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

Vorlesung im Sommersemester 2008

an der Universität Ulm

von Bernhard C. Witt

Zum Dozenten

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

Fachliche Zuordnung

- Vorlesung (VL) im Hauptstudium / Master (CS8925) mit 2+2 SWS = 6 LP

  in den Informatik-Studiengängen wie folgt anrechenbar:

Medieninformatik & Diplom-Informatik & Master:

- **Kernfach** Praktische und Angewandte Informatik

Diplom-Informatik & Master of Computer Science:

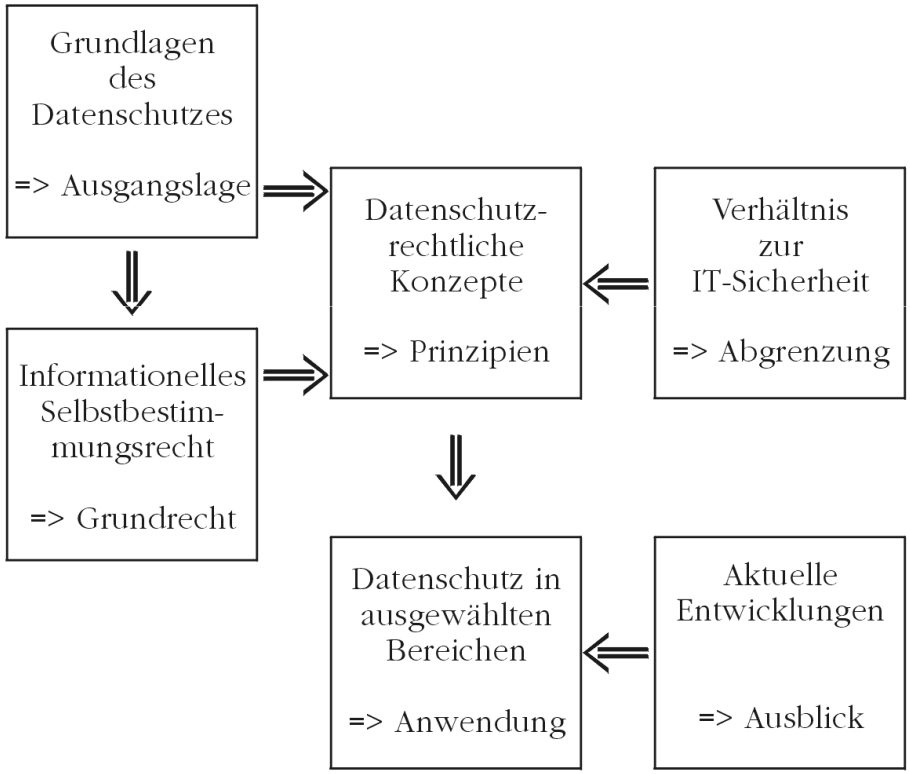
- (alternativ) **Vertiefungsgebiet/Spezialisierung** Informatik und Gesellschaft

Übersicht zur Vorlesung

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

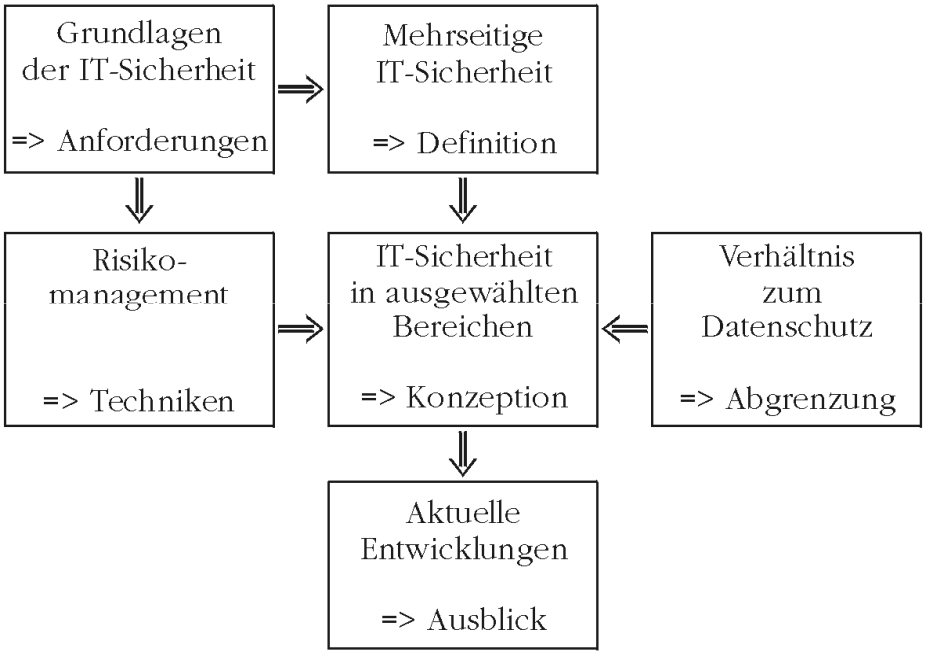
- jeweils **montags** und **mittwochs** 16 – 18 Uhr im H21
- **Vorlesungsmaterial** vorab im Netz unter: www.informatik.uni-ulm.de/datenschutz
- **Übungsblätter + Musterlösungen** ebenfalls
- **Übungen ergänzen (!) Vorlesung**
- **Klausurtermin** noch zu vereinbaren
- Lehrveranstaltung wird didaktisch ausgewertet

Lehrbuch statt Skript (1)



Vorlesung erstreckt sich über alle Kapitel

Lehrbuch statt Skript (2)



Vorlesung erstreckt sich über alle Kapitel

Hinweise

Scheinkriterien:

- 50 % Votieren der (~ 10*5) Aufgaben
  (→ 25 Votierpunkte; Lösungsidee gibt 0,5 Punkte)
  & 5 Aufgabenlösungen erfolgreich präsentieren

Prüfung:

- Klausur!
  (1/3 Vorlesung, 1/3 Übung, 1/3 Anwendungen)
- Erfahrungen: Schnitt bisher ~ 1,8 (bei 78 Prüfungen)
  Aktive Teilnahme an Übungen → Noten besser!

Motivation

- Informationen besonders eigenartiger „Rohstoff“
- Anwendungsbezug der Informatik
- Entwurf von Systemen ggf. mit Personenbezug
- Compliance: Übereinstimmung mit gesetzlichen Erfordernissen bzw. Standards (& Vereinbarungen)
- Berufliche Perspektive (CIO, CISO, Admins etc.)
- Abwehr von Industriespionage
- Ubiquitous Computing
- Kenntnisse in IT-Sicherheit auf Arbeitsmarkt gesucht

Gegenstand der Vorlesung

- grundlegende Einführung in Datenschutz & IT-Sicherheit
- Kennenlernen & Anwendung rechtlicher Anforderungen
- Methoden des (IT-) Risikomanagements
- Konzeption eines Informationssicherheitsmanagements
- Einblick in internationale Standards
- Anwendung gängiger Vorgehensmodelle
- Falldiskussionen & Praxisbeispiele

Lehrziele: Methoden

- Strukturieren und Analysieren auch umfangreicher Texte
- Abstrahieren von Sachverhalten
- Verknüpfung verschiedener Sichtweisen (aus Jura, Informatik und Wirtschaftswissenschaften)
- selbstständiges Aufarbeiten neuen (und ungewohnten) Stoffes
- Beherrschen der Nomenklatur
- Einübung typischer Fertigkeiten
- Anwendung von Kenntnissen in praxisrelevanten Fällen

→ **Erleichterung des Einstiegs in die Berufspraxis**

Lehrziele: Inhalte

- Angabe, Analyse und Anwendung grundlegender Rechtsnormen
- Beherrschen der Nomenklatur
- Erläuterung des informationellen Selbstbestimmungsrechts
- Angabe der Grundsätze beim Datenschutz
- Übertragung der Grundsätze auf neue Problemfälle
- Angabe und Anwendung der Ziele mehrseitiger IT-Sicherheit
- Benennung von Bedrohungen und deren Wirkungen
- Konstruktion von Maßnahmen gegen Bedrohungen
- Kenntnis gängiger Vorgehensmodelle
- Erstellung eines Sicherheitskonzepts/Notfallvorsorgekonzepts
- Durchführung von Risikoanalysen
- Entscheidung über den Umgang mit festgestellten Risiken

Zum Vergleich von Informatik und Jura

- **Informatik und Jura**: konsequente Verwendung definierter Systematik & Fachtermini
- **Informatik** → Definition/Satz/Anwendung;
  Jura → Legaldefinition/Norm/Auslegung mit Abwägung
- **Informatik** → Analogien;
  Jura → Einzelfälle (außer Verfassungsauslegung!)
- **Informatik** → gröbere Bezüge;
  Jura → Detailnachweise

Zur Blitzumfrage

Schwerpunktthema zur Auswahl:

A) Mitarbeiterdatenschutz

- Bewerbung & Personalaktenführung & Mitarbeiterkontrolle
- Mitarbeiterdatenverarbeitung am Beispiel von ERP-Systemen

B) Kundendatenschutz

- Gewinnung & Betreuung/Bindung & Analyse von Kunden
- Kundendatenverarbeitung am Beispiel von CRM-Systemen

C) Sozialdatenschutz

- Umgang mit besonders sensiblen Daten
- Sozialdatenverarbeitung am Beispiel von Krankenkassen

→ ausschlaggebend für Übungsaufgaben!

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

- Klassische Geschichtsdarstellung (Zeitskala)
- Alternative Geschichtsdarstellung (Schutzziele)
- Rechtsgeschichte (Gesetze & Rechtsprechung)

Klassische Geschichtsübersicht

1) Anfänge (vor 1977)

- Persönlichkeitsrecht (Herrenreiter-Urteil) → Privatsphäre
- weltweit 1. Datenschutzgesetz in Hessen

2) 1. BDSG (1977)

- Schutz personenbezogener Daten vor Missbrauch der Beeinträchtigung schutzwürdiger Belange der Betroffenen bei der Datenverarbeitung

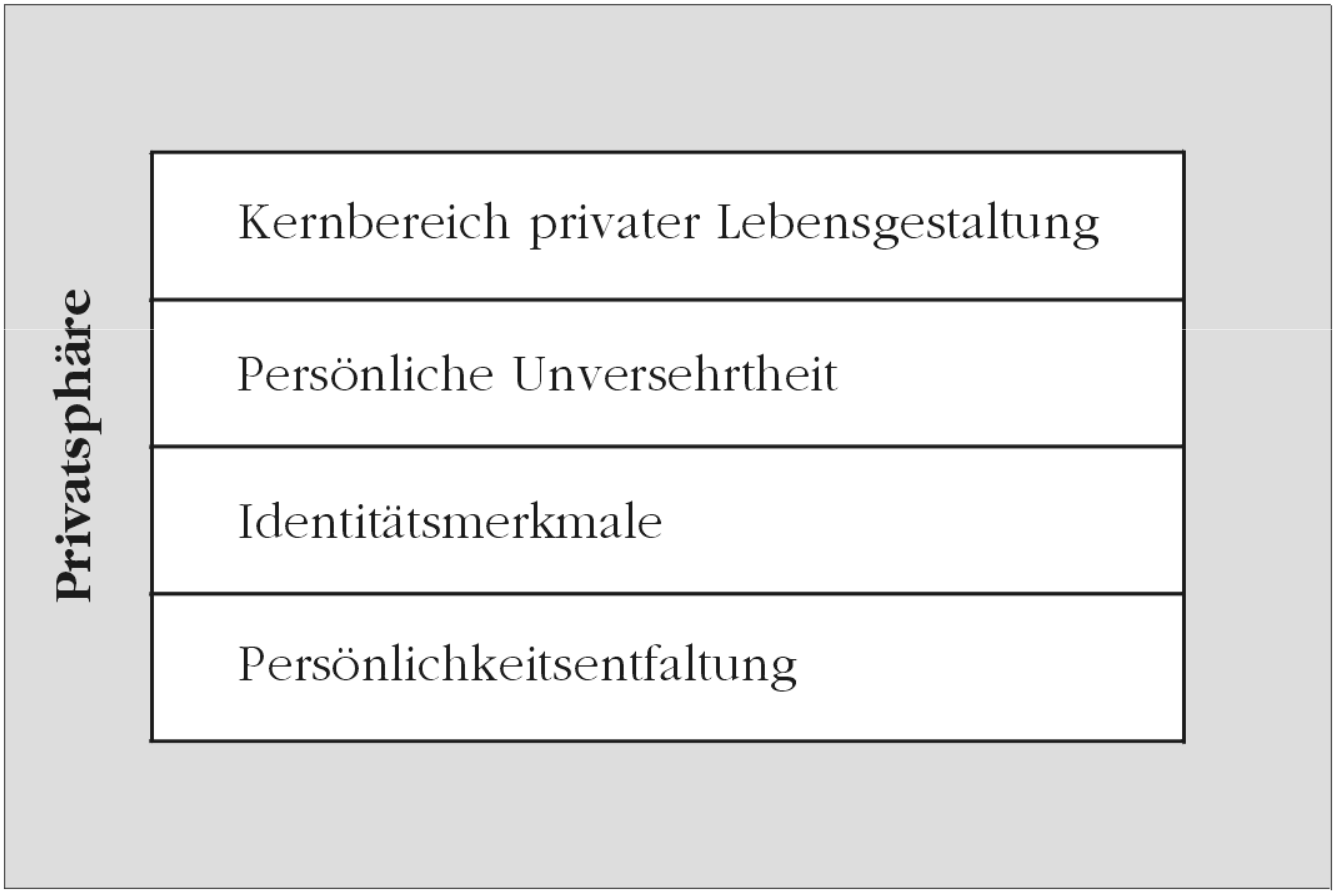
3) 2. BDSG nach Volkszählungsurteil (1990)

- Informationelles Selbstbestimmungsrecht (Volkszählungsurteil)
- Schutz des Einzelnen vor Beeinträchtigung seines Persönlichkeitsrechts beim Umgang mit personenbezogenen Daten

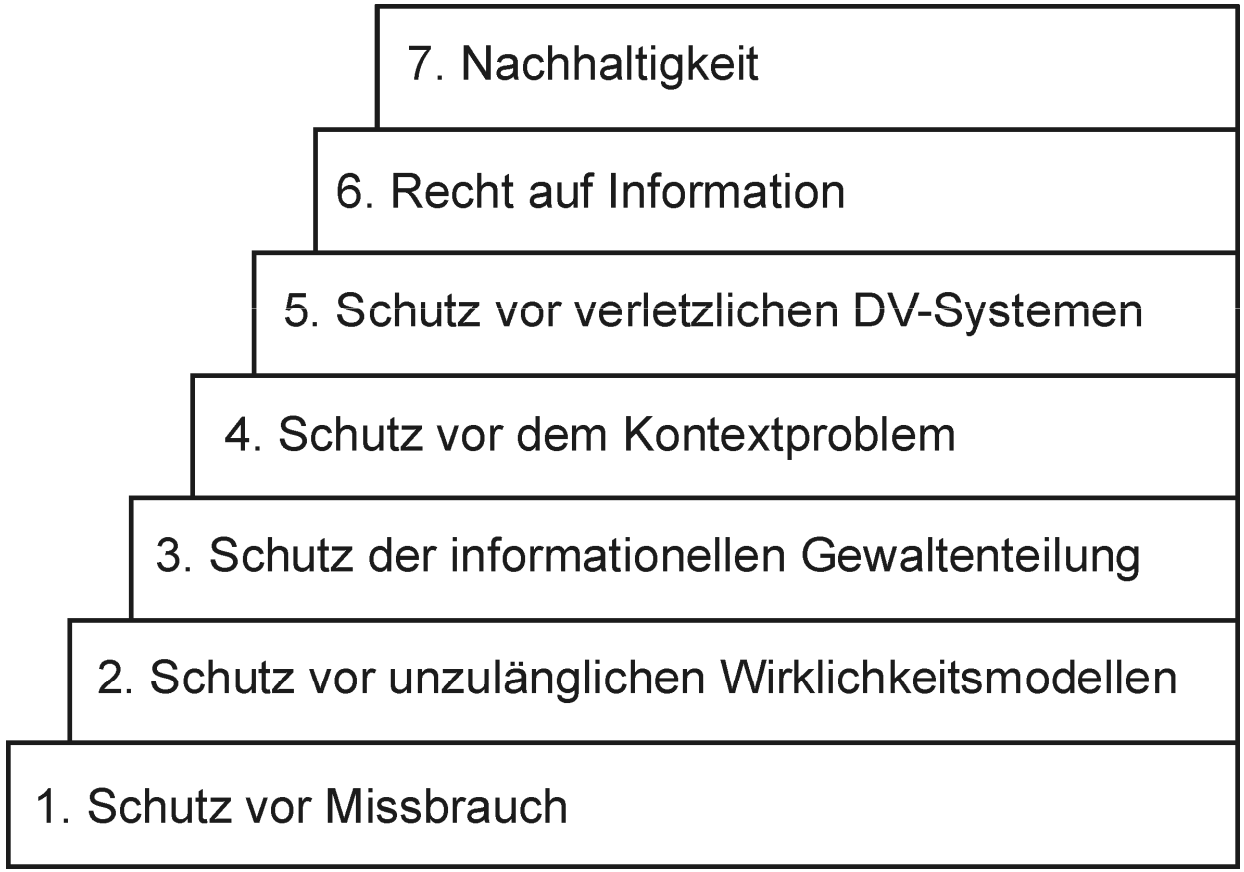
4) 3. BDSG nach EU-DSRL (2001)

- international vergleichbarer Datenschutz
- Vorabkontrolle besonders sensibler Datenverarbeitungen

Bestandteile der Privatsphäre



Alternative Geschichtsübersicht anhand der 7 Schutzziele

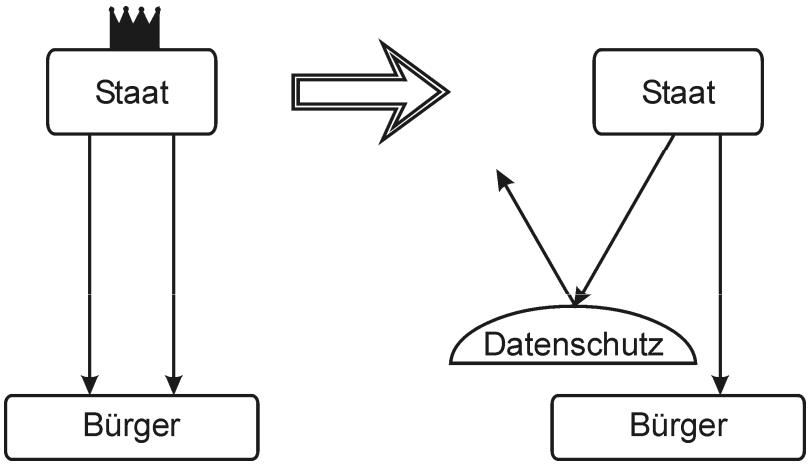


Datenschutz als Abwehrrecht (1)

- Ausgleich des Ungleichgewichtes

→ **Schutz vor Missbrauch** (Ende 60er)

→ Kontrolle durch Datenschutz-beauftragte!



Datenschutz als Abwehrrecht (2)

- im Zuge der
  1. Rasterfahndung

Merkmal 1:	A	B	**D**	G	**H**
Merkmal 2:	A	C	**D**	E	**H**
Merkmal 3:	B	**D**	E	F	**H**

→ **Schutz vor unzulänglichen Wirklichkeitsmodellen** (Ende 70er)

→ Person D & H weisen alle 3 Merkmale auf!

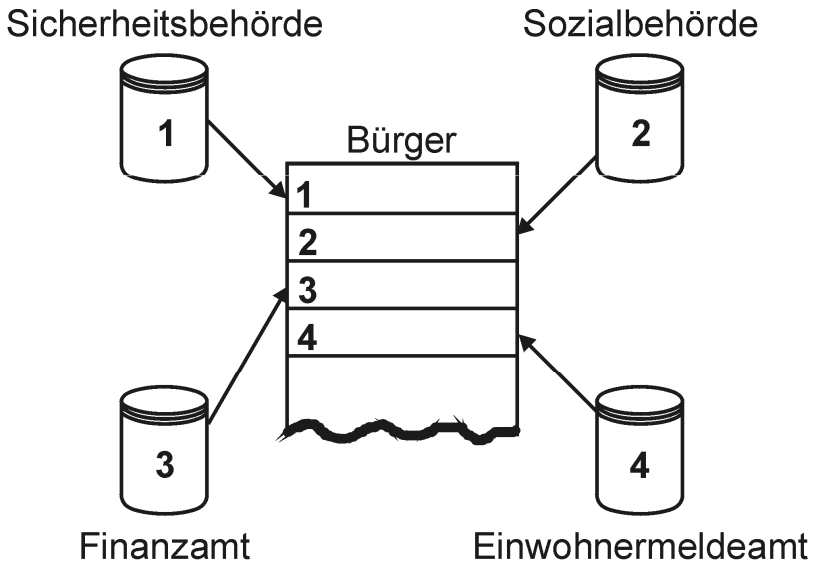
→ keine automatisierte Einzelentscheidung!

Datenschutz als Abwehrrecht (3)

- gegen die Sammelwut des Staates

→ **Schutz der informationellen Gewaltenteilung** (Anfang 80er)

→ personenbezogene Daten anonymisieren!

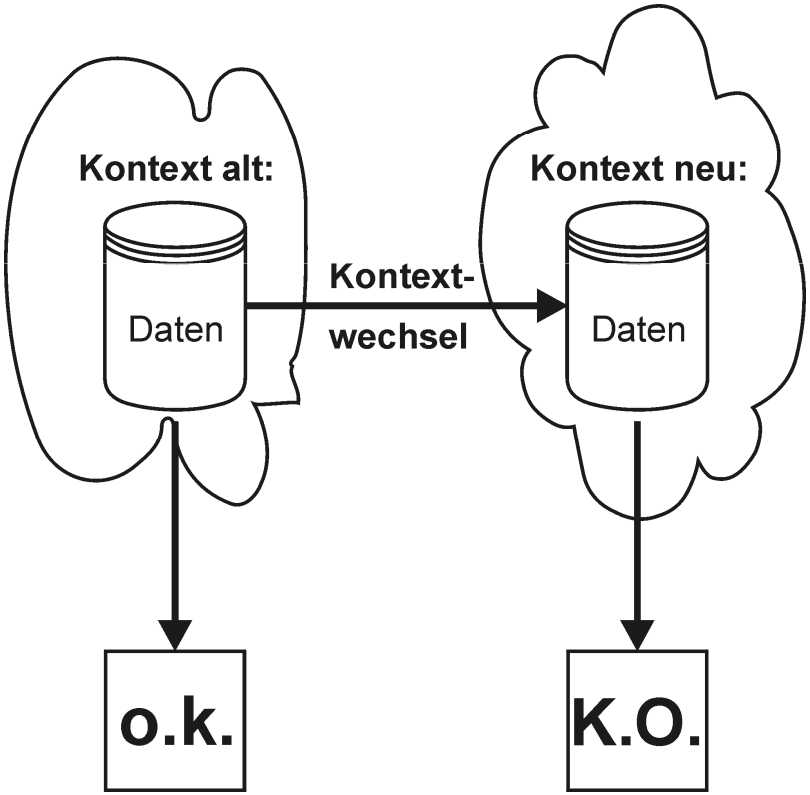


Datenschutz als Abwehrrecht (4)

- gegen die Vernachlässigung des „Alterns“ von Daten

→ **Schutz vor dem Kontextproblem** (Ende 80er)

→ Beachtung von Löschungsfristen!

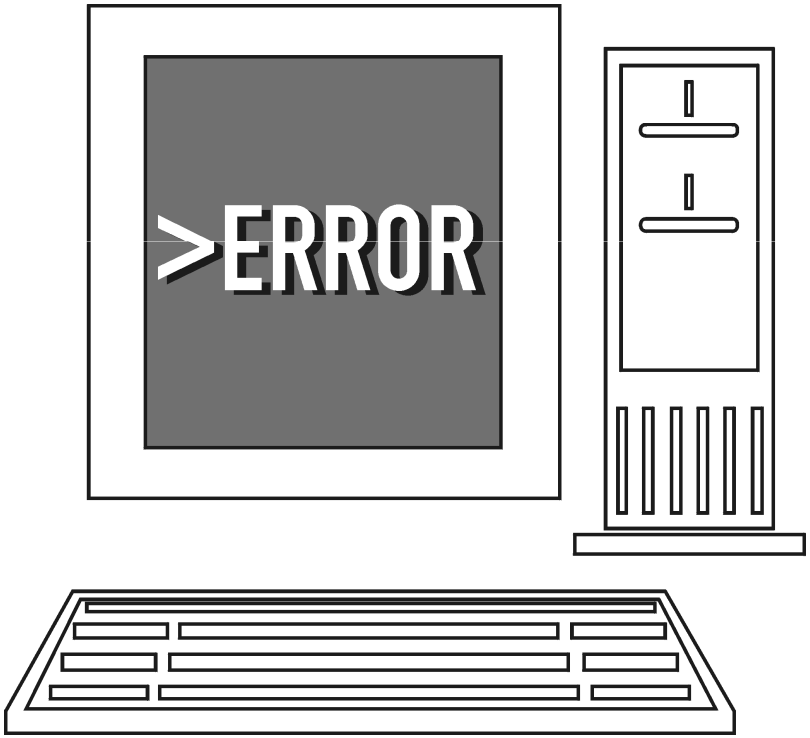


Datenschutz als Abwehrrecht (5)

- gegen den Irrglauben unfehlbarer Software

→ **Schutz vor verletzlichen DV-Systemen** (Anfang 90er)

→ Regelungen zum Schadensersatz!



Datenschutz zur Gestaltung (1)

- die Verwirklichung eigener Rechte erfordert Zugang zu Informationen

→ **Recht auf Information**
(Ende 90er)

→ Akteneinsichtsrecht!

Datenschutz zur Gestaltung (2)

- an Erfordernissen künftiger Generationen orientieren

→ **Nachhaltigkeit**
(Ende 00er?)

- Reversibilität von Entscheidungen!
- Verantwortlichkeit von Handlungen!

