen sind

Eintrittsstufe 5 (sichere Kompromittierung):
eine Kompromittierung kann bereits aufgrund üblicher Basisausstattungen stattfinden

Umgang mit Datenschutzrisiko



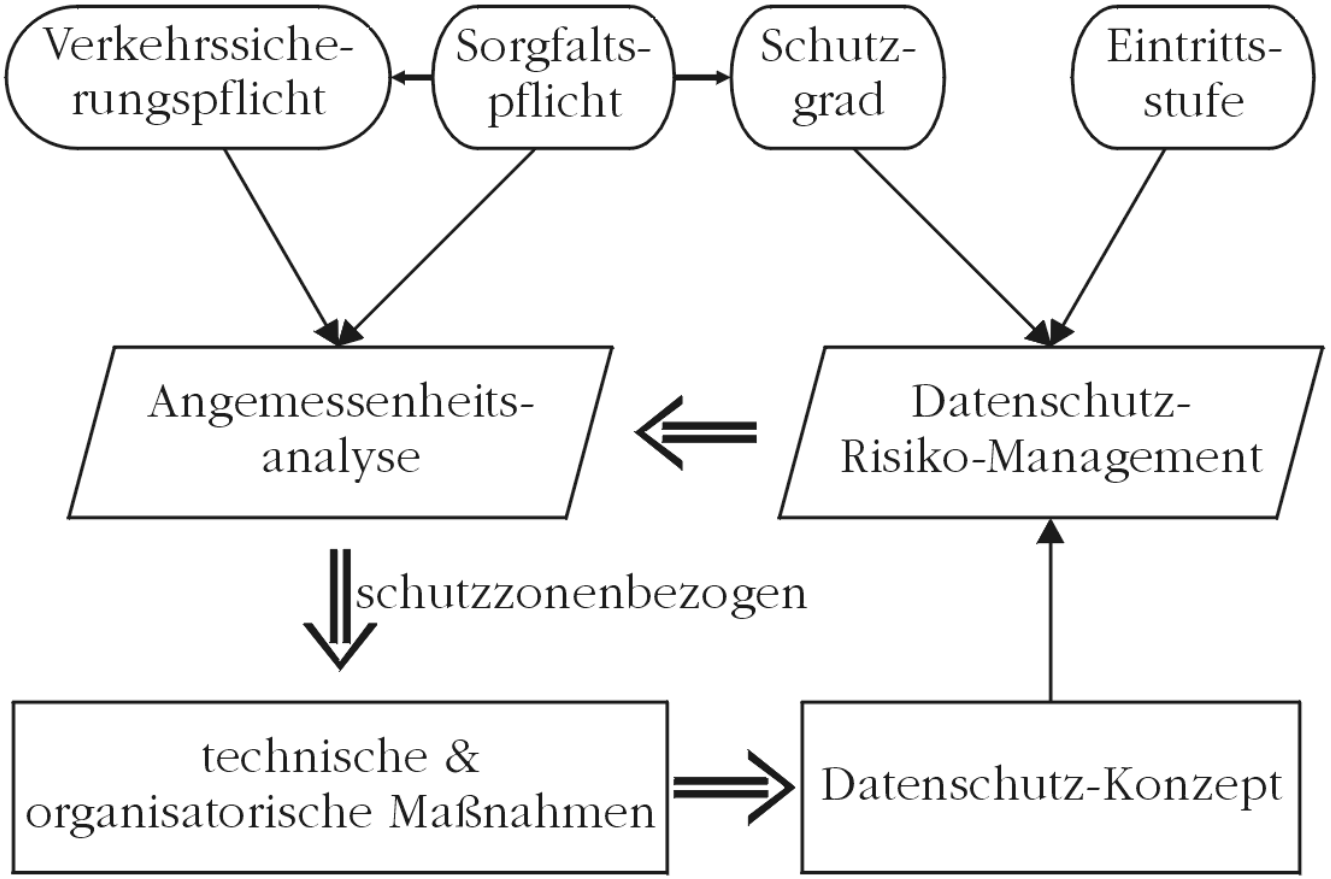
Datenschutzrisiken (vereinfacht)



