Medienrecht I: Datenschutz

Vorlesung im Sommersemester 2008

an der Universität Ulm

Gastvortrag von Bernhard C. Witt

Zum Vortragenden

it.sec
security for your information

Bernhard C. Witt

- Berater für Datenschutz und IT-Sicherheit
- geprüfter fachkundiger Datenschutzbeauftragter
- Industriekaufmann, Diplom-Informatiker
- seit 1998 selbstständig
- seit 2005 Lehrbeauftragter an der Universität Ulm
- Autor zu Datenschutz & IT-Sicherheit in Fachbücher & Artikel

Übersicht

- Was ist Datenschutz?
- Zum Volkszählungsurteil (1983): Informationelles Selbstbestimmungsrecht
- Allgemeine Grundsätze des Datenschutzrechts
- Weitere Regelungen zum Datenschutz
- Mediendatenschutz

Was ist Datenschutz? (1)

Datenschutz =

Schutz des Einzelnen vor Beeinträchtigung seines Persönlichkeitsrechts beim Umgang mit seinen personenbezogenen Daten (nach § 1 Abs. 1 BDSG)

→ Schutz des Individuums (natürliche Person) als Betroffenen

→ Maßgeblich: Persönlichkeitsrecht des Betroffenen

→ Beschränkung auf personenbezogene Daten

Was ist Datenschutz? (2)

personenbezogene Daten =

Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 BDSG)

→ Datenschutz nur für natürliche Personen

→ bestimmbar ist eine Person, wenn der Personenbezug ohne unverhältnismäßigen Aufwand an Zeit, Kosten oder Arbeitskraft hergestellt werden kann

Was ist Datenschutz? (3)

Informationelles Selbstbestimmungsrecht =

Grundrecht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (nach BVerfGE 65, 1 [43])

→ Persönlichkeitsrecht eingeschränkt (durch GG-konforme Gesetze im überwiegenden Allgemeininteresse)

→ Bezug auf Erhebung (Preisgabe) sowie Verarbeitung und Nutzung (Verwendung)

Informationelles Selbstbestimmungsrecht

Art. 2 Abs. 1 GG:

Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

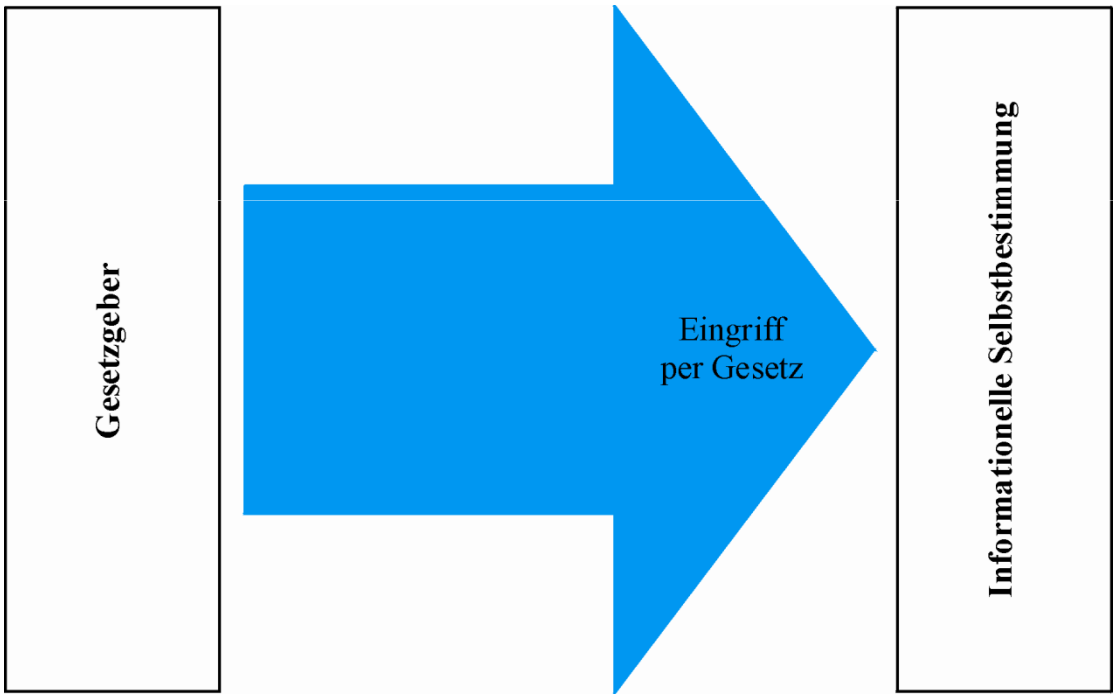
i.V.m.

Art. 1 Abs. 1 GG:

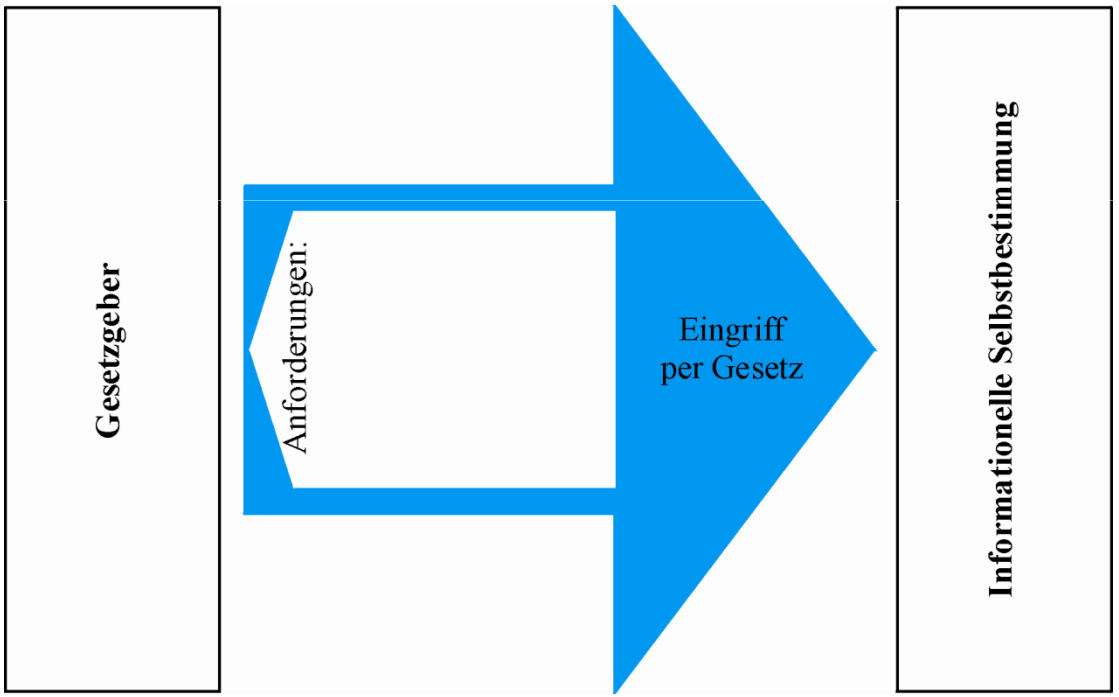
Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

= Handlungsfreiheit kombiniert mit Menschenwürde

Informationelle Selbstbestimmung (1)

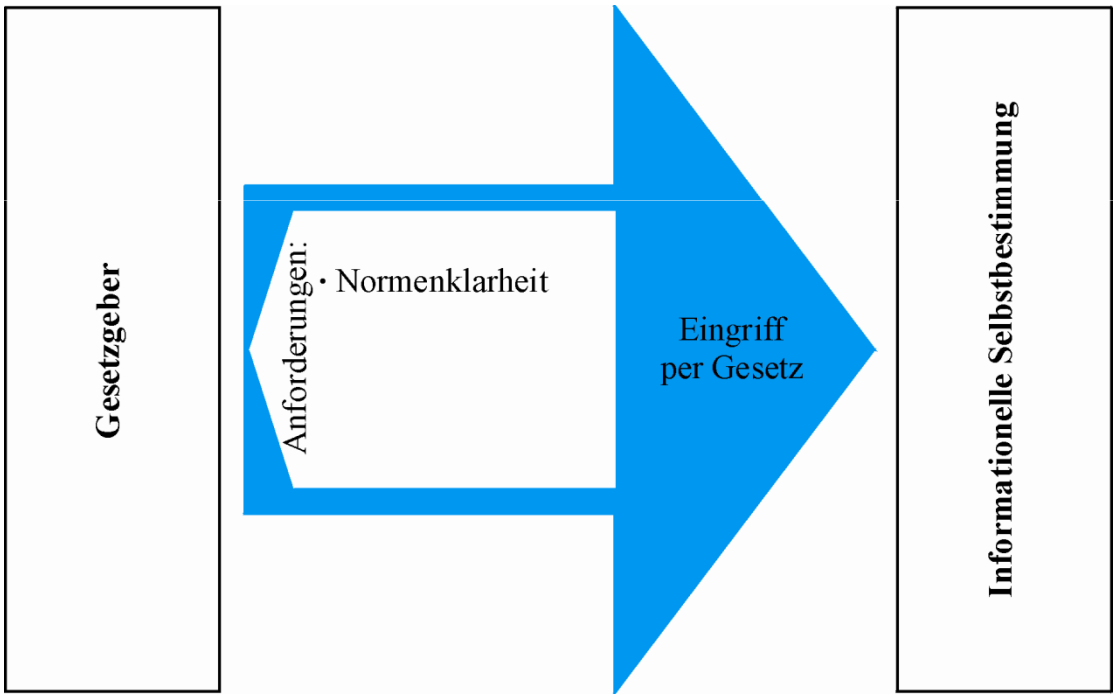


Informationelle Selbstbestimmung (2)



Eingriff erfordert:

Informationelle Selbstbestimmung (3)

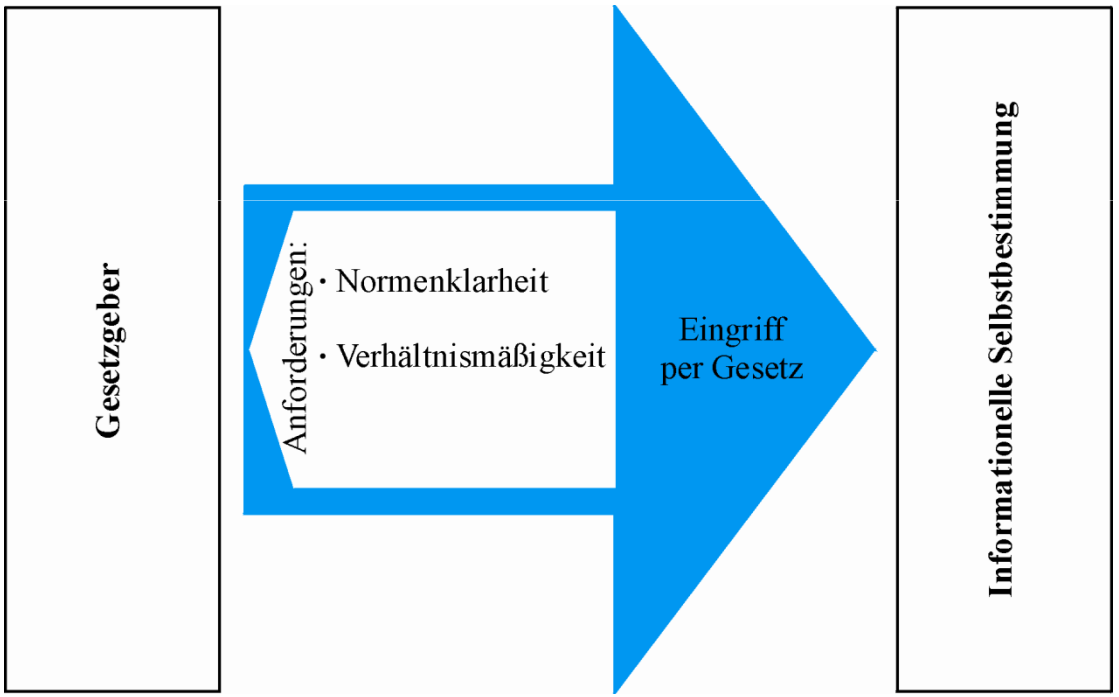


Eingriff erfordert:

Normenklar-heit

Verwendungs-zweck bereichs-spezifisch und präzise bestimmt

Informationelle Selbstbestimmung (4)

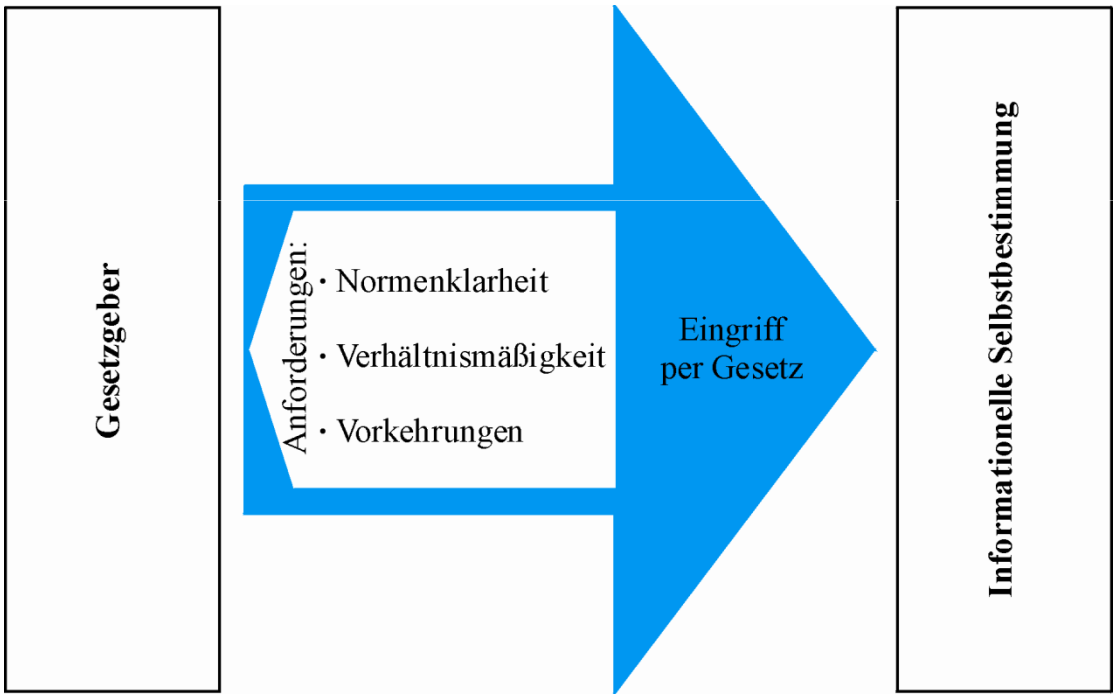


Eingriff erfordert:

Verhältnis-mäßigkeit

personenbezogene Daten müssen für Zweck geeignet und erforderlich sein

Informationelle Selbstbestimmung (5)



Eingriff erfordert:

Vorkehrungen

organisatorische & verfahrensabhängige Maßnahmen, insbesondere im Sinne der Datensparsamkeit

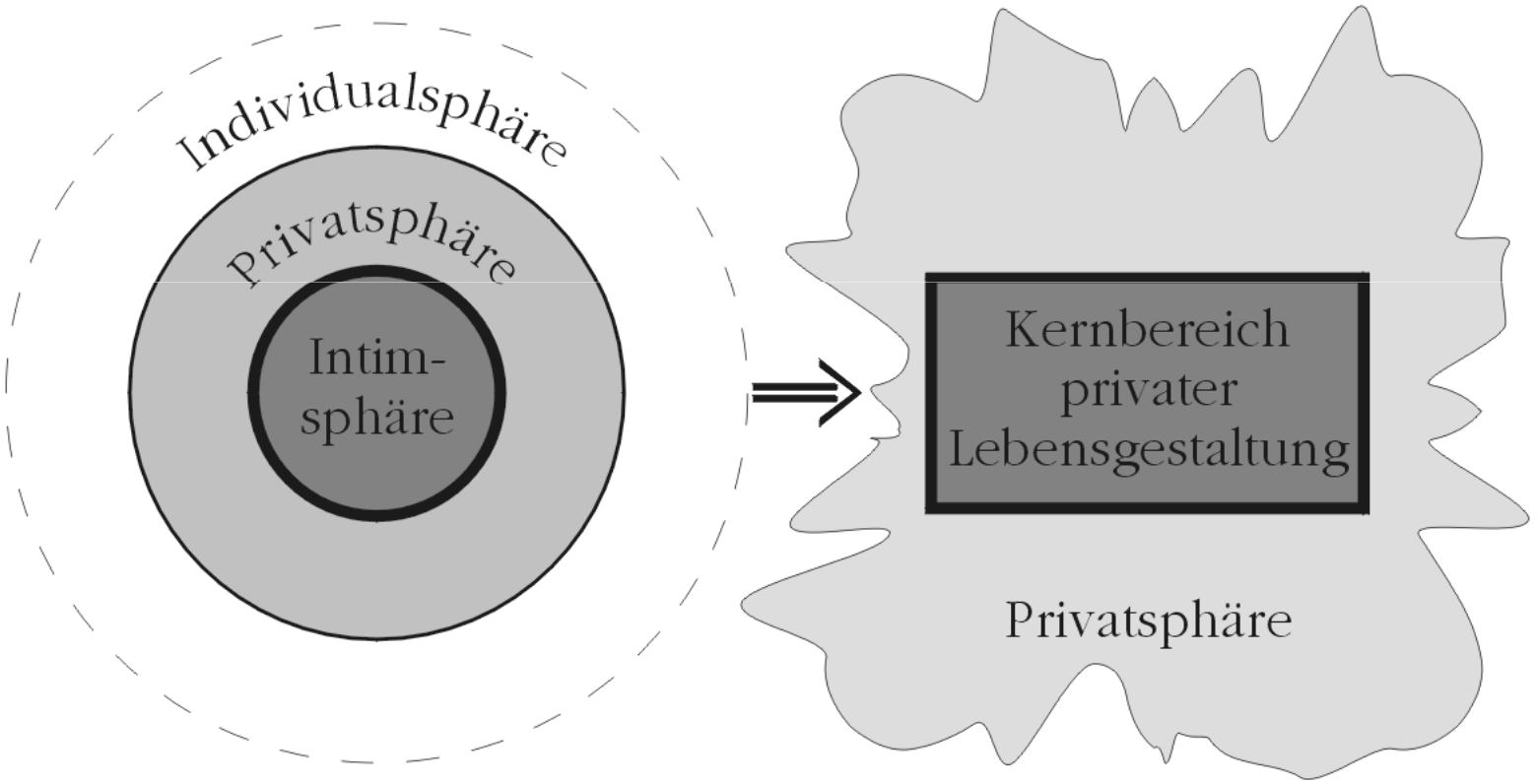
„Schranken-Schranken“

- Das informationelle Selbstbestimmungsrecht ist durch die Schrankentrias der Handlungsfreiheit beschränkt
  (= Schranken)

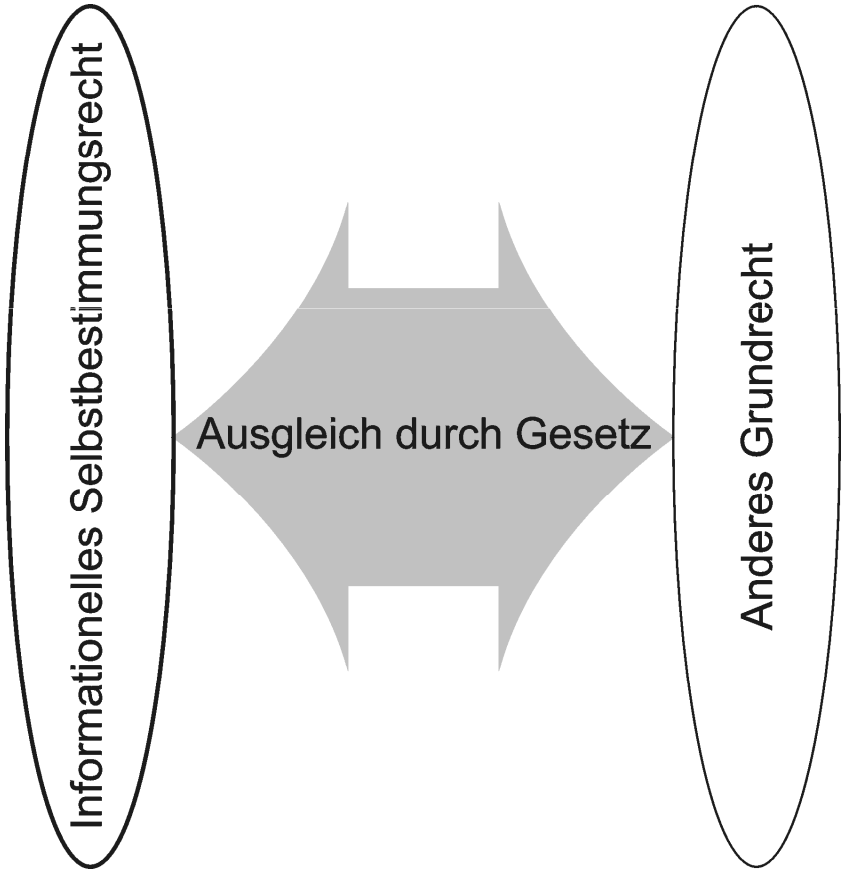
- Jeder Eingriff ins informationelle Selbstbestimmungsrecht erfordert gesetzliche Grundlage!

- Das Gesetz wiederum muss normenklar und verhältnismäßig sein und entsprechende Schutzvorkehrungen beinhalten!
  (= Schranken-Schranken)

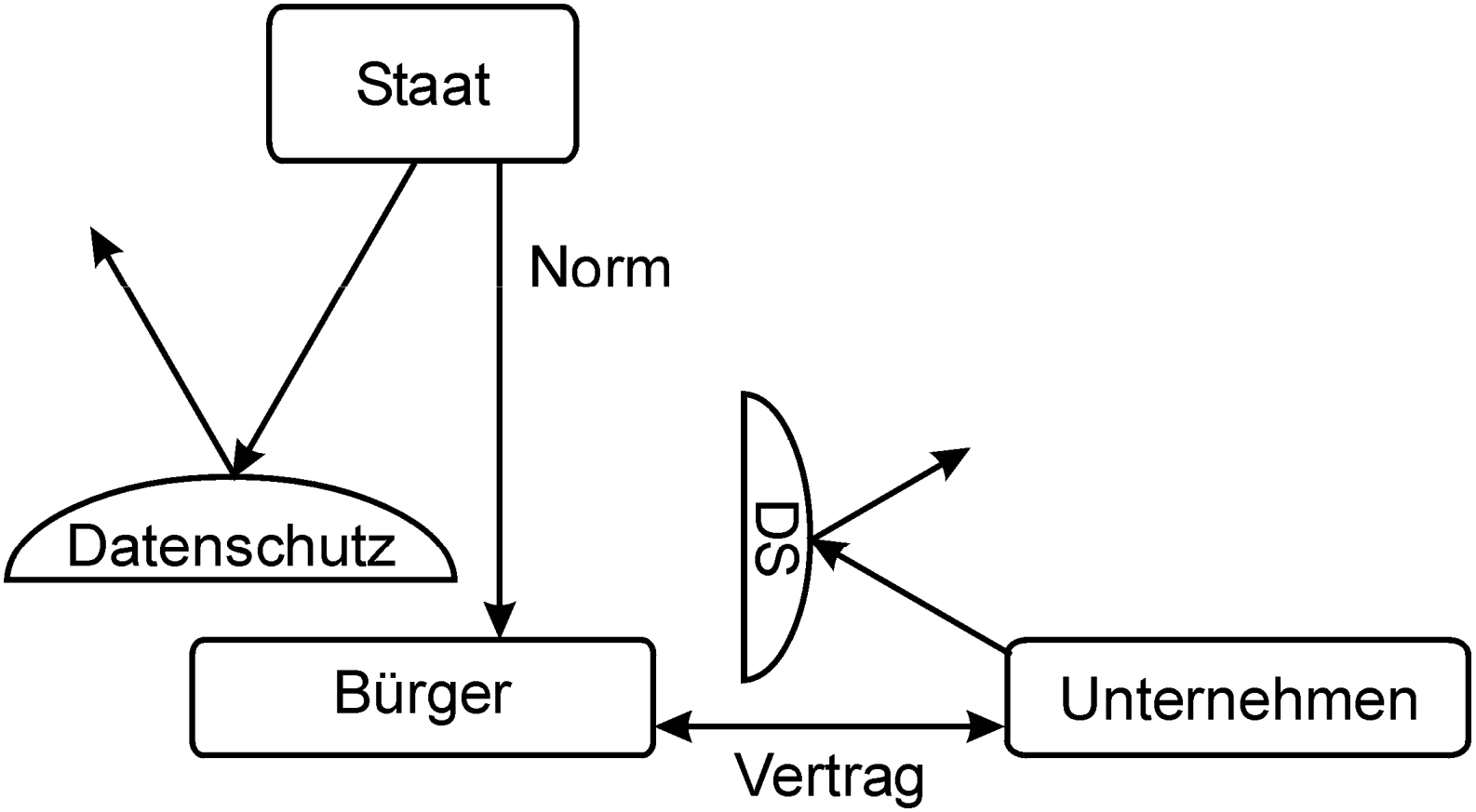
Auflösung der Sphärentheorie



Ausgleich zwischen kollidierenden Grundrechten



Ausstrahlungswirkung



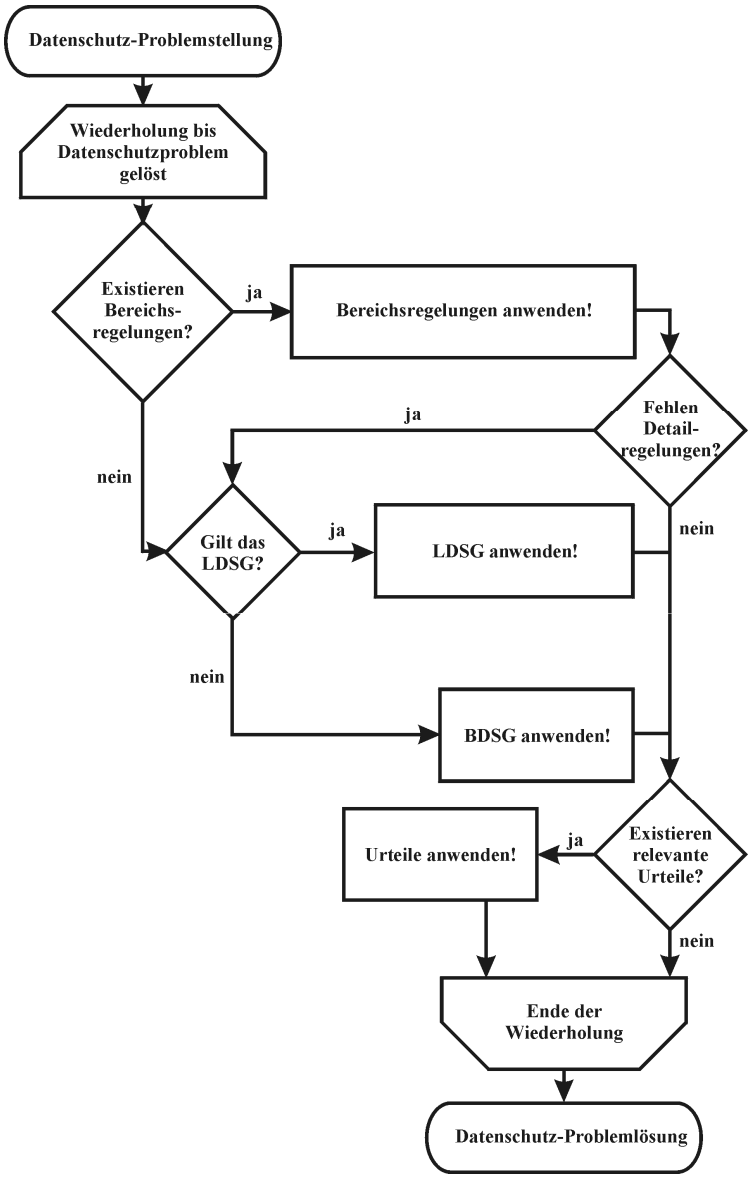
Datenschutzrechtliche Grundsätze

- **Subsidiaritätsprinzip**: Bereichsrecht hat Vorrang!
- **Verbot mit Erlaubnisvorbehalt**: automatisierte Verarbeitung personenbezogener Daten benötigt ausdrückliche Gestattung!
- **Prinzip der Zweckbindung**: Erhebungsgründe bestimmen auch Verarbeitungs- und Nutzungsbefugnisse!
- **Prinzip der Transparenz**: Betroffener muss erkennen können, wie seine Daten automatisiert verarbeitet werden!
- **Verhältnismäßigkeitsprinzip**: Angemessene Zweck-Ziel-Relation bei der automatisierten Verarbeitung zu beachten!
- **Prinzip der Datensparsamkeit**: Personenbezug gering halten!
- **Sitzlandprinzip**: Entscheidend ist der Sitz der verantwortlichen Stelle (nicht der Ort der Verarbeitung)!

Subsidiaritätsprinzip

resultierend aus der Normenklarheit:

- **bereichsspezifische** Regelungen haben immer **Vorrang** vor allgemeinen Regelungen
- fehlende Regelungen des Bereichsrechts werden durch entsprechende Regelungen des **Allgemein-rechts 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

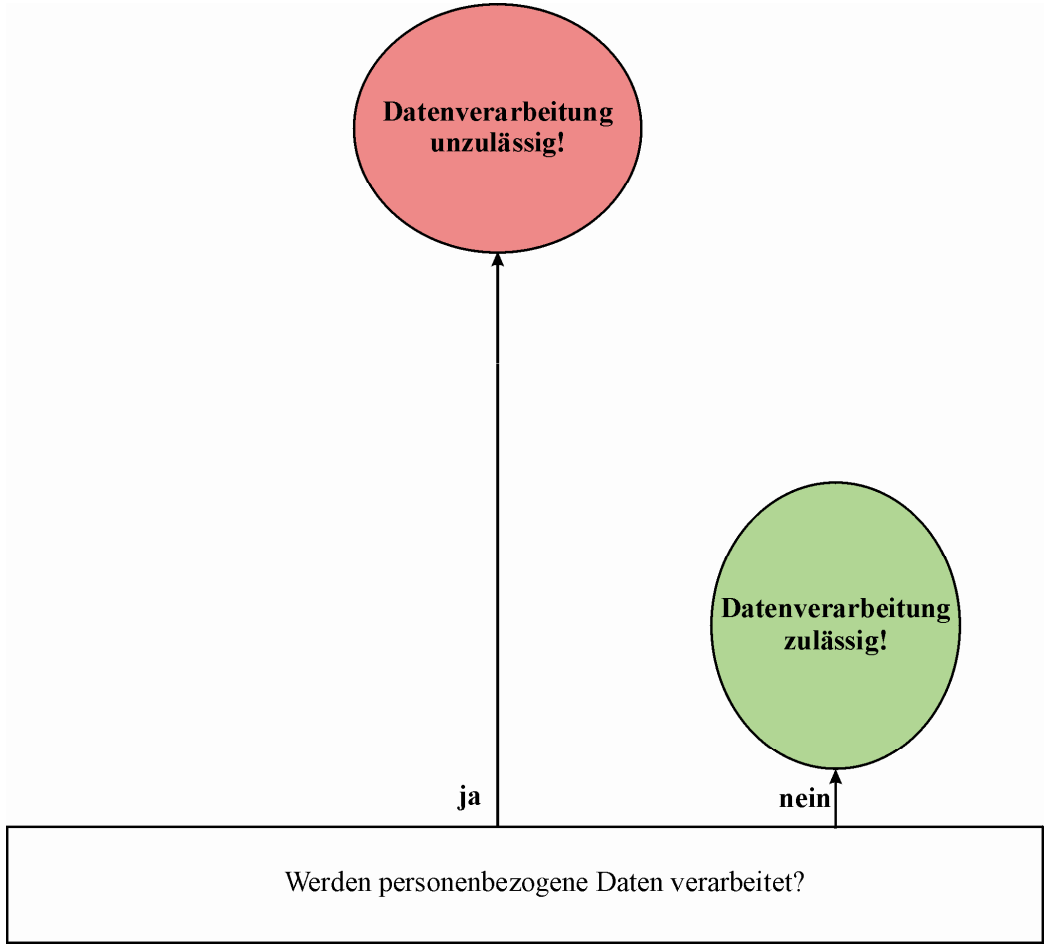
BDSG: Anwendung für
- Unternehmen
- Bundesbehörden
- Behörden im Wettbewerb

LDSGe: Anwendung für
- Landesbehörden
- kommunale Behörden

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

Grundsatz: lex specialis derogat lex generalis!

Verbot mit Erlaubnisvorbehalt (1)

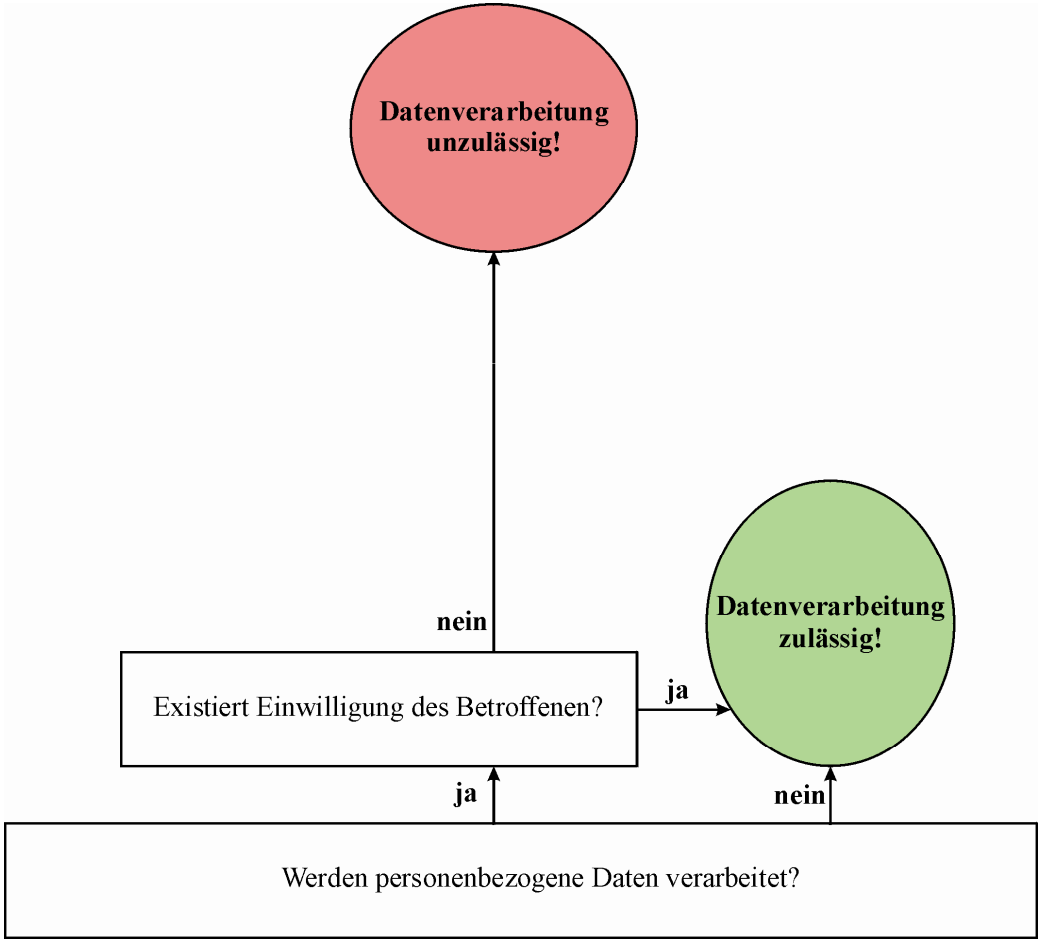


Grundsatz:

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

Eine Gestattung ist jedoch unter Umständen möglich.

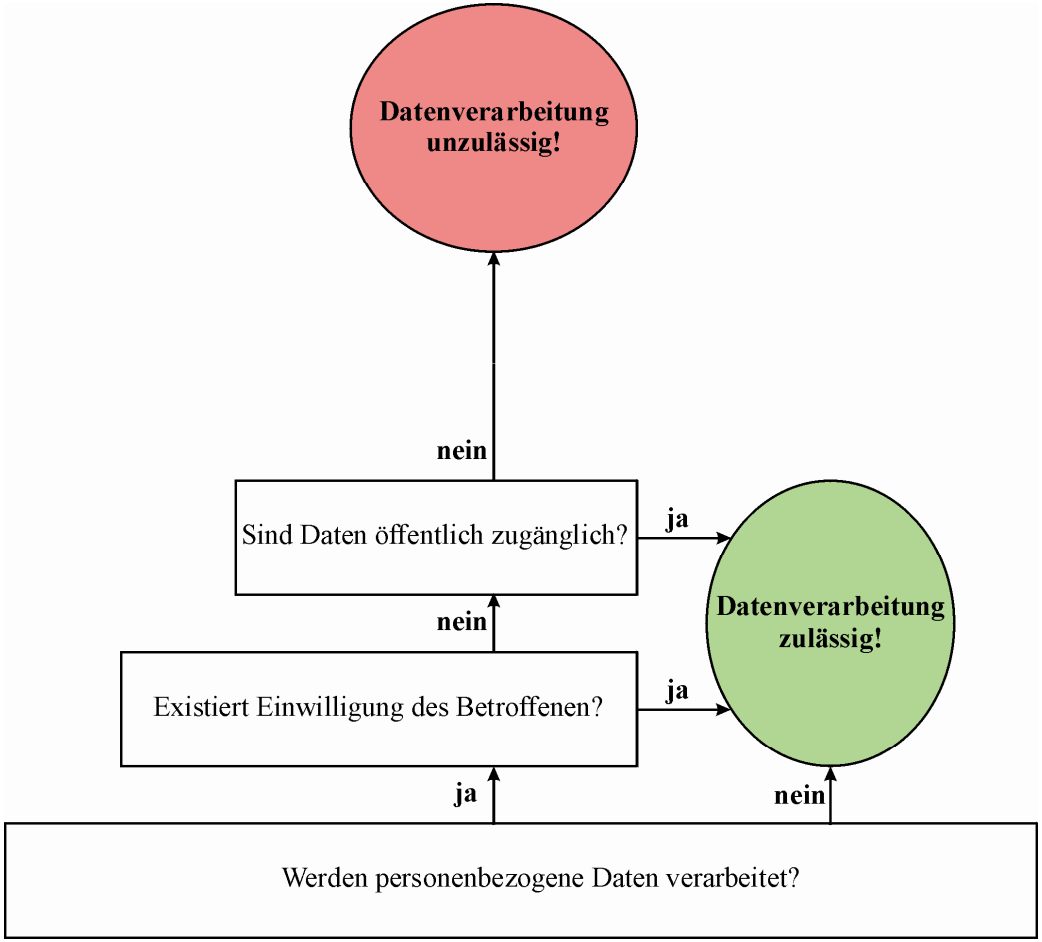
Verbot mit Erlaubnisvorbehalt (2)



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)



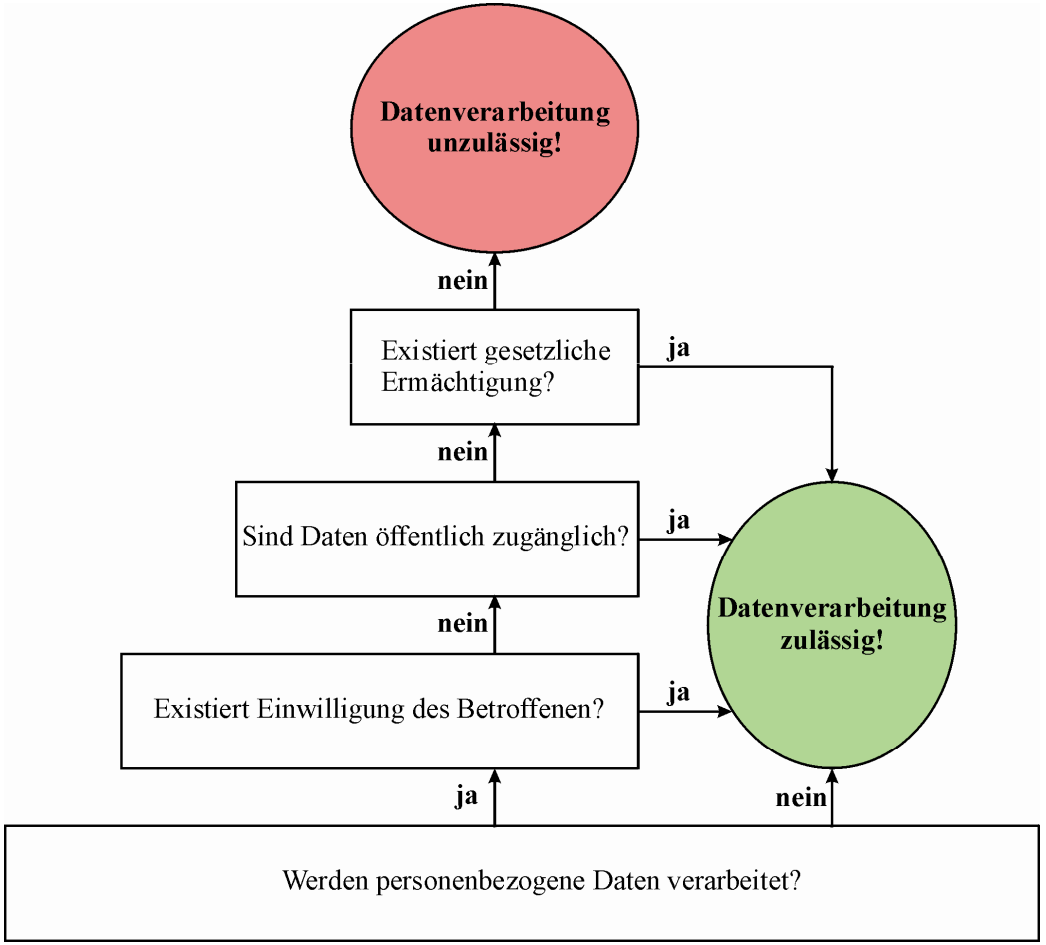
Öffentliche Quellen:

- 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**
- **Verfahren** *(= festgelegte Art & Weise, wie Tätigkeit / Prozess auszuführen ist)* ist zweckabhängig
  → zweckbezogen verknüpfte Verarbeitungsschritte
- jeder Verarbeitungsschritt unterliegt **Zweckbindung**
- **Zweckänderung** nur bei berechtigtem Interesse unter Abwägung möglich
  (→ abhängig vom Schutzgrad)
- teilweise existiert **besondere Zweckbindung** (z.B. zur Datensicherung & Sicherung ordnungsgemäßem Betrieb der DV-Anlagen)

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 & Telemedien-nutzung)

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 ist auf Umstand abzuzielen)
- Koppelungsverbot & **Freiwilligkeit** bei Einwilligung

Verhältnismäßigkeitsprinzip (1)

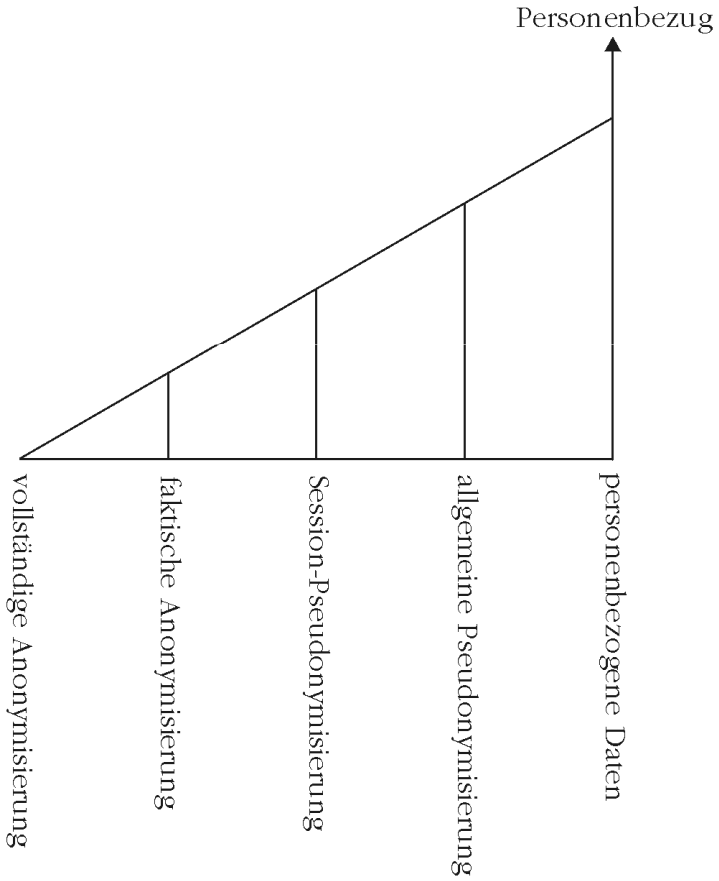
- **Abstufung** zwischen erforderlich (um Aufgaben rechtmäßig, vollständig & in angemessener Zeit erfüllen zu können) und zwingend (unerlässlich für Aufgabenerfüllung)
- maßgeblich ist der **Einzelfall**
- geringerer Eingriff ins informationelle Selbstbestimmungsrecht zu bevorzugen („**Übermaßverbot**“)
- 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)

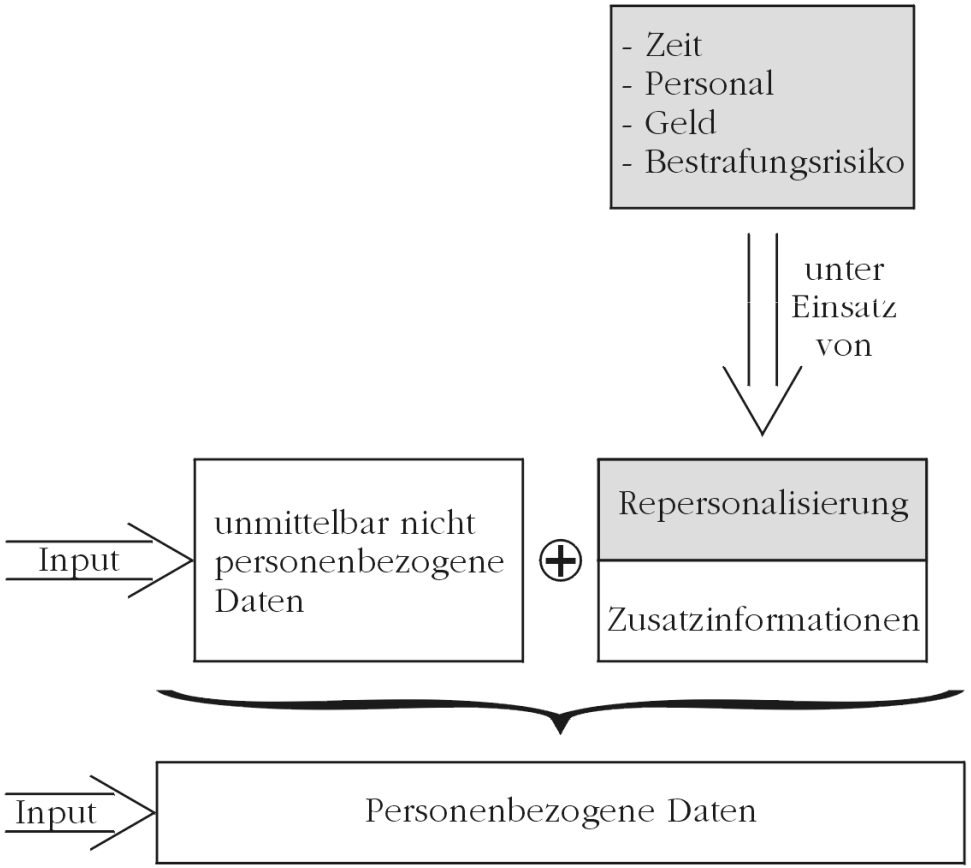
Prinzip der Datensparsamkeit (1)

- **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)



Personenbezogene Daten vs Personenbeziehbare Daten



Weitere Regelungen zum Datenschutzrecht

- Phasen der automatisierten Verarbeitung: Erheben, Verarbeiten (Speichern, Verändern, Übermitteln [an Dritte!], Sperren bzw. Löschen) und Nutzen
- alle Durchführende auf Datengeheimnis verpflichtet!
- Gewährleistung der Betroffenenrechte
- Datenschutzkontrolle durch Datenschutzbeauftragte
- Gewährleistung der Datensicherheit

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!

Der Datenschutzbeauftragte (1)

Erfordernis zur Bestellung eines Datenschutzbeauftragten:

- Erhebung, Verarbeitung (Speicherung, Veränderung, Übermittlung, Sperrung bzw. Löschung) oder Nutzung personenbezogener Daten unter Einsatz von DV-Anlagen durch mind. 10 Personen, die damit ständig beschäftigt sind
- Manuelle Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch mind. 20 Personen
- automatisierte Verarbeitung, die einer Vorabkontrolle unterliegen (wg. Verarbeitung besonderer Arten personenbezogener Daten oder Persönlichkeits-/Fähigkeits-/Leistungs-/Verhaltensbewertung) oder zur geschäftsmäßigen Übermittlung erfolgen, unabhängig von Anzahl tätiger Personen
- Bestellung (beidseitige Vereinbarung) hat schriftlich zu erfolgen!

Der Datenschutzbeauftragte (2)

Aufgaben von Datenschutzbeauftragten:

- Hinwirken auf die Einhaltung datenschutzrechtlicher Vorschriften
- Überwachen der automatisierten Datenverarbeitung, mit der personenbezogene Daten verarbeitet werden
- datenschutzrechtliche Schulung der Personen, die personenbezogene Daten verarbeiten
- Ansprechpartner für Betroffene
- Führen von Verzeichnissen eingesetzter Verfahren automatisierter Verarbeitung von personenbezogenen Daten
- Durchführung der Vorabkontrolle bei besonders riskanten automatisierten Verarbeitungen

Der Datenschutzbeauftragte (3)

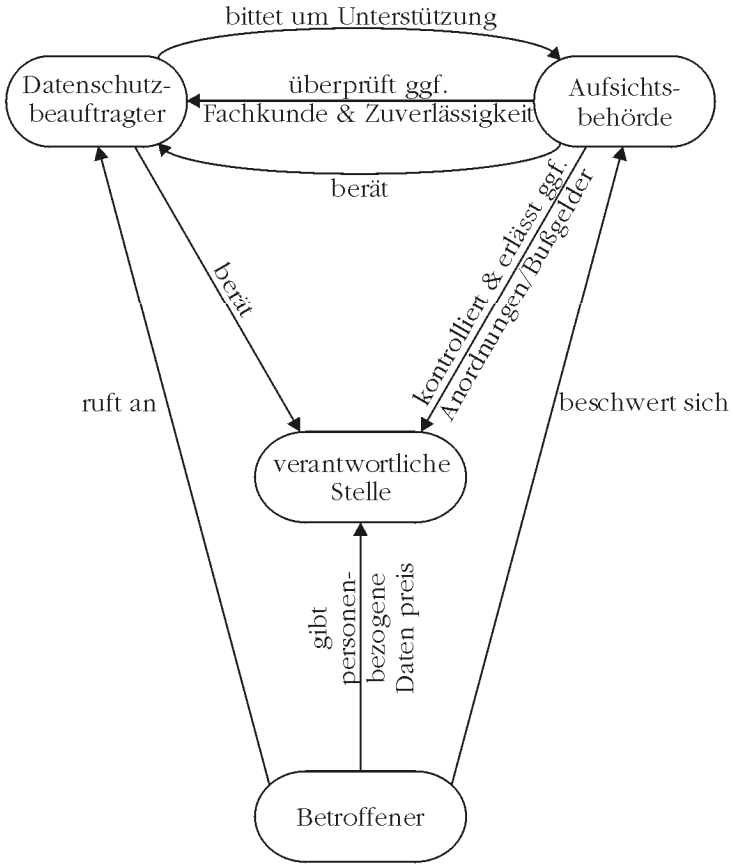
Anforderungen an Datenschutzbeauftragte:

- **Fachkunde**: Datenschutzrecht, Datenverarbeitung, betriebliche Organisation, Didaktik, Psychologie (gem. LG Ulm 1990)
- **Zuverlässigkeit**: Verschwiegenheit, ohne Interessenkonflikte, charakterliche Eignung
- nur natürliche Person kann bestellt werden

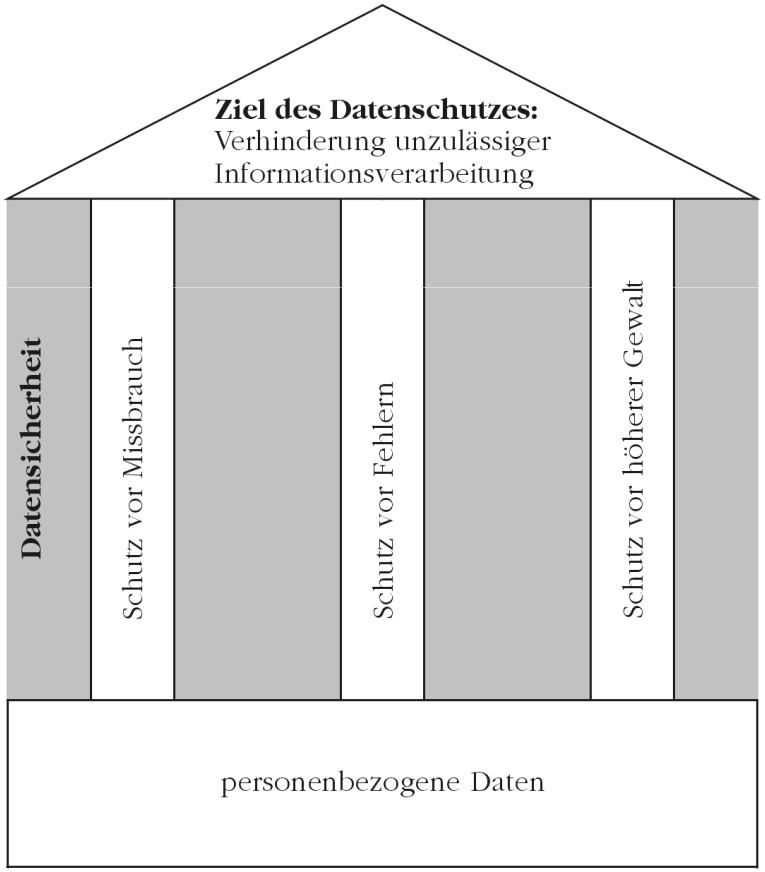
Absicherung des Datenschutzbeauftragten:

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

Checks & Balances bei der Datenschutzkontrolle



Zusammenhang zwischen Datenschutz und Datensicherheit



Datensicherheit =

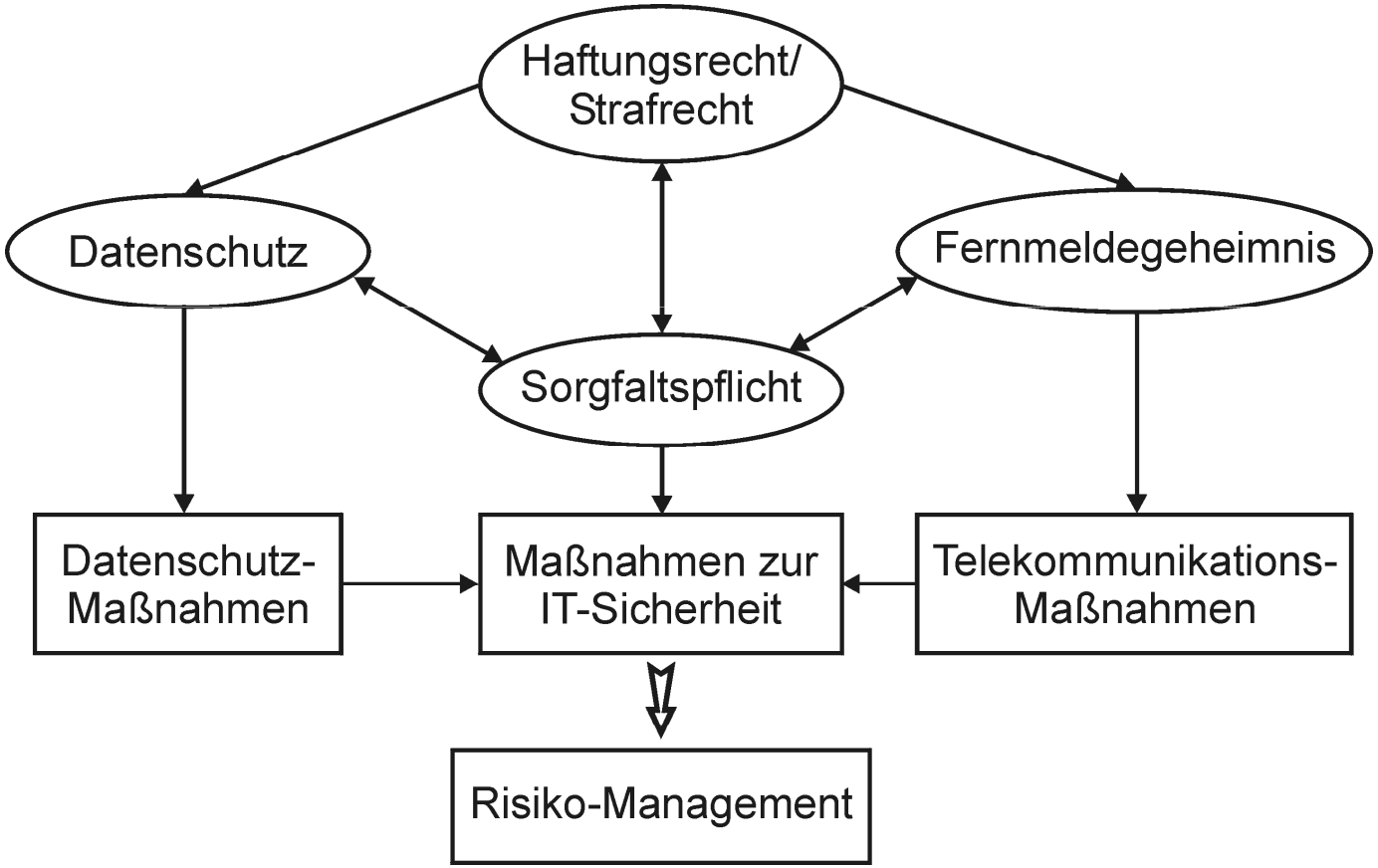
Schutz der gespeicherten Daten vor Beeinträchtigung durch Missbrauch, menschliche oder technische Fehler und höhere Gewalt

