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

Vorlesung im Sommersemester 2016

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, Sicherheit, Datensicherung, Datensicherheit
- technische & organisatorische Maßnahmen (nach BDSG & EU-DS-GVO), Datenschutzkonzept
- Standard-Datenschutzmodell
- Risikobasierter Ansatz im Datenschutzrecht
- Vorabkontrolle zu Datenschutzrisiken
- Bestimmung von Datenschutzrisiken
- Datenschutz-Folgenabschätzung nach der EU-DS-GVO
- Privacy Impact Assessment
- Datenschutzrisiken bei der Auftragsdatenverarbeitung
- Datenschutzfördernde Techniken
- Privacy by Design / Default

Daten vs. Informationen

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

→**Lösung**: Festlegung von Definitionen!

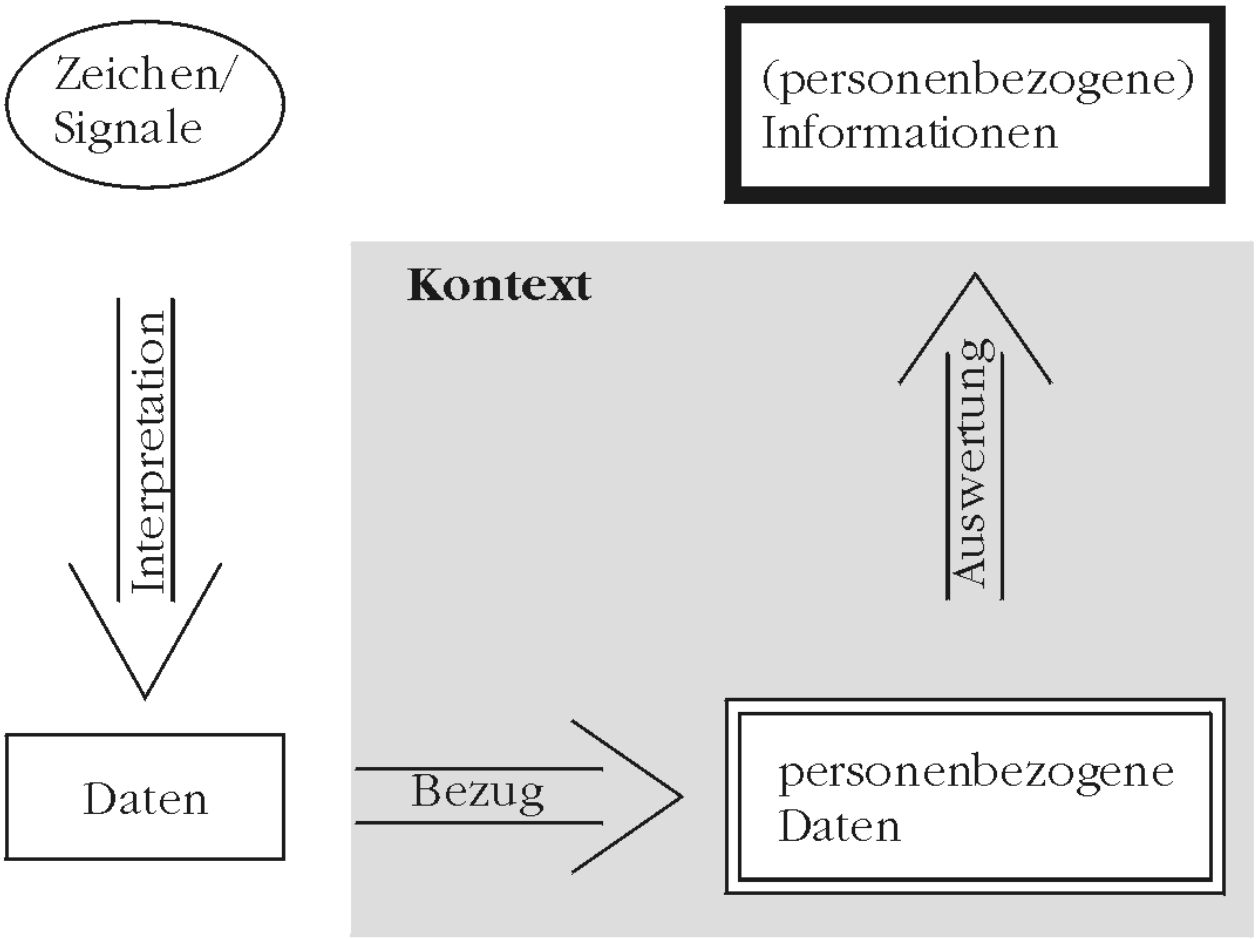
Definition 2: Daten

kontextfreie Angaben, die aus interpretierten Zeichen bzw. Signalen bestehen

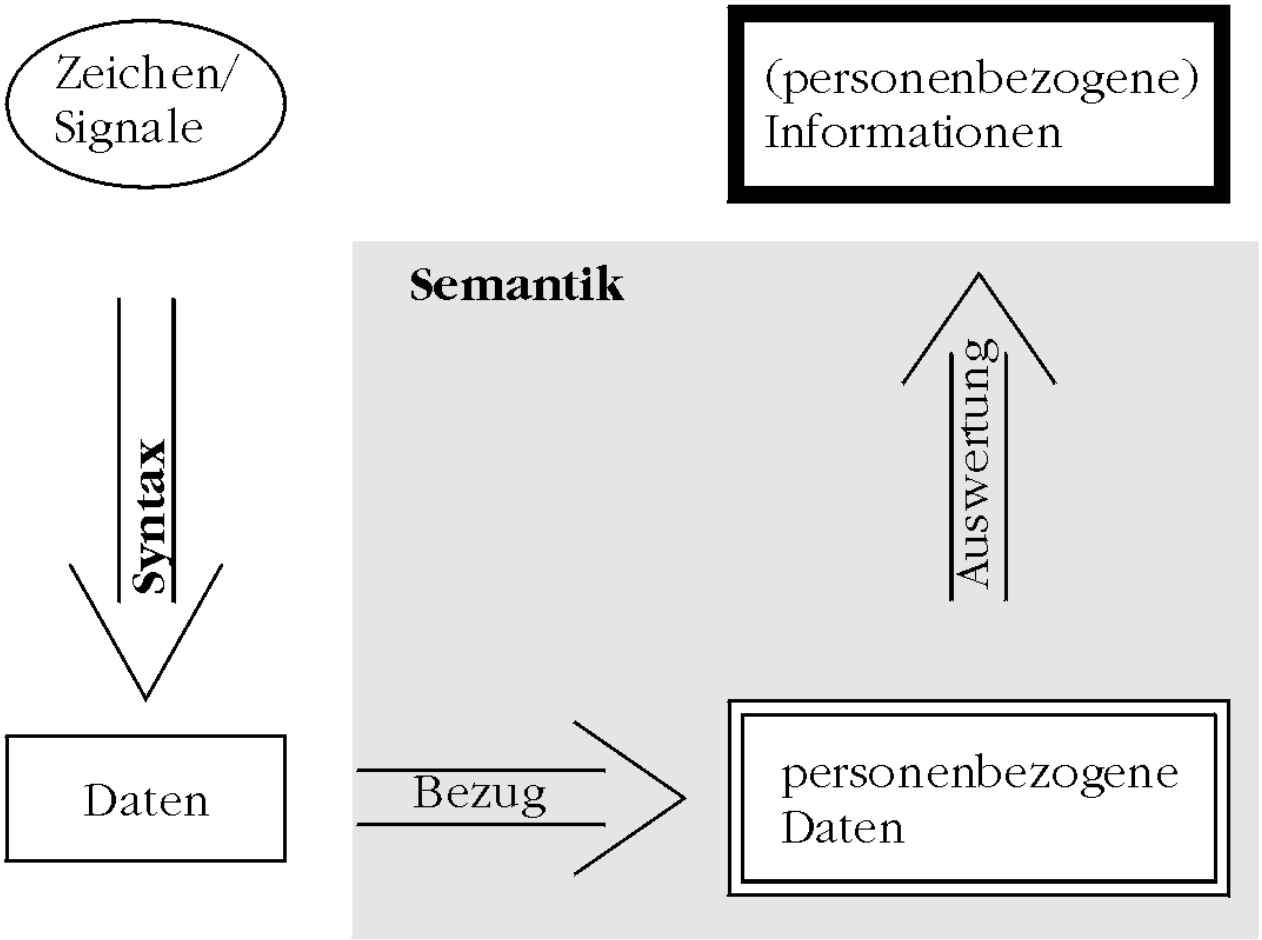
Definition 3: Informationen

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

Vom Datum zur Information (1)



Vom Datum zur Information (2)



Datensicherheit

Definition 4: Sicherheit