Wahrscheinlichkeit:
Eintritt einer Verletzung des informationellen Selbstbestimmungsrechts
1 = möglich
2 = wahrscheinlich
3 = sicher

Schaden:
Grad der Verletzung des informationellen Selbstbestimmungsrechts
1 = niedrig (ohne direkte Wirkung)
2 = mittel (formaler Verstoß)
3 = hoch (Bußgeld/Datenpanne)

Datenschutzkonzept als Sammlung der Schutzvorkehrungen



Datenschutzrisiken bei Auftragsdatenverarbeitung (1)

- Sofern Outsourcingpartner **Auftragsdatenverarbeitung** durchfüh-ren soll, bestehen detaillierte Vorgaben (Schriftformerfordernis, Weisungsgebundenheit, vordefinierter Regelungsumfang, Prüf-pflicht), damit der Auftrag datenschutzrechtlich privilegiert ist
  → Auftragnehmer wird dann Teil der verantwortlichen Stelle!
  → Werden nicht alle Vorgaben vollständig eingehalten, liegt daten-schutzrechtlich dagegen eine sog. „Funktionsübertragung“ vor (diese erfordert zulässigen Übermittlungstatbestand für Auftrag-geber und zulässigen Empfangstatbestand für Auftragnehmer; aufgrund der Zweckänderung zudem Abwägung durchzuführen)
- Auftragnehmer ist anhand seiner Schutzvorkehrungen sorgfältig (!) auszuwählen
  → Prüfpflicht vor Aufnahme der Auftragsdatenverarbeitung
  → Pflicht zur regelmäßig durchzuführenden Auditierung

Datenschutzrisiken bei Auftragsdatenverarbeitung (2)

- Auftragskontrolle kann von beliebiger Stelle durchgeführt werden
- Nichtdurchführung selbst ist strafbewährt (Verstoß gegen Formvorschriften), Folgen waren Auslöser für BDSG-Verschärfung
- Das eigentliche Problem bei der Auftragskontrolle liegt in den **unterschiedlichen Sichtweisen** von Auftraggeber & Auftragnehmer:
  - ° Rechtsfolgen eines Datenschutzverstoßes gelten voll gegenüber der verantwortlichen Stelle (Auftraggeber), Auftragnehmer kann allenfalls in Regress genommen werden (**fehlende Regelungen / Weisungen gehen voll zu Lasten des Auftraggebers**)
  - ° Auftragnehmer nimmt möglicherweise andere Risikobetrachtung vor als der Auftraggeber (hat u.U. höheren „Risikoappetit“)
  - ° Haftung von Verträgen faktisch in Bezug auf Vertragssumme beschränkt, deckt nicht zwingend das Schadensrisiko für Auftraggeber

