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

Vorlesung im Sommersemester 2022

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
✓	Schwerpunktthema: Aktuelles		Konzeption von IT-Sicherheit

- Begriffsklärung: Daten, personenbezogene Daten & Information, Sicherheit, Datensicherung, Datensicherheit
- Ebenen Datenschutzmanagement & Vorgehensmodell nach EU-DSGVO
- technische & organisatorische Maßnahmen nach EU-DSGVO
- Datenschutzkonzept
- Standard-Datenschutzmodell

- Risikobasierter Ansatz im Datenschutzrecht:
  - Bestimmung von Datenschutzrisiken
  - Datenschutz-Folgenabschätzung nach der EU-DSGVO
  - Datenschutzrisiken bei der Auftragsverarbeitung
- Privacy by Design / Default
- Datenschutzverletzung → Übung

Daten vs. Information

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

→**Lösung**: Festlegung von Definitionen!

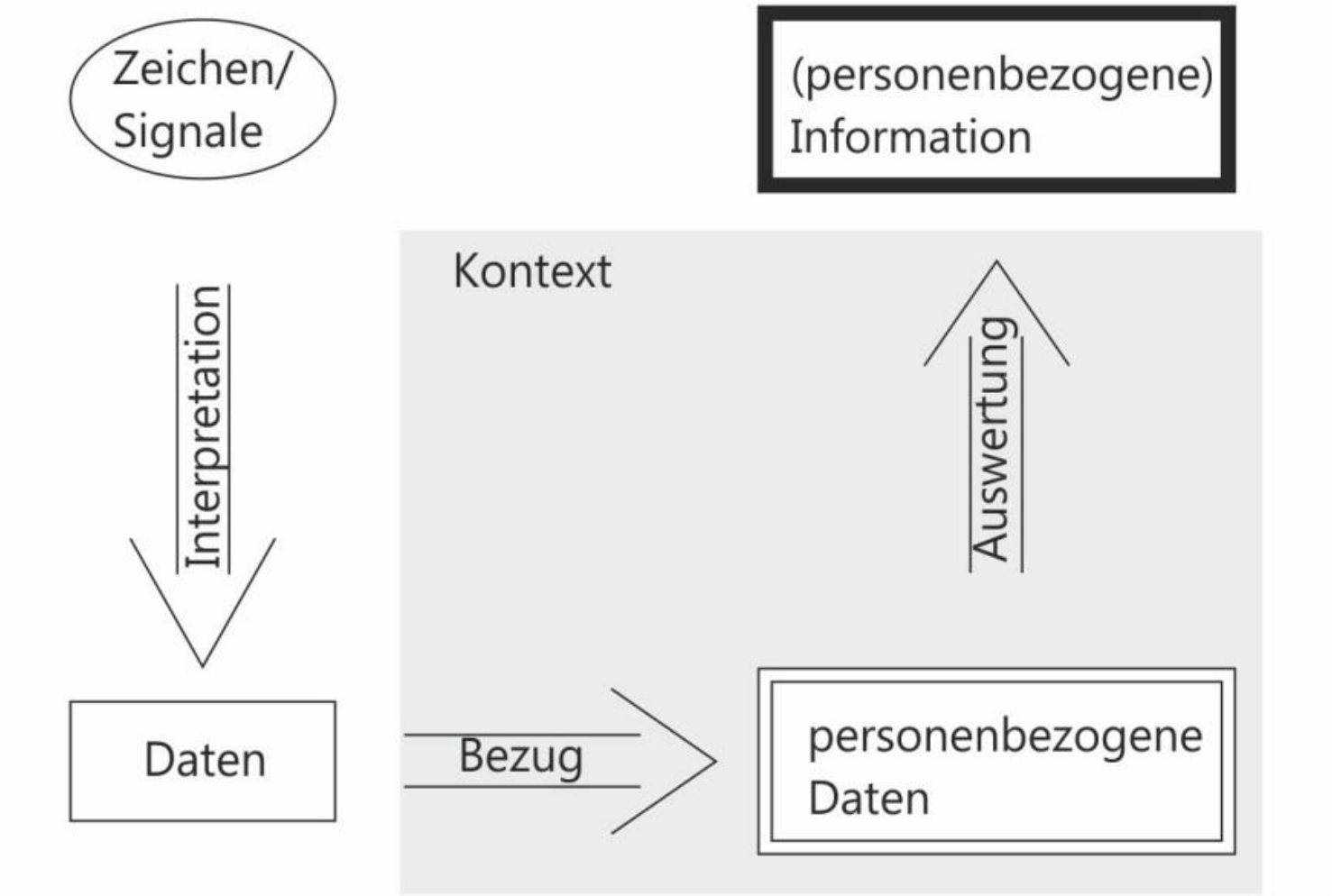
Definition 4: Daten

kontextfreie Angaben, die aus interpretierten Zeichen bzw. Signalen bestehen

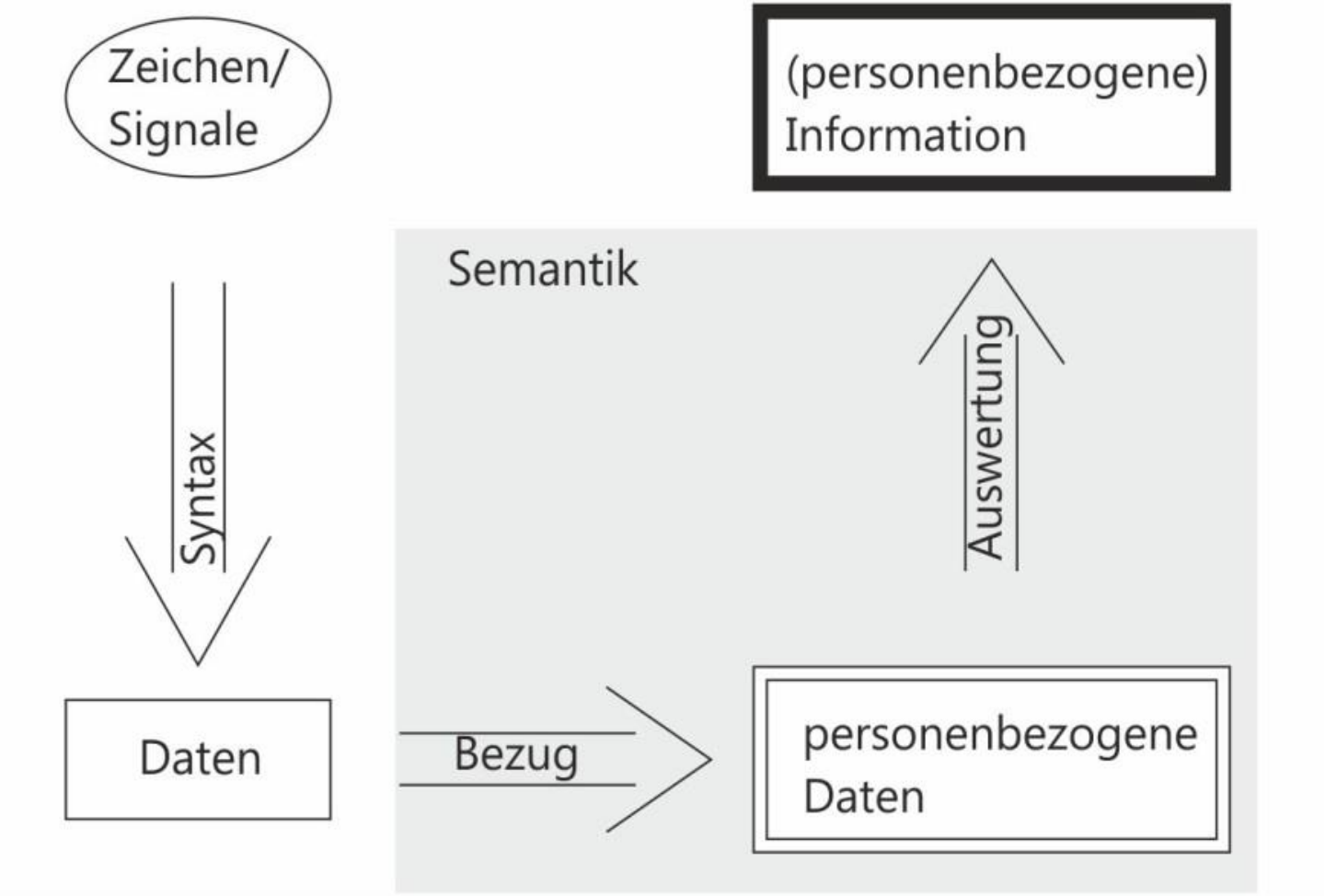
Definition 5: Information

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 6: Sicherheit

Abwesenheit von Gefahren

Definition 7: Datensicherung

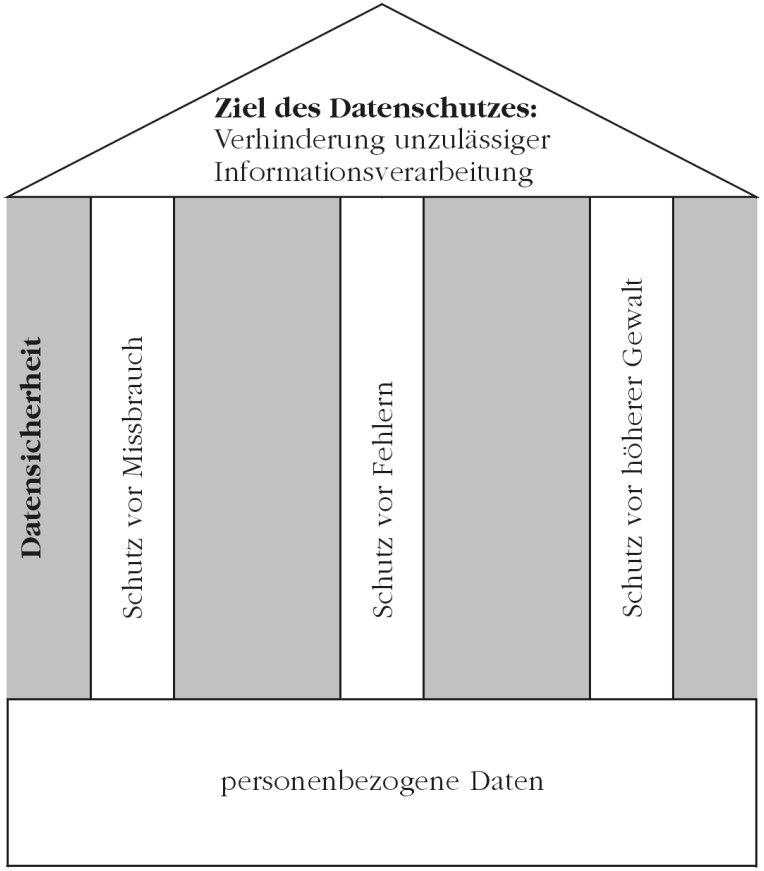
Maßnahmen zur Aufrechterhaltung des DV-Systems, der Daten und Datenträger vor Zerstörung oder Verlust

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

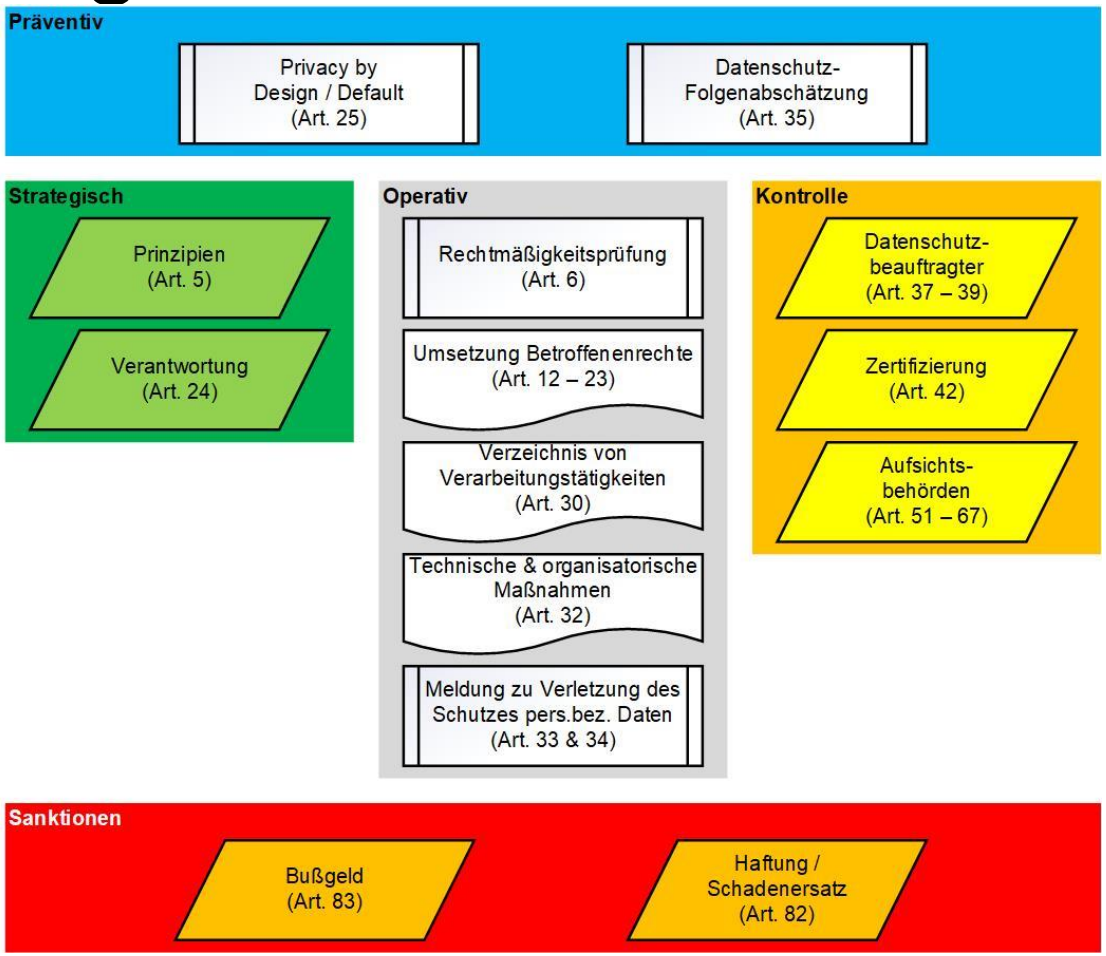
Definition 8: Datensicherheit

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

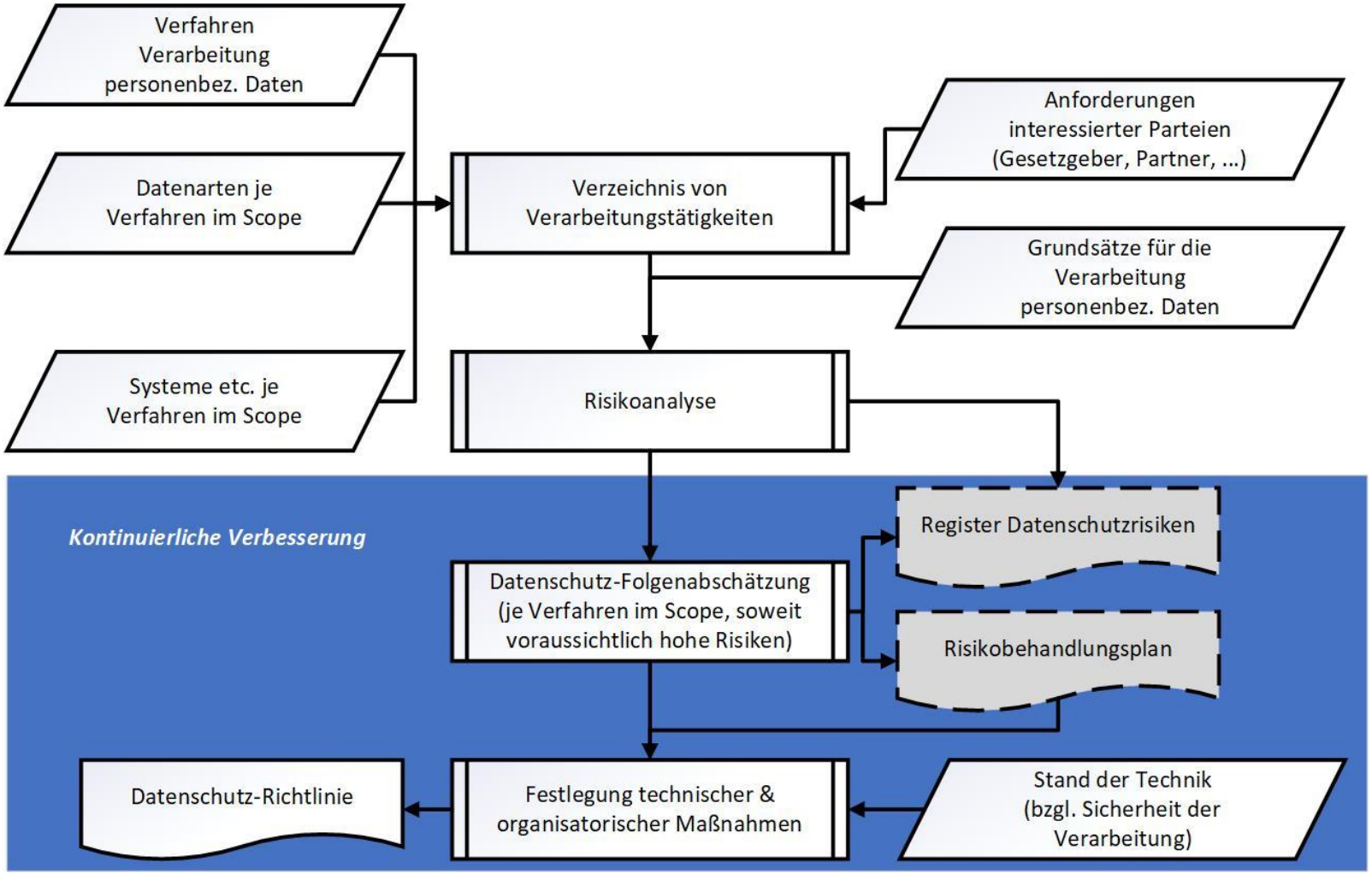
Zusammenhang zwischen Datensicherheit und Datenschutz



Die 5 Ebenen zum Datenschutz-management nach EU-DSGVO



Vorgehensmodell EU-DSGVO



Zertifizierung

Ein von der zuständigen Aufsichtsbehörde nach Art. 42 EU-DSGVO **genehmigtes Zertifizierungsverfahren** kann folgende Nachweise liefern:

- Art. 24 Abs. 3 EU-DSGVO
  → Erfüllung der **Pflichten des Verantwortlichen**
- Art. 25 Abs. 3 EU-DSGVO
  → Erfüllung der Anforderungen zu **Datenschutz durch Technikgestaltung bzw. durch datenschutzfreundlichen Voreinstellung**
- Art. 28 Abs. 5 EU-DSGVO
  → hinreichende Garantien des **Auftragsverarbeiter**s über **Eignung** seiner getroffenen technischen und organisatorischen **Maßnahmen**
- Art. 32 Abs. 3 EU-DSGVO
  → Erfüllung der Anforderungen zur **Sicherheit der Verarbeitung**
- Art. 46 Abs. 2 lit. f EU-DSGVO
  → geeignete Garantien für den **konformen Datentransfer** in Drittstaaten

Derzeit gibt es noch kein genehmigtes Zertifizierungsverfahren in Deutschland! Aber großes Interesse in der Wirtschaft vorhanden!

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**

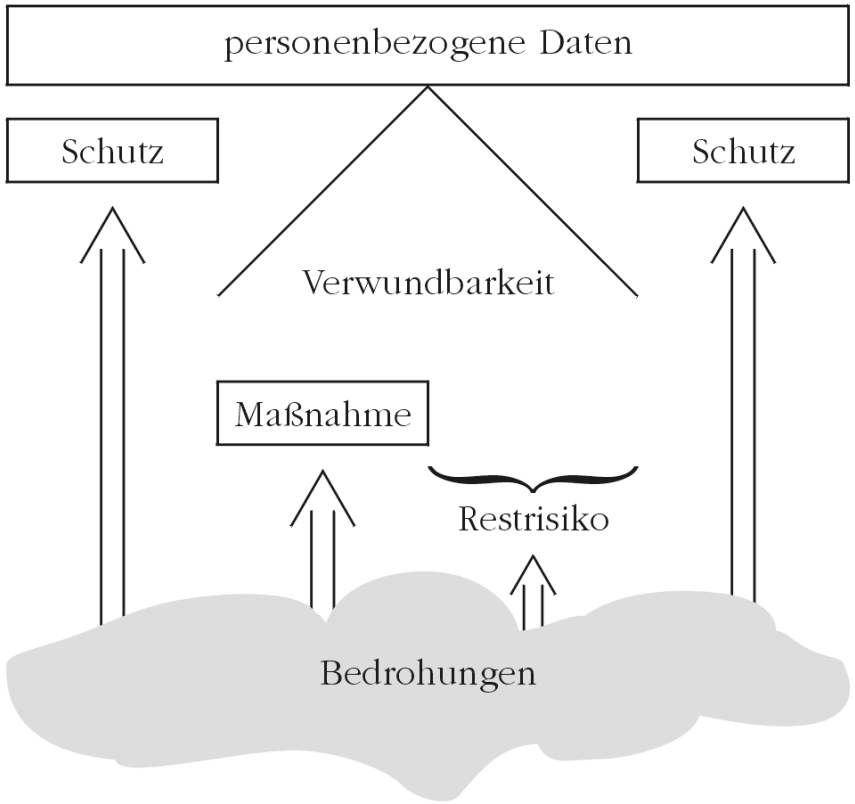
Schutzvorkehrungen nach der EU-DSGVO (3)

- 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

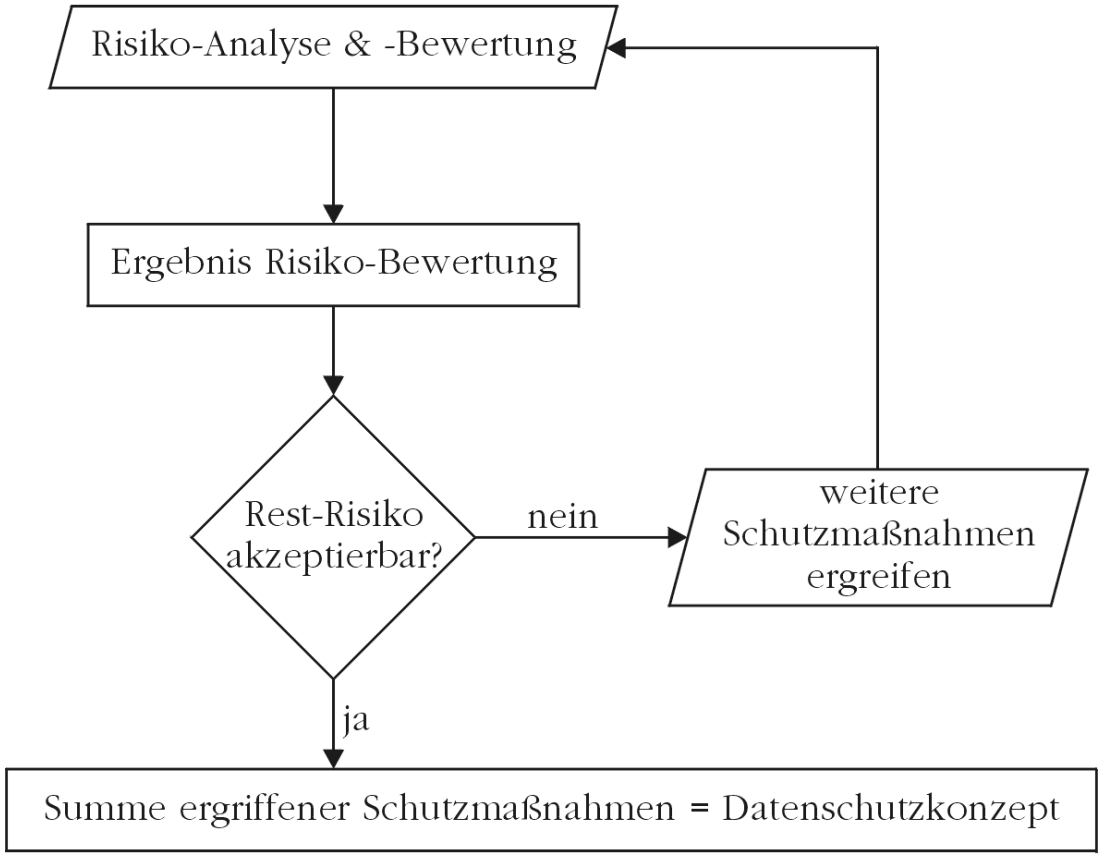
Gewährleistungsziele nach Standard-Datenschutzmodell

- Am 1. Oktober 2015 haben die deutschen Aufsichtsbehörden zum Datenschutz ein Konzept zur Datenschutzberatung und -prüfung auf der Basis **einheitlicher Gewährleistungsziele** entwickelt. 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“ Gewährleistungs-zielen der Datensicherheit, die blauen Gewährleistungsziele sind dagegen am Schutzbedarf von Betroffenen ausgerichtet.
- Version 2.0b aktuell:
  https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/Standard-Datenschutzmodell.html?cms_templateQueryString=standarddatenschutzmodell&cms_sortOrder=score+desc

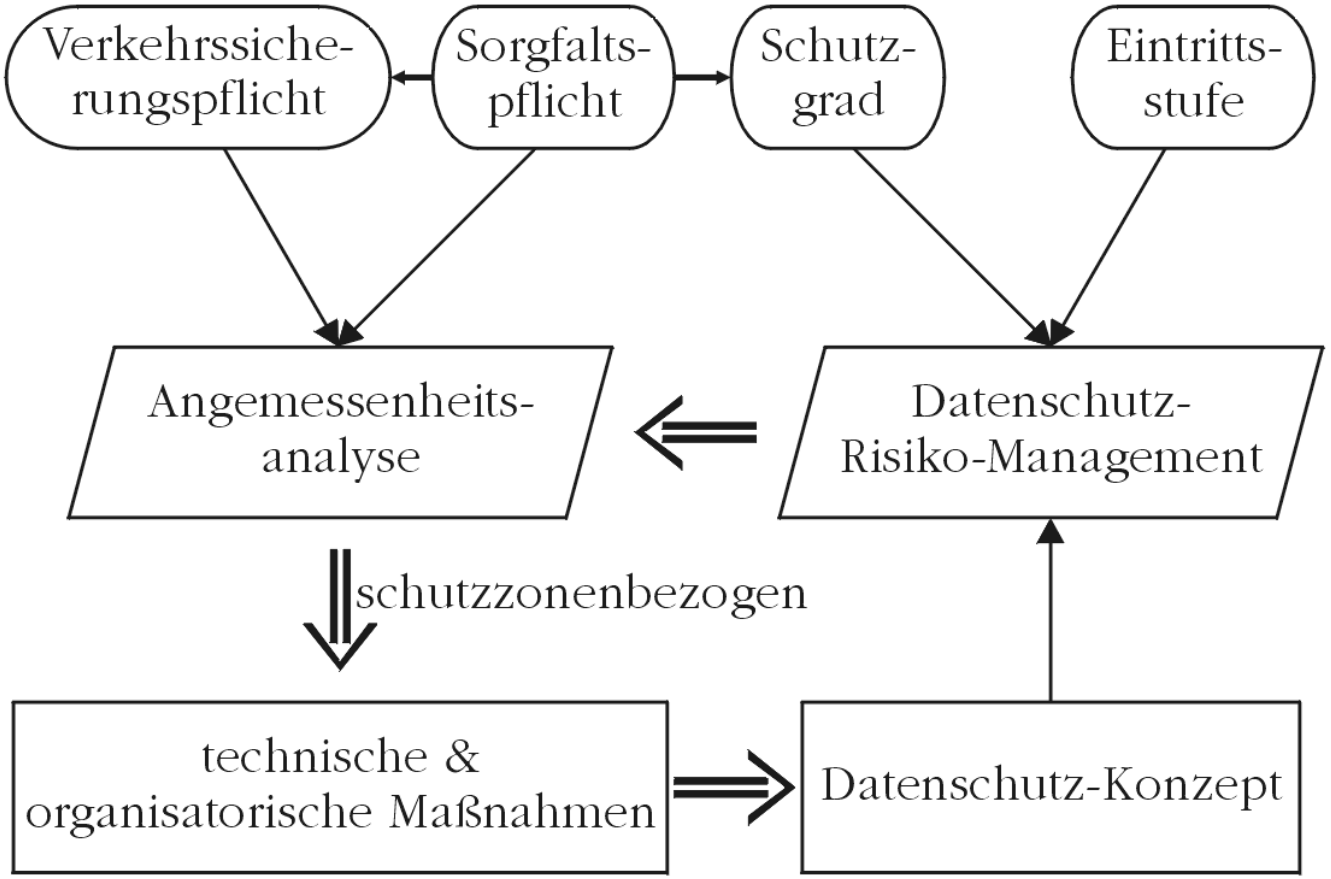
Ziel der technischen & organisatorischen Maßnahmen (1)



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 4 % 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

Risikobasierter Ansatz im Datenschutzrecht (6)

Risikobasierter Ansatz neuer Schwerpunkt im Datenschutzrecht:

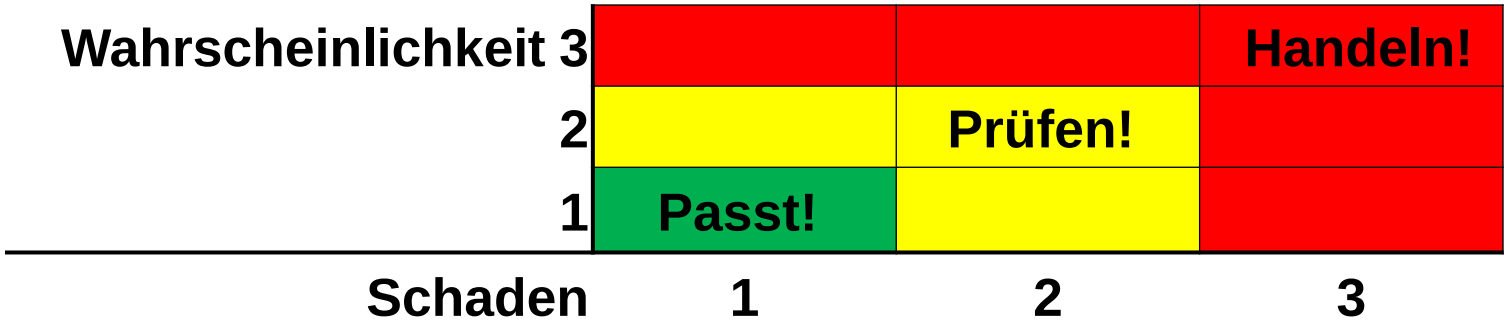
- **Art. 32 Abs. 1 EU-DSGVO**: Maßgebend für das mittels Schutzvorkehrungen (= technische und organisatorische Maßnahmen) erreichte Schutzniveau
- **Art. 33 Abs. 1 EU-DSGVO**: Ab normalem Risiko, d.h. mehr als niedrigem Risiko, ist die Aufsichtsbehörde über eine Verletzung des Schutzes personenbezogener Daten zu informieren
- **Art. 34 Abs. 1 EU-DSGVO**: Ab hohem Risiko müssen Betroffene über eine Verletzung des Schutzes personenbezogener Daten informiert werden
- **Art. 35 Abs. 1 EU-DSGVO**: Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung, sofern die Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko zur Folge hat
- **Art. 35 Abs. 11 EU-DSGVO**: Verpflichtung zur Überprüfung, ob Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird, sofern hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind (dürfte sich dabei vor allem um Steigerungen handeln)

Risikobasierter Ansatz im Datenschutzrecht (7)

Risikobasierter Ansatz neuer Schwerpunkt im Datenschutzrecht: (Fortsetzung)

- **Art. 36 Abs. 1 EU-DSGVO**: Konsultation der Aufsichtsbehörde, sofern bei einer Verarbeitung mit hohem Risiko keine Maßnahmen zur Eindämmung getroffen werden
- **Art. 39 Abs. 2 EU-DSGVO**: Der Datenschutzbeauftragte hat bei seinen Aufgaben die mit den Verarbeitungsvorgängen verbundenen Risiken gebührend Rechnung zu tragen

Datenschutzrisiken (1)



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)
  - unbefugter Aufhebung der Pseudonymisierung (→ immaterieller Schaden)
  - 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 Sicherungsmaßregeln betreffende Daten (nach Art. 10 EU-DSGVO)

  hervorgehen

Datenschutzrisiken (4)

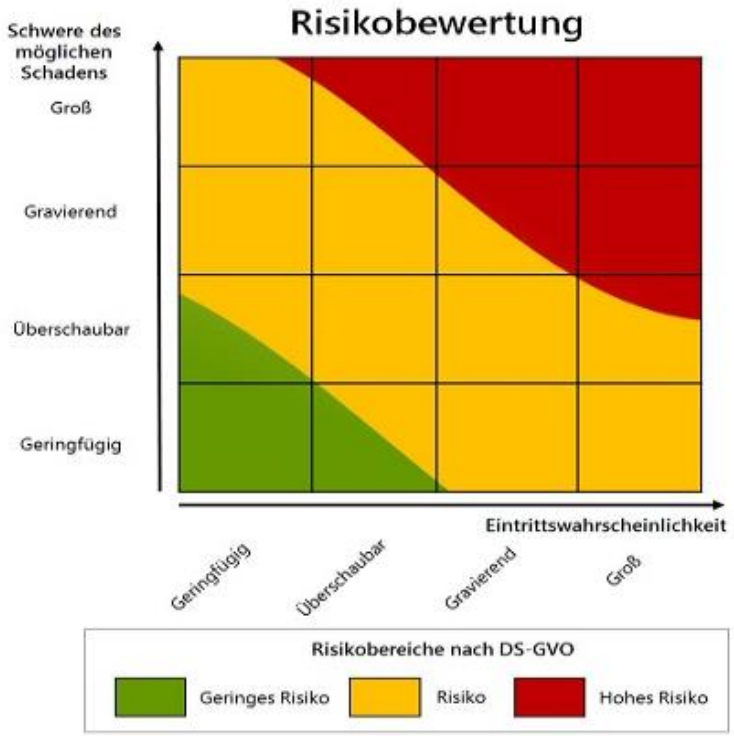
Von einem Schaden ist auszugehen, (2. Fortsetzung)

- 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.

Datenschutzrisiken (5)

Zur Risikobewertung der deutschen Aufsichtsbehörden (siehe DSK Kurzpapier Nr. 18):



Die deutschen Aufsichtsbehörden weichen bei ihrer vorgestellten Methode zur Risikobewertung leider an entscheidender Stelle von gängigen Methoden ab:

- Statt das Risiko als diskrete Funktion zu betrachten (hier mit 4x4 Feldern) weist deren Risikomatrix auf eine kontinuierliche Funktion hin, die es in dieser Form faktisch nicht gibt

Details zum DSK Kurzpapier Nr. 18 unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf

Schönes Beispiel zur Risikobewertung mittels ISO/IEC 29134 dagegen unter https://www.lda.bayern.de/media/04_dsfa_praesentation_baylda_iso29134.pdf

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**

Datenschutz-Folgenabschätzung nach EU-DSGVO (3)

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist			
Nr.	**Maßgebliche Beschreibung der Verarbeitungstätigkeit**	**Typische Einsatzfelder**	**Beispiele**
1	Umfangreiche Verarbeitung von Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, auch wenn es sich nicht um Daten gemäß Art. 9 Abs. 1 und 10 DS-GVO handelt	Betrieb eines Insolvenzverzeichnisses Sozialleistungsträger Große Anwaltssozietät	Ein Unternehmen bietet ein umfassendes Verzeichnis über Privatinsolvenzen an.
2	Umfangreiche Verarbeitung von Daten über den Aufenthalt von Personen	Fahrzeugdatenverarbeitung – Car Sharing / Mobilitätsdienste Fahrzeugdatenverarbeitung – Zentralisierte Verarbeitung der Messwerte oder Bilderzeugnisse von Umgebungssensoren Offline-Tracking von Kundenbewegungen in Warenhäusern, Einkaufszentren o. ä. Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes	Ein Unternehmen bietet einen Car-Sharing-Dienst oder andere Mobilitätsdienstleistungen an und verarbeitet hierfür insbesondere umfangreich Positions- und Abrechnungsdaten. Ein Unternehmen erhebt Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren. Ein Unternehmen verarbeitet die GPS- und WLAN-Daten von Passanten und Kunden, um die Laufwege und das Einkaufsverhalten nachverfolgen zu können.
3	Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Weiterverarbeitung der so zusammengeführten Daten, sofern • die Zusammenführung oder Weiterverarbeitung in großem Umfang vorgenommen werden, • für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den Betroffenen erhoben wurden, • die Anwendung von Algorithmen einschließen, die für die Betroffenen nicht nachvollziehbar sind, und • der Erzeugung von Datengrundlagen dienen, die dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den betroffenen Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen können	Fraud-Prevention-Systeme Scoring durch Auskunfteien, Banken oder Versicherungen	Zur Prävention von Betrugsfällen verarbeitet der Betreiber eines Online-Shops umfassende Datenmengen. Das Ergebnis der Prüfung ist ein Risikowert, der darüber entscheidet, ob einem Käufer der Rechnungskauf als Zahlungsart angeboten wird oder nicht. Eine Auskunftei führt ein Scoring im Hinblick auf die Vertrauenswürdigkeit von Personen durch. Eine Bank führt Scoring durch, um das Ausfallrisiko der Rückzahlungen von Personen zu bestimmen. Eine Versicherung führt ein Scoring durch, um das Risiko einer Person im Hinblick auf bestimmte Eigenschaften oder Aktivitäten der Person zur Bestimmung der Höhe einer Versicherungspolice zu bestimmen.
4	Mobile und für die Betroffenen intransparente optoelektronische Erfassung öffentlicher Bereiche	Fahrzeugdatenverarbeitung – Umgebungssensoren	Ein Unternehmen erhebt Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren.
5	Erfassung und Veröffentlichung von Daten, die zur Bewertung des Verhaltens und anderer persönlicher Aspekte von Personen dienen und von Dritten dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den bewerteten Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen	Betrieb von Bewertungsportalen Inkassodienstleistungen – Forderungsmanagement Inkassodienstleistungen – Factoring	Ein Online-Portal bietet Nutzern die Möglichkeit an, Leistungen von Selbstständigen öffentlich feingranular zu bewerten. Online-Bewertungsportal bspw. für Ärzte, Selbstständige oder Lehrer. Ein Unternehmen verarbeitet für seine Kunden in großem Umfang personenbezogene Daten von Schuldnern, insbesondere Vertragsdaten, Rechnungsdaten und Daten über Vermögensverhältnisse von Schuldnern zur Geltendmachung von Forderungen. Ggf. werden Daten an Auskunfteien übermittelt. Ein Unternehmen lässt sich in großem Umfang Forderungen übertragen um diese auf eigenes Risiko geltend zu machen. Es verbarbeitet hierfür insbesondere Vertragsdaten, Rechnungsdaten, Scoringdaten und Informationen über Vermögensverhältnisse von Schuldnern. Ggf. werden Daten an Auskunfteien übermittelt.
6	Verarbeitung von umfangreichen Angaben über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben, oder diese in andere Weise erheblich beeinträchtigen	Einsatz von Data-Loss-Prevention Systemen, die systematische Profile der Mitarbeiter erzeugen Geolokalisierung von Beschäftigten	Zentrale Aufzeichnung des Internetverlaufs und der Aktivitäten am Arbeitsplatz mit dem Ziel, von Seiten des Verantwortlichen unerwünschtes Verhalten (z.B. Versand interner Dokumente) zu erkennen. Ein Unternehmen lässt Bewegungsprofile von Beschäftigen erstellen (per RFID, Handy-Ortung oder GPS) zur Sicherung des Personals (Wachpersonal, Feuerwehrleute), zum Schutz von wertvollem Eigentum des Arbeitgebers oder eines Dritten (LKW mit Ladung, Geldtransport) oder zur Koordination von Arbeitseinsätzen im Außendienst.
7	Erstellung umfassender Profile über die Interessen, das Netz persönlicher Beziehungen oder die Persönlichkeit der Betroffenen	Betrieb von Dating- und Kontaktportalen Betrieb von großen Sozialen Netzwerken	Ein Webportal erstellt Profile der Nutzer um möglichst passende Kontaktvorschläge zu generieren.
8	Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Weiterverarbeitung der so zusammengeführten Daten, sofern • die Zusammenführung oder Weiterverarbeitung in großem Umfang vorgenommen werden, • für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den Betroffenen erhoben wurden, • die Anwendung von Algorithmen einschließen, die	Big-Data-Analyse von Kundendaten, die mit Angaben aus Drittquellen angereichert wurden	Eine Unternehmen mit umfangreichem Stamm an natürlichen Personen als Kunden, analysiert Daten über das Kaufverhalten der Kunden und die Nutzung der eigenen Webangebote einschließlich des eigenen Webshops, verknüpft mit Bonitätsdaten von dritter Seite und Daten aus der
	für die Betroffenen nicht nachvollziehbar sind, und • der Entdeckung vorher unbekannter Zusammenhänge zwischen den Daten für nicht im Vorhinein bestimmte Zwecke dienen		Werbeansprache über soziale Medien einschließlich der vom Betreiber des sozialen Medium bereitgestellten Daten über die angesprochenen Mitglieder, um Informationen zu gewinnen, die zur Steigerung des Umsatzes eingesetzt werden können.
9	Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der Betroffenen	Telefongespräch-Auswertung mittels Algorithmen	Ein Callcenter wertet automatisiert die Stimmungslage der Anrufer aus.
10	Nicht bestimmungsgemäße Nutzung von Sensoren eines Mobilfunkgeräts im Besitz der Betroffenen oder von Funksignalen, die von solchen Geräten versandt werden, zur Bestimmung des Aufenthaltsorts oder der Bewegung von Personen über einen substantiellen Zeitraum	Offline-Tracking von Kundenbewegungen in Warenhäusern, Einkaufszentren o. ä. Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes	Ein Unternehmen verarbeitet die GPS- und WLAN-Daten von Passanten und Kunden, um die Laufwege und das Einkaufsverhalten nachverfolgen zu können.
11	Automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit der Betroffenen	Telefongespräch-Auswertung mittels Algorithmen	Ein Callcenter wertet automatisiert die Stimmungslage der Anrufer aus.
12	Erhebung personenbezogener Daten über Schnittstellen persönlicher elektronischer Geräte, die nicht gegen ein unbefugtes Auslesen geschützt sind, das die Betroffenen nicht erkennen können	Einsatz von RFID/NFC durch Apps oder Karten	Eine Bank setzt die NFC-Technologie bei Geldkarten ein, um den Zahlungsverkehr zu erleichtern.
13	Erstellung umfassender Profile über die Bewegung und das Kaufverhalten von Betroffenen	Erfassung des Kaufverhaltens unterschiedlicher Personenkreise zur Profilbildung und Kundenbindung unter Zuhilfenahme von Preisen, Preisnachlässen und Rabatten.	Ein Unternehmen verwendet Kundenkarten, welche das Einkaufsverhalten der Kunden erfassen. Als Anreiz zur Verwendung der Kundenkarte erhält der Kunde mit jedem Einkauf Treuepunkte. Mithilfe der gewonnenen Daten erstellt der Anbieter umfassende Kundenprofile.
14	Verarbeitung von Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO – auch wenn sie nicht als „umfangreich" im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist – sofern eine nicht einmalige Datenerhebung mittels Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden.	Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten	Ein Arzt nutzt ein Webportal oder bietet eine App an, um Patienten detailliert und systematisch zu behandeln.
15	Verarbeitung von Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO – auch wenn sie nicht als „umfangreich" im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist – sofern die Daten mittels Sensoren erhoben, an einer zentralen Stelle verarbeitet und dazu verwendet werden, die Leistungsfähigkeit des Betroffenen zu bestimmen	Zentrale Speicherung der Messdaten von Sensoren, die in Fitnessarmbändern oder Smartphones verbaut sind	

Quelle: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorg%C3%A4ngen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf

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 (1)

- 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

Privacy by Design / Default (2)

Vorgaben des Europäischen Datenschutzausschusses vom Oktober 2020:

- Maßnahmen zum **Datenschutz durch Technikgestaltung** müssen
  - demonstriert (!) werden können,
  - robust sein,
  - auch für eine umfangreiche Verarbeitung geeignet sein
  - sowie für die voraussichtliche Einsatzdauer der Verarbeitung und ihrer Bestandteile wie Softwarearchitektur, Prozeduren, Protokolle und darstellbaren Ansichten geeignet sein.
- Beim **Datenschutz durch datenschutzfreundliche Voreinstellung** muss bei einem Verfahren bzw. einer Software ein Startzustand (!) zum Einsatz kommen, der vor allem dem Grundsatz der Datenminimierung Rechnung trägt. Dies betrifft
  - sowohl die Menge (Anzahl als auch Kategorien) personenbezogener Daten
  - als auch den Detaillierungsgrad dieser Daten
  - sowie die Dauer des möglichen Zugriffs auf diese Daten.

Beispiele für entsprechende Schutzvorkehrungen: siehe Übungen!