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

Vorlesung im Sommersemester 2009
an der Universität Ulm
von Bernhard C. Witt

1. Grundlagen des Datenschutzes

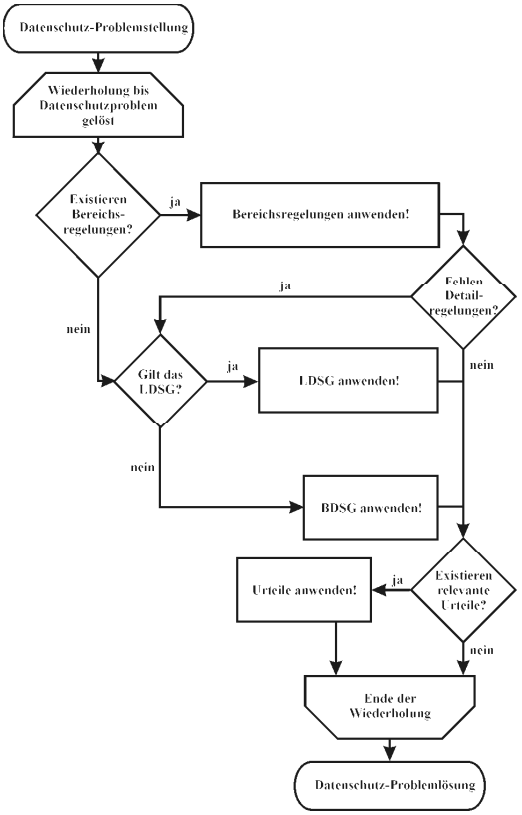
Grundlagen des Datenschutzes		Grundlagen der IT-Sicherheit	
✓	Geschichte des Datenschutzes		Anforderungen zur IT-Sicherheit
➔	Datenschutzrechtliche Prinzipien		Mehrseitige IT-Sicherheit
	Technischer Datenschutz		Risiko-Management
	Schwerpunktthema zur Vertiefung		Konzeption von IT-Sicherheit

- Subsidiarität
- Verbot mit Erlaubnisvorbehalt
- Zweckbindung
- Transparenz
- Vorrang der Direkterhebung
- Verhältnismäßigkeit
- Datensparsamkeit
- Kontrollprinzip vs Lizenzprinzip
- Betroffenenrechte
- Abgrenzungen
- Datenschutzkontrolle

Subsidiaritätsprinzip

resultierend aus der Normenklarheit:

- **bereichsspezifische** Regelungen haben immer **Vorrang** vor allgemeinen Regelungen
- fehlende Regelungen des Bereichsrechts werden durch entsprechende Regelungen des **Allgemeinrechts aufgefangen**
- gesetzliche Regelungen stehen in **Hierarchie** zueinander (ggf. dennoch Verbindung verschiedener Rechtsnormen oder gegenseitige Verdrängung), Lücken werden durch **Richterrecht** geschlossen



