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

Vorlesung im Sommersemester 2023

an der Universität Ulm

von Bernhard C. Witt

Zum Dozenten

it.sec

Bernhard C. Witt

- Principal Consultant für Datenschutz und Informationssicherheit
- Head of IT Governance, Risk & Compliance Management
- geprüfter fachkundiger Datenschutzbeauftragter (UDIS)
- zertifizierter ISO/IEC 27001 Lead Auditor (British Standards Institution)
- Industriekaufmann, Diplom-Informatiker
- seit 2005 Lehrbeauftragter an der Universität Ulm
- seit 2007 Leitungsgremium GI-FG Management v. Informationssicherheit
- seit 2011 Mitglied im DIN-Arbeitsausschuss „IT-Sicherheitsverfahren“
- seit 2012 Leitungsgremium GI-FG Datenschutzfördernde Technik
- 11/2016 – 03/2023 Sprecher GI-Fachbereich Sicherheit

Fachliche Zuordnung

Vorlesung im Masterprogramm (**CS8925**) mit 3 V + 1 Ü = **6 LP**

In den **Informatik-Studiengängen** wie folgt anrechenbar:

Informatik, Medieninformatik, Software-Engineering, Künstliche Intelligenz (Master):

- **Kernbereich** Praktische Informatik

Informatik & Medieninformatik, Software-Engineering (Bachelor):

- **Vertiefungsbereich**

In den **Wirtschaftswissenschaften & Comp. Sc. and Eng.** (Master):

- **Profilbereich** Informatik

In **Informationssystemtechnik** (Master):

- **Vertiefungsbereich** Informatik

Ergänzende Veranstaltungen im WS (aus Institut für Verteilte Systeme):
LV „Sicherheit in IT-Systemen“ (2+2)
LV „Privacy Engineering and Privacy Enhancing Technologies“ (3+1)

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** 14 – 18 Uhr (**Beginn: 14:15 Uhr**) **in H21** (O28)
- Außerhalb der LV Kommunikation über zugehörige Mailing-Liste (datenschutz.informatik@lists.uni-ulm.de), Abo dringend zu empfehlen
- **Vorlesungsmaterial** (Vorlesungsfolien + Übungsblätter) jeweils vorab, Musterlösungen jeweils nach den Übungsterminen **unter**: **https://www.uni-ulm.de/?id=36570**
- **Übungen ergänzen (!) Vorlesung**; an Übungstagen zuerst Übung, dann Vorlesung
- Übungen am 24.04., 15.05. & 05.06. (DS); 19.06., 03.07. & 17.07. (ITS)
- **Klausurtermin** noch zu vereinbaren (üblich: August + Dezember)
- Lehrveranstaltung wird voraussichtlich didaktisch ausgewertet

Hinweise (1)

Kriterien für Notenbonus:

- 50 % Votieren der 6*5 Aufgaben
  (→ 15,0 Votierpunkte; Lösungsidee gibt 0,5 Punkte)
  & 3 Aufgabenlösungen erfolgreich präsentieren*
  * bzw. anteilig weniger bei dauerhaft mehr als 10 Teilnehmern

Prüfung (mit Notenbonus!):

- Klausur
  (1/3 Vorlesung, 1/3 Übung, 1/3 Anwendungen)
- Erfahrungen: Schnitt ~ 2,1 (bei 604 Prüfungen)
  Aktive Teilnahme an Übungen (eigene (!) Lösungen)
  → Notenbonus & bessere Prüfungsvorbereitung
  → ~ 0,8 Notenstufen besser!

Hinweise (2)

Zur evtl. geplanten Aufzeichnung der LV durch Teilnehmende:

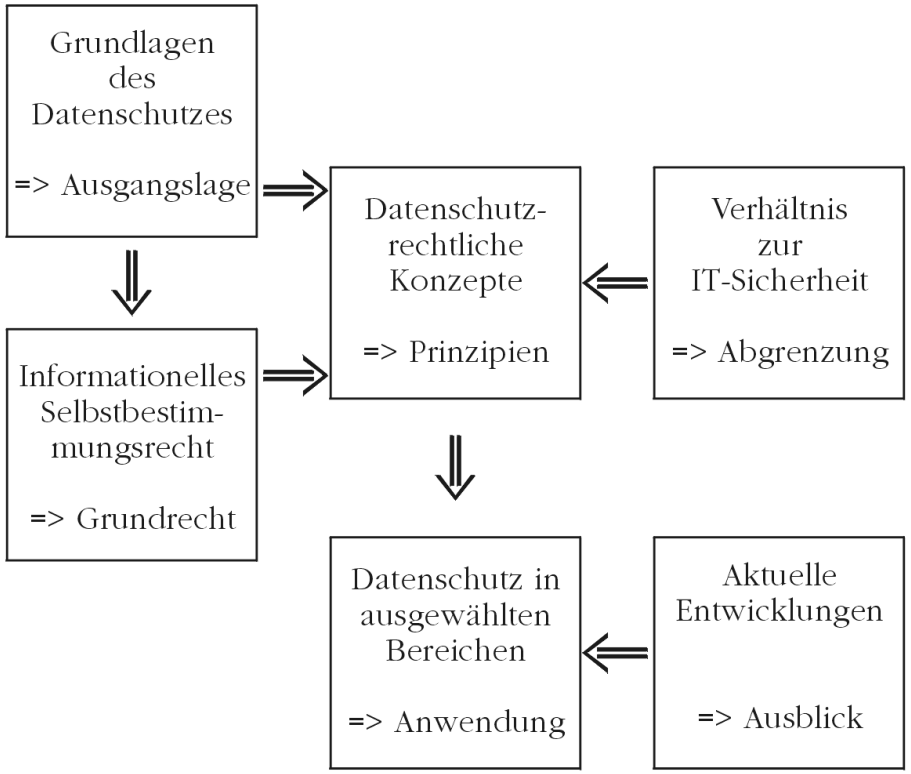
- Eine visuelle und/oder akustische Aufzeichnung der LV ist nicht gestattet!
- Die LV ist keine öffentliche Veranstaltung
- Tangiert werden sowohl die Rechte des Dozenten (Datenschutz & Urheberrecht!) als auch der Teilnehmer (Datenschutz)

  → Aufzeichnung nur mit Einwilligung aller Betroffenen zulässig

  → Aufzeichnungswunsch ist jeweils zu Beginn darzustellen

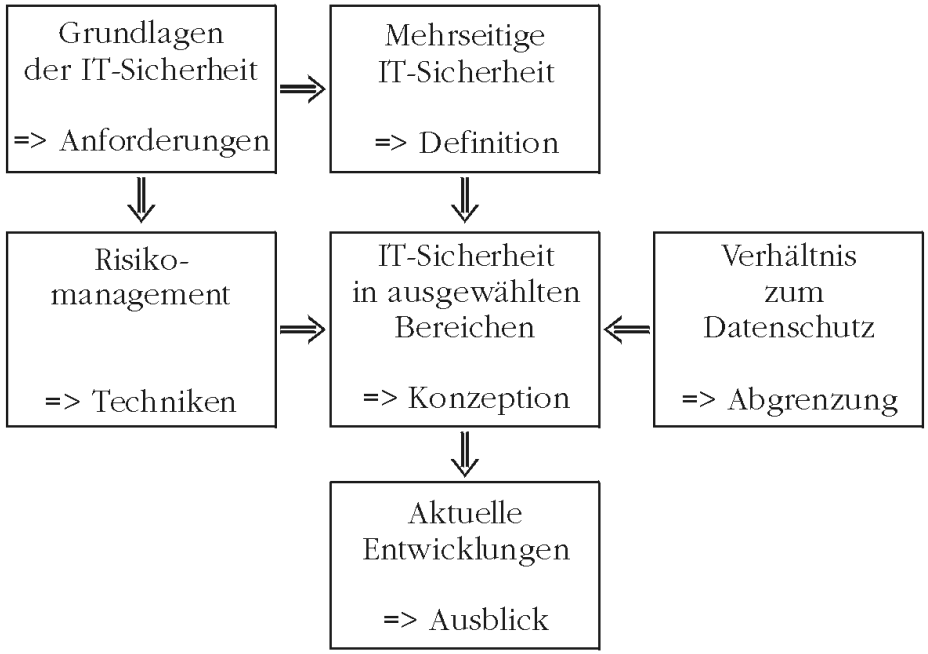
- **Es gibt keine offizielle Aufzeichnung der LV!**

Lehrbuch statt Skript (1)