Ergebnis der 7 Schutzziele

- Datenschutz hat viele Facetten
- Datenschutz entstanden als Abwehrrecht gegen übermächtigen Staat
- Ausrichtung des Datenschutzes verändert sich
- Datenschutz ist eher Schutz der Informationen über Personen
- Datenschutz ist Schutz vor unerwünschten Verfahren
- Informationstechnik beschleunigt Entwicklung des Datenschutzes

Rechtsgeschichte: Gesetze

1970 Hessen: (erstes!) Datenschutzgesetz
1977 BRD: Bundesdatenschutzgesetz (Version 1)
1978 NRW: Grundrecht auf Datenschutz in Landesverfassung
1980 BRD: Sozialgesetzbuch X
1990 BRD: Bundesdatenschutzgesetz (Version 2)
1995 EU: Datenschutzrichtlinie
1997 BRD: Informations- u. Kommunikationsdienstegesetz
1998 Brandenburg: Akteneinsichts- u. Informationszugangsgesetz
1998 BRD: Großer Lauschangriff
2001 BRD: Bundesdatenschutzgesetz (Version 3)
2002 BRD: Terrorismusbekämpfungsgesetz
2006 BRD: Informationsfreiheitsgesetz
2006 BRD: Bürokratieabbaugesetz → BDSG (Version 4)

Rechtsgeschichte: Urteile (1)

1958 **BGH: Herrenreiterurteil**
(Schadensersatz für die Verletzung des Persönlichkeitsrechts)

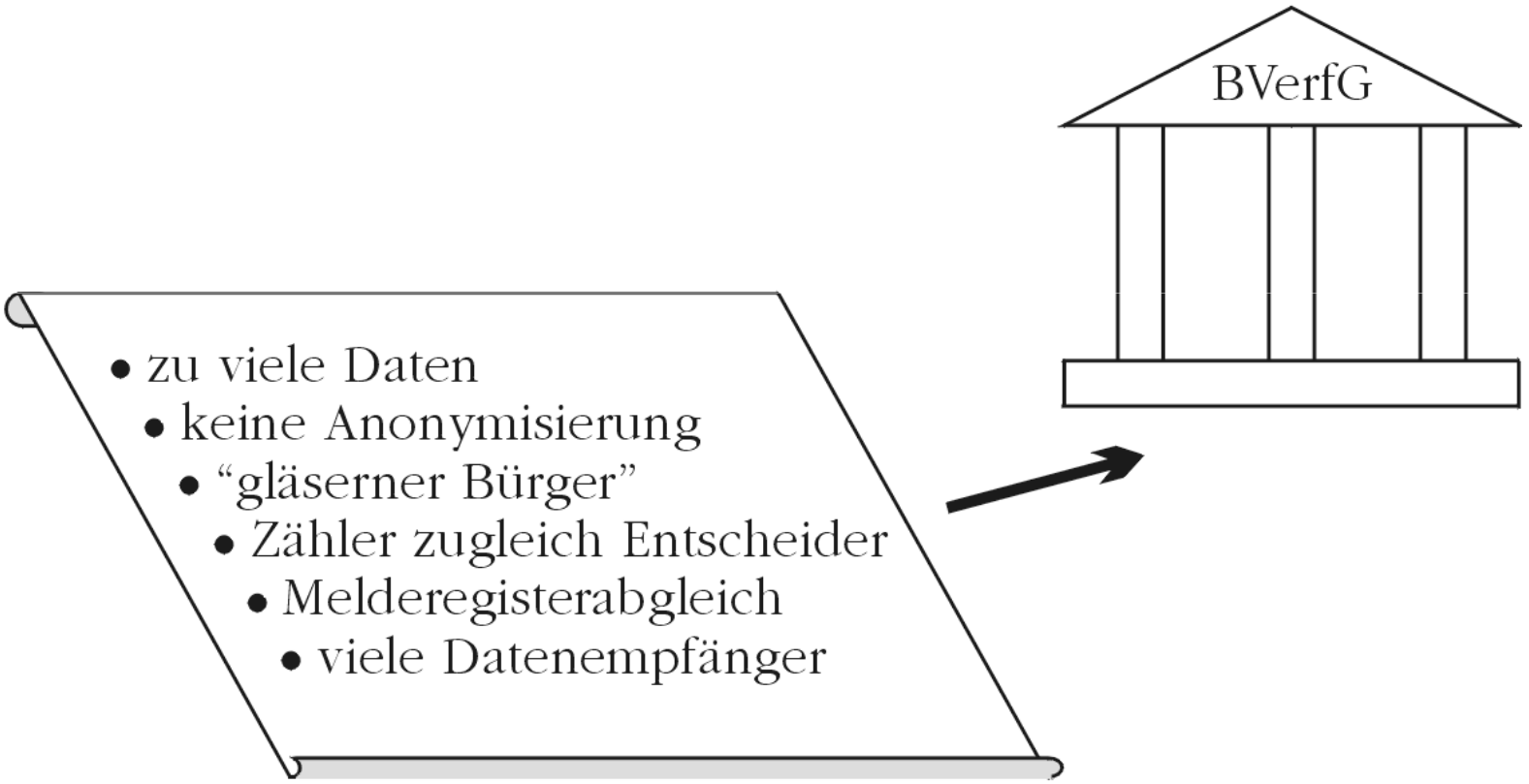
1969 **BVerfG: Mikrozensusbeschluss**
(Menschen nicht als Sachen behandeln)

1970 **BVerfG: Scheidungsaktenbeschluss**
(unantastbarer Bereich privater Lebensführung)

1973 **BVerfG: Lebachurteil**
(Eingriff ins Persönlichkeitsrecht zeitlich begrenzt)

1983 **BVerfG: Volkszählungsurteil**
(informationelles Selbstbestimmungsrecht)

Gründe für Volkszählungsurteil



Definition „informationelles Selbstbestimmungsrecht“

- Zitat aus BVerfGE 65, 1 [43]:
  „Das Grundrecht (des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

Definition 1: Informationelles Selbstbestimmungsrecht

Grundrecht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen

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.

→ Schrankentrias als Schranken!

Einschränkung des inform. Selbstbestimmungsrechts (1)

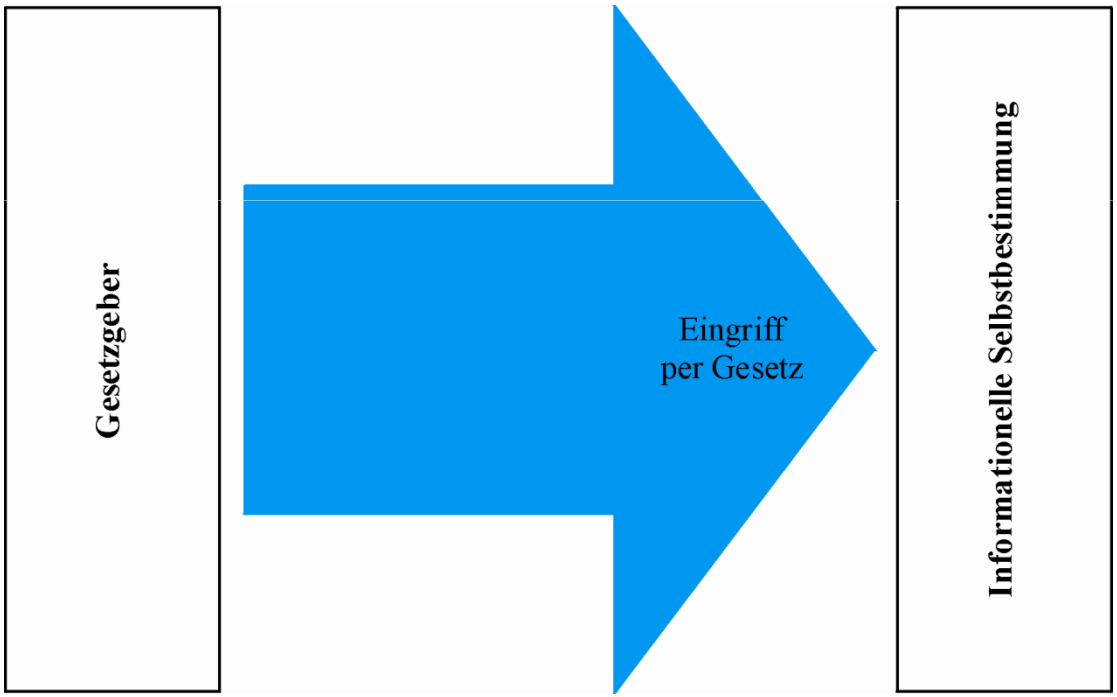
- Zitate aus BVerfGE 65, 1 [43f]
  (Hervorhebung von mir)
  „Der Einzelne ... ist ... eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit.“
  → „Grundsätzlich muß daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung **im überwiegenden Allgemeininteresse** hinnehmen.“
  „Diese Beschränkungen bedürfen ... einer (verfassungs-mäßigen) gesetzlichen Grundlage ... die damit dem rechts-staatlichen Gebot der **Normenklarheit** entspricht (und dem) Grundsatz der **Verhältnismäßigkeit**“

Einschränkung des inform. Selbstbestimmungsrechts (2)

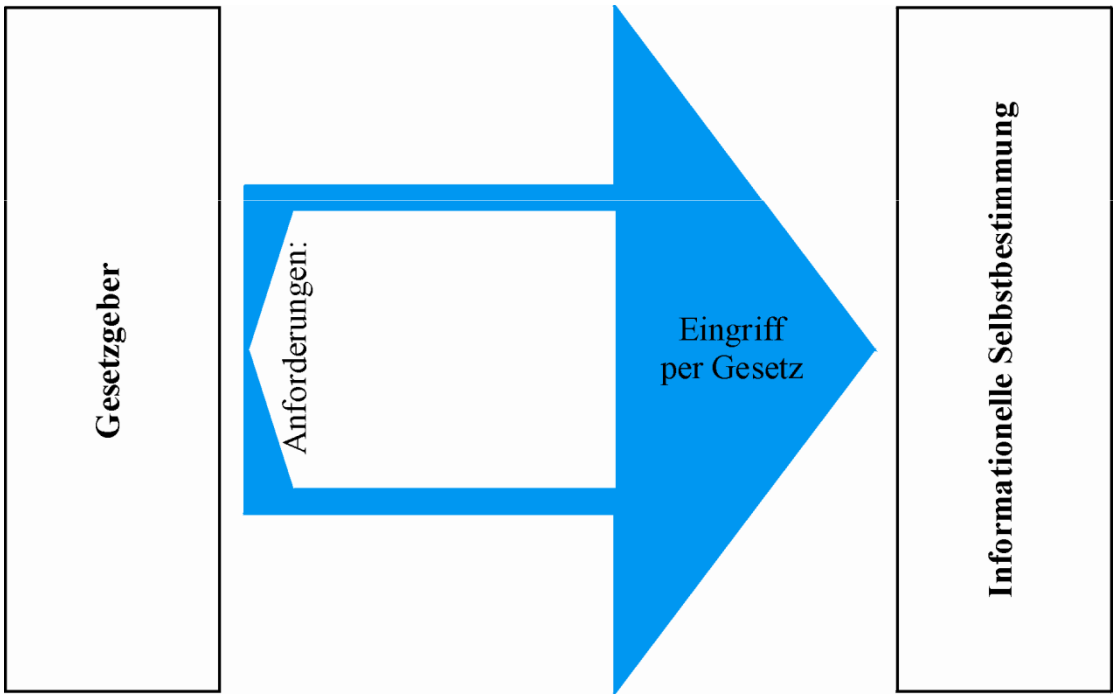
- Zitate aus BVerfGE 65, 1 [44f]
  (Hervorhebung von mir)
  Es gibt „unter den Bedingungen der automatischen Datenverarbeitung **kein ‚belangloses' Datum** mehr."