Subsidiarität: Anzuwendendes Recht

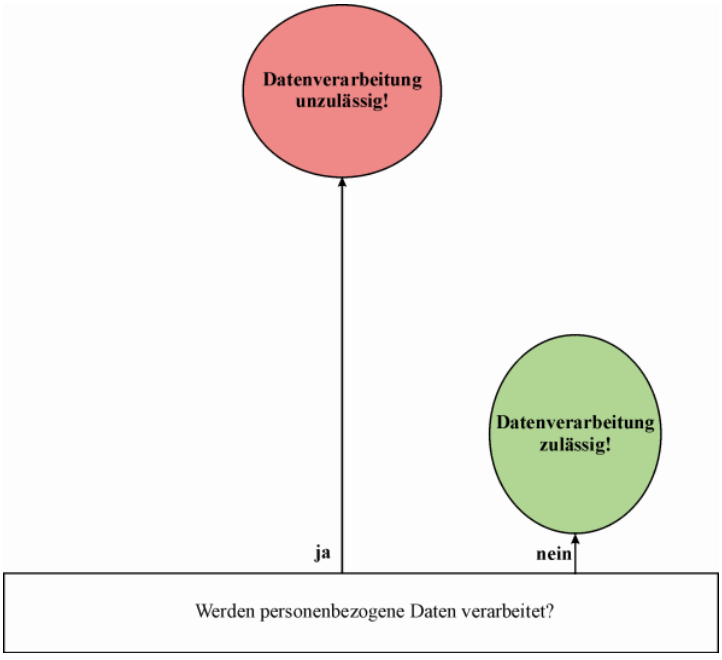
Abgrenzung BDSG & LDSGe

BDSG: Anwendung für	**LDSGe**: Anwendung für
• Unternehmen • Bundesbehörden • Behörden im Wettbewerb	• Landesbehörden • kommunale Behörden

keine Anwendung, wenn DV zur ausschließlichen persönlichen bzw. familiären Tätigkeit!

Grundsatz: lex specialis hat Vorrang! [→ Subsidiarität!]

Verbot mit Erlaubnisvorbehalt (1)

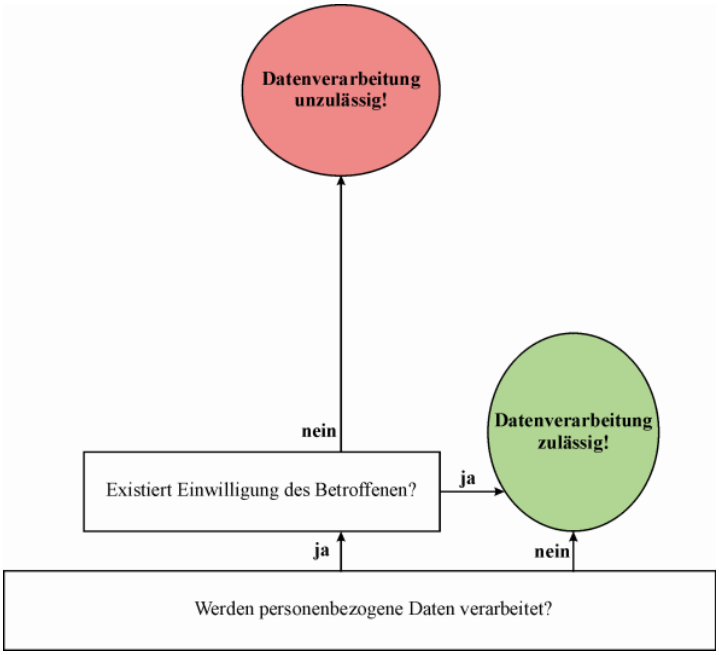


Grundsatz:

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

Eine Gestattung ist jedoch unter Umständen möglich.

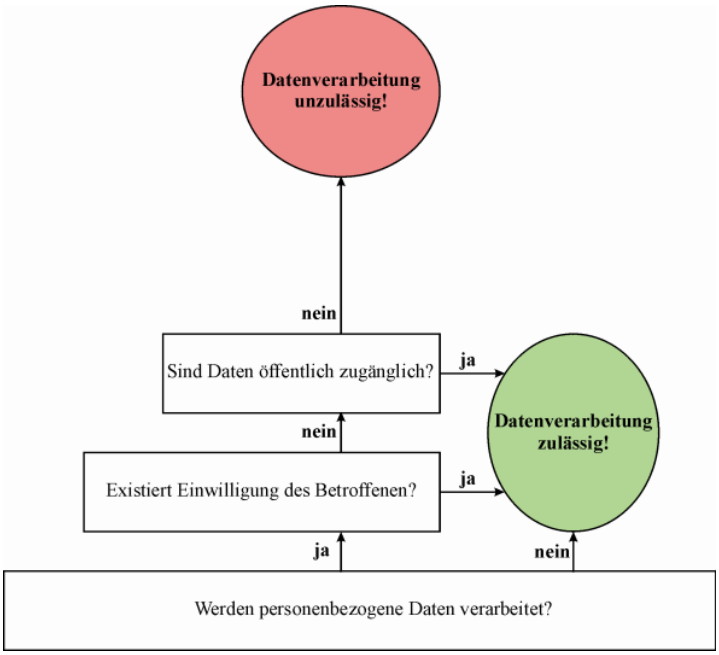
Verbot mit Erlaubnisvorbehalt (2)



Anforderungen an die Einwilligung:

- der Betroffene muss frei entscheiden können
- dem Betroffenen muss vorher der Zweck der geplanten Verarbeitung mitgeteilt werden
- der Betroffene soll über seine Rechte sowie die Folgen einer Ablehnung aufgeklärt werden
- die Einwilligung soll schriftlich erfolgen

Verbot mit Erlaubnisvorbehalt (3)



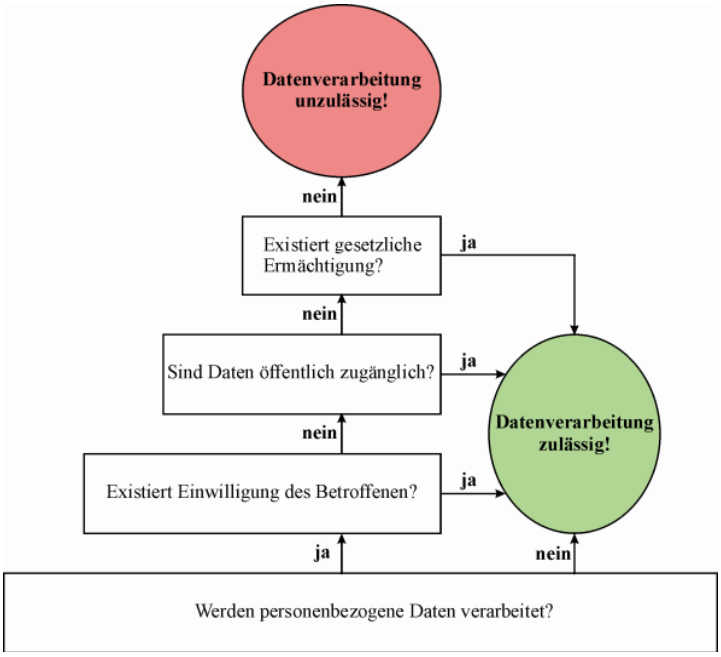
Öffentliche Quellen:

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

Hinweis:

- bei besonderen Arten personenbezogener Daten (z.B. Religionszugehörigkeit, Gesundheitsdaten) sind Daten nur öffentlich, wenn sie durch den Betroffenen selbst öffentlich gemacht wurden
- Unzulässig veröffentlichte Daten bleiben unzulässig

Verbot mit Erlaubnisvorbehalt (4)



Gesetzliche Erlaubnis:

- entweder im Datenschutzgesetz selbst
- oder in einer anderen Rechtsvorschrift (Gesetz, Verordnung, Satzung eines autonomen öffentlich-rechtlichen Verbandes mit gesetzlicher Ermächtigung), die verfassungsgemäß (normenklar und verhältnismäßig) ist

→ stellt **Regelfall** dar! (wg. Verweis auf Vertragsverhältnis bzw. vertragsähnliches Vertrauensverhältnis in § 28 BDSG)

Prinzip der Zweckbindung

- Erfordernis der **Zweckfestlegung** bei der Erhebung
- Zweck abhängig von geplanter **Verwendung**
- Datenschutzrechtlich relevante **Verfahren**
  (= festgelegte Art & Weise, wie Tätigkeit / Prozess auszuführen ist)
  zweckabhängig
  → zweckbezogen verknüpfte Verarbeitungsschritte
- Verarbeitungsschritte unterliegen **Zweckbindung**
- **Zweckänderung** nur bei berechtigtem Interesse unter Abwägung (→ abhängig vom Schutzgrad)
- teilweise existiert **besondere Zweckbindung**

