

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

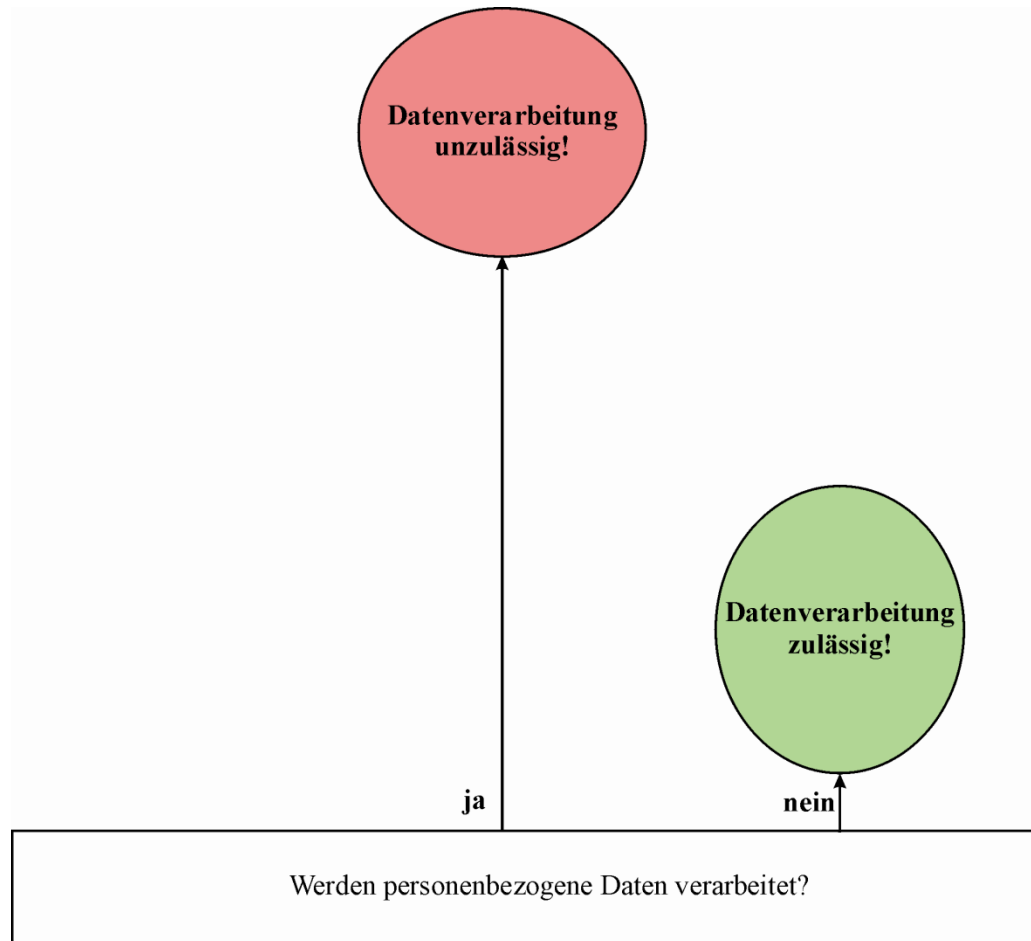
Vorlesung im Sommersemester 2022
an der Universität Ulm
von Bernhard C. Witt

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

- Verbot mit Erlaubnisvorbehalt
- Zweckbindung
- Transparenz
- Datenminimierung & begrenzte Speicherung
- Verhältnismäßigkeit
- Angemessene Sicherheit → Teil 1d
- Betroffenenrechte → Übung
- Abgrenzungen
- Datenschutzkontrolle

Verbot mit Erlaubnisvorbehalt (1)



Grundsatz:

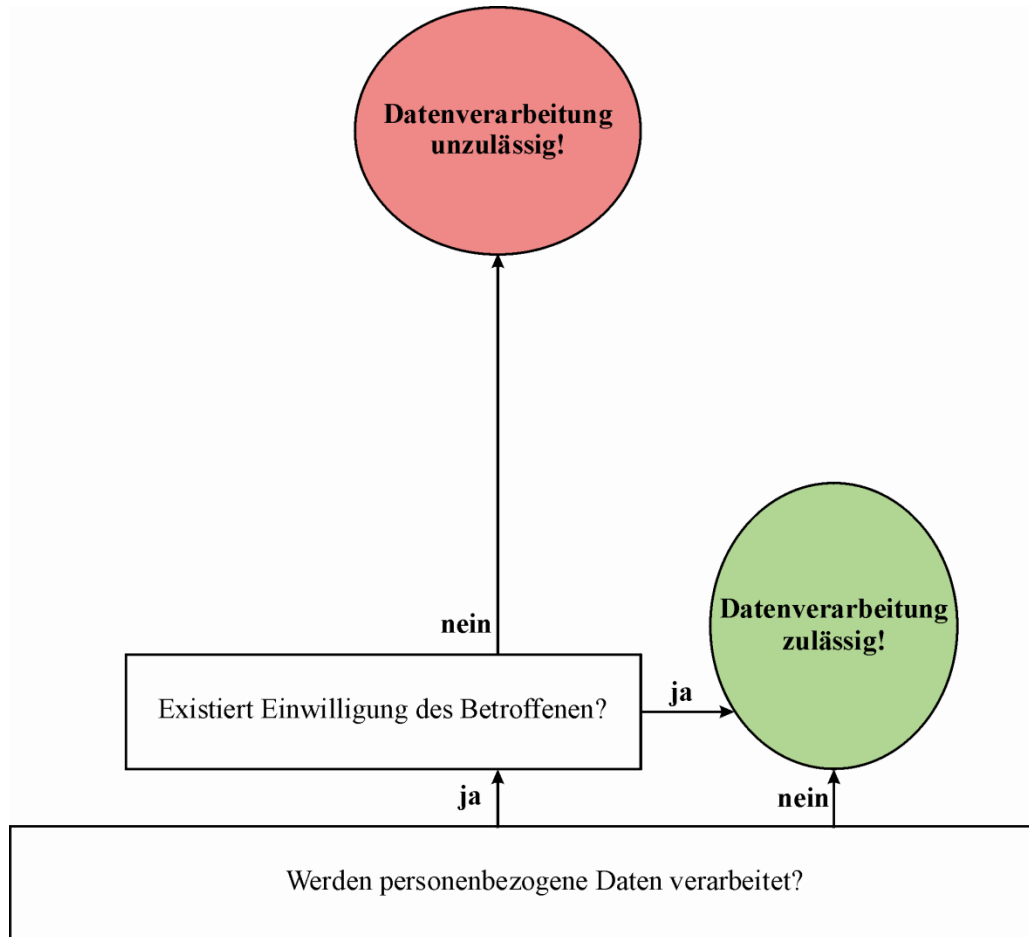
Die Verarbeitung personenbezogener Daten ist grundsätzlich **verboten!**

Eine Gestattung ist jedoch unter Umständen auf Basis von Art. 6 Abs. 1 EU-DSGVO möglich.

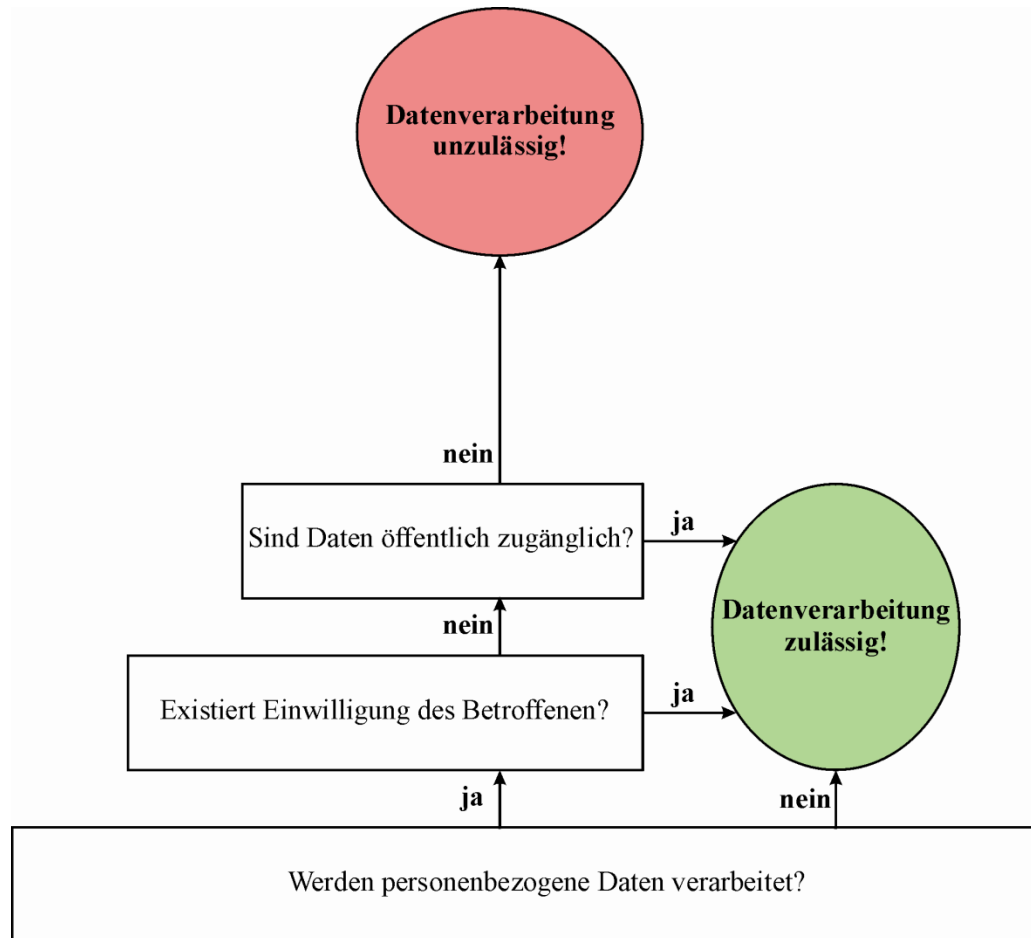
Verbot mit Erlaubnisvorbehalt (2)

Anforderungen an die Einwilligung (Art. 7 EU-DSGVO):

- der Betroffene muss frei entscheiden können (Art. 4 Nr. 11 EU-DSGVO)
- dem Betroffenen muss vorher der Zweck der geplanten Verarbeitung und ggf. Empfänger, etwaige verfolgte berechnigte Interessen & geplante Drittstaatenübermittlung mitgeteilt werden (Art. 13 Abs. 1 EU-DSGVO)
- Einwilligung schriftlich oder konkludent abzugeben (Art. 4 Nr. 11 EU-DSGVO)
- die Einwilligung ist jederzeit widerrufbar (Art. 7 Abs. 3 EU-DSGVO)



Verbot mit Erlaubnisvorbehalt (3)



Öffentliche Quellen:

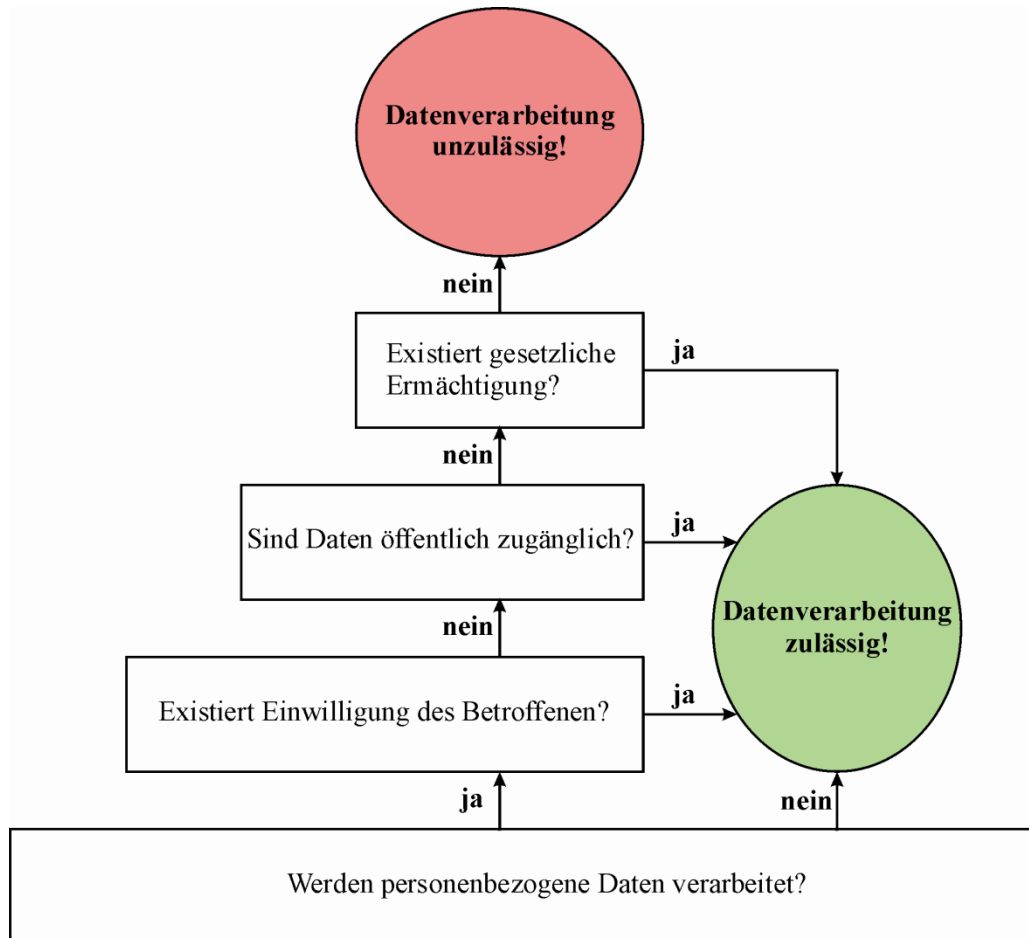
- Adress- und Telefonbücher
- öffentliche Register
- Veröffentlichungen
- Internet (sofern nicht passwortgeschützt)

Verarbeitung nach Art. 6 Abs. 1 lit.

f EU-DSGVO unter Beachtung:

- bei besonderen Kategorien personenbezogener Daten (z.B. Religionszugehörigkeit, Gesundheitsdaten) sind Daten nur öffentlich, wenn sie durch den Betroffenen selbst öffentlich gemacht wurden (Art. 9 Abs. 2 lit. e EU-DSGVO)
- Unzulässig veröffentlichte Daten bleiben unzulässig
- Betroffener über Verarbeitung zu informieren (Art. 14 EU-DSGVO)

Verbot mit Erlaubnisvorbehalt (4)



Gesetzliche Erlaubnis:

- entweder EU-DSGVO selbst
- oder in einer anderen Rechtsvorschrift (Gesetz, Verordnung, Satzung eines autonomen öffentlich-rechtlichen Verbandes mit gesetzlicher Ermächtigung), die verfassungsgemäß (normenklar und verhältnismäßig) ist und nicht gegen die Vorgaben aus der EU-DSGVO verstoßen

→ stellt **Regelfall** dar!

Verbot mit Erlaubnisvorbehalt (5)

Nach Art. 5 Abs. 1 lit. a der EU-DSGVO müssen personenbez. Daten **auf rechtmäßige Weise und nach Treu und Glauben** verarbeitet werden

→ rechtmäßige Weise: im Einklang mit Art. 6 Abs. 1 der EU-DSGVO:

- a) **Einwilligung** des Betroffenen für einen o. mehrere bestimmte Zwecke
- b) Erfüllung eines **Vertrags mit dem Betroffenen** bzw. zur Durchführung vorvertraglicher Maßnahmen auf Anfrage des Betroffenen
- c) Erfüllung einer **rechtlichen Verpflichtung** der verantwortlichen Stelle
- d) **Schutz lebenswichtiger Interessen** des Betroffenen oder einer anderen natürlichen Person
- e) Wahrnehmung einer **öffentlichen Aufgabe**, die der verantwortlichen Stelle übertragen wurde
- f) **Wahrung berechtigter Interessen** der verantwortlichen Stelle oder eines Dritten, sofern nicht die Interessen oder Grundrechte & Grundfreiheiten des Betroffenen zum Schutz personenbezogener Daten überwiegen (→ Abwägung nötig! Nicht auswählbar für Behörden)

→ Treu und Glauben: Vertrauensschutz (erfüllte gegenseitige Erwartung)

Verbot mit Erlaubnisvorbehalt (6)

Nach Art. 9 Abs. 1 der EU-DSGVO ist die **Verarbeitung besonderer Kategorien personenbezogener Daten verboten**, soweit nicht die Ausnahmen aus Art. 9 Abs. 2 der EU-DSGVO greifen

Zu den besonderen Kategorien personenbezogener Daten zählen:

- Daten zur rassischen und ethnischen Herkunft
- Daten über politische Meinungen
- Daten über religiöse oder weltanschauliche Überzeugungen
- Daten über die Gewerkschaftszugehörigkeit
- Genetische Daten
- Biometrische Daten
- Gesundheitsdaten
- Daten zum Sexualleben oder zur sexuellen Orientierung

Verbot mit Erlaubnisvorbehalt (7)

Zulässige **Ausnahmen** für Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 2 der EU-DSGVO:

- a) Ausdrückliche Einwilligung des Betroffenen, soweit Einwilligung gesetzlich nicht verboten ist
- b) Erforderliche Angabe nach Arbeitsrecht, Recht der sozialen Sicherheit bzw. Sozialschutz
- c) Zum Schutz lebenswichtiger Interessen des Betroffenen bzw. einer anderen natürlichen Person, wobei der Betroffene aus körperlichen oder rechtlichen Gründen außerstande für Einwilligung sein muss
- d) Auf Grundlage einer geeigneten Garantie bei Tendenzschutzbetrieb
- e) Vom Betroffenen selbst offensichtlich öffentlich gemachte Daten
- f) Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
- g) Vorgeschiedener Rechtsakt (EU-weit oder in Mitgliedsstaat)
- h) Gesundheitsvorsorge, Arbeitsmedizin, medizinische Diagnostik, Versorgung oder Behandlung im Gesundheits- bzw. Sozialbereich
- i) Öffentliche Gesundheit
- j) Archivierung im öffentlichen Interesse, wissenschaftliche oder historische Forschung bzw. Statistik (unter Berücksichtigung von Art. 89 der EU-DSGVO)

Prinzip der Zweckbindung

- Nach Art. 5 Abs. 1 lit. b der EU-DSGVO müssen personenbezog. Daten für **festgelegte, eindeutige und legitime Zwecke** erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht mehr zu vereinbarenden Weise weiterverarbeitet werden!
- Erfordernis zur **Zweckfestlegung** (Haupt- und Nebenzwecke) bei der Erhebung
- Zweck abhängig von geplanter **Verwendung**
- **Verfahren** (= *festgelegte Art & Weise, wie Tätigkeit / Prozess im Daten-Life-Cycle auszuführen ist*)
im Datenschutzrecht kontextsensitiv/zweckabhängig
→ zweckbezogen verknüpfte Verarbeitungsschritte
- Verarbeitungsschritte unterliegen **Zweckbindung**
- **Zweckänderung** nur bei berechtigtem Interesse unter Abwägung (→ abhängig vom Schutzgrad; muss mit ursprünglichen Zweck aber vereinbar sein!)
- teilweise existiert **besondere Zweckbindung**

Prinzip der Transparenz

- Nach Art. 5 Abs. 1 lit. a der EU-DSGVO müssen personenbezogene Daten in einer für die betroffene Person nachvollziehbare Weise verarbeitet werden!
- Betroffener muss folglich ihn betreffende Verfahren kennen
- **Informationspflicht** bei Direkterhebung beim Betroffenen (Art. 13 der EU-DSGVO)
- **Benachrichtigungspflicht** bei fehlender Direkterhebung, inkl. Angabe, aus welcher Quelle Daten stammen (Art. 14 der EU-DSGVO)
- **Auskunftsrecht** des Betroffenen (Art. 15 der EU-DSGVO)
- **Einwilligung muss** von verantwortlicher Stelle **nachgewiesen werden** (Art. 7 Abs. 1 der EU-DSGVO)
- Es existieren **besondere Informationspflichten** (z.B. bei Verletzung des Schutzes personenbezog. Daten sowie Logik & Tragweite Profiling)
- Anlegen des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 der EU-DSGVO

Verzeichnis von Verarbeitungstätigkeiten

Nach Art. 30 Abs. 1 der EU-DSGVO ist Bestandteil des **Verzeichnisses von Verarbeitungstätigkeiten**:

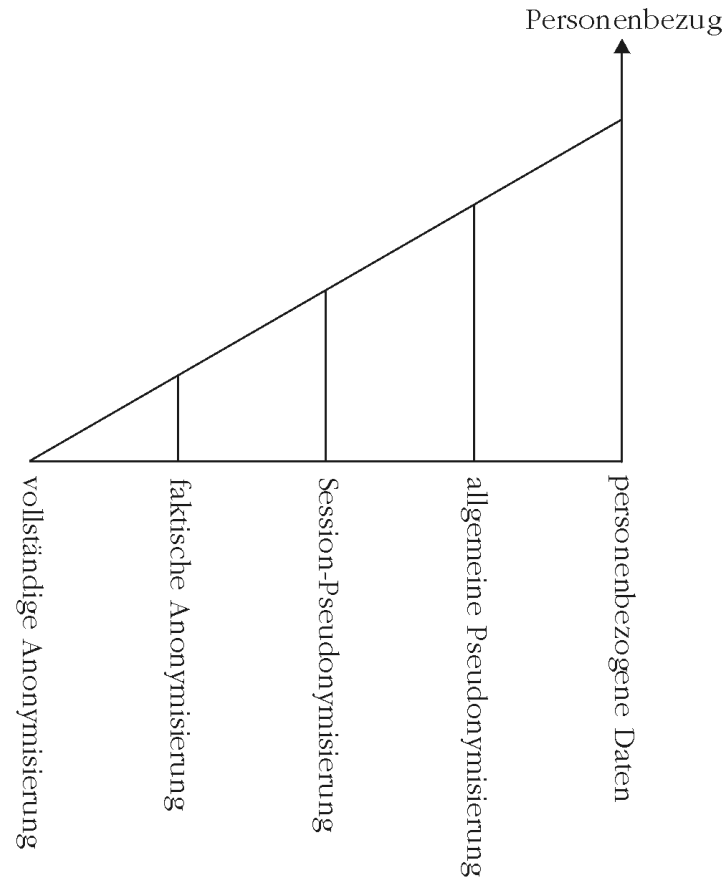
- a) Angaben zur verantwortlichen Stelle und der zugehörigen Kontaktdaten (inkl. Datenschutzbeauftragter)
- b) Zwecke der Verarbeitung
- c) Kategorien der Betroffenen und personenbezogener Daten
- d) Kategorien von Empfänger
- e) Angaben zur Übermittlung in Drittländer oder internationalen Organisationen
- f) Lösungsfristen je Datenkategorie
- g) Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (nach Art. 32 Abs. 1 der EU-DSGVO)

Davon unterliegen a) bis f) den Informationspflichten gegenüber dem Betroffenen; f) im Sinne von geplanter Speicherdauer.

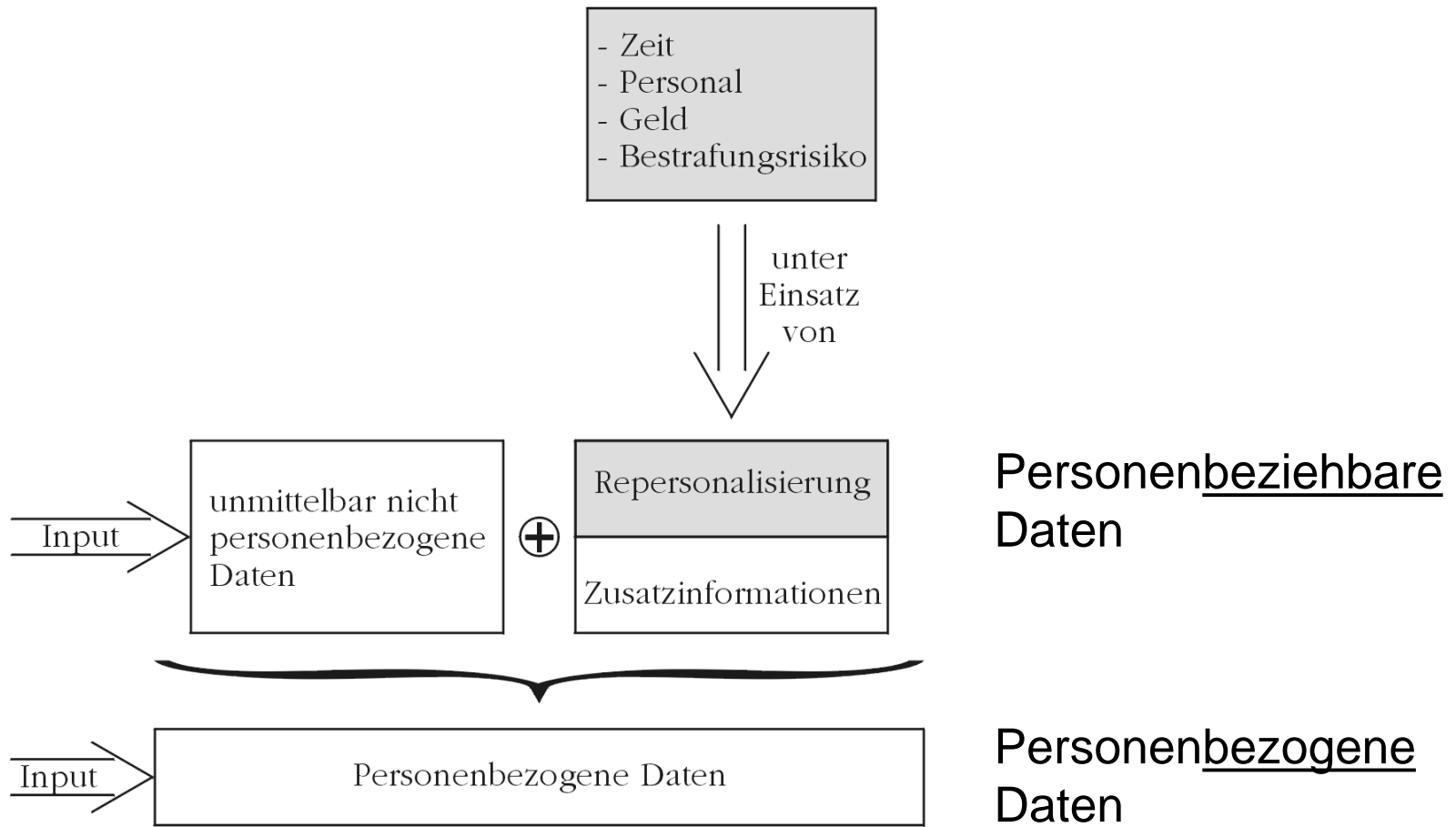
Prinzip der Datenminimierung (1)

- Nach Art. 5 Abs. 1 lit. c EU-DSGVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein
- Anforderung zur **Gestaltung** der eingesetzten IT-Systeme (maßgeblich für privacy by design)
- Verbot **unnötiger Vorratsdatenhaltung**
- **Vermeidung** des Personenbezugs, sofern dieser nicht unbedingt (zur Erfüllung des Verwendungszwecks unmittelbar) erforderlich ist
- Verwendung **datenschutzfreundlicher Techniken**
- Ermöglichung **anonymer** und **unbeobachteter** Nutzung von Telemedien
- Betrifft alle Phasen der automatisierten Verarbeitung

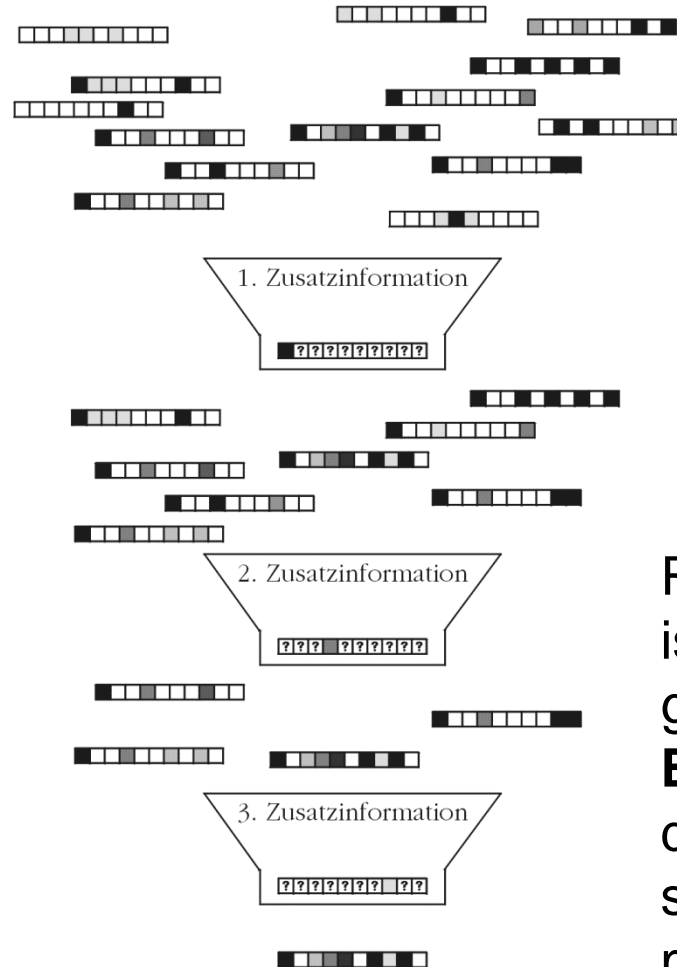
Prinzip der Datenminimierung (2)



Repersonalisierung (1)



Repersonalisierung (2)



Repersonalisierung ist zugleich die größte Gefahr bei **Big Data** aufgrund der zur Verfügung stehenden Datenmenge!

Prinzip der begrenzten Speicherung

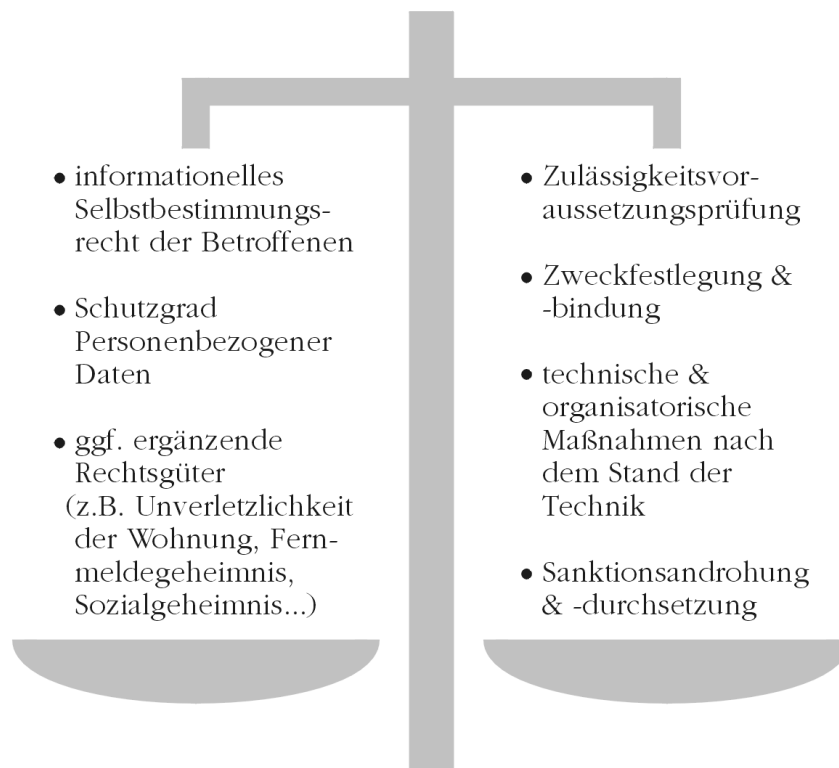
- Nach Art. 5 Abs. 1 lit. e der EU-DSGVO müssen personenbezogene Daten in einer Form gespeichert werden, die die **Identifikation der betroffenen Personen nur so lange** ermöglicht, **wie** es für die Zwecke, für die sie verarbeitet werden, **erforderlich** ist
- An vielen Stellen der EU-DSGVO wird daher ausdrücklich eine Pseudonymisierung der Daten eingefordert:
 - Erleichterung bei Zweckänderung (Art. 6 Abs. 4 lit. e)
 - Einschränkung bei Auskunftsrechten (Art. 12 Abs. 2)
 - Umsetzung von Privacy by Design bzw. by Default (Art. 25)
 - Empfohlene Maßnahme zur Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. a)

Verhältnismäßigkeitsprinzip (1)

- Abstufung zwischen **erforderlich** (um Aufgaben rechtmäßig, vollständig & in angemessener Zeit erfüllen zu können) und **zwingend** (unerlässlich für Aufgabenerfüllung)
- maßgeblich ist der **Einzelfall**
- **geringerer Eingriff** ins informationelle Selbstbestimmungsrecht vorrangig (z.B. mittels Anonymisierung)
- Je **weniger** eine automatisierte Verarbeitung unter **Einfluss** des Betroffenen stattfindet, **desto mehr Gewicht haben** seine **Schutzrechte** bei der Abwägung nach Art. 6 Abs. 1 lit. f EU-DSGVO
- Automatisierte Verarbeitung nach „**Treu und Glauben**“
- Beachtung von **Schutzgraden** & technischem / organisatorischem Ausgleich (**Zumutbarkeit**)
- öffentliche Stelle restriktiver als nicht-öffentliche (da Abwehrrecht statt mittelbarer Wirkung)

Verhältnismäßigkeitsprinzip (2)

- **Eingriffe** in Grundrechte müssen **verhältnismäßig** sein
(= **geeignet, erforderlich & angemessen**)
- **Sonst:**
Schmerzensgeld bei unverhältnismäßiger Videoüberwachung von Beschäftigten:
 - Hess. LAG 2010: 7.000 €
 - LAG Berlin 2012: 14.000 €
 - AG Frankfurt 2013: 3.500 €



Weitere Regelungen zum Datenschutzrecht

- Gewährleistung der **Betroffenenrechte**
[→ Übungen!]
- **Datenschutzkontrolle:**
 - Selbstkontrolle durch Betroffene
 - Eigenkontrolle durch Datenschutzbeauftragte
 - Fremdkontrolle durch Aufsichtsbehörde

Der Datenschutzbeauftragte (1)

Aufgaben von Datenschutzbeauftragten (nach Art. 39 EU-DSGVO):

- **Unterrichtung & Beratung** des Verantwortlichen bzw. Auftragsverarbeiters und der Beschäftigten **über datenschutzrechtliche Pflichten**
 - Schulung der Beschäftigten, die personenbezogene Daten verarbeiten
 - Mitwirkung bei Abschluss von Verträgen, Betriebsvereinbarungen, Policies und Dienstanweisungen, sobald personenbezogene Daten betroffen sind
- **Überwachung** der Einhaltung datenschutzrechtlicher Vorschriften
- Beratung zur und Überwachung der **Datenschutz-Folgenabschätzung**
- **Ansprechpartner** für Aufsichtsbehörde
- **Ansprechpartner** für Betroffene nach Art. 38 Abs. 4 EU-DSGVO
- Übernahme weiterer Aufgaben nach Art. 38 Abs. 6 EU-DSGVO, soweit daraus kein Interessenkonflikt resultiert

Unter Berücksichtigung der mit den Verarbeitungsvorgängen verbundenen Risiken

Der Datenschutzbeauftragte (2)

Anforderungen an Datenschutzbeauftragte:

- Nach Art. 37 Abs. 5 EU-DSGVO wird der Datenschutzbeauftragte benannt auf der Grundlage seiner beruflichen Qualifikation und seines **Fachwissens auf dem Gebiet des Datenschutzes und der Datenschutzpraxis**
- **Fachkunde:** Datenschutzrecht, Datenverarbeitung, betriebliche Organisation, Didaktik, Psychologie [Beschluss des LG Ulm, 1990]
- nur natürliche Person kann bestellt werden

Absicherung des Datenschutzbeauftragten:

- **Frühzeitige Einbindung** in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen (Art. 38 Abs. 1 EU-DSGVO)
- **Unterstützung** durch Unternehmen (Art. 38 Abs. 2 EU-DSGVO)
- **Weisungsfreiheit** (Art. 38 Abs. 3 EU-DSGVO)
- **Keine Benachteiligung** wegen Aufgabenerfüllung (Art. 38 Abs. 3 EU-DSGVO)
- Bericht an höchste Managementebene (Art. 38 Abs. 3 EU-DSGVO)

Der Datenschutzbeauftragte (3)

Typische Tätigkeiten eines Datenschutzbeauftragten:

- Recherchen zur aktuellen Rechtslage (Auswertung aktueller Urteile)
- Lesen & Auswerten zahlreicher & umfangreicher Fachartikel & Fachliteratur
- Vorbereitung von & Teilnahme an & Protokollierung der Meetings (Geschäftsführung, IT-Leitung, Fachverantwortliche)
- Erstellung von Stellungnahmen & Verzeichnis von Verarbeitungstätigkeiten
- Durchführung & Dokumentation von Vor-Ort-Kontrollen & Vertragskontrollen
- Unterstützung bei der Durchführung von Datenschutz-Folgenabschätzungen
- Erstellung & Begutachtung von Sicherheitskonzepten
- Planung & Durchführung von Mitarbeiterschulungen
- Gespräche mit Aufsichtsbehörden

Der Datenschutzbeauftragte (4)

Unerfreuliche Erfahrungen eines Datenschutzbeauftragten:

- komplexe Materie erfordert permanente Erneuerung der Informationsbasis
- verspätete Information (z.B. durch nachzuholende Vorabkontrolle) hat Mehrarbeit & Mehrkosten zur Folge
- Eigenschaft als Miesmacher gegenüber „schöner neuer Welt“
- Abwägungserfordernis führt teilw. zu fehlender Trennschärfe
- Feststellung von Fehlverhalten wichtiger Mitarbeiter & von strukturellen Defiziten
- festgestellte Datenschutzverstöße teilweise Kündigungsgrund von Mitarbeitern
- Durchsicht von Festplatten mit (Kinder-) Pornographie
- Anrufung mit Ziel der Verhinderung arbeitsrechtlicher Aufklärung