  „Erst wenn Klarheit darüber besteht, zu welchem **Zweck** Angaben verlangt werden und welche Verknüpfungs- und Verwendungsmöglichkeiten bestehen, läßt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten."
  „Ein überwiegendes Allgemeininteresse wird regelmäßig überhaupt nur an Daten mit Sozialbezug bestehen"

Informationelle Selbstbestimmung (1)

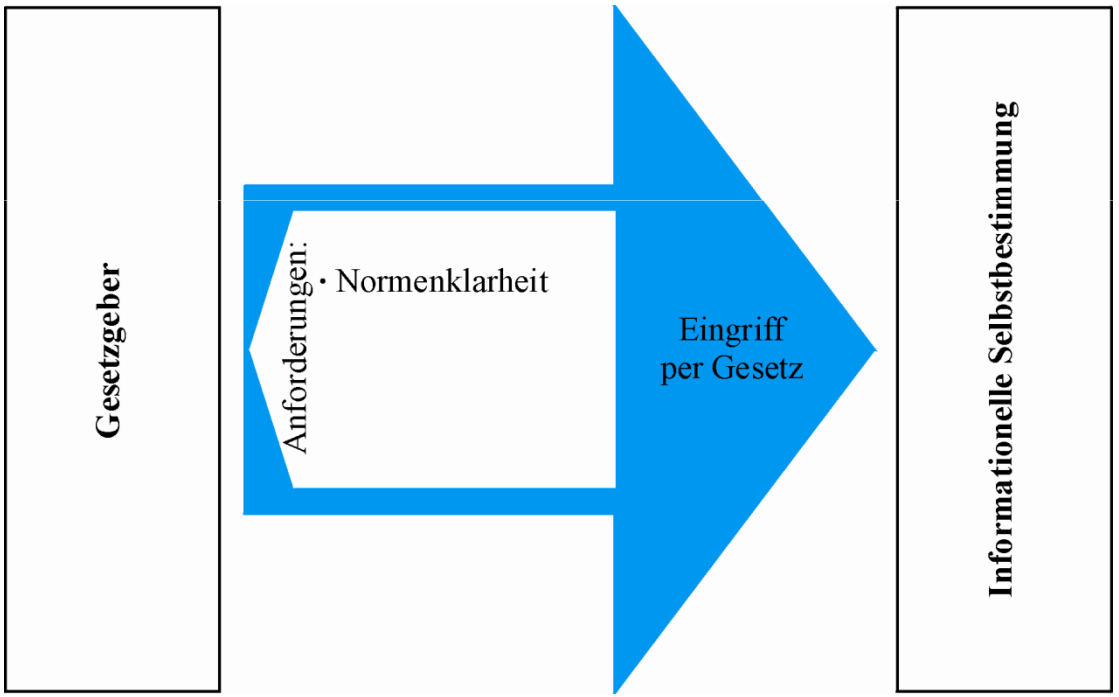


Informationelle Selbstbestimmung (2)



Eingriff erfordert:

Informationelle Selbstbestimmung (3)

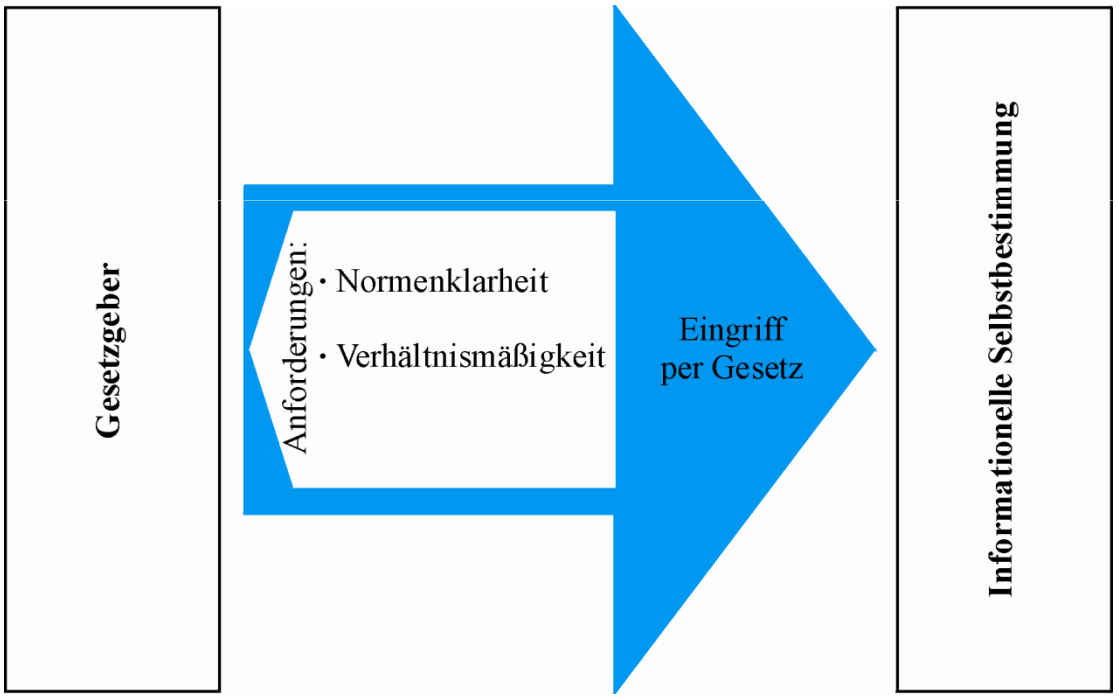


Eingriff erfordert:

Normenklar-heit

Verwendungs-zweck bereichs-spezifisch und präzise bestimmt

Informationelle Selbstbestimmung (4)

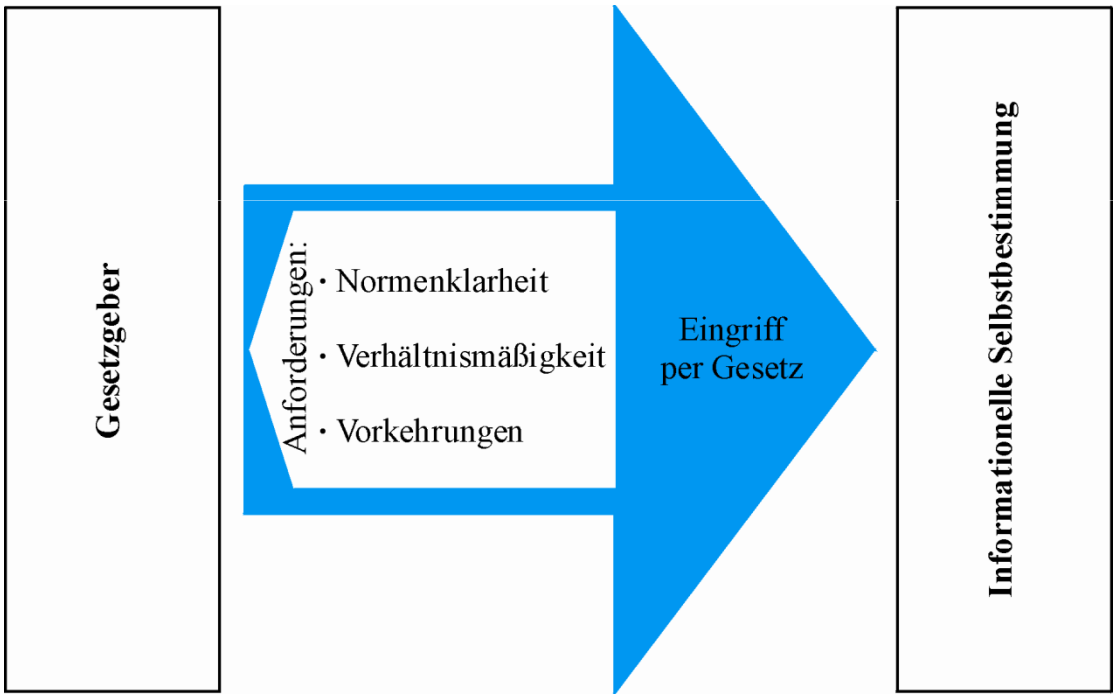


Eingriff erfordert:

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

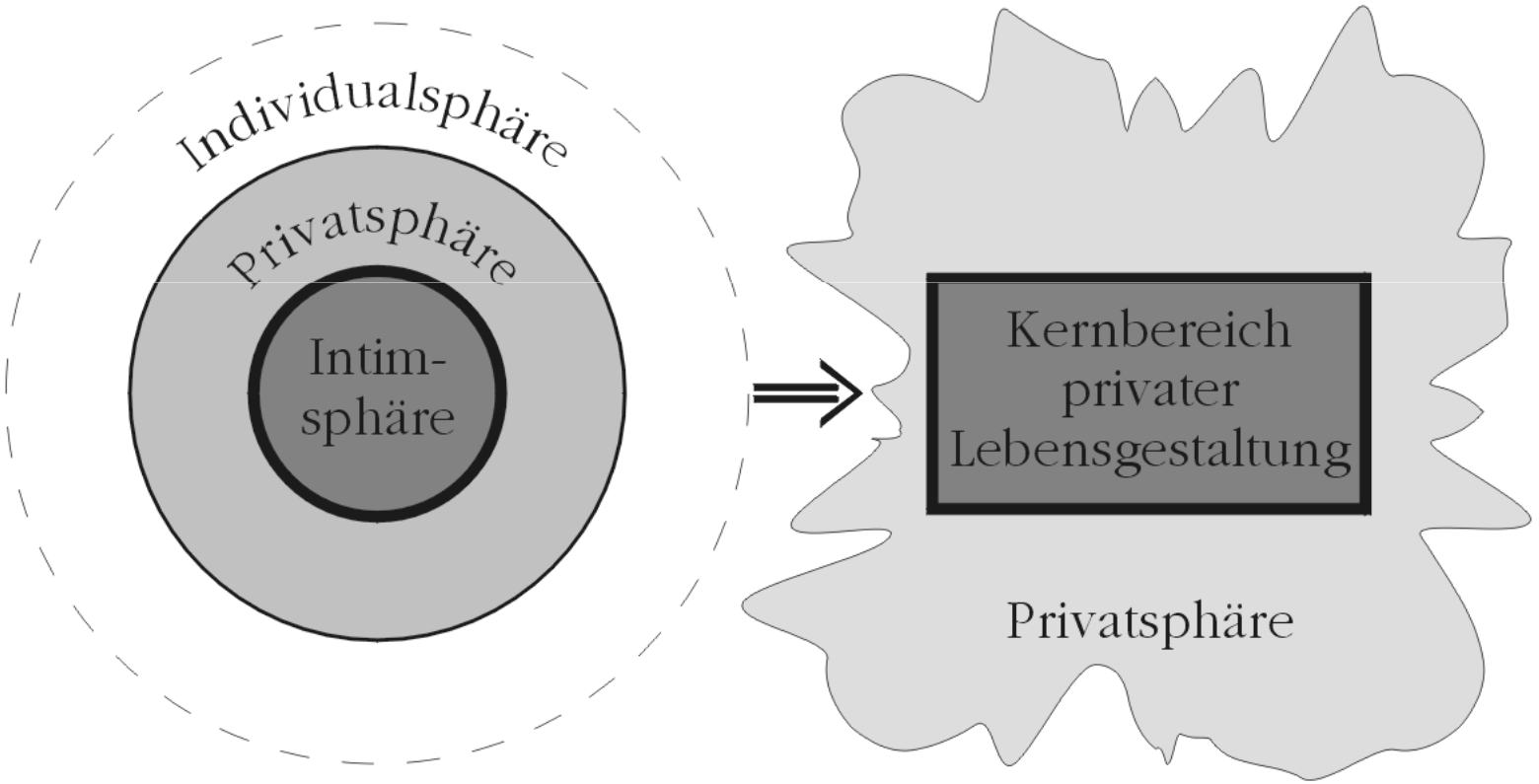
„Schranken-Schranken“

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

- Jeder Eingriff ins informationelle Selbstbestimmungsrecht erfordert gesetzliche Grundlage!

- Das Gesetz wiederum muss normenklar, verhältnismäßig und datensparsam sein!
  (= Schranken-Schranken)

Auflösung der Sphärentheorie



Rechtsgeschichte: Urteile (2)

1999 **BVerfG: Fernmeldeüberwachungsurteil**
(Sicherheitsbehörden haben Einschreitschwellen zu berücksichtigen)

2004 **BVerfG: Urteil zum Großen Lauschangriff**
(absolut geschützter Kernbereich privater Lebensgestaltung)

2006 **BVerfG: Rasterfahndungsbeschluss**
(Eingriff durch Sicherheitsbehörden erst bei hinreichend konkreter Gefahr für hochrangige Rechtsgüter)

2008 **BVerfG: Urteil zur Online-Durchsuchung**
(Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme)

Hinweis zum Fernmeldegeheimnis

Grundlage: **Art. 10 Abs. 1 GG**
„Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich."

Ausprägungen:

- Telekommunikation → Fernmeldegeheimnis
  § 88 TKG: „Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche."

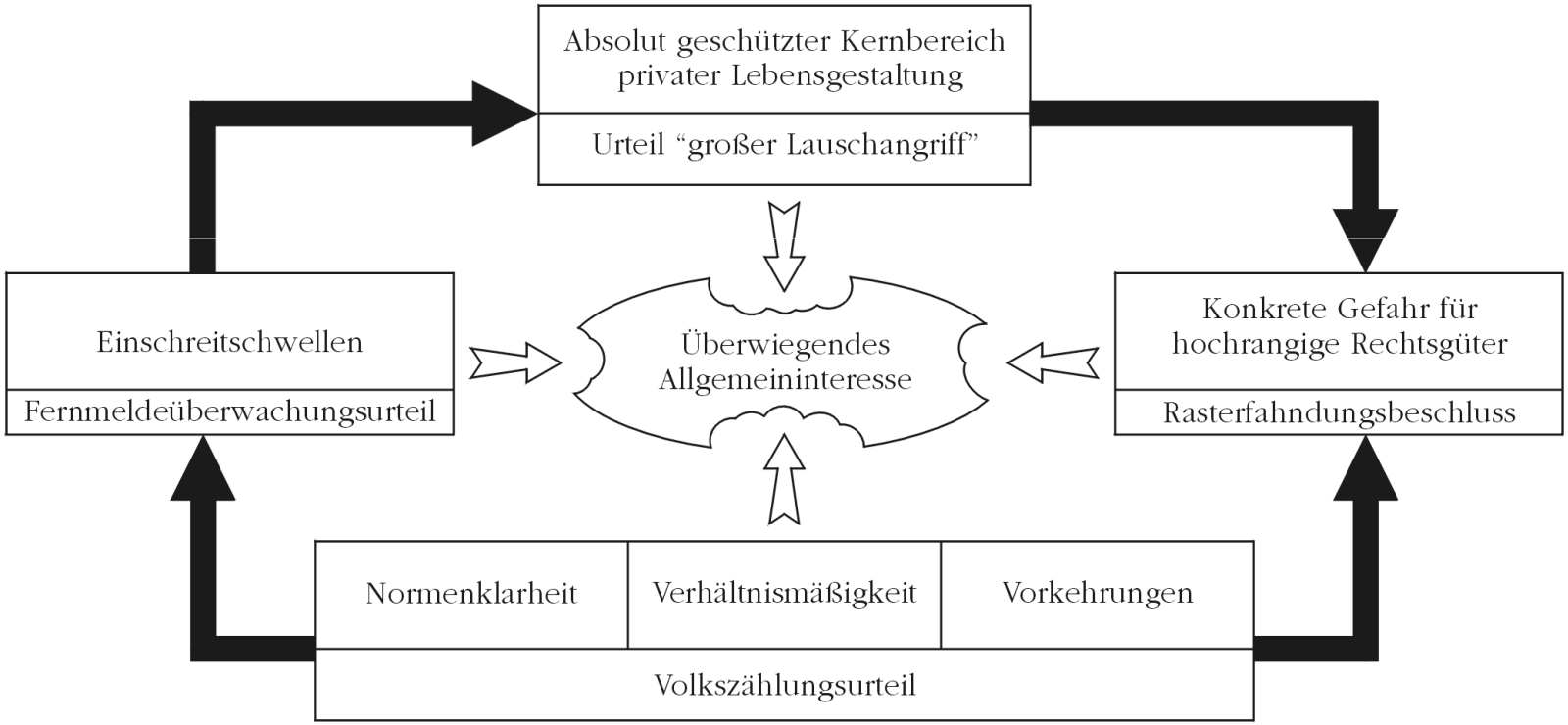
Allgemeines Persönlichkeitsrecht

Grundlage: **Art. 2 Abs. 1 GG**

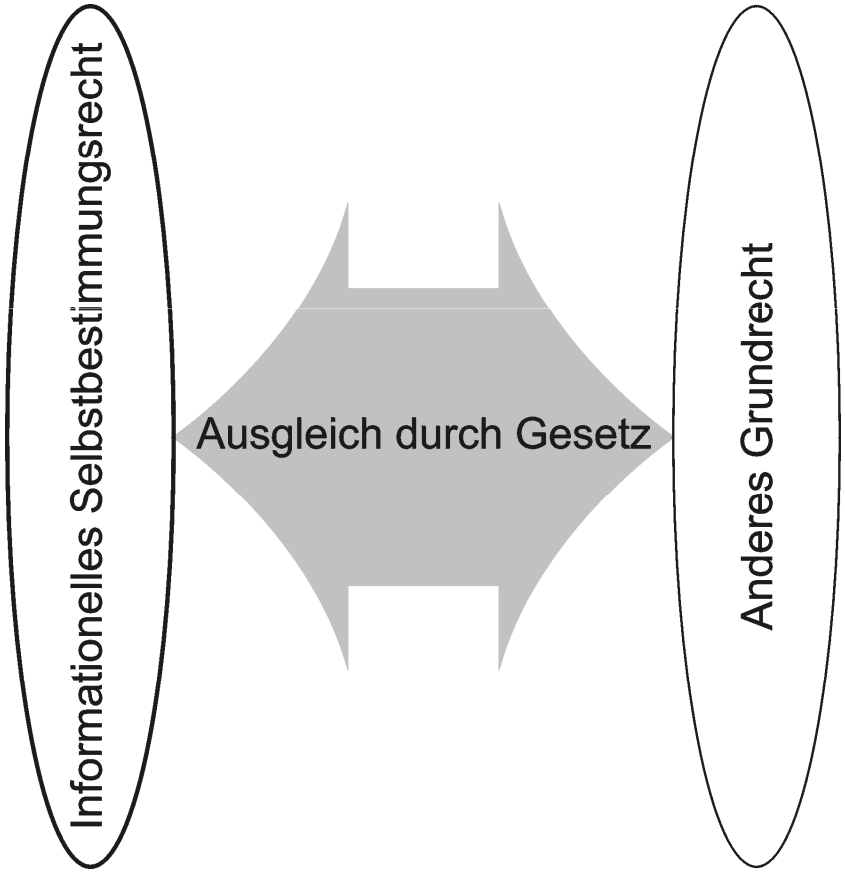
Ausprägungen:

- Informationelles Selbstbestimmungsrecht → Datenschutz
- Urheberrecht → Urheberschutz (§ 2 UrhG)
- Recht am eigenen Namen → Namensschutz (§ 12 BGB)
- Recht am eigenen Bild → Bildnisschutz
  analog: KunstUrhG
  digital: BDSG, soweit KunstUrhG nicht prioritär
- Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

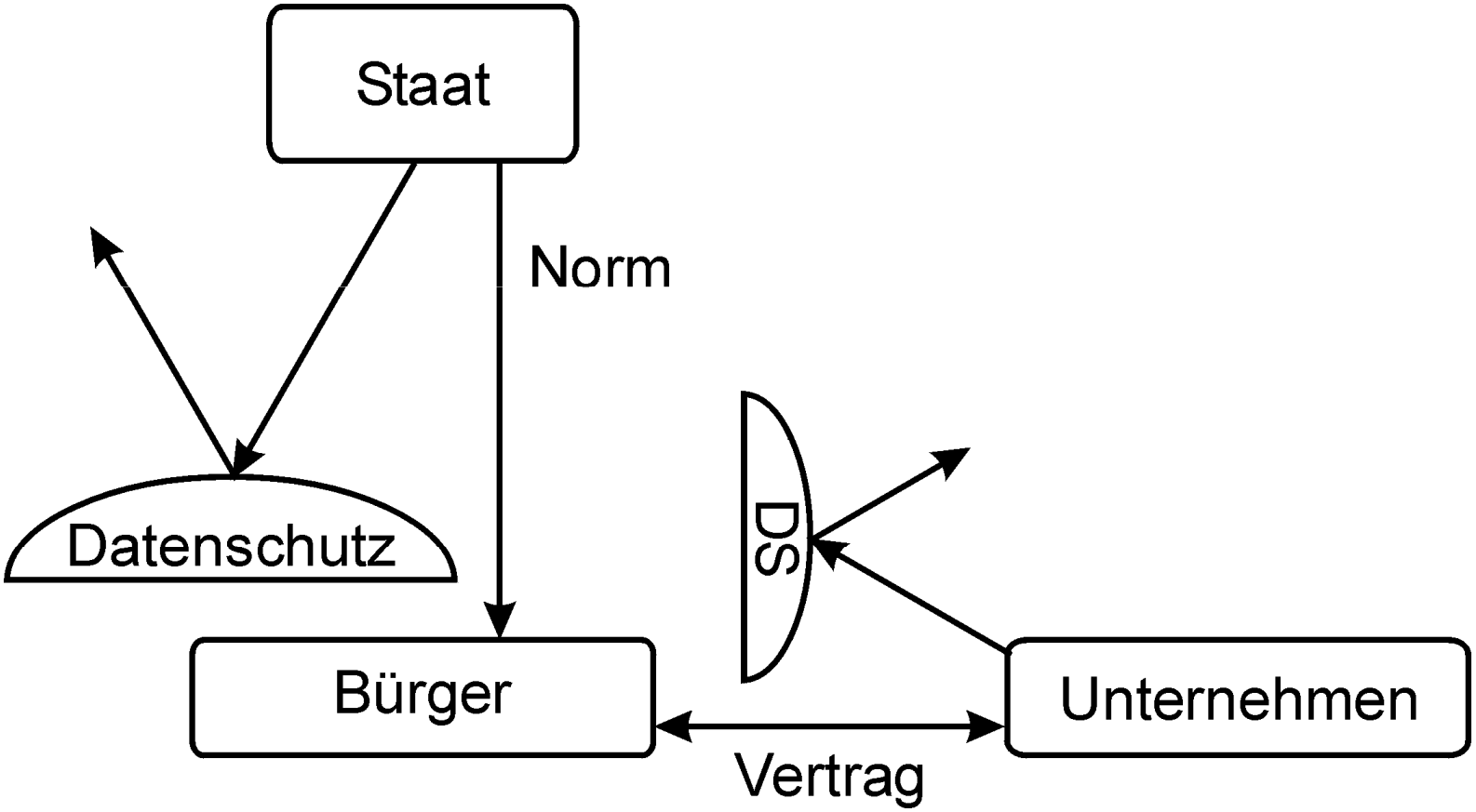
Beschränkung beim „überwiegenden Allgemeininteresse“



Ausgleich zwischen kollidierenden Grundrechten



Ausstrahlungswirkung



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

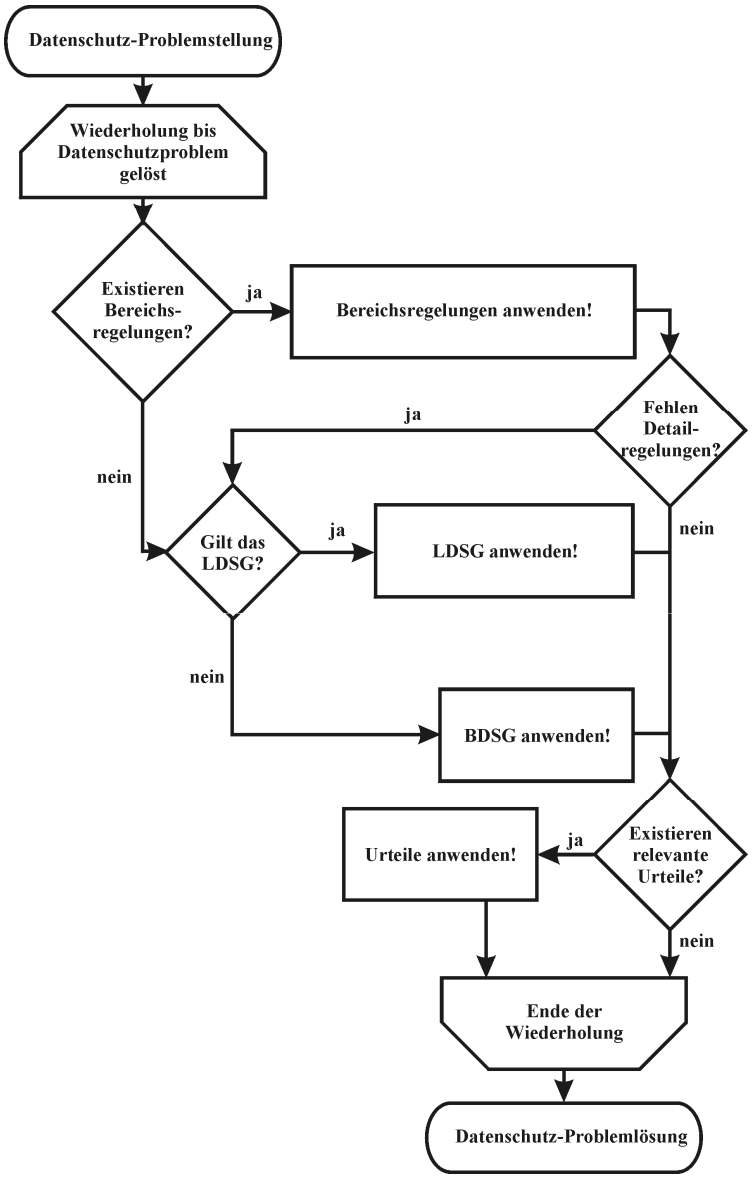
- Subsidiarität
- Verbot mit Erlaubnisvorbehalt
- Zweckbindung
- Transparenz
- Vorrang der Direkterhebung
- Verhältnismäßigkeit
- Datensparsamkeit
- Kontrollprinzip vs Lizenzprinzip
- Betroffenenrechte
- Abgrenzungen
- Der Datenschutzbeauftragte

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

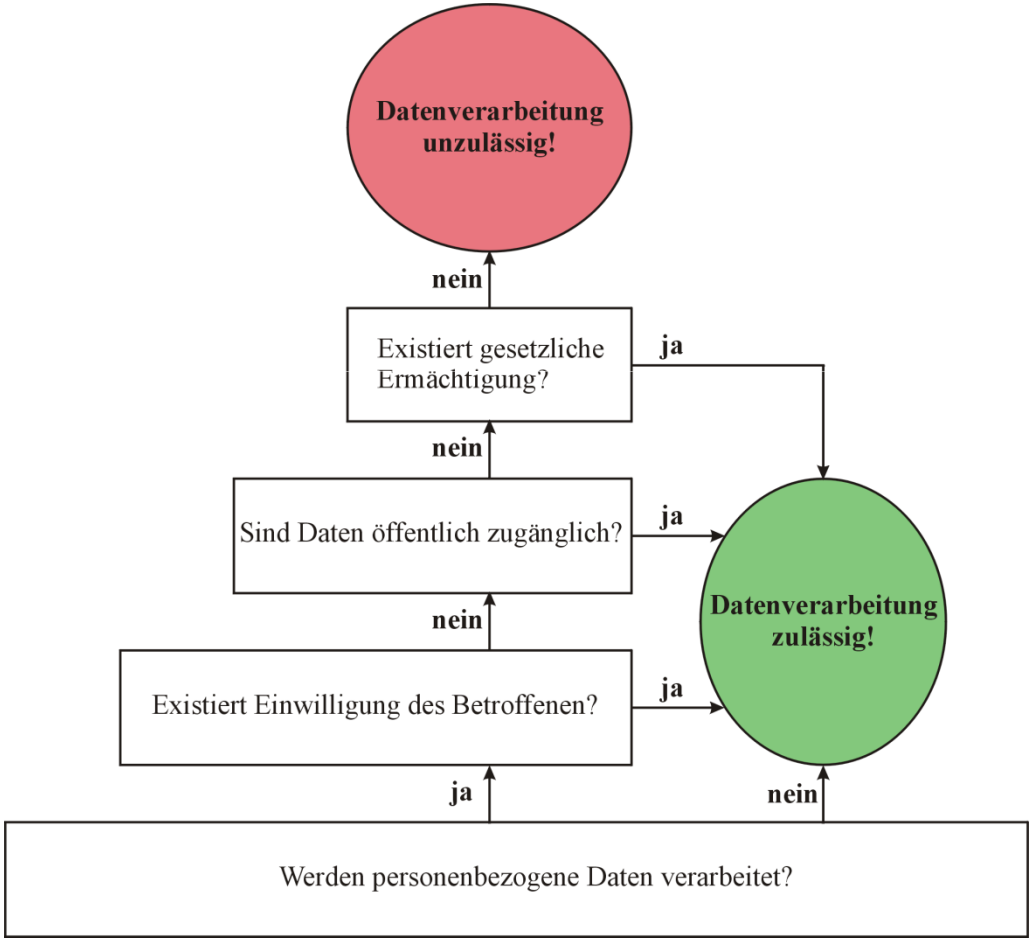
BDSG: Anwendung für
- Unternehmen
- Bundesbehörden
- Behörden im Wettbewerb