  → **In der Praxis leider oft vernachlässigte Datenschutzrisiken!**

Datensicherheit

Definition 4: Sicherheit

Abwesenheit von Gefahren

Definition 5: Datensicherung

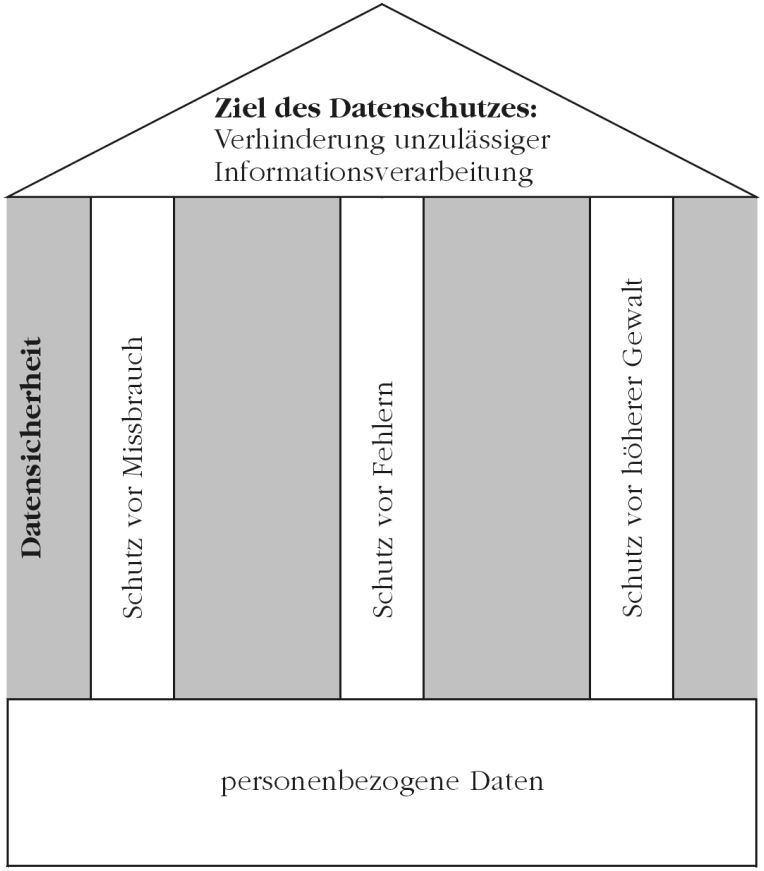
Maßnahmen zur Erhaltung und Sicherung des DV-Systems, der Daten und Datenträger vor Missbrauch, Fehler und höherer Gewalt

→ Datensicherung zielt insb. auf **Ausfallsicherheit** ab!

Definition 6: Datensicherheit

Schutz der gespeicherten Daten vor Beeinträchtigung durch Missbrauch, menschliche oder technische Fehler und höhere Gewalt

Zusammenhang zwischen Datensicherheit und Datenschutz



Begriff der IT-Sicherheit

Definition 7: IT-Sicherheit nach § 2 Abs. 2 BSIG

Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit **von Informationen** betreffen, durch Sicherheitsvorkehrungen in oder bei der Anwendung von informationstechnischen Systemen/Komponenten

- → Datensicherung v.a. Teil der Verfügbarkeit: Ausfallsicherheit
- → Datensicherheit nur Spezialfall der IT-Sicherheit hinsichtlich der Daten (statt informationstechnischer Systeme/Komponenten)
- → IT-Sicherheit zielt auf Schutz der Informationen ab
- → **technische & organisatorische Maßnahmen (= Schutzvorkehrungen) dienen Datenschutz und IT-Sicherheit**

Klassische IT-Sicherheit vs Mehrseitige IT-Sicherheit

Klassische IT-Sicherheit:

- **Verfügbarkeit**
- Unversehrtheit = **Integrität**
- **Vertraulichkeit**

→ Vermeidung unzureichender Beeinträchtigungen der IT-Systeme, Daten, Funktionen und Prozesse in Bestand, Nutzung oder Verfügbarkeit

→ Verlässlichkeit der IT-Systeme

→ Sicherheit der Systeme

Mehrseitige IT-Sicherheit:

- klassische IT-Sicherheit
- ergänzt um **weitere Sicherheitsziele** (insbesondere Authentizität und Verbindlichkeit)

→ Berücksichtigung der Interessen aller Beteiligten

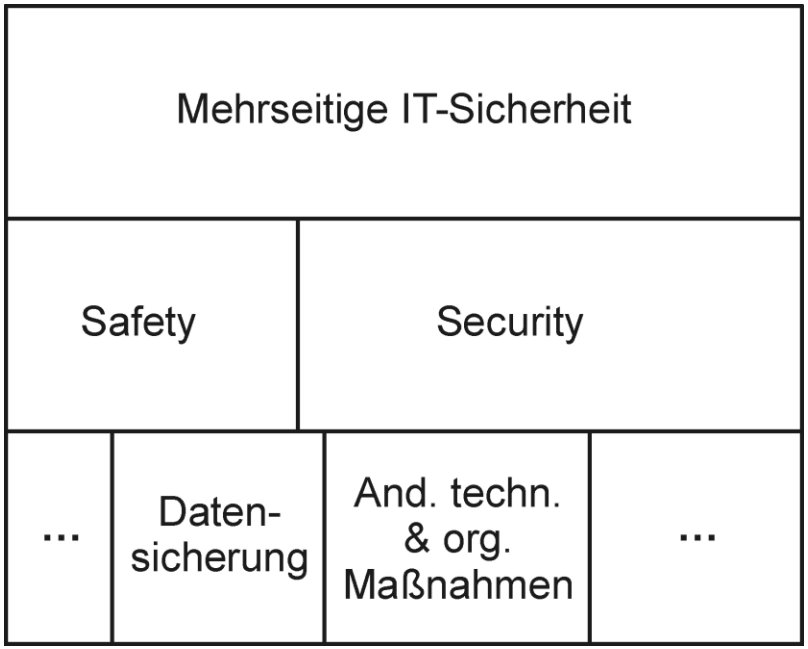
→ Verlässlichkeit und Beherrschbarkeit der IT-Systeme

→ Sicherheit der Systeme und vor den Systemen

Abgrenzung zwischen Datensicherheit & IT-Sicherheit

- Schutz vor unbeabsichtigten Ereignissen: Safety
  ≠ Safety-Begriff im Sinne des Schutzes vor Personenschaden!
- Schutz gegen beabsichtigte Angriffe: Security

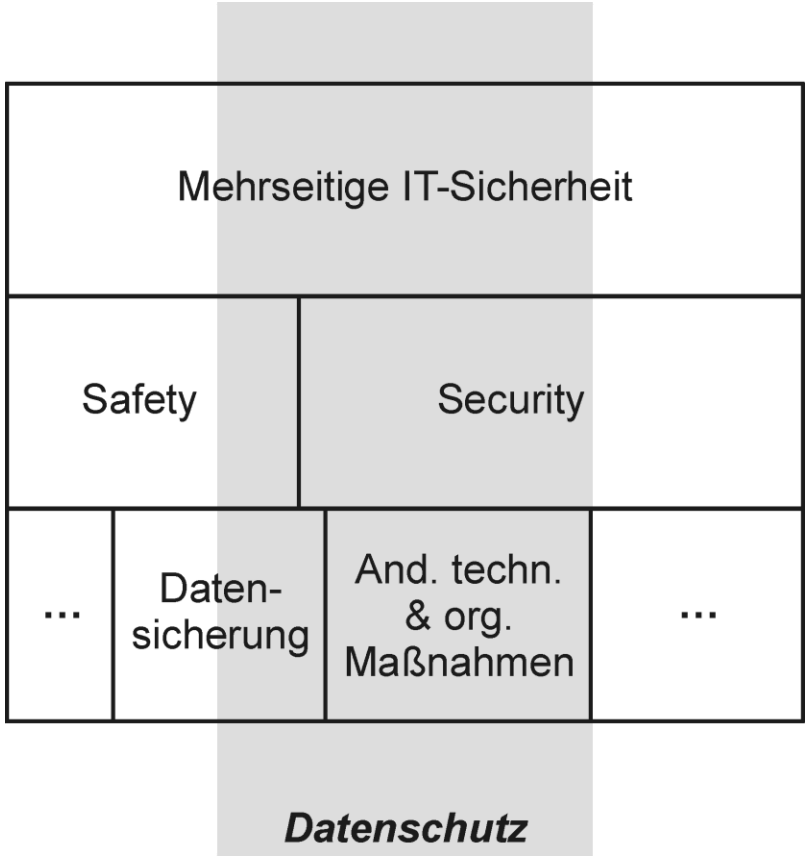
→ **IT-Sicherheit = Safety + Security**



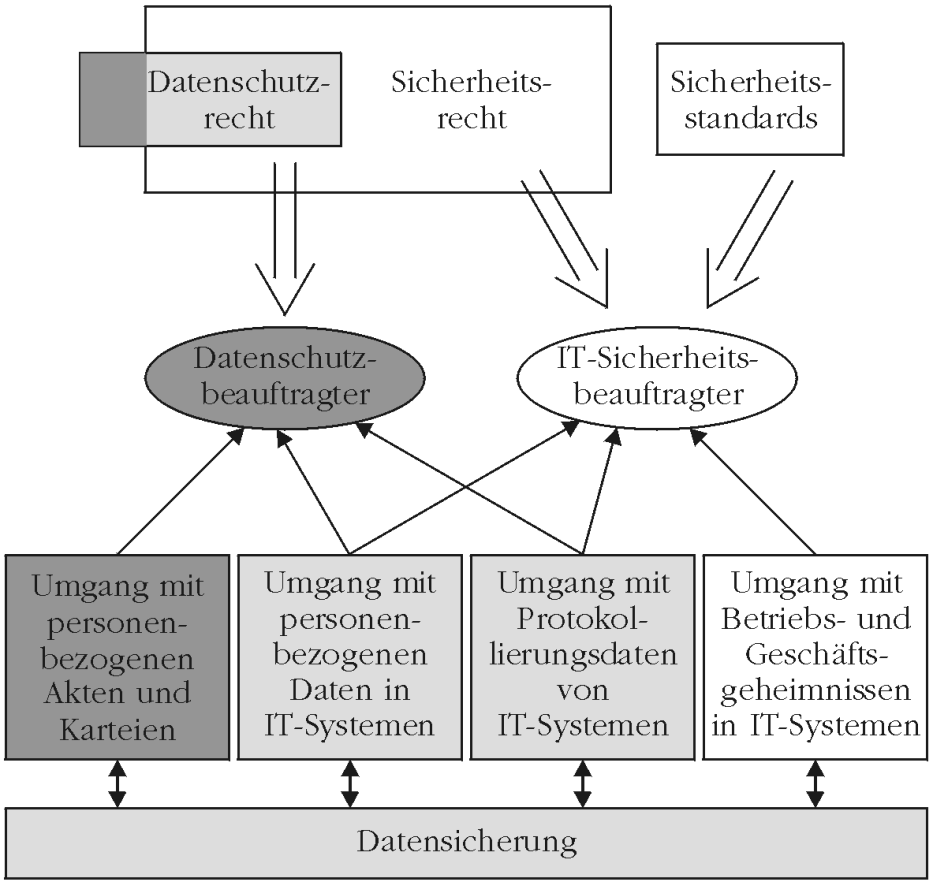
Abgrenzung zwischen Datensicherheit & IT-Sicherheit

Zusammenhang zwischen mehrseitiger IT-Sicherheit und Datenschutz:

- Überschneidung bei der Verarbeitung personenbezogener Daten
- Schwerpunkt liegt auf Security



Unterschiede zwischen DSB & IT-Sicherheitsbeauftragter



Datenschutz-Folgenabschätzung nach EU-DSGV-Entwurf (1)

- Jede verantwortliche Stelle hat sicherzustellen, dass die konkrete Datenverarbeitung **in Einklang mit der EU-DSGVO** durchgeführt wird, dabei die **Betroffenenrechte gewährleistet** werden, und muss dies **nachweisen** können (Art. 22 Abs. 1 + Art. 23 Abs. 1).
- Die **Wirksamkeit** der dazu eingesetzten Maßnahmen muss (von unabhängiger Seite) **überprüft** werden (Art. 22 Abs. 3).
- **Nur benötigte Daten** dürfen verarbeitet werden (Art. 23 Abs. 2).
- Gleiches gilt für **Auftragsdatenverarbeitungen** (Art. 26 Abs. 1).
- Schutzvorkehrungen müssen **Schutzniveau** gewährleisten, das den von der Verarbeitung ausgehenden **Risiken und** der **Art der** zu schützenden **Daten** angemessen ist (Art. 30 Abs. 1).
- Maßnahmen nach der Risikobewertung zu treffen zum Schutz vor unbeabsichtigter / widerrechtlicher Zerstörung, unbeabsichtigtem Verlust, zur Vermeidung unrechtmäßiger Verarbeitung wie z.B. unbefugte Offenlegung / Verbreitung / Einsichtnahme (Art. 30 Abs. 2)

Datenschutz-Folgenabschätzung nach EU-DSGV-Entwurf (2)