Abwesenheit von Gefahren

Definition 5: Datensicherung

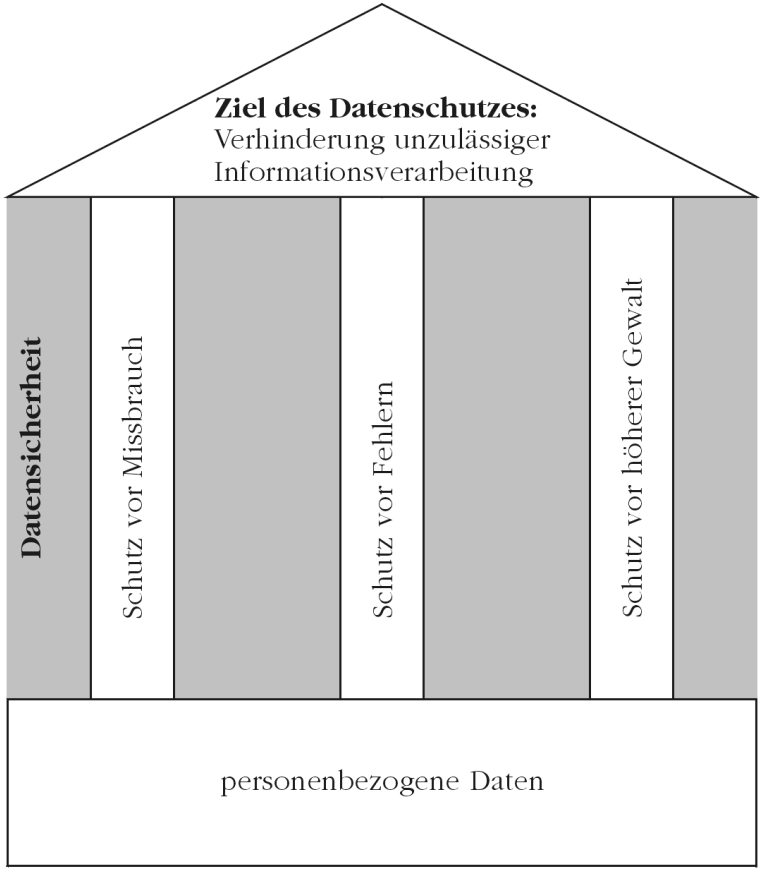
Maßnahmen zur Aufrechterhaltung des DV-Systems, der Daten und Datenträger vor Zerstörung oder Verlust

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

Definition 6: Datensicherheit

Schutz der gespeicherten Daten vor Beeinträchtigung durch Miss-brauch, menschliche oder technische Fehler und höhere Gewalt

Zusammenhang zwischen Datensicherheit und Datenschutz



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>**

Schutzvorkehrungen nach der EU-DS-GVO (1)

- Nach Art. 32 Abs. 1 der EU-DS-GVO gilt, dass **geeignete** technische und organisatorische Maßnahmen zu treffen sind unter Berücksichtigung von
  - Stand der Technik
  - Implementierungskosten
  - Art, Umfang, Umstände & Zwecke der Verarbeitung
  - sowie unterschiedliche Eintrittswahrscheinlichkeit & Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen
- Dabei ist ein **dem Risiko angemessenes Schutzniveau** zu gewährleisten
- Die Maßnahmen sind nach Art. 24 Abs. 1 erforderlichenfalls zu **überprüfen und aktualisieren**

Schutzvorkehrungen nach der EU-DS-GVO (2)