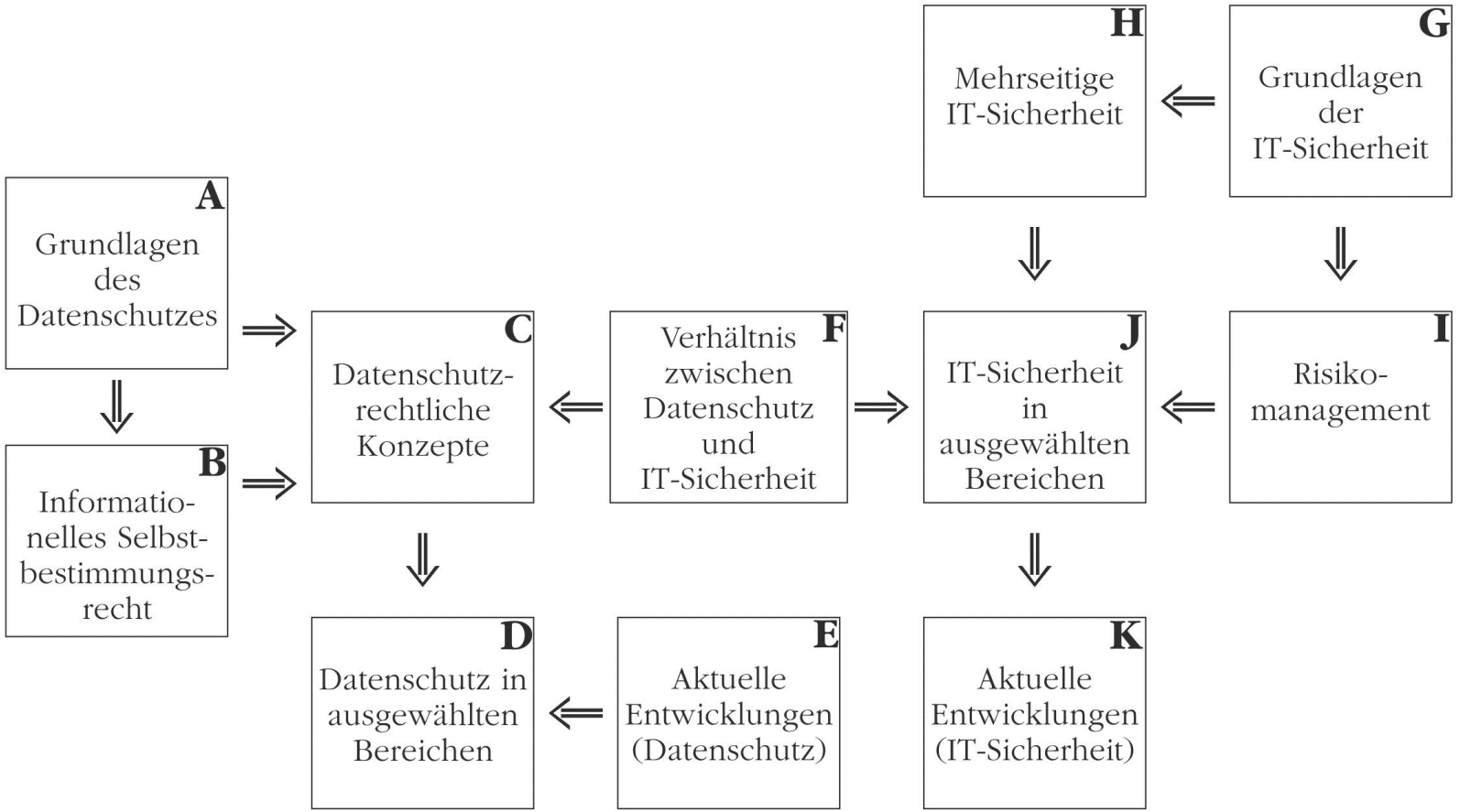
Vorlesung erstreckt sich über alle Kapitel

Lehrbuch statt Skript (2)



Vorlesung erstreckt sich über alle Kapitel

Lehrbücher zusammengefasst



Zusammenhang LV – Lehrbücher

Grundlagen des Datenschutzes		Grundlagen der IT-Sicherheit		Kenntnisse:
A+B	Geschichte des Datenschutzes	**G**	Anforderungen zur IT-Sicherheit	**Anforderungen**
C	Datenschutzrechtliche Prinzipien	**H**	Mehrseitige IT-Sicherheit	**Basistechniken**
A+C+F	Technischer Datenschutz	**I**	Risiko-Management	
D	Schwerpunktthema zur Vertiefung	**J**	Konzeption von IT-Sicherheit	**Anwendung**

- Das Kapitel „Grundlagen des Datenschutzes“ des Lehrbuchs „Datenschutz kompakt und verständlich“ ist in der LV auf die Kapitel „Geschichte des Datenschutzes“ und „Technischer Datenschutz“ aufgeteilt.
- Das Kapitel „Datenschutzrechtliche Prinzipien“ des Lehrbuchs „Datenschutz kompakt und verständlich“ ist in der LV auf die Kapitel „Datenschutzrechtliche Prinzipien“ und „Technischer Datenschutz“ aufgeteilt.
- Das Kapitel „Verhältnis zur IT-Sicherheit“ des Lehrbuchs „Datenschutz kompakt und verständlich“ sowie das Kapitel „Verhältnis zum Datenschutz“ des Lehrbuchs „IT-Sicherheit kompakt und verständlich“ ist in der LV im Kapitel „Technischer Datenschutz“ zusammengefasst
- Die Kapitel zu den „Aktuellen Entwicklungen“ werden nur indirekt behandelt.

