

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

Vorlesung im Sommersemester 2017  
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
	Mitarbeiterdatenschutz		Konzeption von IT-Sicherheit

- Begriffsklärung: Daten, personenbezogene Daten & Informationen, Sicherheit, Datensicherung, Datensicherheit
- technische & organisatorische Maßnahmen nach EU-DSGVO
- Datenschutzkonzept
- Standard-Datenschutzmodell
- Risikobasierter Ansatz im Datenschutzrecht:
  - Bestimmung von Datenschutzrisiken
  - Datenschutz-Folgenabschätzung nach der EU-DSGVO
  - Privacy Impact Assessment
  - Datenschutzrisiken bei der Auftragsverarbeitung
- Privacy by Design / Default

# Daten vs. Informationen

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

→ **Lösung:** Festlegung von Definitionen!

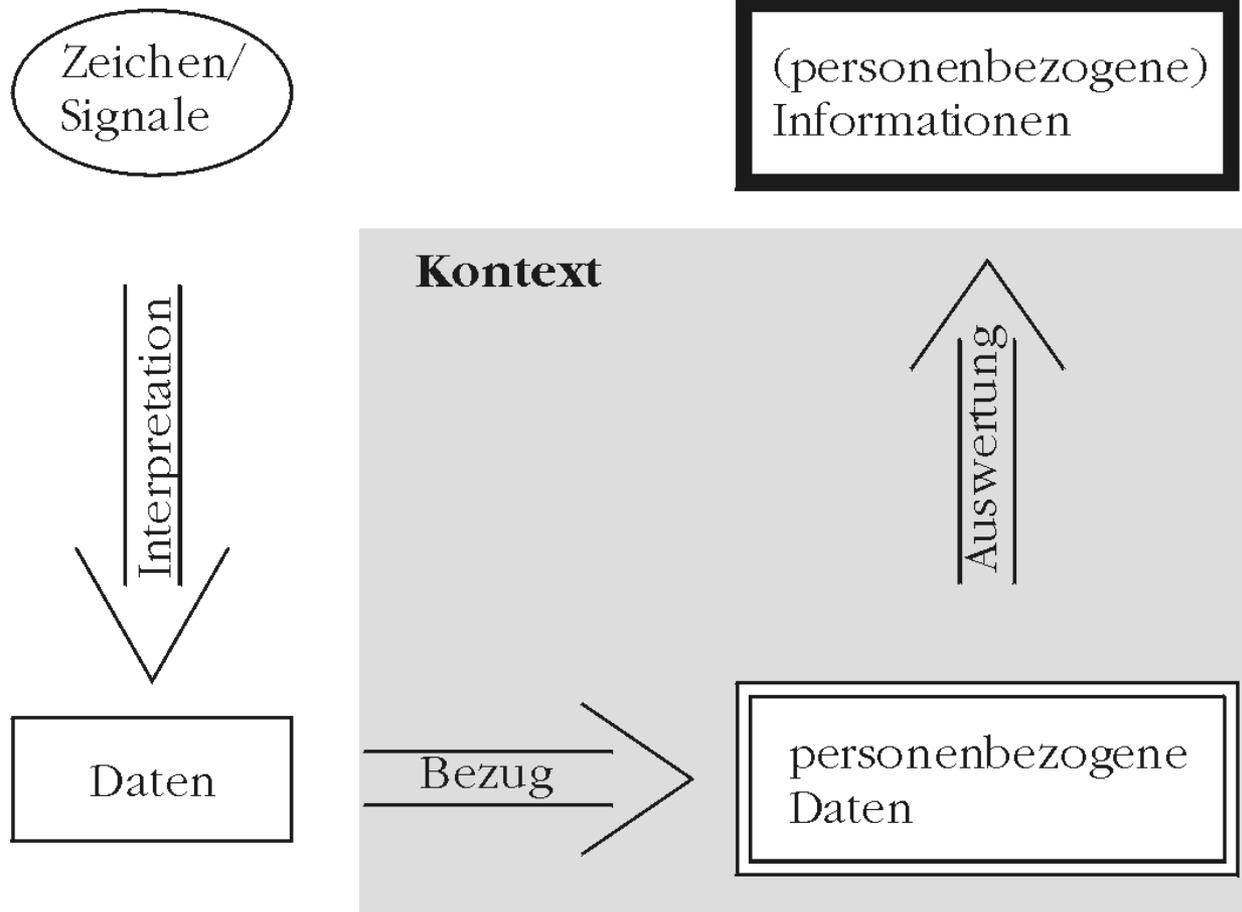
## **Definition 2: Daten**

kontextfreie Angaben, die aus interpretierten Zeichen bzw. Signalen bestehen

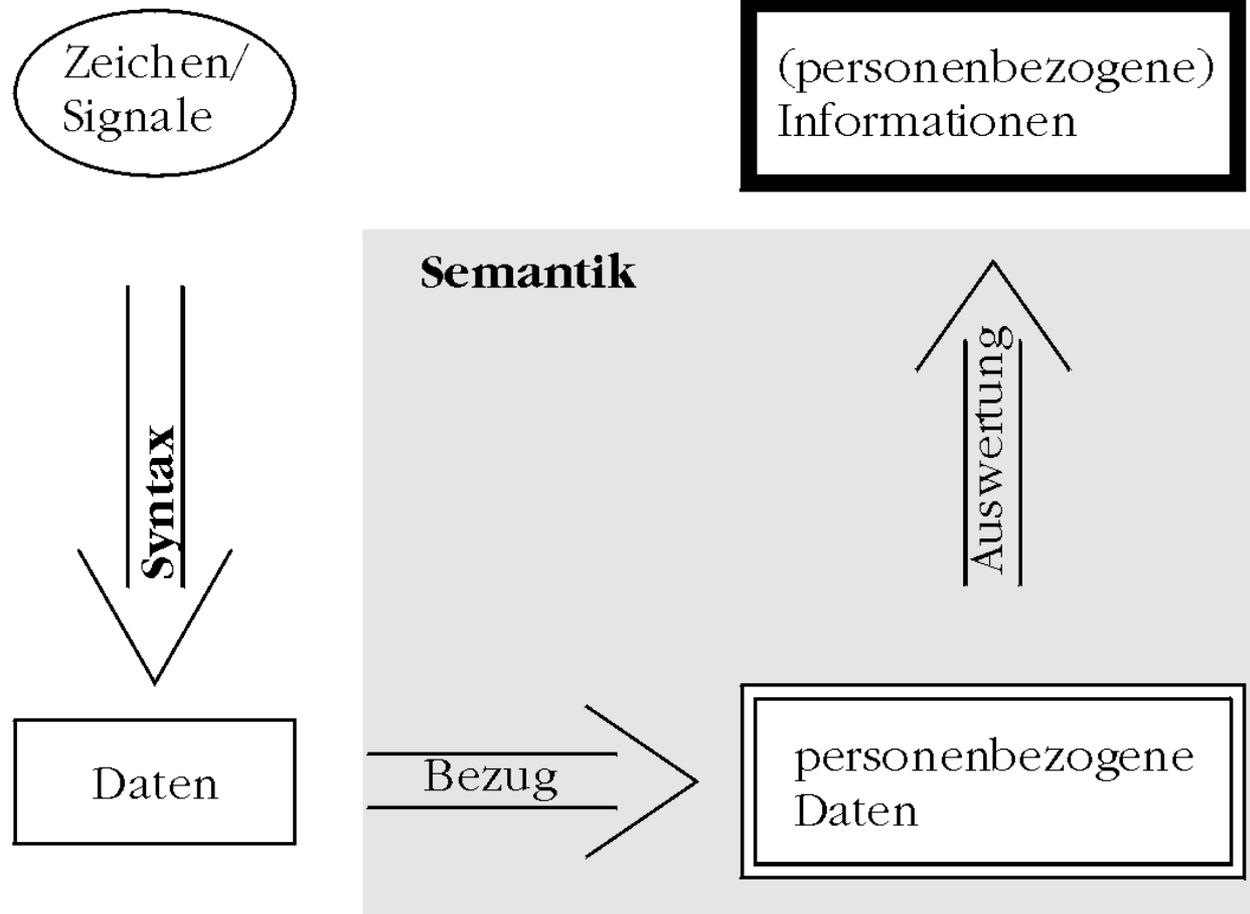
## **Definition 3: Informationen**

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**

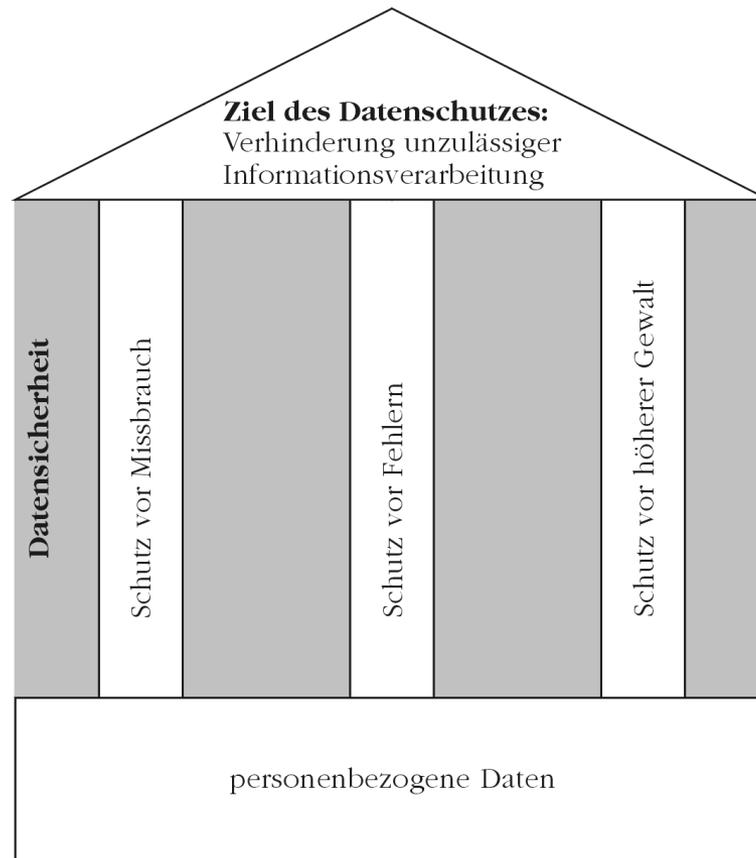