- Zu treffende Maßnahmen schließen u.A. Folgendes ein (nach Art. 32 Abs. 1):
  - **a) Pseudonymisierung und Verschlüsselung** personenbezogener Daten
  - b) Fähigkeit zur **Sicherstellung von**
    - **Vertraulichkeit**
    - **Integrität**
    - **Verfügbarkeit**
    - **Belastbarkeit**

    der Systeme & Dienste im Zusammenhang mit der Verarbeitung auf Dauer
  - c) Fähigkeit zur **raschen (!) Wiederherstellung**
    - der Verfügbarkeit personenbezogener Daten
    - und des Zugangs zu diesen Daten

    bei einem physischen oder technischen **Zwischenfall**
  - d) Verfahren zur regelmäßigen **Überprüfung, Bewertung & Evaluierung der Wirksamkeit dieser Maßnahmen**

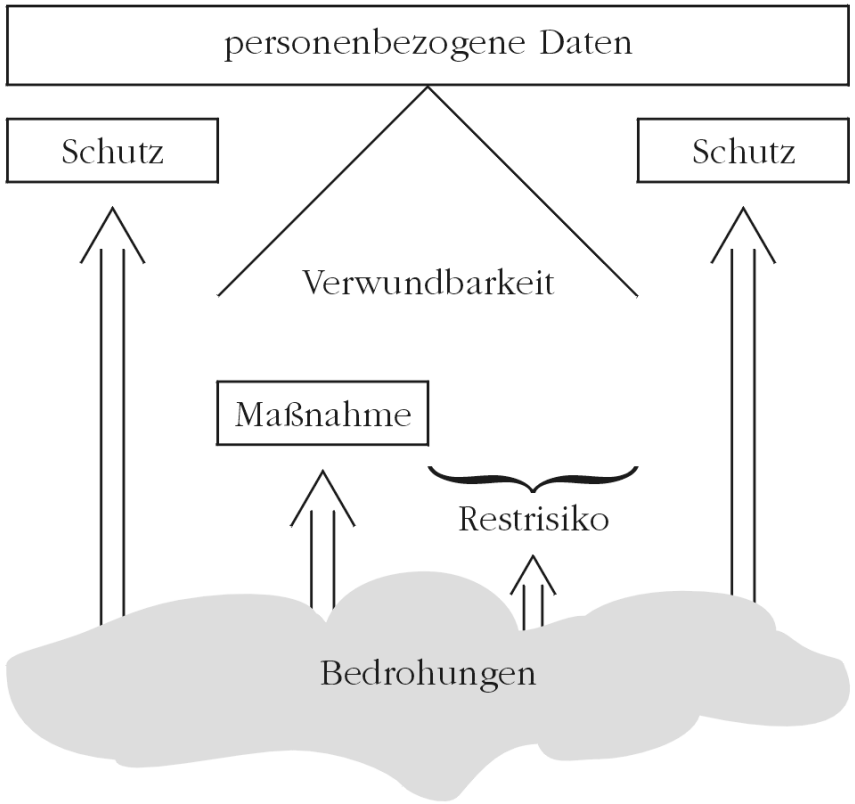
Schutzvorkehrungen nach der EU-DS-GVO (3)

- Nach Art. 32 Abs. 2 der EU-DS-GVO ist bei der Beurteilung des angemessenen Schutzniveaus **insbesondere die Risiken** zu berücksichtigen, die **mit der Verarbeitung verbunden** sind; insbesondere hinsichtlich
  - Vernichtung bzw. Verlust (ob unbeabsichtigt oder unrechtmäßig)
  - Veränderung (ob unbeabsichtigt oder unrechtmäßig)
  - unbefugte Offenbarung von bzw. unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden
- Genehmigte Verhaltensregeln (nach Art. 40) oder genehmigte Zertifizierungsverfahren (nach Art. 42) können nach Art. 32 Abs. 3 als **Nachweis für die Erfüllung der Anforderungen** herangezogen werden
- Ausführende Personen, die Zugang zu personenbezogenen Daten haben, dürfen diese Daten nach Art. 32 Abs. 4 nur auf Anweisung der verantwortlichen Stelle verarbeiten, sofern sie nicht durch geltendes Recht zur Verarbeitung verpflichtet sind

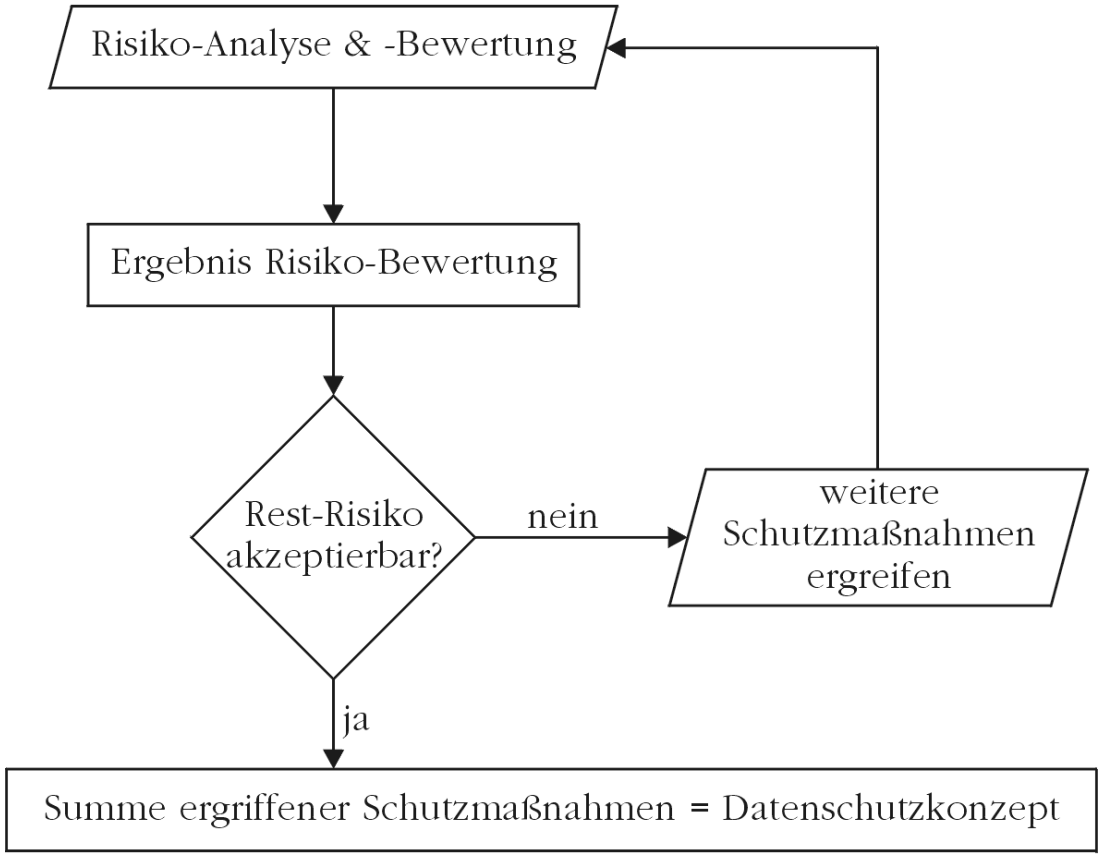
Gewährleistungsziele nach Standard-Datenschutzmodell