Literaturhinweise: Datenschutz

Im Semesterapparat verfügbar:

- Bernhard C. Witt: Datenschutz kompakt und verständlich; Vieweg + Teubner, 2. Auflage, 2010 [3. Auflage erscheint voraussichtlich 2024)

Zum Hintergrund der Vorlesung zudem empfehlenswert:

- Koreng/Lachenmann: Formularhandbuch Datenschutzrecht, C.H. Beck, 3. Auflage, 2021
- Petrlic/Sorge: Datenschutz – Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, Springer Vieweg, 2017
- Kühling/Klar/Sackmann: Datenschutzrecht; C.F. Müller, 4. Auflage, 2018
- Tinnefeld/Buchner/Petri/Hof: Einführung in das Datenschutzrecht; DeGruyter Oldenbourg, 7. Auflage, 2019
- EU-DSGVO/BDSG-Kommentare & Tätigkeitsberichte von BfDI & LfDs
- Zeitschriften: Datenschutz und Datensicherheit, Recht der Datenverarbeitung, Computer und Recht, MultiMedia und Recht, Zeitschrift für Datenschutz

Literaturhinweise: IT-Sicherheit

Im Semesterapparat verfügbar:

- Bernhard C. Witt: IT-Sicherheit kompakt und verständlich; Vieweg, 2006 [2. Auflage erscheint voraussichtlich 2025]

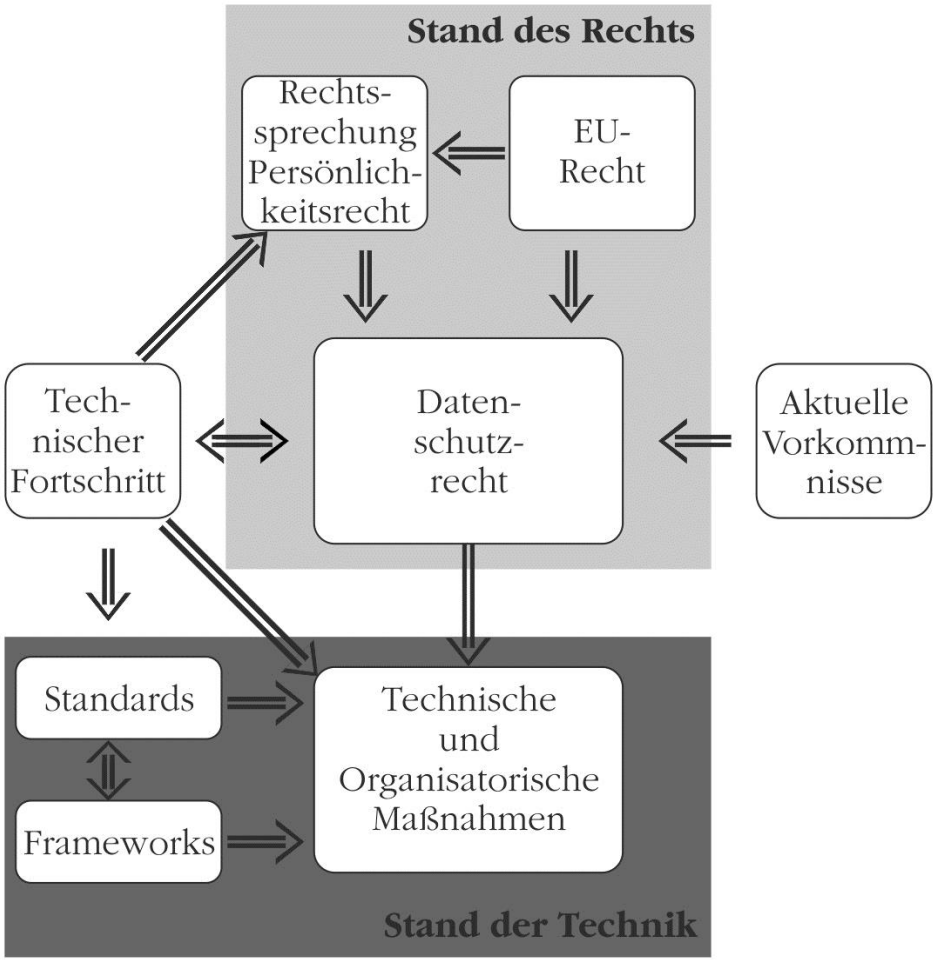
Zum Hintergrund der Vorlesung empfehlenswert:

- Hans-Peter Königs: IT-Risikomanagement mit System; Springer Vieweg, 5. Auflage, 2017
- Sebastian Klipper: Information Security Risk Management, Springer Vieweg, 2. Auflage, 2015
- Bruce Schneier: Secrets & Lies – IT-Sicherheit in einer vernetzten Welt; dpunkt, 2001
- Günter Müller & Andreas Pfitzmann (Hrsg): Mehrseitige Sicherheit in der Kommunikationstechnik; Addison Wesley, 1997
- Claudia Eckert: IT-Sicherheit; München, De Gruyter Oldenbourg, 10. Auflage, 2018
- Zeitschriften: <kes>, IEEE security & privacy, IT-SICHERHEIT

Motivation

- Informationen besonders eigenartiger „Rohstoff“
- Anwendungsbezug der Informatik
- Entwurf von Systemen ggf. mit Personenbezug
- Zukunftsthema Compliance: Übereinstimmung mit gesetzlichen Erfordernissen bzw. Standards (& Vereinbarungen)
- Datenschutz/Compliance „Treiber“ für technische Innovationen
- Datenschutz und IT-Sicherheit sind Querschnittsthemen
- IT-Sicherheit im Zuge NSA-Datensammlung wichtiger geworden
- Berufliche Perspektive (DSB, CIO, CISO, ISB, Admins etc.)
- Abwehr von Industriespionage / Schutz kritischer Infrastrukturen
- Ubiquitous Computing, Cloud Computing, Internet of Things
- Privacy by Design, Privacy by Default, Security by Design
- Kenntnisse aus LV auf Arbeitsmarkt gesucht (Fachkräftemangel)

Zusammenhänge



Gegenstand der Vorlesung

- **grundlegende Einführung** in Datenschutz & organisatorischer IT-Sicherheit (mit Einblick in die EU-Datenschutz-Grundverordnung und ins IT-Sicherheitsgesetz)
- Behandlung **entscheidungsrelevanter Fragen zur Ethik**
- Kennenlernen & Anwendung **rechtlicher Anforderungen**
- Methoden des (IT-) **Risikomanagements**
- Konzeption von **Informationssicherheit**
- Einblick in internationale **Standards**
- Anwendung gängiger **Vorgehensmodelle**
- **Falldiskussionen & Praxisbeispiele**

→ LV liefert Einblick in das **Management von Informationssicherheit mit starkem Datenschutzbezug**

Lehrziele: Methoden

- Strukturieren und Analysieren auch umfangreicher Texte
- Abstrahieren von Sachverhalten
- Verknüpfung verschiedener Sichtweisen (aus Jura, Informatik und Wirtschaftswissenschaften; sowie über ethische Fragen, d.h. inkl. Philosophie!)
- selbstständiges Aufarbeiten neuen (und ungewohnten) Stoffes
- Beherrschen der Nomenklatur
- Einübung typischer Fertigkeiten
- Anwendung von Kenntnissen in praxisrelevanten Fällen