Maßnahmen zur Aufrechterhaltung des DV-Systems, der Daten und Datenträger vor Zerstörung oder Verlust

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

## **Definition 6: Datensicherheit**

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

# Zusammenhang zwischen Datensicherheit und Datenschutz



# Schutzvorkehrungen nach der EU-DSGVO (1)

- Nach Art. 32 Abs. 1 der EU-DSGVO 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-DSGVO (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**

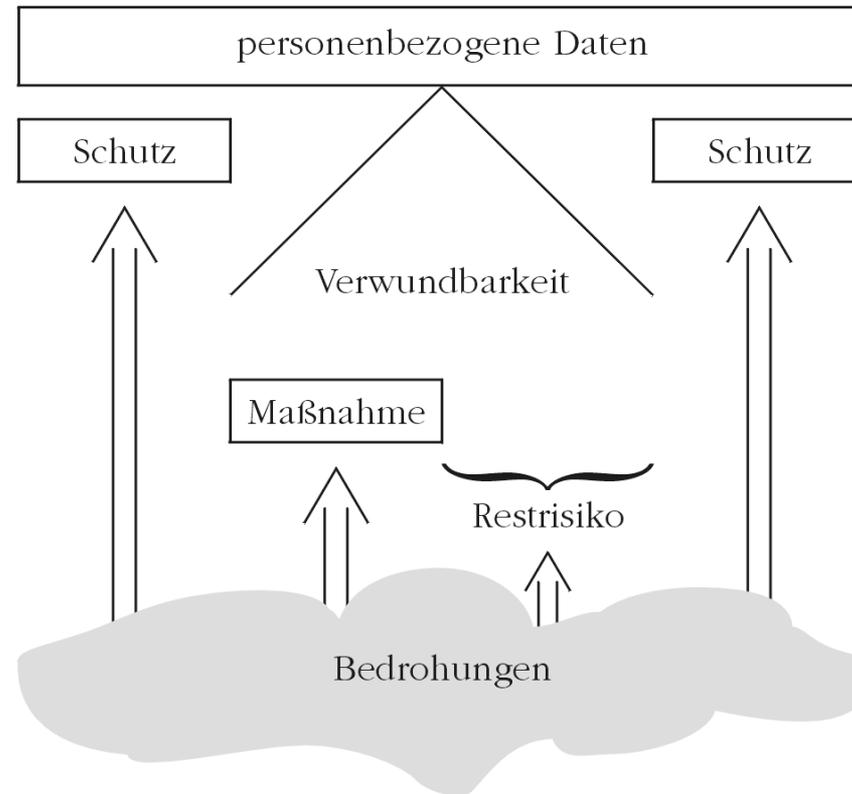
# Schutzvorkehrungen nach der EU-DSGVO (3)

- Nach Art. 32 Abs. 2 der EU-DSGVO 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

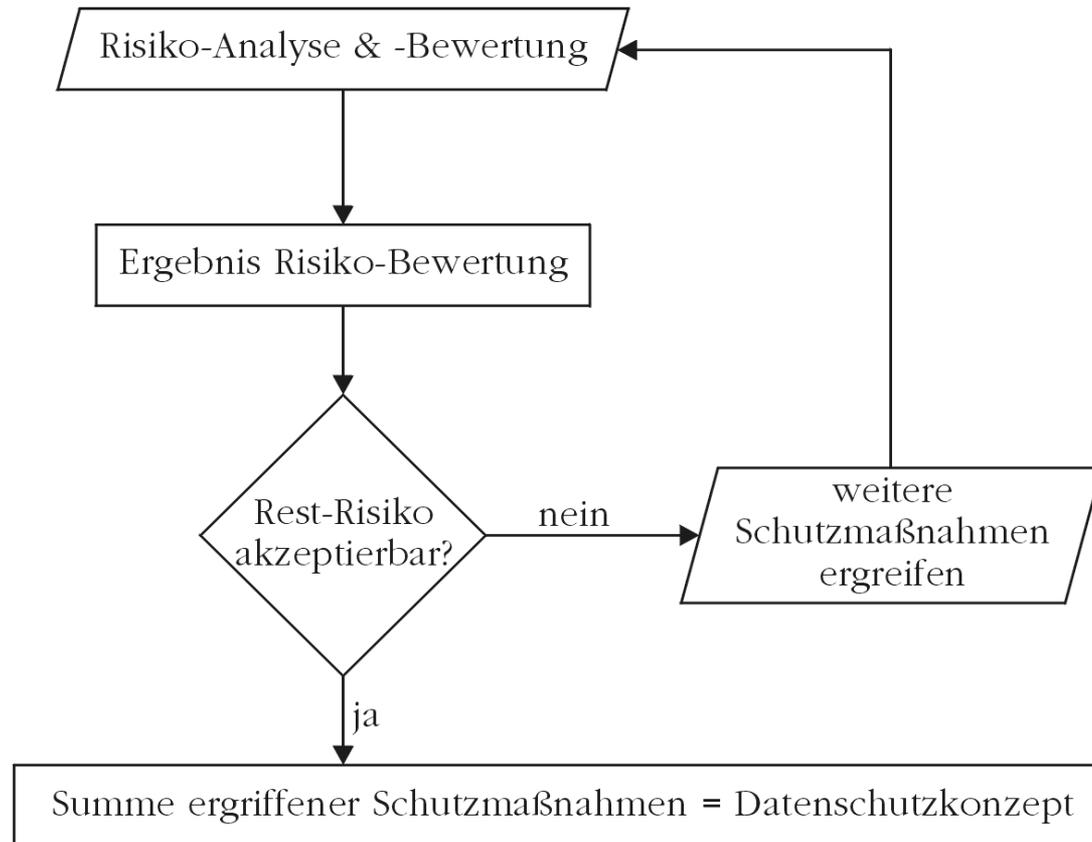
# Gewährleistungsziele nach Standard-Datenschutzmodell

- 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.