Prinzip der Transparenz

- Betroffener muss ihn betreffende Verfahren kennen
- Anlegen von **Verfahrensverzeichnissen**
- **Nachvollziehbarkeit** durchgeführter Verfahren
- **Information** des Betroffenen bei Einwilligung
- **Auskunftsrecht** des Betroffenen
- **Benachrichtigungspflicht** bei fehlender Direkterhebung
- es existieren **besondere Informationspflichten** (z.B. zu Videoüberwachung & Chipkarten)

Zum Verfahrensverzeichnis

- **jedes** einzelne Verfahren zur Verarbeitung personenbezogener Daten aufzuführen
- inhaltliche Anforderung aus § 4e BDSG (Meldepflicht gegenüber Aufsichtsbehörden, sofern kein Datenschutzbeauftragter bestellt wurde)
- Einsichtsrecht für **Jedermann**
- Unterteilung in öffentlichen Teil und nicht öffentlichen Teil
- der nicht öffentliche Teil unterscheidet sich bei nicht-öffentlichen Stellen (BDSG) von öffentlichen Stellen (jeweiliges LDSG bzw. BDSG)
- eine fundierte Datenschutzkontrolle erfordert detailliertere Angaben, als das Gesetz vorschreibt (Grund für Beschränkung: Betriebsgeheimnisse und Technikoffenheit!)

Vorrang der Direkterhebung

- damit Betroffener Datenerhebung im Sinne des informationellen Selbstbestimmungsrechts **beeinflussen** kann
- **Transparenz** am höchsten bei Direkterhebung
- **Ausnahmen** nur zulässig, wenn Daten bereits von Betroffenem veröffentlicht wurden oder aufgrund gesetzlicher Vorschriften einsehbar/nutzbar sind (z.B. öffentliche Register)
- **Schriftform** der Einwilligung zur normenklaren Willenserklärung (→ bei konkludenter Einwilligung auf Umstand abzielen)
- Koppelungsverbot & **Freiwilligkeit** bei Einwilligung

Verhältnismäßigkeitsprinzip (1)

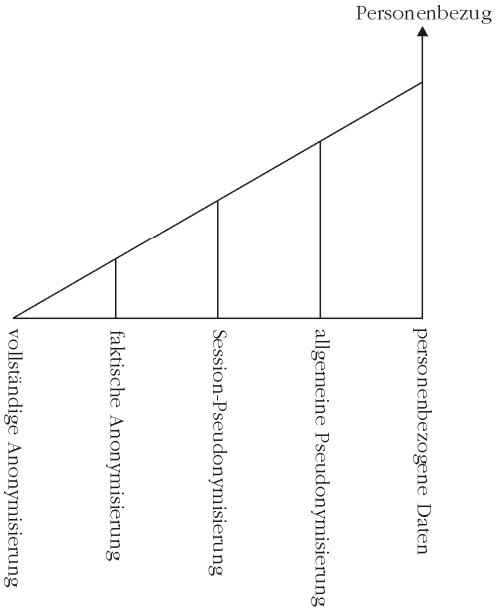
- Abstufung zwischen **erforderlich** (um Aufgaben rechtmäßig, vollständig & in angemessener Zeit erfüllen zu können) und **zwingend** (unerlässlich für Aufgabenerfüllung)
- maßgeblich ist der **Einzelfall**
- **geringerer Eingriff** ins inf. Selbstbestimmungsrecht vorrangig (z.B. mittels Anonymisierung)
- Autom. 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)

Prinzip der Datensparsamkeit (1)

- Anforderung zur **Gestaltung** der eingesetzten IT-Systeme
- Verbot **unnötiger Vorratsdatenhaltung**
- **Vermeidung** des Personenbezugs, sofern dieser nicht unbedingt erforderlich ist
- Verwendung **datenschutzfreundlicher Techniken**
- Ermöglichung **anonymer** und **unbeobachteter** Nutzung von Telemedien

Prinzip der Datensparsamkeit (2)



Kontrollprinzip vs Lizenzprinzip

Kontrollprinzip:

- Grundsätzliche Erlaubnis
- Einschränkung durch Normen
- Tätigkeit nur im Rahmen geltender Normen
- Kontrolle der Konformität mit Normen

Lizenzprinzip:

- Grundsätzliches Verbot
- Genehmigung auf Antrag mit Auflagen
- Tätigkeit nur im Rahmen der Genehmigung
- Kontrolle der Einhaltung der Auflagen

Weitere Regelungen zum Datenschutzrecht

- Gewährleistung der Betroffenenrechte
- Abgrenzungen:
  - Übermitteln vs Nutzen
  - Auftragsdatenverarbeitung vs Funktionsübertragung
- DV-Durchführende auf Datengeheimnis verpflichtet [ohne Folie]
- Datenschutzkontrolle:
  - Selbstkontrolle durch Betroffene
  - Eigenkontrolle durch Datenschutzbeauftragte
  - Fremdkontrolle durch Aufsichtsbehörde

Betroffenenrechte

- Recht auf **Auskunft**
- Recht auf **Berichtigung** unrichtiger personenbezogener Daten, auf **Löschung** unzulässiger personenbezogener Daten oder auf **Sperrung** nicht mehr benötigter personbezogener Daten
- Recht auf **Anrufung** des zuständigen Datenschutzbeauftragten
- Recht auf **Schadensersatz** bei schweren Verstößen

Niemand darf wegen der Geltendmachung seiner Rechte benachteiligt werden!

Übermitteln vs Nutzen (1)

Übermittlung:

- Transfer an oder Kenntnisnahme bzw. Abruf durch **Dritten**, also außerhalb der verantwortlichen Stelle (§ 3 Abs. 4 Nr. 3 BDSG i.V.m. § 3 Abs. 8 Satz 2 BDSG)

Nutzung:

- Kenntnisnahme oder Verwendung (ohne Veränderung, Speicherung oder Übermittlung), also z.B. Auswertung, innerhalb der gleichen verantwortlichen Stelle (§ 3 Abs. 5 BDSG)

Übermitteln vs Nutzen (2)

Übermittlung:

- Datenweitergabe an verbundene, aber eigenständige Unternehmen (§ 3 Abs. 4 BDSG i.V.m. § 3 Abs. 7 und 8 BDSG)
- Auftragsdatenverarbeitung außerhalb der EU (§ 11 BDSG i.V.m. § 3 Abs. 8 Satz 3 BDSG)

Nutzung:

- Auskunftserteilung an Betroffenen (§§ 19 und 34 BDSG i.V.m. § 3 Abs. 8 Satz 3 BDSG)
- Transfer an Auftragnehmer innerhalb EU (§ 11 BDSG i.V.m. § 3 Abs. 8 Satz 3 BDSG)

Übermitteln vs Nutzen (3)

Übermittlung:

→ **Verfügungsgewalt** über weitergegebene Daten liegt bei **neuer** verantwortlicher Stelle!

Nutzung:

→ **Verfügungsgewalt** über weitergegebene Daten liegt weiterhin bei **alter** verantwortlicher Stelle!

Auftragsdatenverarbeitung vs Funktionsübertragung

Auftragsdatenverarbeitung		Funktionsübertragung
◻ schriftliche Vereinbarung		◻ hinreichend eigenständige Aufgabe
◻ klare Beschreibung der Tätigkeiten		◻ eigenverantwortliche Tätigkeit des Auftragnehmers
◻ keine grundlegenden Entscheidungen zum Inhalt durch Auftragnehmer	VS	◻ Mitteilung an Betroffenen
◻ Weisungsrecht des Auftraggebers		◻ Übermittlungsbefugnis des Auftraggebers
◻ keine hoheitliche Tätigkeit		◻ Erhebungsbefugnis des Auftragnehmers
		◻ Verfolgung eigener Zwecke möglich
		◻ inhaltliche Entscheidungen durch Auftragnehmer
		◻ kein Weisungsrecht des Auftraggebers

Der Datenschutzbeauftragte (1)