Technische & organisatorische Maßnahmen zum Datenschutz

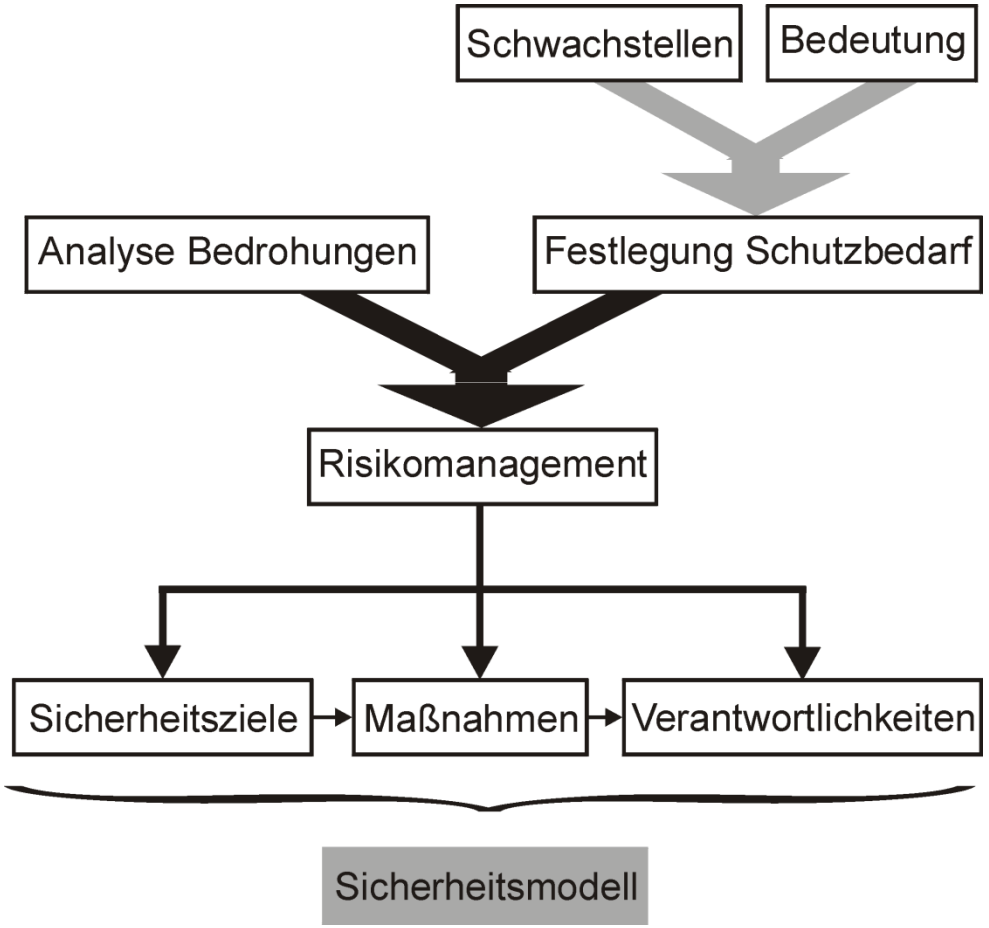
- **Zutrittskontrolle**: Einrichtung physischer Schutzzonen
- **Zugangskontrolle**: Nutzung von IT-Systemen erst nach Authentifizierung
- **Zugriffskontrolle**: Zugriff gemäß begründetem Berechtigungs-konzept
- **Weitergabekontrolle**: Informationsfluss & Perimeterschutz
- **Eingabekontrolle**: Zuordnung von Verantwortung
- **Auftragskontrolle**: Aufgabenerfüllung gemäß Weisungskette
- **Verfügbarkeitskontrolle**: Schutz der Daten vor Zerstörung oder Verlust
- **Datentrennungskontrolle**: Zweckgebundene & -getrennte Datenverarbeitung

→ **Angemessenheit nach Schutzgrad & Verletzlichkeit**

Übersicht Sicherheitsrecht



IT-Risiko-Manage-ment



Ziele der IT-Sicherheit (1)

Verfügbarkeit =
Gewährleistung, dass das IT-System (für befugte Nutzer) zugänglich und funktionsfähig ist

→ Prozessausführung in vorgesehener Weise zum geplanten Zeitpunkt im vorgegebenen Zeitrahmen

→ Sicherung vor Ausfällen und ungewolltem Verlust

→ betrifft auch die Vollständigkeit des Datenbestands (Nutzdaten, Passwortdaten, Konfigurationsdaten & Protokolldaten)

Ziele der IT-Sicherheit (2)

Vertraulichkeit =
Gewährleistung, dass die Daten des IT-Systems nur durch befugte Nutzer interpretiert werden

→ kein unbefugter Informationsgewinn

→ Daten für Unbefugte nicht zugänglich (auch nicht über verdeckte Kanäle)

→ ergänzt durch Anonymität/Pseudonymität, Unbeobachtbarkeit & Verdecktheit aus Kommunikationstechnik

Ziele der IT-Sicherheit (3)

Integrität =
Gewährleistung, dass die Daten des IT-Systems nur durch befugte Nutzer verändert werden

→ Vorliegen korrekter (= originalgetreuer und unverfälschter) und aktueller Daten

→ Feststellbarkeit von Manipulationen (Datenqualität)

→ zielt auf die Vollständigkeit des Datenbestandes ab

→ stellt Anforderungen an disaster recovery

Ziele der IT-Sicherheit (4)

Zurechenbarkeit =

Gewährleistung, dass jederzeit festgestellt werden kann, welcher Nutzer einen Prozess ausgelöst hat

→ Verantwortlichkeit & Authentizität (Glaubwürdigkeit)

→ Diese Daten kommen vom betreffenden Kommunikationspartner

→ Die betreffenden Daten kommen von diesem Kommunikationspartner

→ Kern des Rechtemanagements

Ziele der IT-Sicherheit (5)

Rechtsverbindlichkeit =

Gewährleistung, dass Daten und Vorgänge gegenüber Dritten rechtskräftig nachgewiesen werden können

→ Transparenz (Nachvollziehbarkeit)

→ Verhinderung falschen Abstreitens

→ Nachweis zugesicherter Eigenschaften

→ Voraussetzung für Auditierbarkeit

→ Ausgleich für fehlenden Augenscheinbeweis

Mediendatenschutz: Schichtenmodell

Inhalt:	Datenschutzgesetze bzw. Spezialrecht
Dienst:	Telemediengesetz bzw. Rundfunk-Staatsvertrag bzw. Telekommunikationsgesetz
Transfer:	Telekommunikationsgesetz

Mediendatenschutz: Datenarten

- **Bestandsdaten** = (notwendige) Vertragsdaten
- **Verkehrsdaten** = Verbindungsdaten
- **Nutzungsdaten** = Abrechnungsdaten (erforderliche Verbindungsdaten & genutzte Telemediendienste)

  Hinweis: Geschäftsmäßigkeit zielt auf Dauerhaftigkeit, Gewinnerzielungsabsicht nicht maßgeblich!

- **Inhaltsdaten**

Zur elektronischen Einwilligung

- eindeutige und **bewußte Handlung** des Telemedien-Nutzers (z.B. durch gesonderte Bestätigung der Eingabe → „**opt-in**“ mit Bestätigung)
- mit **Protokollierung** (zur Nachprüfbarkeit)
- jederzeitige **Abrufbarkeit** und **Widerrufbarkeit** der Einwilligung durch den Telemedien-Nutzer
- **keine Kopplung** an andere Rechtsgeschäfte zulässig
- Telemedien-Nutzer ist **vor** der Erhebung personenbezogener Daten über Art, Umfang und Zweck der geplanten Verarbeitung verständlich zu informieren (= **Datenschutzerklärung**)

Literaturhinweise

An der Uni Ulm verfügbar:

- Alexander Roßnagel (Hrsg): Handbuch Datenschutzrecht; München, C.H. Beck, 2003
- Bernhard C. Witt: Datenschutz an Hochschulen; Ulm, LegArtis, 2004
- Marie-Theres Tinnefeld, Eugen Ehmann, Rainer W. Gerling: Einführung in das Datenschutzrecht; München, Oldenbourg, 2005
- Bernhard C. Witt: Datenschutz kompakt und verständlich; Wiesbaden, Vieweg, 2008

Zum Hintergrund außerdem empfehlenswert:

- Gerhard Kongehl (Hrsg), Sebastian Greß, Gerhard Weck, Hannes Federrath: Datenschutz-Management; Planegg, WRS, Loseblattsammlung, Stand: Januar 2008
- Tätigkeitsberichte des BfDI & der LfDs
- Zeitschriften: Datenschutz und Datensicherheit, Recht der Datenverarbeitung, Computer und Recht, MultiMedia und Recht