→ **Erleichterung des Einstiegs in die Berufspraxis**

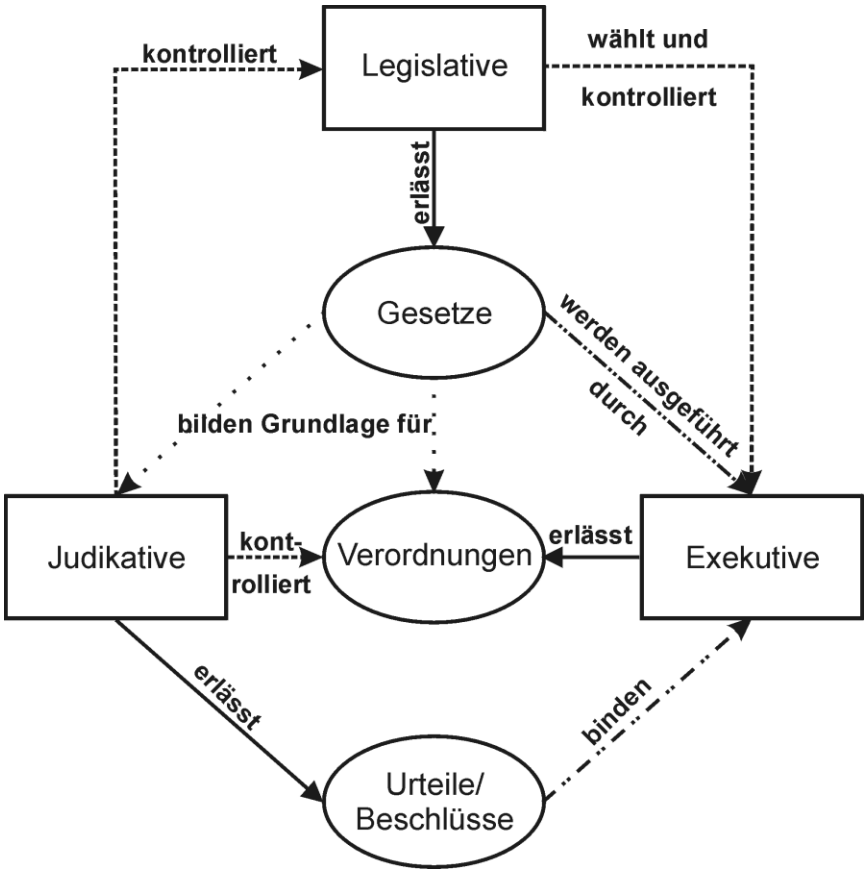
Lehrziele: Inhalte

- Angabe, Analyse und Anwendung grundlegender Rechts-normen
- 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

Zum Verständnis: Gewaltenteilung



Ethische Fragestellungen (1)