- Am 1. Oktober 2015 haben die deutschen Aufsichtsbehörden zum Datenschutz ein Konzept zur Datenschutzberatung und -prüfung auf der Basis **einheitlicher Gewährleistungsziele** verabschiedet. Danach sind folgende Gewährleistungsziele zu verfolgen (unter Angabe von zugehörigen Maßnahmen):
  - Datensparsamkeit (grundlegend → übergeordnet)
  - Verfügbarkeit
  - Integrität
  - Vertraulichkeit
  - Nichtverkettbarkeit
  - Transparenz
  - Intervenierbarkeit
- Die grünen Gewährleistungsziele zählen zu den „klassischen“ Gewährleistungszielen der Datensicherheit, die blauen Gewährleistungsziele sind dagegen am Schutzbedarf von Betroffenen ausgerichtet.

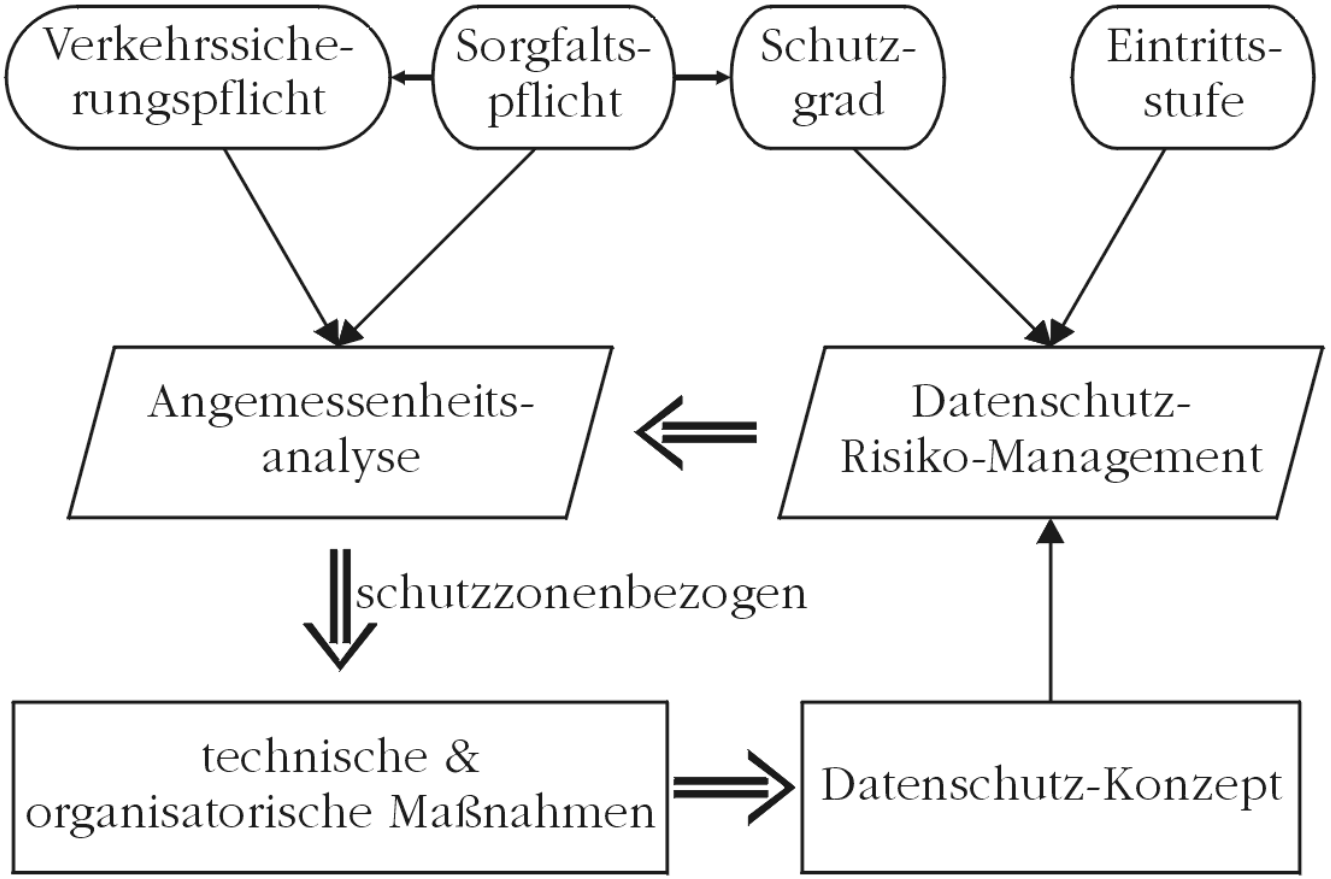
Ziel der technischen & organisatorischen Maßnahmen (1)



Ziel der technischen & organisatorischen Maßnahmen (2)



Datenschutzkonzept als Sammlung der Schutzvorkehrungen



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 [mit i.d.R. geringer Eintrittswahrscheinlichkeit]
- Zudem besteht **Meldepflicht bei Datenpannen**, sofern
  ° Unbefugter Kenntnis über sensible Daten erhalten hat
  ° Schwerwiegende Beeinträchtigungen für die Betroffenen drohen
  → Reputationsverlust! (+ indirekter finanzieller Schaden) [tritt i.d.R. eher ein]
- Meldepflicht gegenüber Aufsichtsbehörde und den Betroffenen