- **Maßnahmen** nach der Risikobewertung zu treffen (Art. 30 Abs. 2)
  - ° zum Schutz vor unbeabsichtigter / widerrechtlicher Zerstörung,
  - ° zum Schutz vor unbeabsichtigtem Verlust,
  - ° zur Vermeidung unrechtmäßiger Verarbeitung, wie z.B. unbefugte Offenlegung / Verbreitung / Einsichtnahme
- Bergen Verarbeitungsvorgänge aufgrund ihres **Wesens**, **Umfangs** oder ihrer **Zwecke** konkrete Risiken für die Rechte & Freiheiten der Betroffenen ist **Datenschutz-Folgenabschätzung** durchzuführen (Art. 33 Abs. 1), vor allem in den Fällen (Art. 33 Abs. 2)
  - ° systematischer & umfassender Auswertung der Persönlichkeit
  - ° der Verarbeitung besonders sensibler Daten, der Daten über Kinder, genetischer bzw. biometrischer Daten
  - ° weiträumiger Videoüberwachung
  - ° sonstiger Verarbeitungen gemäß einer vorgegebenen Liste der Aufsichtsbehörden (bisher leer)

Datenschutz-Folgenabschätzung nach EU-DSGV-Entwurf (3)

- Bei der Folgenabschätzung ist den **Betroffenenrechten & -interessen** Rechnung zu tragen und die Risiken in Bezug auf die Rechte & Freiheiten der Betroffenen zu bewerten (Art. 33 Abs. 3).
- Die Meinung der Betroffenen oder ihrer Vertreter ist einzuholen (Art. 33 Abs. 4).
- Die Folgenabschätzung wird von beliebiger Stelle durchgeführt; die Durchführung der Folgenabschätzung aber vom Datenschutzbeauftragten überwacht (Art. 37 Abs. 1), sofern einer bestellt werden musste.
- Die **Nicht-Durchführung** der Folgenabschätzung kann mit einer **Geldbuße bis zu 1 Mio EUR bzw. bis zu 2 % des Jahresumsatzes** geahndet werden (Art. 79 Abs. 6 lit. i)!

Kennzeichen datenschutz-fördernder Techniken

= Privacy Enhancing Technologies (PET; 1995)

- **Ziel**: weniger Risiken für die Privatsphäre der Betroffenen durch Ausgestaltung eingesetzter Informations- und Kommunikations-technik unter Reduktion des Personenbezugs (→ Anonymität)
- setzt bereits im **Vorfeld** der Verarbeitung personenbezogener Daten an → Datenvermeidung!
- wichtiges Hilfsmittel vorausschauender Technikgestaltung
- unabhängig von etwaigen Rechtsnormen
- Rückwirkung auf rechtliche Entwicklung („Stand der Technik“)
- frühere Bezeichnung: „**Systemdatenschutz**“ (Podlech)

→ datenschutzgerechte & datenschutzfördernde Technik zur strukturellen & systemanalytische Ergänzung des individuellen Rechtsschutzes der Betroffenen

Prinzipien datenschutz-fördernder Techniken (1)

Datensparsamkeit & Systemdatenschutz

- je weniger personenbezogene Daten herausgegeben werden (müssen), desto leichter lassen sich entsprechende Techniken anwenden

→ nur erforderliche Daten verarbeiten

→ frühestmögliche Anonymisierung

→ frühestmögliche Löschung

→ Verschlüsselung bei Kommunikation

→ Kern des privacy by design principles!

→ Beispiel: prepaid-Chipkarten, Mix-Netz, Transaktionspseudonym (z.B. mit verdeckter Zufallszahl bei elektronischem Geld)

Prinzipien datenschutz-fördernder Techniken (2)

Selbstdatenschutz & Transparenz

- Selbstbestimmung und Steuerung durch Nutzer

→ Nutzer entscheidet selbst, wie anonym er Dienste in Anspruch nimmt

→ Verarbeitung wird verständlich offengelegt (Verfahrensverzeichnis) und ist nachprüfbar (→ Identitätsmanagement)

→ Formulierung eigener Schutzziele

→ Nutzung vertrauenswürdiger Institutionen (Trust Center)

→ Unterstützung durch Anwendung der Betroffenenrechte

→ Unterstützung für Umsetzung des privacy by design principles

→ Beispiel: Platform for Privacy Preferences (P3P auf www.w3.org/P3P/)