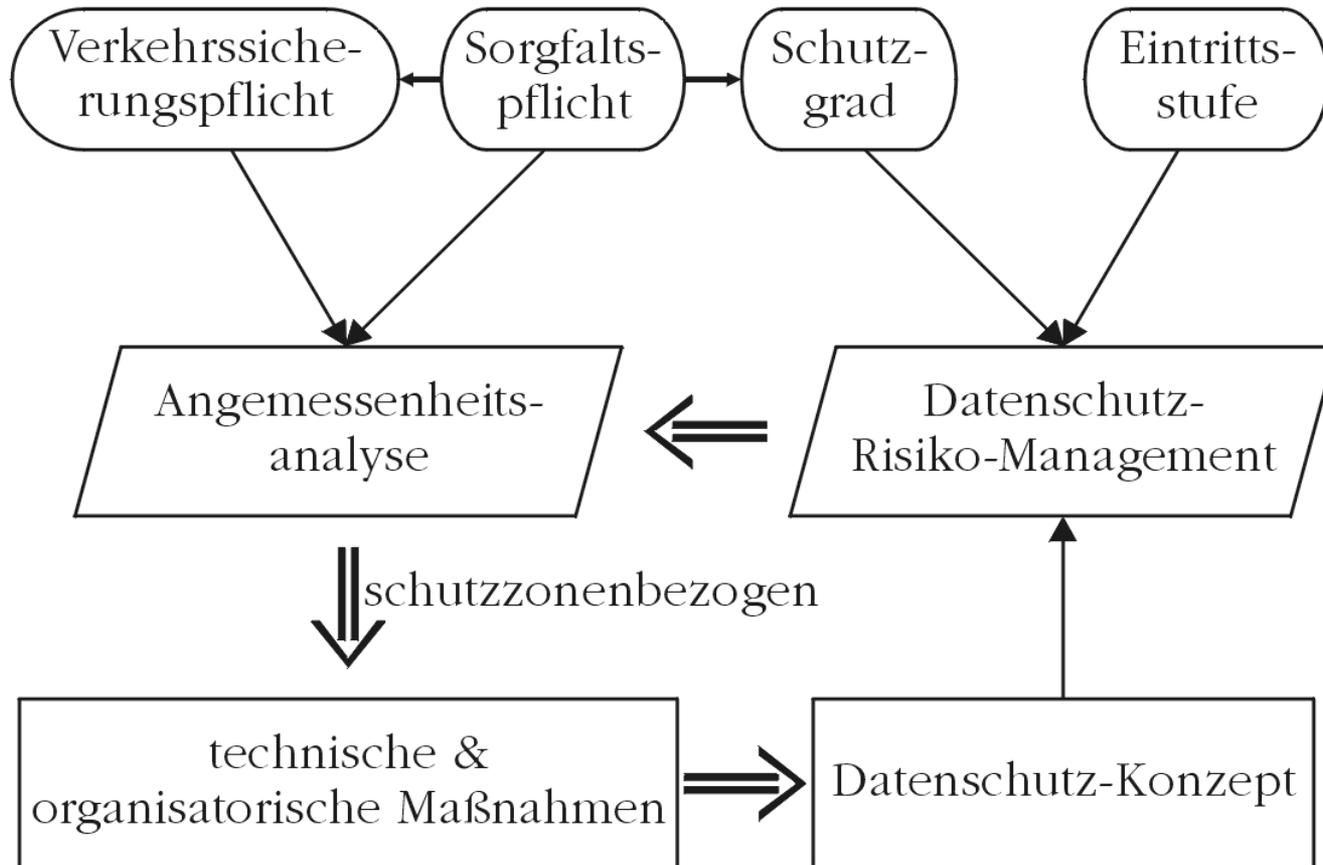
# Ziel der technischen & organisatorischen Maßnahmen (1)



# Ziel der technischen & organisatorischen Maßnahmen (2)



# Datenschutzkonzept als Sammlung der Schutzvorkehrungen



# Risikobasierter Ansatz im Datenschutzrecht (1)

Im Rahmen der EU-DSGVO gilt:

- **Verstöße gegen Pflichten** der verantwortlichen Stelle bzw. des Auftragnehmers sind nach Art. 83 Abs. 4 lit. a der EU-DSGVO 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 bußgeldbewährt!**

# Risikobasierter Ansatz im Datenschutzrecht (2)

Im Rahmen der EU-DSGVO gilt:

- Folgende Verstöße sind nach Art. 83 Abs. 5 der EU-DSGVO 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 bußgeldbewährt!**
- Gleiches gilt für die Nichtbefolgung von Anweisungen der Aufsichtsbehörde

# Risikobasierter Ansatz im Datenschutzrecht (3)

- Bußgeld wird aber 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 von Verletzung des Schutzes personenbezogener Daten** nach Art. 33 EU-DSGVO, sofern die Sicherheit der Verarbeitung
  - unbeabsichtigt (→ versehentlich/fahrlässig) oder
  - unrechtmäßig (→ absichtlich)verletzt wurde (wg. Legaldefinition aus Art. 4 Nr. 12 EU-DSGVO) mit dem Ziel
  - \* Vernichtung personenbezogener Daten (→ Verletzung Verfügbarkeit)
  - \* Verlust personenbezogener Daten (→ Verletzung Verfügbarkeit)
  - \* Veränderung personenbezogener Daten (→ Verletzung Integrität)
  - \* unbefugte Offenlegung von personenbezogenen Daten (→ Verletzung Vertraulichkeit)
  - \* unbefugter Zugang zu personenbezogenen Daten (→ Verletzung Vertraulichkeit)→ erhöht die Wahrscheinlichkeit für Fremdkontrolle durch Aufsichtsbehörde  
→ Meldung entfällt, wenn kein Risiko für Rechte & Freiheiten natürlicher Person

# Risikobasierter Ansatz im Datenschutzrecht (4)

- **Meldung** von Verletzungen des Schutzes personenbezogener Daten **an betroffene Person**, wenn die Verletzung voraussichtlich (!) ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat (nach Art. 34 Abs. 1 EU-DSGVO)
  - Bei Eintritt einer Verletzung der Sicherheit nach Art. 32 EU-DSGVO ist eine die Gründe der Verletzung berücksichtigende Datenschutz-Folgenabschätzung durchzuführen!
  - Diese Datenschutz-Folgenabschätzung ist auf die individuellen Risiken der Betroffenen abzustellen!
- Meldung nach Art. 34 Abs. 3 EU-DSGVO entbehrlich, wenn
  - geeignete Schutzvorkehrungen zum Zugangsschutz getroffen wurden
  - nachfolgende Schutzvorkehrungen sicherstellen, dass das hohe Risiko aller Wahrscheinlichkeit nach nicht mehr besteht (→ Nachweispflicht!)
  - die Meldung mit einem unverhältnismäßigen Aufwand verbunden wäre (dann hat aber eine öffentliche Bekanntmachung zu erfolgen!)
- → **Meldung an Betroffene führt zu Reputationsrisiko!**
- → indirekter finanzieller Schaden wahrscheinlich!

# Risikobasierter Ansatz im Datenschutzrecht (5)

- **Risikomanagement im Datenschutz:**
  - **Vorgaben des Gesetzgebers:**
    1. Durchführung Zulässigkeitsprüfung wg. „Verbot mit Erlaubnisvorbehalt“ für jedes Verfahren (aufgrund Art. 5 Abs. 1 lit. a EU-DSGVO)
    2. Durchführung einer Erforderlichkeitsprüfung zu Daten (wg. Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c EU-DSGVO)
    3. Ergreifung erforderlicher Schutzvorkehrungen nach Art. 32 EU-DSGVO (Verletzung von Integrität & Vertraulichkeit aufgrund Art. 5 Abs. 1 lit. f EU-DSGVO besonders folgenreich)
    4. Durchführung der Datenschutz-Folgenabschätzung bei riskanten Verfahren
    5. Durchführung der Auftragskontrolle bei Auftragsverarbeitung
- **Technische & organisatorische Maßnahmen** müssen Schutzgrad der Daten entsprechen (→ Adäquatheit) und angemessen sein (→ Wirtschaftlichkeitsprüfung [Implementierungskosten])
  - Zusammenfassung der Maßnahmen = Datenschutzkonzept
  - Stand der Technik in Art. 32 EU-DSGVO ausdrücklich vorgeschrieben

# Datenschutzrisiken (1)

Wahrscheinlichkeit	3			<b>Handeln!</b>
	2		<b>Prüfen!</b>	
	1	<b>Passt!</b>		
	Schaden	1	2	3

## Wahrscheinlichkeit:

Eintritt einer Verletzung des Schutzes personenbezogener Daten

1 = möglich (erfordert aber hohen Mitteleinsatz)

2 = wahrscheinlich

3 = sicher (Kompromittierung leicht durchführbar)

## Schaden:

Grad der Verletzung des Schutzes personenbezogener Daten

1 = niedrig (ohne direkte Wirkung)

2 = mittel (formaler Verstoß)

3 = hoch (Bußgeld/Meldepflicht)

# Datenschutzrisiken (2)

Nach Erwägungsgrund 75 sind hinsichtlich der **Schäden** relevant:

- Physische Schäden
- Materielle Schäden
- Immaterielle Schäden

Von einem Schaden ist auszugehen,

- wenn die Verarbeitung zu
  - einer Diskriminierung (→ immaterieller Schaden)
  - einem Identitätsdiebstahl oder -betrug (→ materieller oder immaterieller Schaden)
  - einem finanziellen Verlust (→ materieller Schaden)
  - einer Rufschädigung (→ immaterieller Schaden)
  - einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten (→ immaterieller Schaden)
  - der unbefugten Aufhebung der Pseudonymisierung (→ immaterieller Sch.)
  - oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen (→ materieller oder immaterieller Schaden)

führen kann

# Datenschutzrisiken (3)

Von einem Schaden ist auszugehen, (1. Fortsetzung)

- wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren,
- wenn personenbezogene Daten (nach Art. 9 EU-DSGVO) verarbeitet werden, aus denen
  - die rassische oder ethnische Herkunft,
  - politische Meinungen,
  - religiöse oder weltanschauliche Überzeugungen
  - oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen,
  - und genetische Daten,
  - Gesundheitsdaten
  - oder das Sexualleben
  - bzw. strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen betreffende Daten (nach Art. 10 EU-DSGVO) verarbeitet werden

# Datenschutzrisiken (4)

Von einem Schaden ist auszugehen, (2. Fortsetzung)

- wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die
  - die Arbeitsleistung,
  - wirtschaftliche Lage,
  - Gesundheit,
  - persönliche Vorlieben oder Interessen,
  - die Zuverlässigkeit
  - oder das Verhalten,
  - den Aufenthaltsort oder Ortswechsel betreffen,analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen,
- wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden
- oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

# Datenschutz-Folgenabschätzung nach EU-DSGVO (1)

- Nach Art. 35 Abs. 1 der EU-DSGVO 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 der EU-DSGVO 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

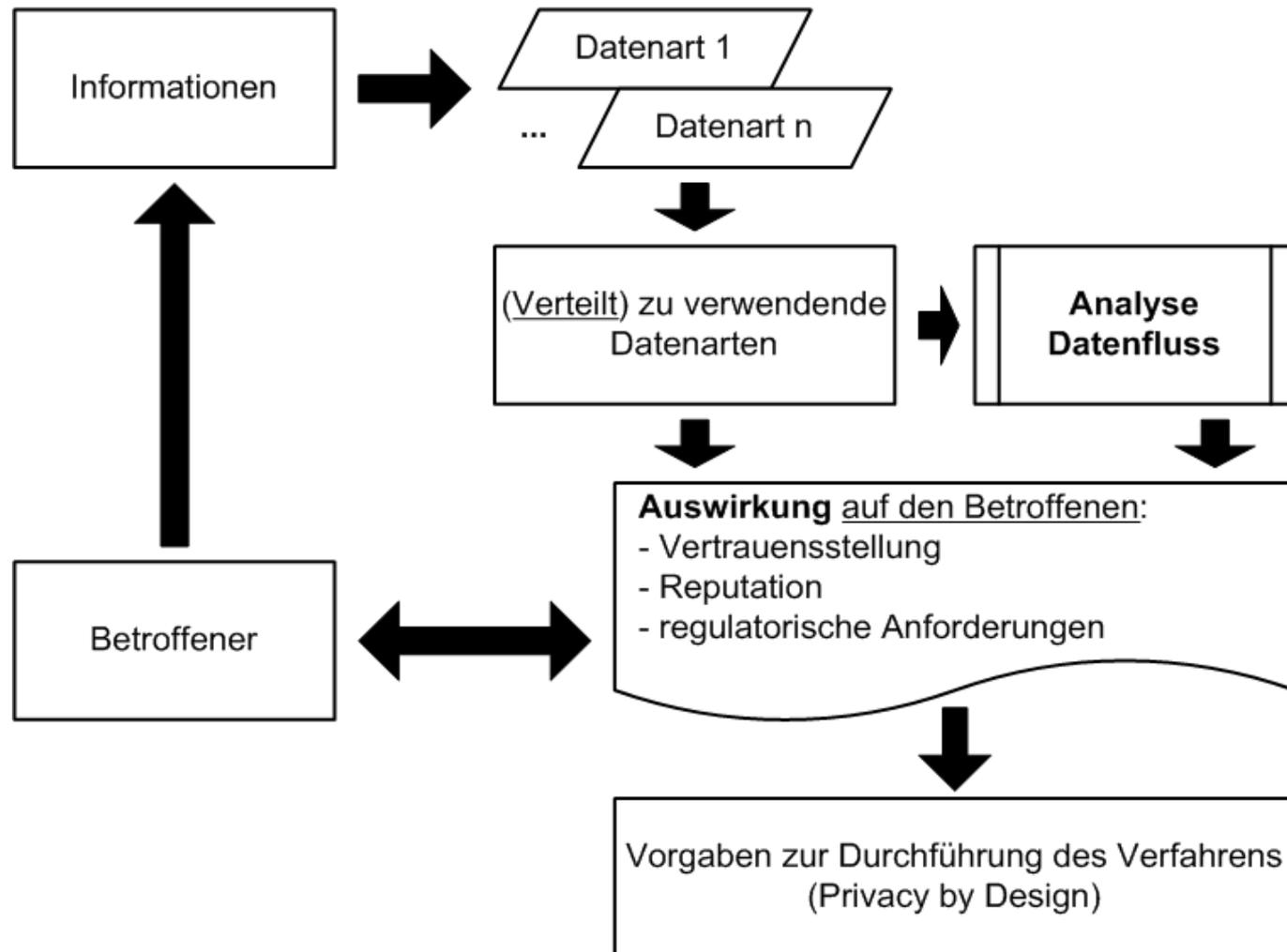
# Datenschutz-Folgenabschätzung nach EU-DSGVO (2)

- Nach Art. 35 Abs. 7 der EU-DSGVO 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-DSGVO**
- Zur Datenschutz-Folgenabschätzung ist ggf. der **Standpunkt des Betroffenen** zur beabsichtigten Verarbeitung einzuholen nach Art. 35 Abs. 9 EU-DSGVO
- Änderungen bei den Risiken führen nach Art. 35 Abs. 11 EU-DSGVO 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 kurz vor Veröffentlichung [Ende Juni 2017])
- 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 Verarbeitungsbedingungen (Art. 35)		
	Rechtmäßigkeit	Treu & Glauben	Transparenz	Zweckbindung	Datenminimierung	Speicherbegrenzung	Vertraulichkeit	Integrität	Verfügbarkeit	Belastbarkeit	Wiederherstellbarkeit	Vermeidung technikspezifischer Risiken	Vermeidung zweckbezogener Risiken	Vermeidung datenartenbezogener Risiken
<b>Unterscheidung je nach Verarbeitungsaspekt</b>														
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.

# Auftragsverarbeitung nach EU-DSGVO (1)

- Nach Art. 28 Abs. 1 der EU-DSGVO 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-DSGVO** 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)

# Auftragsverarbeitung nach EU-DSGVO (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-DSGVO 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

# Privacy by Design / Default

- Nach Art. 25 Abs. 1 der EU-DSGVO sind **Datenschutzgrundsätze** wie etwa Datenminimierung **wirksam umzusetzen** und die notwendigen **Garantien zur Einhaltung der EU-DSGVO** 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