→ **Datenschutzrisiken = Risiken des Datenschutzrechtsverstoßes**

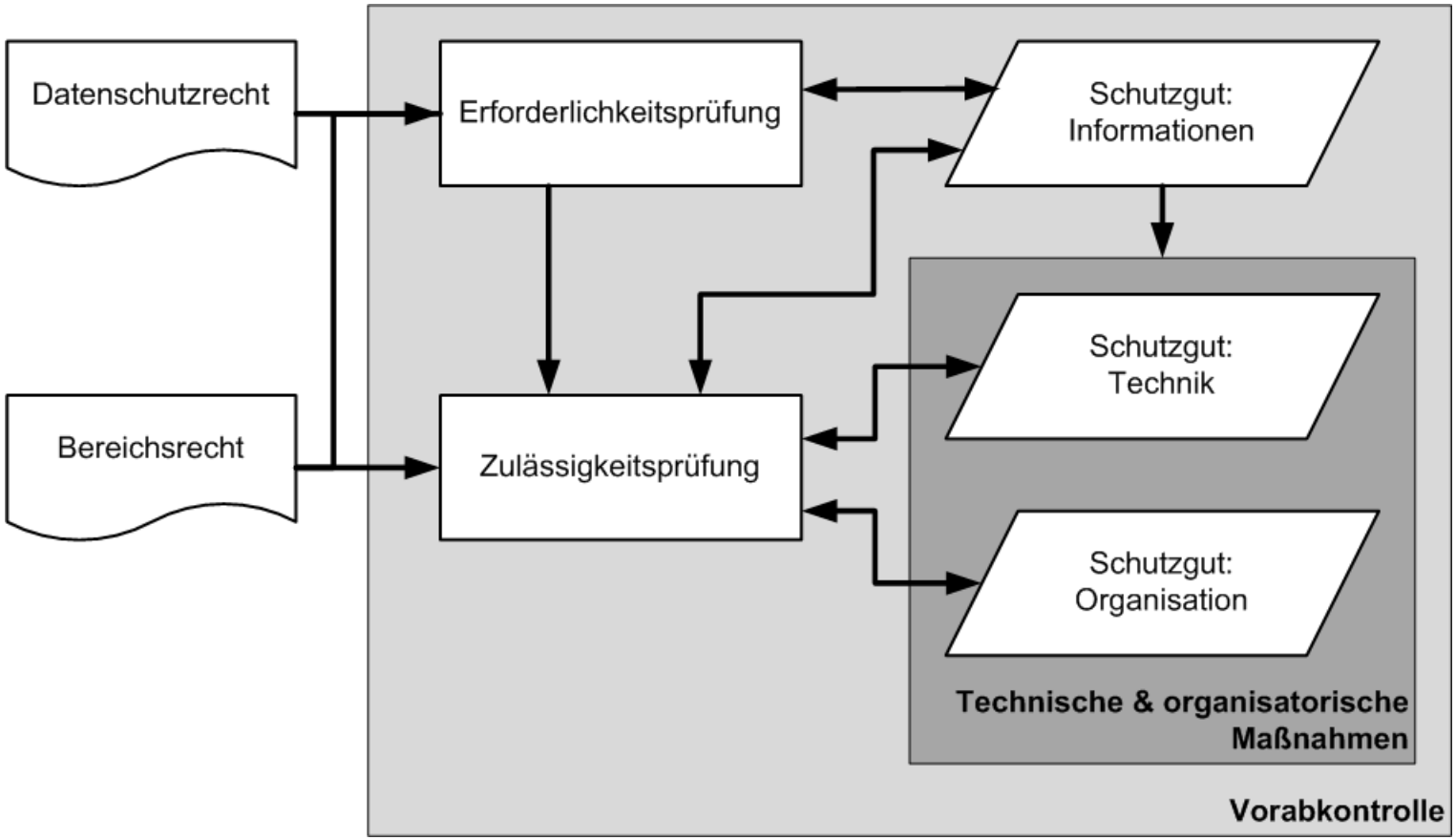
Risikobasierter Ansatz im Datenschutzrecht (2)

- **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
- **Technische & organisatorische Maßnahmen** müssen Schutzgrad der Daten entsprechen (→ Adäquatheit) und angemessen sein (→ Wirtschaftlichkeits-prüfung)
  ° 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

Risikobasierter Ansatz im Datenschutzrecht (3)

- 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)

Risikobasierter Ansatz im Datenschutzrecht (4)



Risikobasierter Ansatz im Datenschutzrecht (5)

Im Rahmen der EU-DS-GVO ist der Strafrahmen deutlich erweitert worden:

- **Verstöße gegen Pflichten** der verantwortlichen Stelle bzw. des Auftragnehmers sind nach Art. 83 Abs. 4 lit. a der EU-DS-GVO mit **Geldbußen von bis zu 10 Mio. € bzw. von bis zu 2 % des weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahres fällig. Das betrifft u.A.:
  - Missachtung von Privacy by Design / Default (Art. 25)
  - Nichteinhaltung von Auflagen zur Auftragsdatenverarbeitung (Art. 28)
  - Unvollständiges Verzeichnis von Verarbeitungstätigkeiten (Art. 30)
  - Unzureichende Maßnahmen zur Sicherheit der Verarbeitung (Art. 32)
  - Unzureichende Meldungen von Verletzungen des Schutzes personenbezogener Daten (Art. 33 + 34)
  - Unzureichende Datenschutz-Folgenabschätzung (Art. 35)
  - Nichtbenennung eines Datenschutzbeauftragten (Art. 37 bis 39)
  - Fehlerhafte Zertifizierungen (Art. 42 + 43)

→ **Unzureichender technischer Datenschutz strafbewährt!**

Risikobasierter Ansatz im Datenschutzrecht (6)

Im Rahmen der EU-DS-GVO ist der Strafrahmen deutlich erweitert worden:

- Folgende Verstöße sind nach Art. 83 Abs. 5 der EU-DS-GVO mit **Geldbußen von bis zu 20 Mio. € bzw. von bis zu 2 % des weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahres fällig:
  - **Verstöße gegen die Grundsätze für die Verarbeitung** (einschließlich der Bedingungen für die Einwilligung!) nach Art. 5, 6, 7 & 9 (also auch einer unzureichenden Handhabung von besonderen Kategorien personenbezogener Daten)
  - **Verstöße gegen die Betroffenenrechte** nach Art. 12 bis 22
  - **Unzulässige Übermittlung von Daten in Drittstaaten** nach Art. 44 bis 49
  - Nichteinhaltung der Vorschriften für besondere Verarbeitungssituationen nach Art. 85 bis 91 gemäß den Rechtsvorschriften der Mitgliedsstaaten
  - Behinderung der Aufsichtsbehörden

→ **Unzureichende Rechtmäßigkeit der Verarbeitung strafbewährt!**

- Gleiches gilt für die Nichtbefolgung von Anweisungen der Aufsichtsbehörde

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 (→ Zulässigkeits-prüfung)
- Ein besonderer Augenmerk gilt den vorgesehenen **technischen und organisatorischen Maßnahmen**, die wirksam ein besonderes Risiko vermeiden helfen (→ Ermittlung wirksamer Schutzvorkehrungen)

→ Vorabkontrolle = Instrument präventiver Compliance

- Vorabkontrolle ist durch den Datenschutzbeauftragten durchzuführen
- Nichtdurchführung selbst ist nicht strafbewährt, sondern nur die po-tenziellen 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

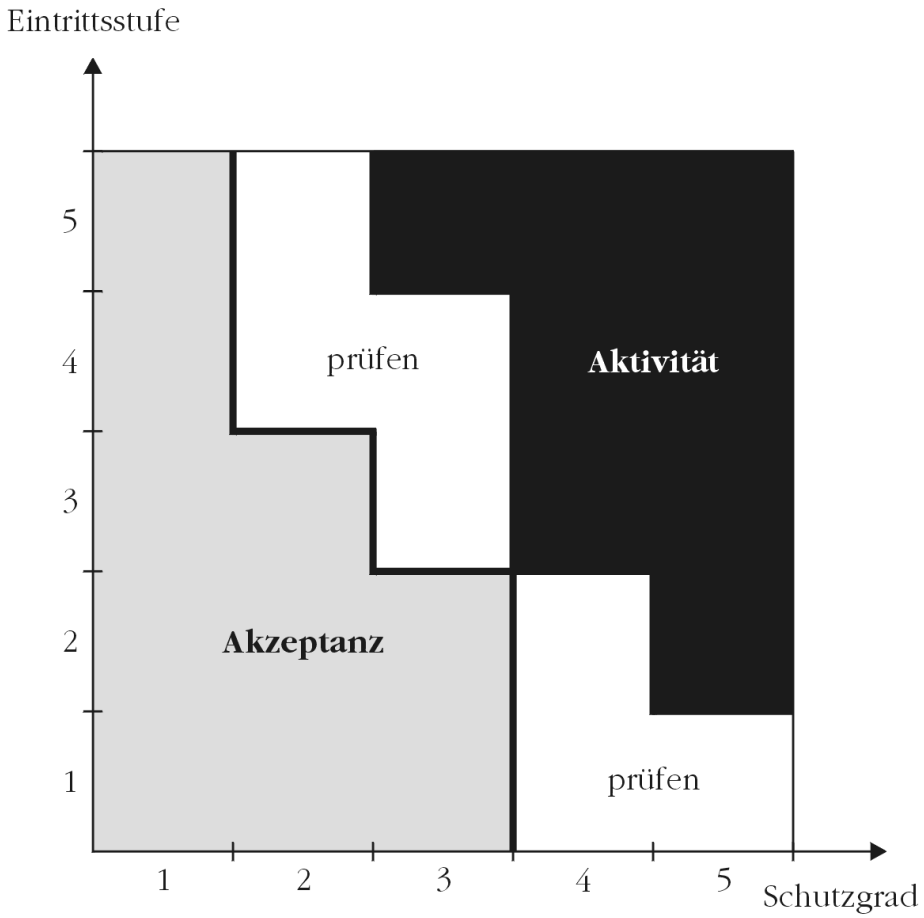
Eintrittsstufe 2 (unwahrscheinliche Komprom.):
ein Störer oder Angreifer muss über erhebliche Ressourcen oder Kenntnisse verfügen, um eine Kompromittierung erreichen zu können

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

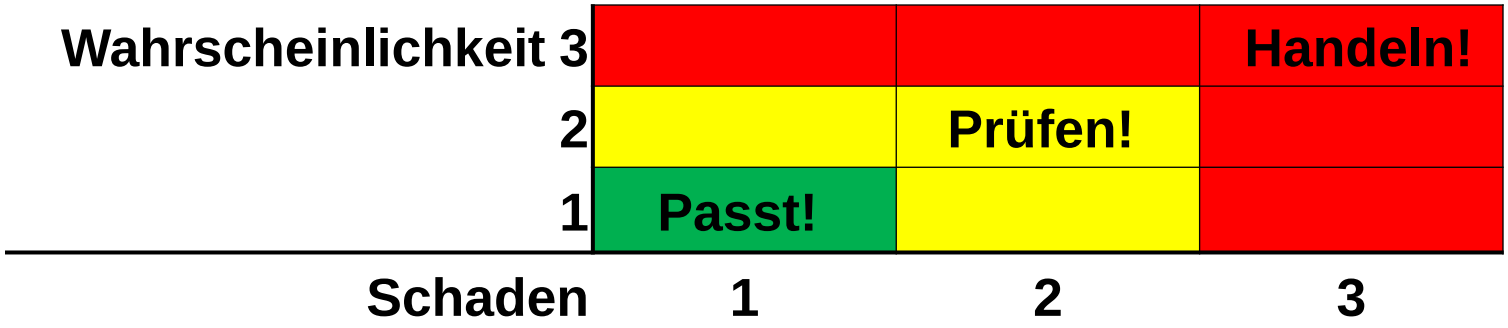
Eintrittsstufe 4 (wahrscheinliche Komprom.):
für eine Kompromittierung sind keine Ressourcen oder Kenntnisse erforderlich, die nicht leicht zu beschaffen sind

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)

Datenschutz-Folgenabschätzung nach EU-DS-GVO (1)