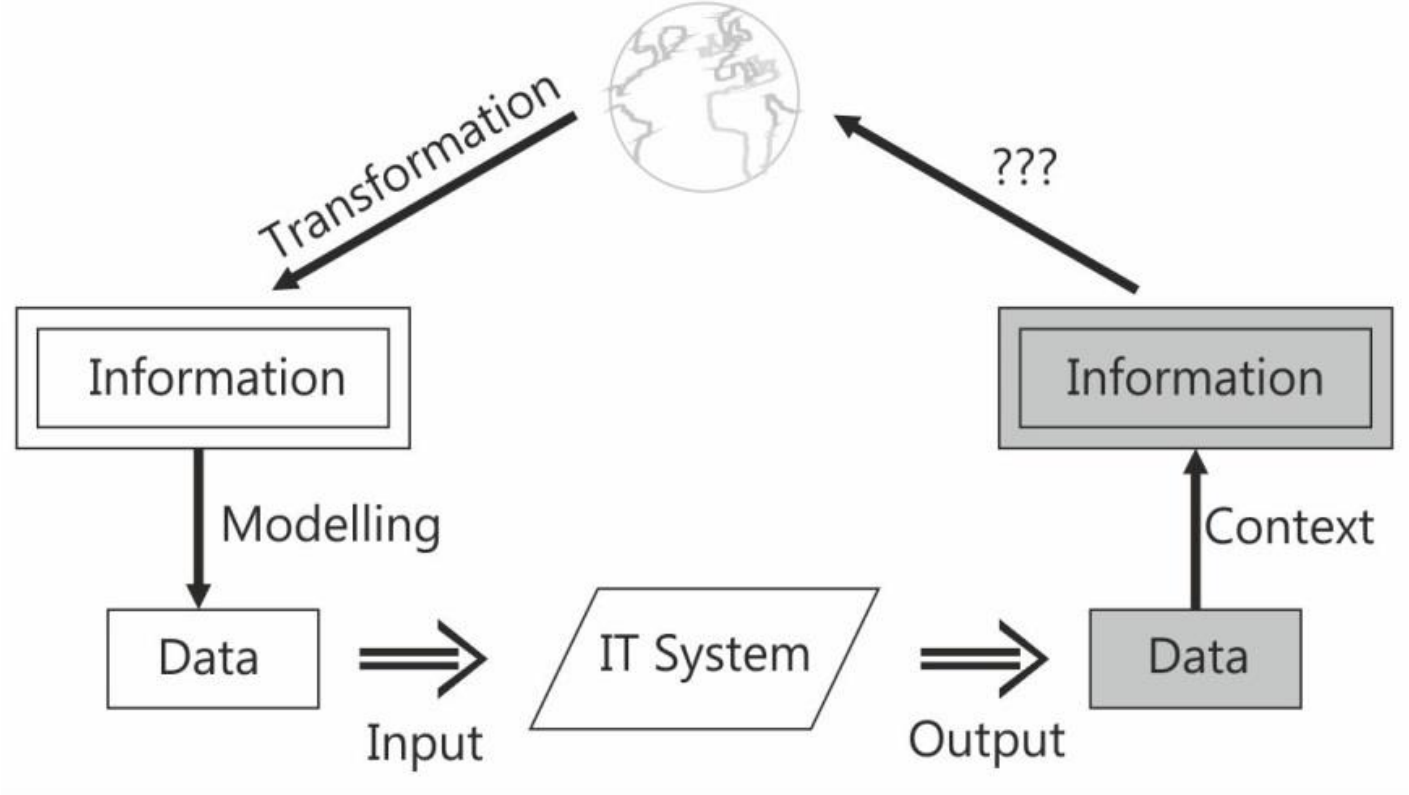
Definition 1: Ethik

Reflexives Nachdenken über gutes Handeln

- → **Neuer kategorischer Imperativ** (Hans Jonas):
  „Handle so, dass die Wirkungen Deiner Handlungen mit der Permanenz menschlichen Lebens verträglich sind“
- → Handlungsfreiheit begrenzt & Zielen untergeordnet
- → Menschliches Wohl (vor allem die **Menschenwürde**) ausschlaggebend für Grenzen der Handlungsfreiheit
- → In der Praxis gibt es viele Grenzfälle, bei denen man sich entscheiden muss
- → Wesentlich: Vereinbarkeit des Handelns mit Grundfreiheiten (Menschen-rechte) & Förderlichkeit für Grundfreiheiten
- → **Angepasster neuer kategorischer Imperativ**:
  „Konstruiere IT-Systeme so, dass dadurch kein Schaden für die Gesellschaft entsteht (Verfassungs- & Sozialverträglichkeit)“

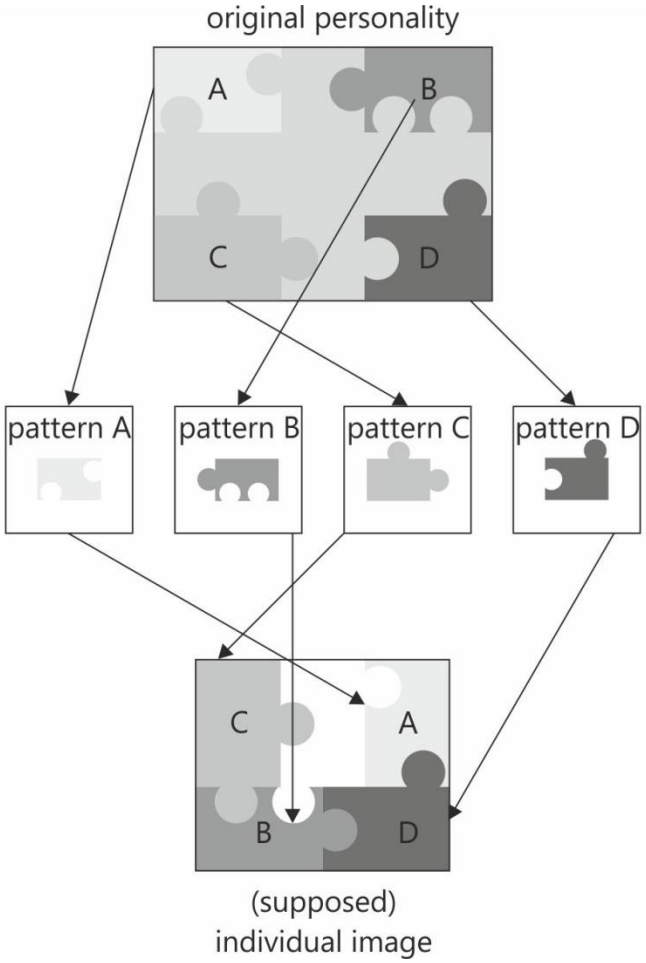
Ethische Fragestellungen (2)

- In der Informationsverarbeitung wird die reale Welt im Rahmen der Transformation abstrahiert und dann modelliert
- Abbildung via IT-System nicht zwingend inhaltsgleich



Ethische Fragestellungen (3)

Beispiel: Abbildung von Persönlichkeitsprofilen



- Ein Persönlichkeitsprofil setzt sich zusammen aus vielen einzelnen Komponenten zu einer Person
- Einige dieser Komponenten sind IT-bezogen modelliert (= Pattern), andere nicht (ggf. sogar gar nicht geeignet modellierbar!)
- Das sich selbst bei Sicht auf alle Pattern ergebende Bild entspricht daher in keinem Fall der originären Persönlichkeit (Folge aus Gödel-schen Unvollständigkeitssatz)

→ **Inhärente ethische Unschärfe**!

→ Unschärfe entscheidungsrelevant?