Aufgaben von Datenschutzbeauftragten:

- **Hinwirken** auf die Einhaltung datenschutzrechtlicher Vorschriften
- datenschutzrechtliche und -technische **Überwachung** der automatisierten Datenverarbeitung, mit der personenbezogene Daten verarbeitet werden
- datenschutzrechtliche **Schulung** der Personen, die personenbezogene Daten verarbeiten & Verpflichtung dieser auf das Datengeheimnis (IT, Personalabteilung, Poststelle, Empfang, Betriebsdatenerfassung, ggf. Vertrieb)
- **Mitwirkung** bei Abschluss von Verträgen, Betriebsvereinbarungen, Policies und Dienstanweisungen
- **Ansprechpartner** für Betroffene (→ Prüfung von Beschwerden)
- Durchführung der **Vorabkontrolle** bei besonders riskanten automatisierten Verarbeitungen

Der Datenschutzbeauftragte (2)

Anforderungen an Datenschutzbeauftragte:

- **Fachkunde**: Datenschutzrecht, Datenverarbeitung, betriebliche Organisation, Didaktik, Psychologie [Urteil des LG Ulm, 1990]
- **Zuverlässigkeit**: Verschwiegenheit, ohne Interessenkonflikte, charakterliche Eignung
- nur natürliche Person kann bestellt werden

Absicherung des Datenschutzbeauftragten:

- unmittelbar der Geschäftsführung unterstellt
- Weisungsfreiheit
- Benachteiligungsverbot → Kündigungsschutz
- Unterstützung durch Unternehmen

Der Datenschutzbeauftragte (3)

Typische Tätigkeiten eines Datenschutzbeauftragten:

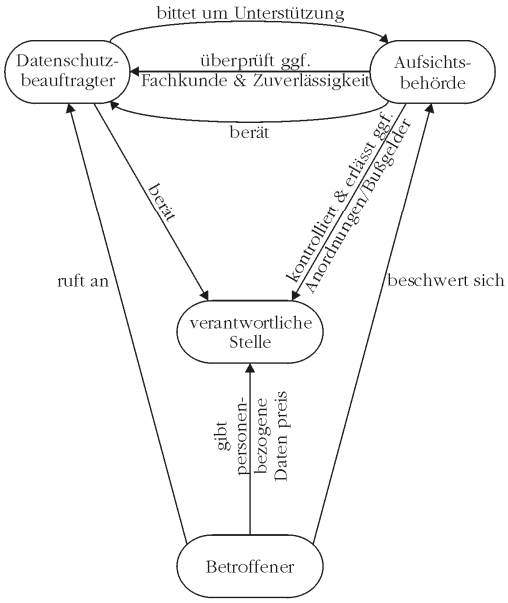
- Recherchen zur aktuellen Rechtslage (Auswertung aktueller Urteile)
- Lesen & Auswerten zahlreicher & umfangreicher Fachartikel & Fachliteratur
- Vorbereitung von & Teilnahme an & Protokollierung der Meetings (Geschäftsführung, IT-Leitung, Fachverantwortliche)
- Erstellung von Stellungnahmen & Verfahrensverzeichnissen
- Durchführung & Dokumentation von Vor-Ort-Kontrollen & Vertragskontrollen (u.a. zur Abgrenzung einer Auftrags-DV)
- Durchführung von Vorabkontrollen bei kritischen DV
- 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 hat Mehrarbeit & Mehrkosten zur Folge
- Buhmann bei Verlangsamung einer „schönen neuen Welt“
- Feststellung von Fehlverhalten wichtiger Mitarbeiter & strukturellen Defiziten
- festgestellte Datenschutzverstöße teilweise Kündigungsgrund von Mitarbeitern
- Durchsicht von Festplatten mit (Kinder-) Pornographie
- Anrufung mit Ziel der Verhinderung arbeitsrechtlicher Aufklärung

Checks & Balances bei der Datenschutzkontrolle



Unterschiede zwischen DSB & IT-Sicherheitsbeauftragter