- Nach Art. 35 Abs. 1 der EU-DS-GVO hat die verantwortliche Stelle bei vorgesehenen Verarbeitungsvorgängen vorab eine **Abschätzung der Folgen** für den Schutz personenbezogener Daten durchzuführen, sofern
  - die Form der Verarbeitung, insbesondere aufgrund der Verwendung neuer Technologien
  - aufgrund von Art, Umfang, Umstände & Zwecken der Verarbeitung

  voraussichtlich ein **hohes Risiko für die Rechte und Freiheiten natürlicher Personen** zur Folge hat
- Nach Art. 35 Abs. 3 ist die Durchführung einer Datenschutz-Folgenabschätzung erforderlich:
  a) Systematische & umfassende Bewertung persönlicher Aspekte (insb. **Profiling**)
  b) Umfangreiche Verarbeitung **besonderer Kategorien** personenbez. Daten
  c) Systematische umfangreiche **Überwachung** öffentlich zugänglicher Bereiche

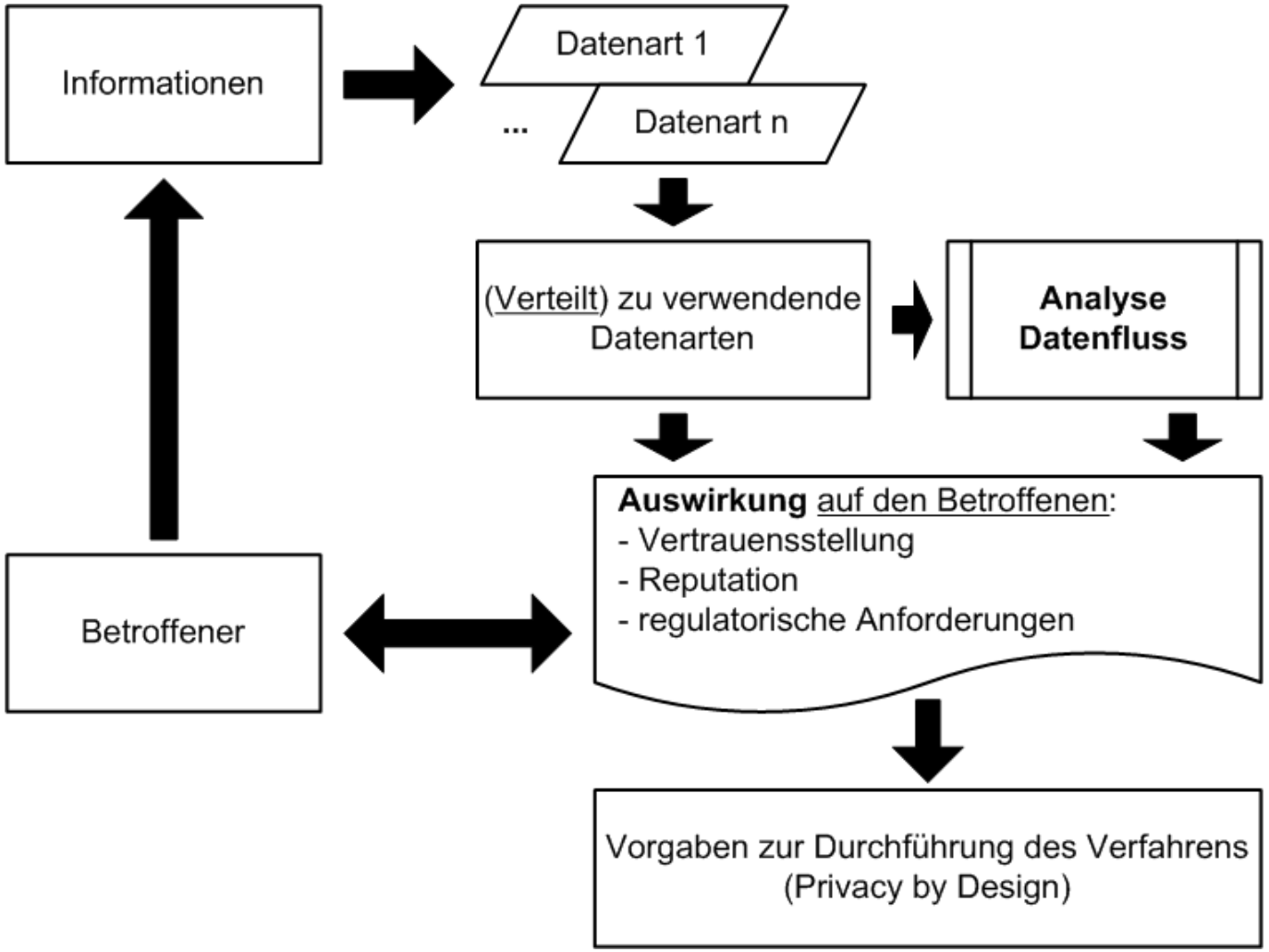
Datenschutz-Folgenabschätzung nach EU-DS-GVO (2)

- Nach Art. 35 Abs. 7 der EU-DS-GVO hat eine Datenschutz-Folgenabschätzung mindestens Folgendes zu enthalten:
  a) Systematische Beschreibung der **geplanten Verarbeitungsvorgänge** und der **Zwecke der Verarbeitung**, ggf. einschließlich der von der verantwortlichen Stelle verfolgten berechtigten Interessen
  b) Bewertung der **Notwendigkeit & Verhältnismäßigkeit** der Verarbeitungsvorgänge **in Bezug auf den Zweck**
  c) Bewertung der **Risiken für die Rechte und Freiheiten der Betroffenen**
  d) Zur Bewältigung der Risiken geplanten **Abhilfemaßnahmen** (einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren zum Schutz personenbezogener Daten) **und** dem **Nachweis zur Einhaltung der EU-DS-GVO**
- Zur Datenschutz-Folgenabschätzung ist ggf. der **Standpunkt des Betroffenen** zur beabsichtigten Verarbeitung einzuholen nach Art. 35 Abs. 9
- Änderungen bei den Risiken führen nach Art. 35 Abs. 11 erforderlichenfalls zu einer **Überprüfung der Abschätzung**

Privacy Impact Assessment (1)