Ethische Fragenstellungen (4)

- **Europäische Union** basiert auf ethischem **Wertekanon**:
  - **EU-Grundrechtecharta** (seit 2007 verbindlich)
  - Zentrale Werte der EU sind (siehe https://ec.europa.eu/component-library/eu/about/eu-values/):
    - Menschenwürde → Basis für ethisches Handeln
    - Freiheit → Grenze für ethisches Handeln
    - Demokratie [→ ohne unmittelbaren Bezug]
    - Gleichberechtigung → Gleichbehandlungsgrundsatz
    - Rechtsstaatlichkeit → Compliance zu geltendem Recht
    - Menschenrechte → Handlungsanleitung für ethisches Handeln
- Zu einzelnen Themenfeldern wurden diese Werte übertragen in ethische Prinzipien, die bei entsprechenden Vorhaben innerhalb der EU zu beachten sind, siehe z.B. **Ethik-Leitlinien für eine vertrauenswürdige KI** (siehe https://op.europa.eu/de/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1)

EU-Leitlinie vertrauenswürdige KI

Die in den 2019 veröffentlichten Leitlinien dargestellten **ethischen Grundsätze** sind nicht nur für KI anwendbar:

- Achtung der menschlichen Autonomie → Intervenierbarkeit für Betroffene (Datensouveränität)
- Schadensverhütung → Vorsorgliche Gefahrenprävention
- Fairness → Chancengleichheit & Verhältnismäßigkeit
- Erklärbarkeit → Transparenz als Voraussetzung für Vertrauen

Stehen diese Grundsätze in Spannung zueinander, bedarf dies einer Kenntnisnahme und Lösung → erfolgt i.d.R. durch Aushandlung (in der LV am Beispiel mehrseitiger IT-Sicherheit näher ausgeführt)

→ Ethische Werte & ethische Grundsätze konkretisieren insoweit den aufgeführten angepassten neuen kategorischen Imperativ

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

- Schwerpunktthema **Datenschutz**: **OTT-Dienste + KI & Datenschutz**
- EU-Grundrechtecharta: Datenschutz + Schutz privater Kommunikation
- Details zu Datenschutz & elektronische Kommunikation für Over-the-top-Dienste (interpersonelle Kommunikationsdienste wie E-Mail, Instant Messenger und Videokonferencing) nach neuem TKG & TTDSG in der Übung
- Schwerpunktthema **IT-Sicherheit**: **KRITIS nach IT-SiG 2.0 & NIS2-Richtlinie + Cybersicherheit (neue Gefährdungsszenarien) + KI & IT-Sicherheit**

Auszug EU-Grundrechtecharta

Art. 8: Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

→ Datenschutz ist **Jedermannsrecht**

→ Treu & Glauben = **Vertrauensschutz** (gegenseitige Erwartungshaltung!)

→ **Verarbeitungszwecke** müssen eindeutig **festgelegt** werden

→ Datenverarbeitung nur nach **Einwilligung** des Betroffenen **oder** aufgrund **Gesetz**

→ **Betroffenenrecht** auf Auskunft über erhobene Daten & Berichtigung

→ **Datenschutzkontrolle** durch unabhängige Stelle (gemeint: Aufsichtsbehörde)

Fortsetzung EU-Grundrechtecharta

Art. 7: Achtung des Privat- und Familienlebens

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

- → Recht auf Achtung privater Kommunikation ist ebenso **Jedermannsrecht**
- → Recht eng verknüpft mit Privatleben (Privatheit)
- → „Achtung“ **= Vertraulichkeitsschutz**
- → **Vertraulichkeitsschutz** ist Voraussetzung für andere Grundrechte
- → **Briefgeheimnis, Postgeheimnis & Fernmeldegeheimnis** basieren auf diesem Vertraulichkeitsschutz
- → Recht auf Achtung privater Kommunikation ergänzt Datenschutz
- → Recht auf Achtung privater Kommunikation liefert eigenes Schutzniveau

Zum Fernmeldegeheimnis

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

Ausprägung:

- Telekommunikation → Fernmeldegeheimnis
  § 3 Abs. 1 TTDSG: „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."
- **§ 3 Nr. 24 TKG**: „interpersoneller Telekommunikationsdienst" = ein […] Dienst, der einen direkten interpersonellen und interaktiven Informationsaustausch über Telekommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglicht, wobei die Empfänger von den Personen bestimmt werden, die die Telekommunikation veranlassen oder daran beteiligt sind *(nur wenn in Hauptfunktion!)*

Kennzeichen von Privatheit

Freie Persönlichkeitsentfaltung

Direkt:

- Vertraulicher Rückzugsraum zum Nachdenken
- Vertrauliche Kommunikation (mündlich, brieflich, elektronisch)
- Freiraum für eigene Entscheidungen (keine vollständige Fremdbestimmung)

Indirekt:

- Keine unbefugte Manipulation vertraulicher Daten
- Keine Vollzeitüberwachung
- Vertraulicher Umgang mit Gesundheitsdaten
- Gerechtfertigter Verlass in Vertrauensinstanzen