LDSGe: Anwendung für
- Landesbehörden
- kommunale Behörden

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

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

Verbot mit Erlaubnisvorbehalt



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)

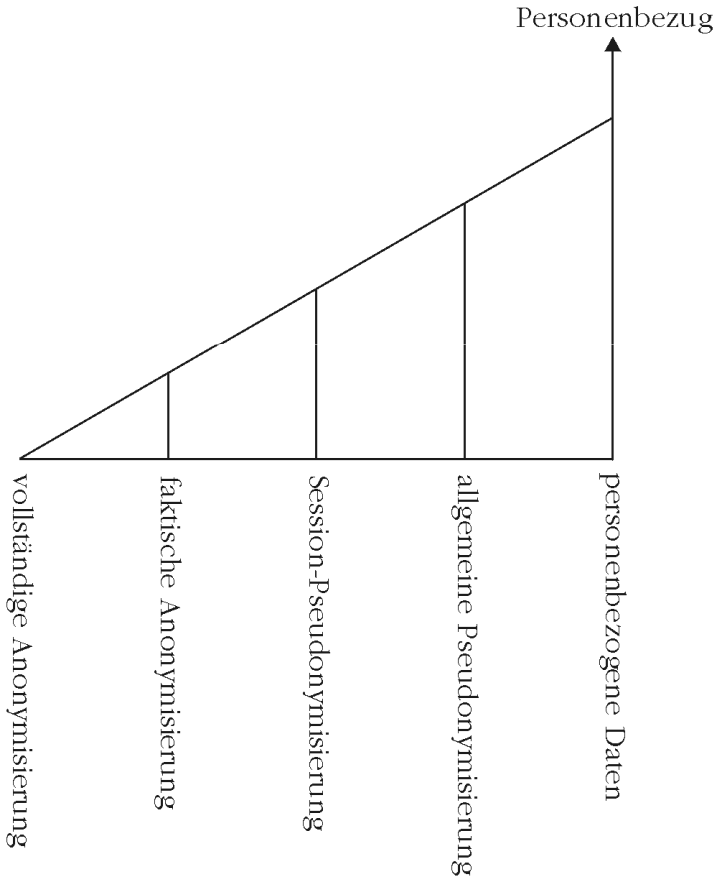
- Abstufung zwischen erforderlich (um Aufgaben rechtmäßig, vollständig & in angemessener Zeit erfüllen zu können) und zwingend (unerlässlich für Aufgabenerfüllung)
- maßgeblich ist der Einzelfall
- geringerer Eingriff ins inf. Selbstbestimmungsrecht vorrangig (z.B. mittels Anonymisierung)
- Autom. Verarbeitung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

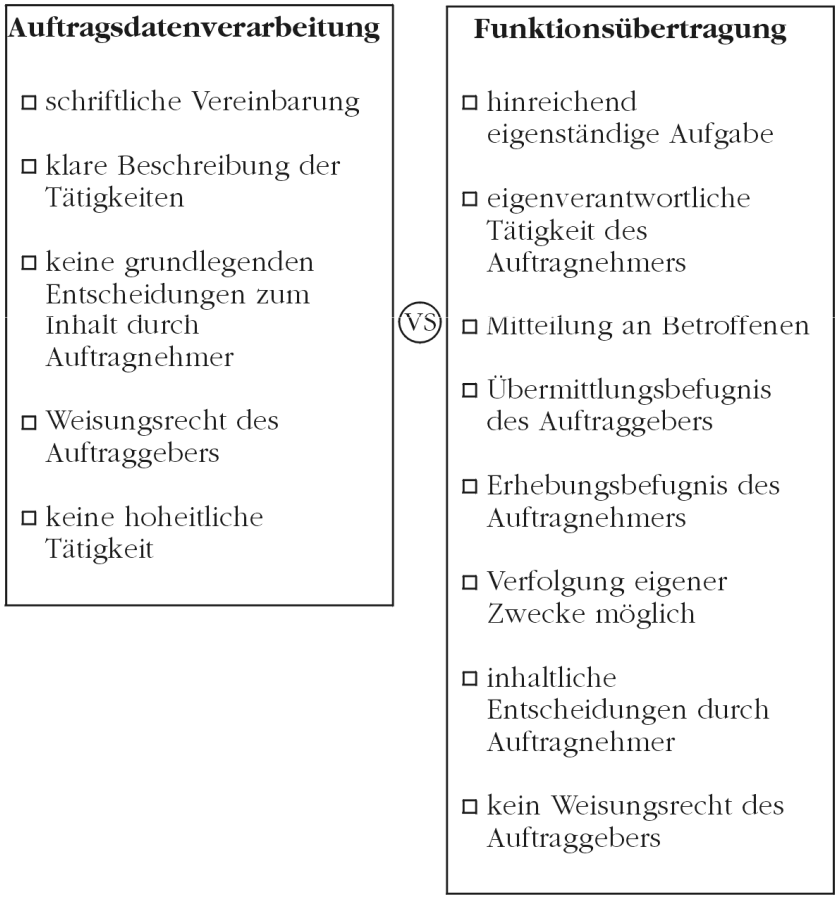
- DV-Durchführende auf Datengeheimnis verpflichtet
- Gewährleistung der Betroffenenrechte
- Auftragsdatenverarbeitung vs Funktionsübertragung
- Datenschutzkontrolle durch Datenschutzbeauftragte

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!

Auftragsdatenverarbeitung vs Funktionsübertragung



Der Datenschutzbeauftragte (1)

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 (2)

Anforderungen an Datenschutzbeauftragte:

- **Fachkunde**: Datenschutzrecht, Datenverarbeitung, betriebliche Organisation, Didaktik, Psychologie
- **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:

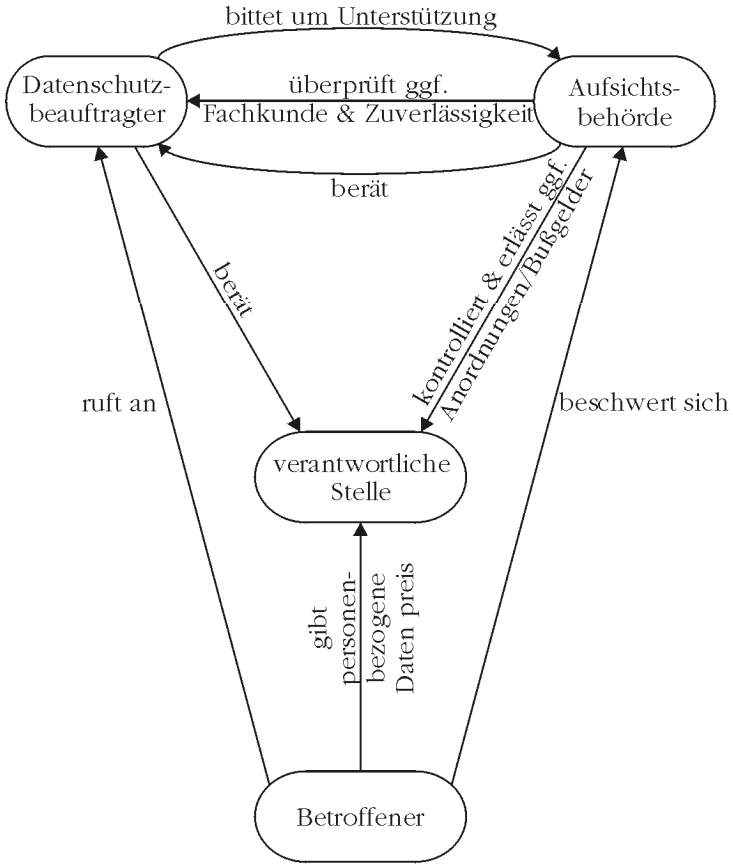
- Recherchen zur aktuellen Rechtslage
- Lesen & Auswerten von Fachartikeln
- Vorbereitung von & Teilnahme an & Protokollierung von Meetings (Geschäftsführung, IT-Leitung, Fachverantwortliche)
- Erstellung von Stellungnahmen & Verfahrensverzeichnissen
- Durchführung & Dokumentation von Vor-Ort-Kontrollen & 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)

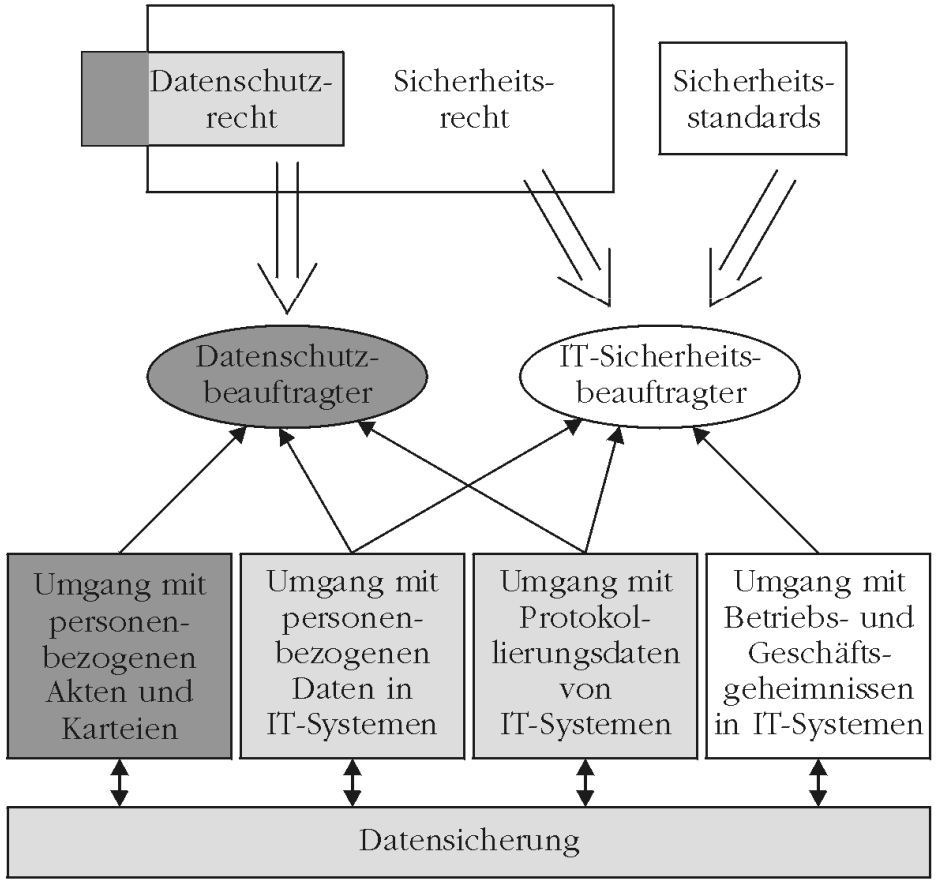
Unerfreuliche Erfahrungen eines Datenschutzbeauftragten:

- komplexe Materie erfordert permanente Erneuerung der Informationsbasis
- verspätete Information hat Mehrarbeit zur Folge
- Buhmann bei Verlangsamung der „schönen neuen Welt“
- Feststellung von Fehlverhalten wichtiger Mitarbeiter & strukturellen Defiziten
- festgestellte Datenschutzverstöße teilweise Kündigungsgrund von Mitarbeiter
- Durchsicht von Festplatten mit (Kinder-) Pornographie
- Anrufung mit Ziel der Verhinderung arbeitsrechtlicher Aufklärung

Checks & Balances bei der Datenschutzkontrolle



Unterschiede zwischen DSB & IT-Sicherheitsbeauftragter



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

- Begriffsdefinitionen
- klassische IT-Sicherheit vs mehrseitige IT-Sicherheit vs Datensicherheit
- technische & organisatorische Maßnahmen & Datenschutzrisiken
- datenschutzfreundliche Techniken

Daten vs Informationen

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

→**Lösung**: Festlegung von Definitionen!

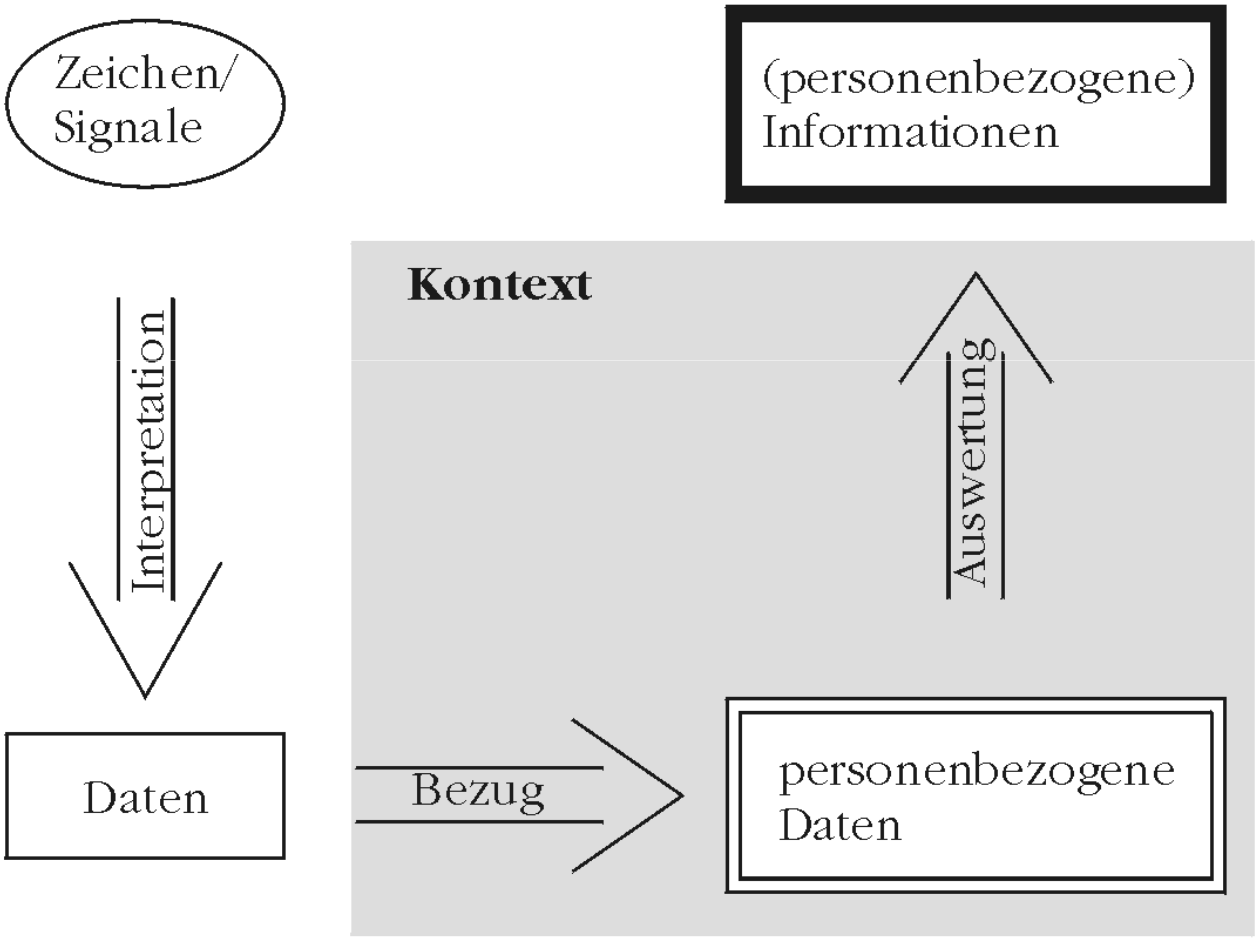
Definition 2: Daten

kontextfreie Angaben, die aus interpretierten Zeichen bzw. Signalen bestehen

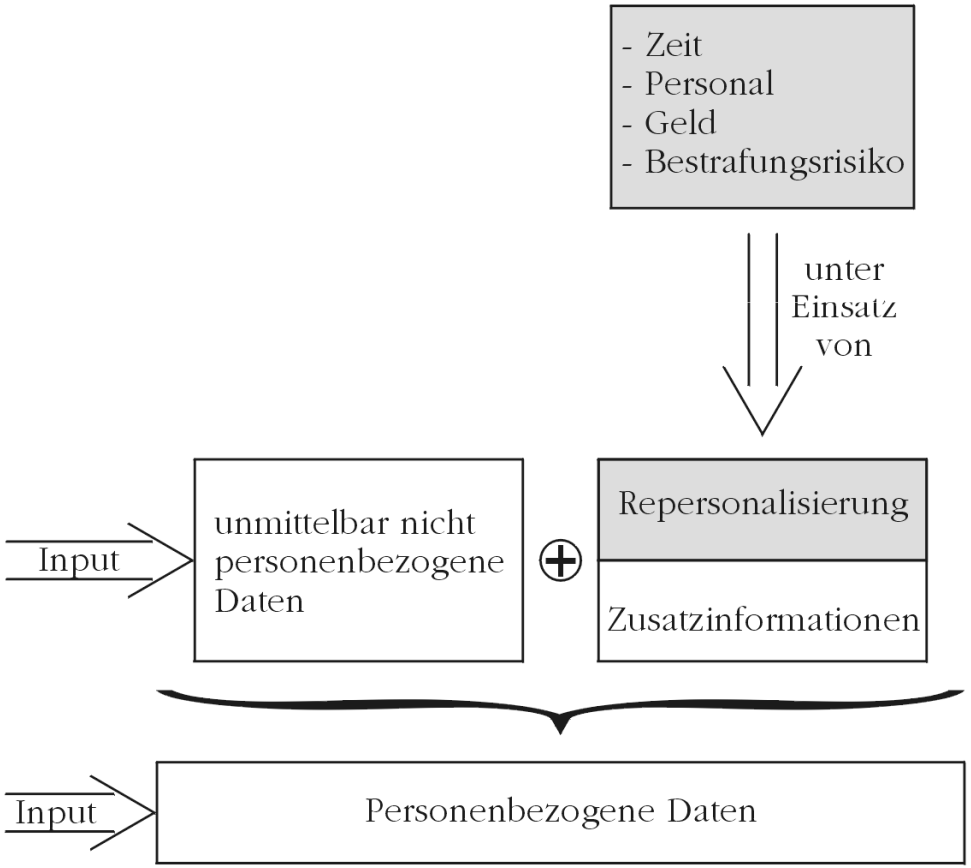
Definition 3: Informationen

Daten, die (durch den Menschen) kontextbezogen interpretiert werden und (prozesshaft) zu Erkenntnisgewinn führen

Vom Datum zur Information



Personenbezogene Daten vs Personenbeziehbare Daten



Begriffsdefinitionen zur Datensicherheit

Definition 4: Sicherheit

Abwesenheit von Gefahren

Definition 5: Datensicherung

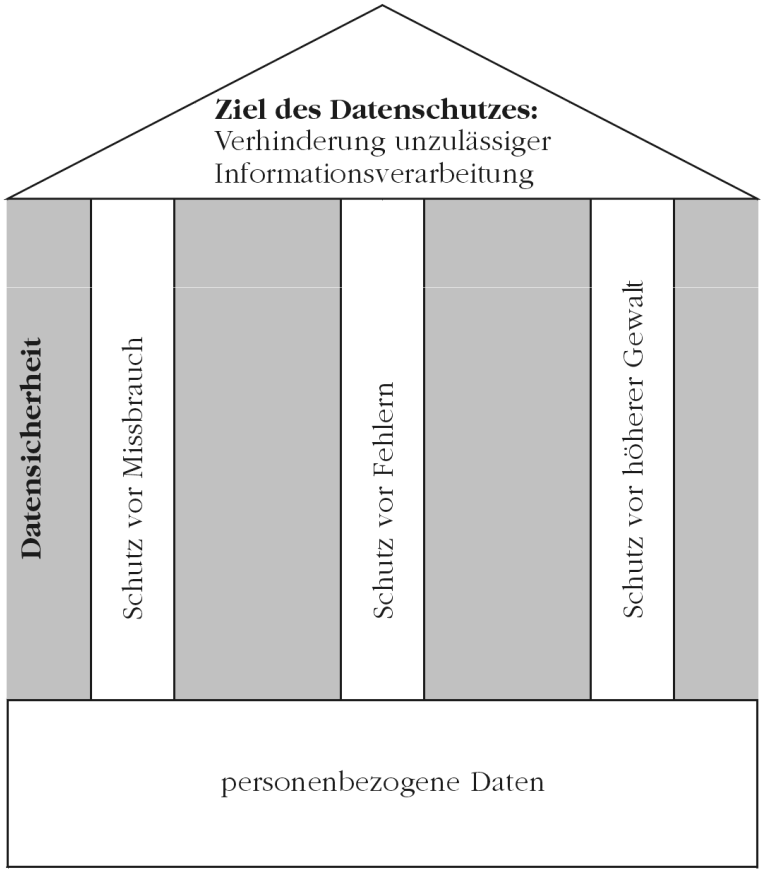
Maßnahmen zur Erhaltung und Sicherung des DV-Systems, der Daten und Datenträger vor Missbrauch, Fehler und höherer Gewalt

→ 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



Begriffsdefinitionen zur IT-Sicherheit

Definition 7: IT-Sicherheit nach § 2 Abs. 2 BSIG

Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen in oder bei der Anwendung von informationstechnischen Systemen/Komponenten

- → Datensicherung nur Teil der Verfügbarkeit: Ausfallsicherheit
- → Datensicherheit nur Spezialfall der IT-Sicherheit hinsichtlich der Daten (statt informationstechnischer Systeme/Komponenten)
- → **technische & organisatorische Maßnahmen dienen Datenschutz und IT-Sicherheit**

Klassische IT-Sicherheit vs Mehrseitige IT-Sicherheit

Klassische IT-Sicherheit:

- Verfügbarkeit
- Unversehrtheit = Integrität
- Vertraulichkeit

→ Vermeidung unzureichender Beeinträchtigungen der IT-Systeme, Daten, Funktionen und Prozesse in Bestand, Nutzung oder Verfügbarkeit

→ Verlässlichkeit der IT-Systeme

→ Sicherheit der Systeme

Mehrseitige IT-Sicherheit:

- klassische IT-Sicherheit
- ergänzt um weitere Sicherheitsziele (insb. Authentizität und Verbindlichkeit)

→ Berücksichtigung der Interessen aller Beteiligten

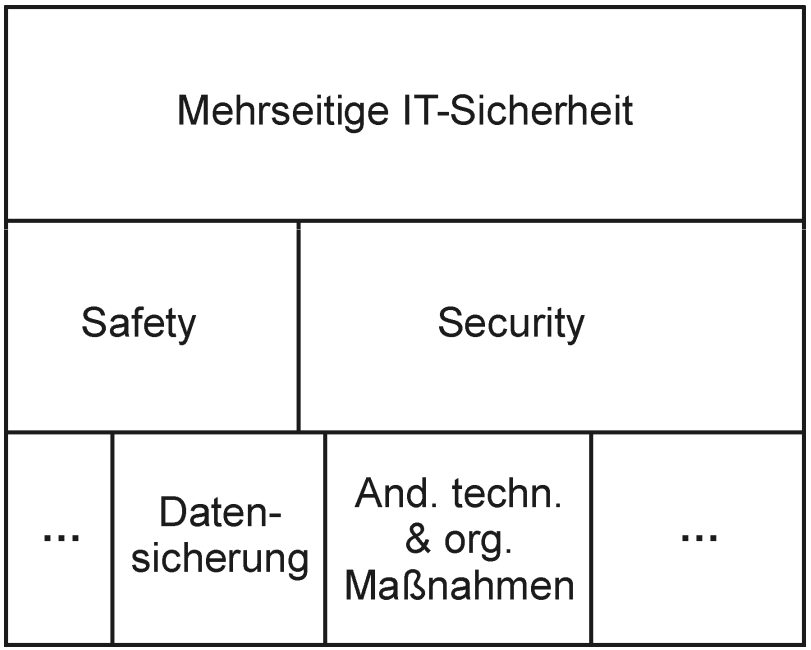
→ Verlässlichkeit und Beherrschbarkeit der IT-Systeme

→ Sicherheit der Systeme und vor den Systemen

Abgrenzung zwischen Datensicherheit & IT-Sicherheit

- Schutz vor unbeabsichtigten Ereignissen: Safety
- Schutz gegen beabsichtigte Angriffe: Security

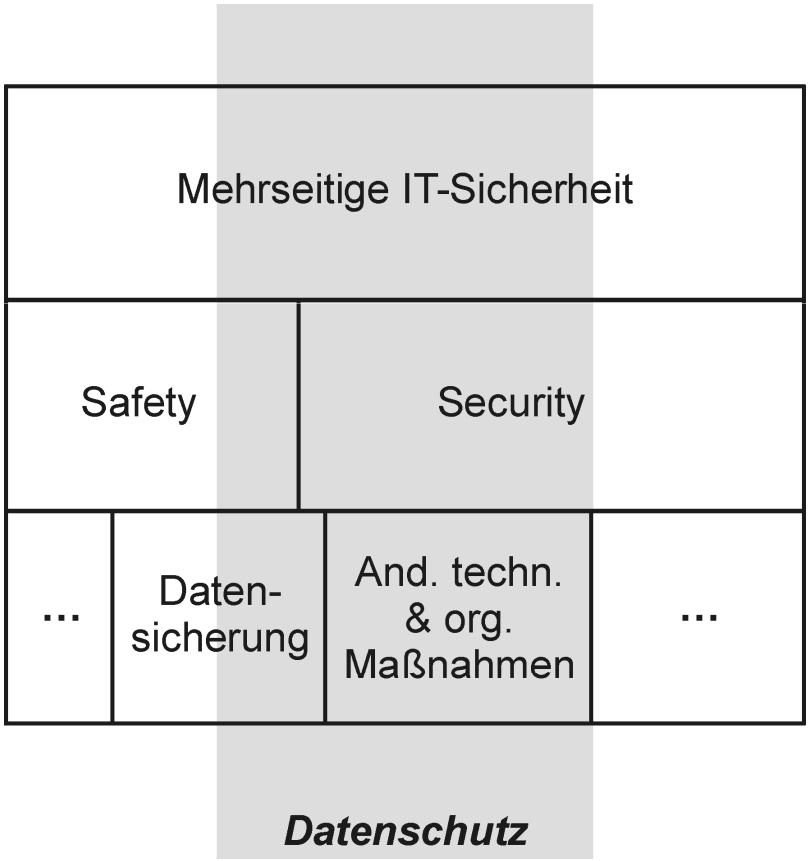
→ **IT-Sicherheit = Safety + Security**



Abgrenzung zwischen Datensicherheit & IT-Sicherheit

Zusammenhang zwischen mehrseitiger IT-Sicherheit und Datenschutz:

- Überschneidung bei der Verarbeitung personen-bezogener Daten
- Schwerpunkt liegt auf Security

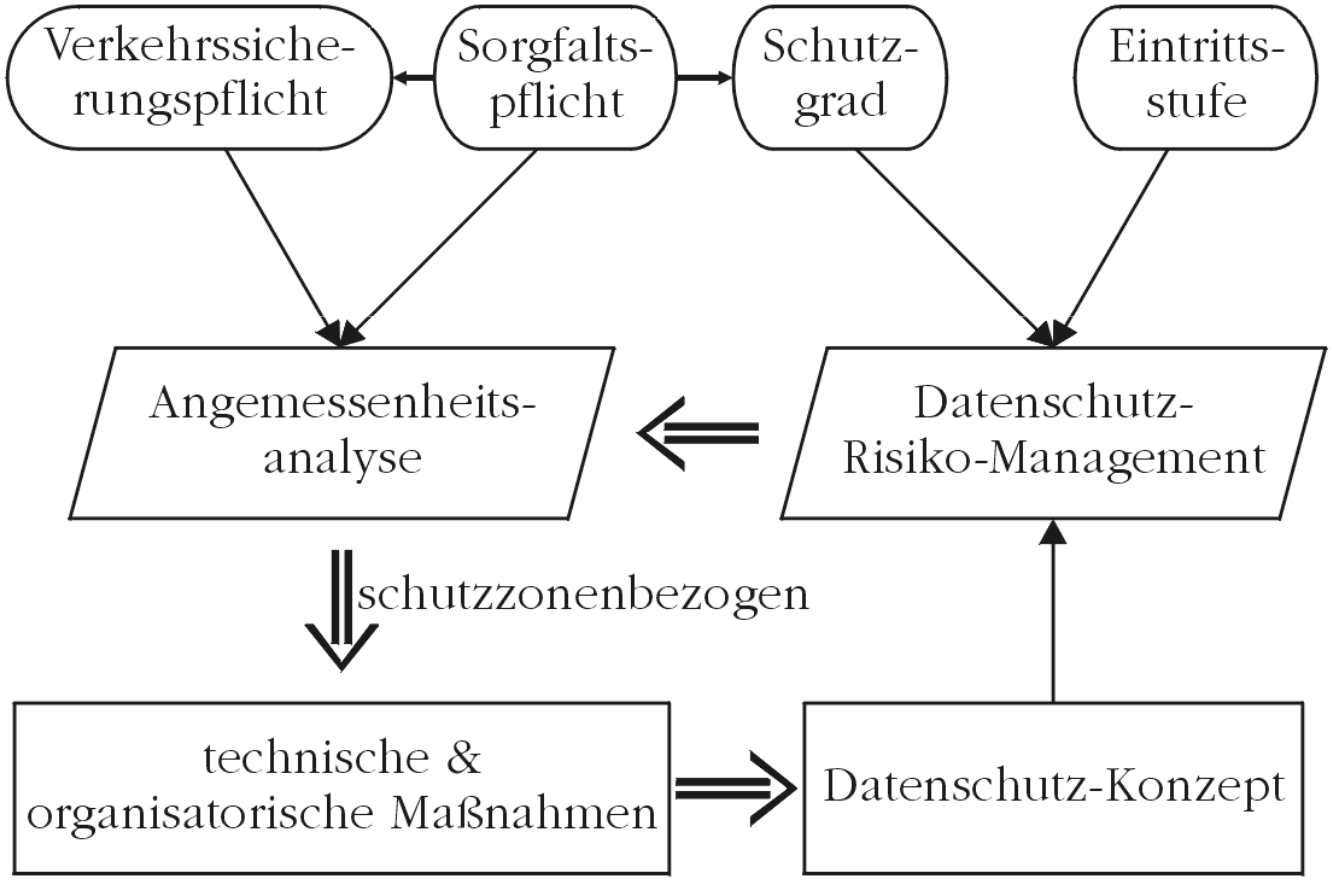


Technische & organisatorische Maßnahmen zum Datenschutz

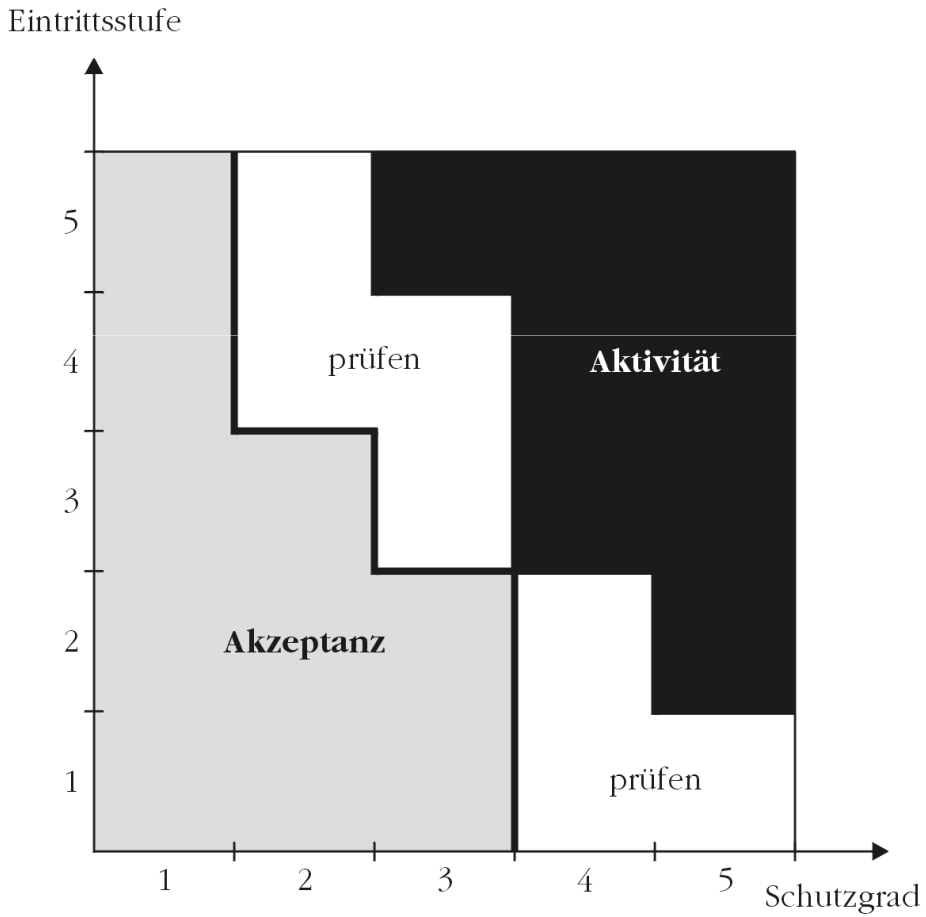
- **Zutrittskontrolle**: Einrichtung physischer Schutzzonen
- **Zugangskontrolle**: Nutzung von IT-Systemen erst nach Authentifizierung
- **Zugriffskontrolle**: Zugriff gemäß begründetem Berechtigungskonzept
- **Weitergabekontrolle**: Einrichtung von Perimeterschutz
- **Eingabekontrolle**: Zuordnung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

→ **Angemessenheit nach Schutzgrad & Verletzlichkeit**

Datenschutzkonzept



Ergebnis Datenschutzrisiko



Kennzeichen datenschutz-freundlicher Techniken

= Privacy Enhancing Technologies (PET; 1995)

- Ziel: weniger Risiken für die Privatsphäre der Betroffenen durch Ausgestaltung eingesetzter Informations- und Kommunikations-technik unter Reduktion des Personenbezugs (→ Anonymität)
- setzt bereits im Vorfeld der Verarbeitung personenbezogener Daten an → Datenvermeidung!
- wichtiges Hilfsmittel vorausschauender Technikgestaltung
- unabhängig von etwaigen Rechtsnormen
- Rückwirkung auf rechtliche Entwicklung („Stand der Technik“)

→ datenschutzgerecht & datenschutzfördernd

frühere Bezeichnung: „Systemdatenschutz“ (Podlech)
→ strukturelle, systemanalytische Ergänzung des individuellen Rechtsschutzes der Betroffenen

Prinzipien datenschutz-freundlicher Techniken (1)

Datensparsamkeit & Systemdatenschutz

- je weniger personenbezogene Daten herausgegeben werden (müssen), desto leichter lassen sich entsprechende Techniken anwenden

→ nur erforderliche Daten verarbeiten

→ frühestmögliche Anonymisierung

→ frühestmögliche Löschung

→ Verschlüsselung bei Kommunikation

→ Beispiel: prepaid-Chipkarten, Mix-Netz, Transaktionspseudonym (z.B. mit verdeckter Zufallszahl bei elektronischem Geld)

Prinzipien datenschutz-freundlicher Techniken (2)

Selbstdatenschutz & Transparenz

- Selbstbestimmung und –steuerung des Nutzers

→ Nutzer entscheidet selbst, wie anonym er Dienste in Anspruch nimmt

→ Verarbeitung wird verständlich offengelegt (Verfahrensverzeichnis) und ist nachprüfbar (→ Identitätsmanagement)

→ Formulierung eigener Schutzziele

→ Nutzung vertrauenswürdiger Institutionen (Trust Center)

→ Unterstützung durch Anwendung der Betroffenenrechte

→ Beispiel: Platform for Privacy Preferences (P3P auf www.w3.org/P3P/)

Beispiel für datenschutzfreundliche Technik: DC-Netz (1)

Teilnehmer A	
Nachricht:	**1011**
Symm. Schlüssel mit B	1100
Symm. Schlüssel mit C	1001
Übertragung 1	**1110**

Teilnehmer B	
Nachricht:	**0000**
Symm. Schlüssel mit A	1100
Symm. Schlüssel mit C	0101
Übertragung 2	**1001**

Teilnehmer C	
Nachricht:	**0000**
Symm. Schlüssel mit A	1001
Symm. Schlüssel mit B	0101
Übertragung 3	**1100**

Übertragung 1	1110
Übertragung 2	1001
Übertragung 3	1100
Ergebnis:	**1011**

DC-Netz = Dining Cryptographers Network (David Chaum 1988)

- Verfahren zur Anonymität des Senders
- für jedes Nutzbit werden n Schlüsselbits bei n Teilnehmer über unsicheren Kanal gesandt und mittels Vernam-Chiffre (per XOR) summiert
- die Teilnehmer vereinbaren paarweise gemeinsame Schlüssel

Beispiel für datenschutzfreundliche Technik: DC-Netz (2)

Vorteile:

- Verfahren garantiert die Anonymität des Senders
- Vernam-Chiffre macht Verfahren mathematisch beweisbar sicher (nutzt one-time-pad-Eigenschaft)
- aktiver Angreifer kann aufgespürt werden, da der Sender den korrekten Wert der überlagerten Nachricht kennt und überprüfen kann

Nachteile:

- Austausch der paarweisen Schlüssel muss sicher erfolgen
- eignet sich nur für die Kommunikation einer beschränkten Gruppe, bei der alle Teilnehmer kommunizieren müssen
- Verfahren muss synchronisiert ablaufen

Andere datenschutz-freundliche Techniken

- **MIX-Netz**: Kommunikation wird über einen Nachrichtenvermittler (Zwischenknoten) abgewickelt, der genügend viele Datenpakete von genügend vielen Sendern sammelt und leitet diese so verändert weiter, dass außer Sender oder MIX-Station keiner die Pakete zuordnen kann. (Empfänger-Anonymität durch „anonyme Rückadressen“ realisierbar) → asynchrone Kommunikation
- anonymisierende Proxies (z.B. anonymizer.com, rewebber.com)
- Verfahren mit Berücksichtigung von Verkehrsanalysen (z.B. AN.ON/JAP = MIX-Netz unter JAP.inf.tu-dresden.de)
- Cookie-Austausch (z.B. CookieCooker.de) bzw. Cookie-Filter (z.B. webwasher.com)

Literaturhinweise

In Semesterapparat 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 der Vorlesung 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