- Privacy Impact Assessment (PIA) = Prozess zur Identifikation von Datenschutzrisiken bei der automatisierten Verarbeitung personenbezogener Daten, der Analyse der Auswirkung dieser Risiken und des daraus resultierenden Umgangs mit diesen Risiken (Normierung als ISO/IEC 29134 derzeit in Arbeit)
- PIA werden in der Praxis eingesetzt, um systematisch Problemfelder beim Umgang mit personenbezogenen Daten zu ermitteln
  → Prüfung, ob in einem IT-Projekt eine PIA durchzuführen ist (durch Analyse der Datenfelder und des Datenflusses)
  → Auswirkung auf die informationelle Selbstbestimmung der Betroffenen und hinsichtlich Vertrauensverlust, Reputationsschäden & Gesetzesverstößen
  → Auswahl einer adäquaten datenschutzkonformen Lösung
  → Reduzierung der Folgen auf ein akzeptables Maß
  → Vermeidung des Eintritts einer (meldepflichtigen) Datenpanne
  → Nachweis für Compliance mit Datenschutzvorschriften
- PIA ist eine zentrale Methode für Privacy by Design

Privacy Impact Assessment (2)



Privacy Impact Assessment (3) nach der EU-DS-GVO

Wirkung auf Rechte und Freiheiten des Betroffenen	Zielvorgabe aufgrund der Grundsätze (Art. 5)						Zielvorgabe aufgrund der Schutzziele (Art. 32)					Zielvorgabe aufgrund der Verarbeitungs-bedingungen (Art. 35)		
	Rechtmäßigkeit	Treu & Glauben	Transparenz	Zweckbindung	Datenminimierung	Speicherbegrenzung	Vertraulichkeit	Integrität	Verfügbarkeit	Belastbarkeit	Wiederherstellbarkeit	Vermeidung technikspezifischer Risiken	Vermeidung zweckbezogener Risiken	Vermeidung datenartenbezogener Risiken
Unterscheidung je nach Verarbeitungsaspekt														
potenzielles Risiko 1	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung
potenzielles Risiko 2	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
potenzielles Risiko n	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung	Wirkung

Bei dem jeweils identifizierten potenziellen Risiko ist die Wirkung auf die Erreichung der Zielvorgabe für die Rechte und Freiheiten der Betroffenen darzustellen; dies kann insbesondere auch „keine“ sein.

Datenschutzrisiken bei Auftragsdatenverarbeitung (1)

- Sofern Outsourcingpartner **Auftragsdatenverarbeitung** durchführen soll, bestehen detaillierte Vorgaben (Schriftformerfordernis, Weisungsgebundenheit, vordefinierter Regelungsumfang, Prüfpflicht), damit der Auftrag datenschutzrechtlich privilegiert ist
  → Auftragnehmer wird dann Teil der verantwortlichen Stelle!
  → Werden nicht alle Vorgaben vollständig eingehalten, liegt datenschutzrechtlich dagegen eine sog. „Funktionsübertragung“ vor (diese erfordert zulässigen Übermittlungstatbestand für Auftraggeber 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!**

Auftragsdatenverarbeitung nach EU-DS-GVO (1)

- Nach Art. 28 Abs. 1 der EU-DS-GVO darf eine Verarbeitung personenbezogener Daten im Auftrag nur durch einen Auftragsverarbeiter erfolgen, der hinreichend Garantien für geeignete technische & organisatorische Maßnahmen bietet, um die Verarbeitung **im Einklang mit der EU-DS-GVO** durchzuführen und den **Schutz der Betroffenenrechte** zu gewährleisten
- **Unterauftragnehmer** bedürfen der schriftlichen Genehmigung (Art. 28 Abs. 2) und haben gleiche Pflichten zu erfüllen wie Auftragnehmer (Art. 28 Abs. 4)
- Auftragstätigkeit bedarf eines **Vertrags** (Art. 28 Abs. 3), der beinhalten muss:
  - Gegenstand & Dauer der Verarbeitung
  - Art & Zweck der Verarbeitung
  - Art der personenbezogenen Daten
  - Kategorien betroffener Personen
  - Pflichten & Rechte der verantwortlichen Stelle
- Vom Auftragnehmer dürfen personenbezogene Daten **nur auf** dokumentierte **Weisung** der verantwortlichen Stelle verarbeitet werden (Art. 28 Abs. 3 lit. a)

Auftragsdatenverarbeitung nach EU-DS-GVO (2)

- Ausführende Personen müssen **auf Vertraulichkeit verpflichtet** sein (Art. 28 Abs. 3 lit. b)
- Der Auftragnehmer muss alle erforderlichen **Maßnahmen** nach Art. 32 der EU-DS-GVO ergreifen (Art. 28 Abs. 3 lit. c)
- **Nach Abschluss der Erbringung der Verarbeitungsleistungen** sind alle personenbezogenen **Daten** nach Wahl der verantwortlichen Stelle **zu löschen oder zurückzugeben**, sofern nach geltendem Recht keine Verpflichtung zur Speicherung der Daten besteht (Art. 28 Abs. 3 lit. g)
- Einhaltung genehmigter Verhaltensregeln (nach Art. 40) oder eines genehmigten Zertifizierungsverfahrens nach (Art. 42) kann nach Art. 28 Abs. 5 als **Nachweis hinreichender Garantien** herangezogen werden

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/)

Privacy by Design / Default

- Nach Art. 25 Abs. 1 der EU-DS-GVO sind **Datenschutzgrundsätze** wie etwa Datenminimierung **wirksam umzusetzen** und die notwendigen **Garantien zur Einhaltung der EU-DS-GVO** in die Verarbeitung aufzunehmen; dabei ist zu berücksichtigen (wie bei allen Maßnahmen)
  - Stand der Technik
  - Implementierungskosten
  - Art, Umfang, Umstände & Zwecke der Verarbeitung
  - sowie die unterschiedliche Eintrittswahrscheinlichkeit & Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen
- Die verantwortliche Stelle hat daher **geeignete technische und organisatorische Maßnahmen** (wie z.B. Pseudonymisierung) zu treffen sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung
- Durch **Voreinstellung** grundsätzlich nur Daten verarbeiten, die für den jeweiligen **bestimmten Verarbeitungszweck erforderlich** sind (Art. 25 Abs. 2)
- Betrifft neben Menge der erhobenen personenbezogenen Daten den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit