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

Vorlesung im Sommersemester 2011

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

Kundendatenschutz:

- Abgrenzung & Übersicht
- Kundendatenverwaltung
- Kundengewinnung
- Kundenbetreuung/-bindung
- Kundendatenanalyse

Mediendatenschutz:

- Schichtenmodell
- Einordnungen

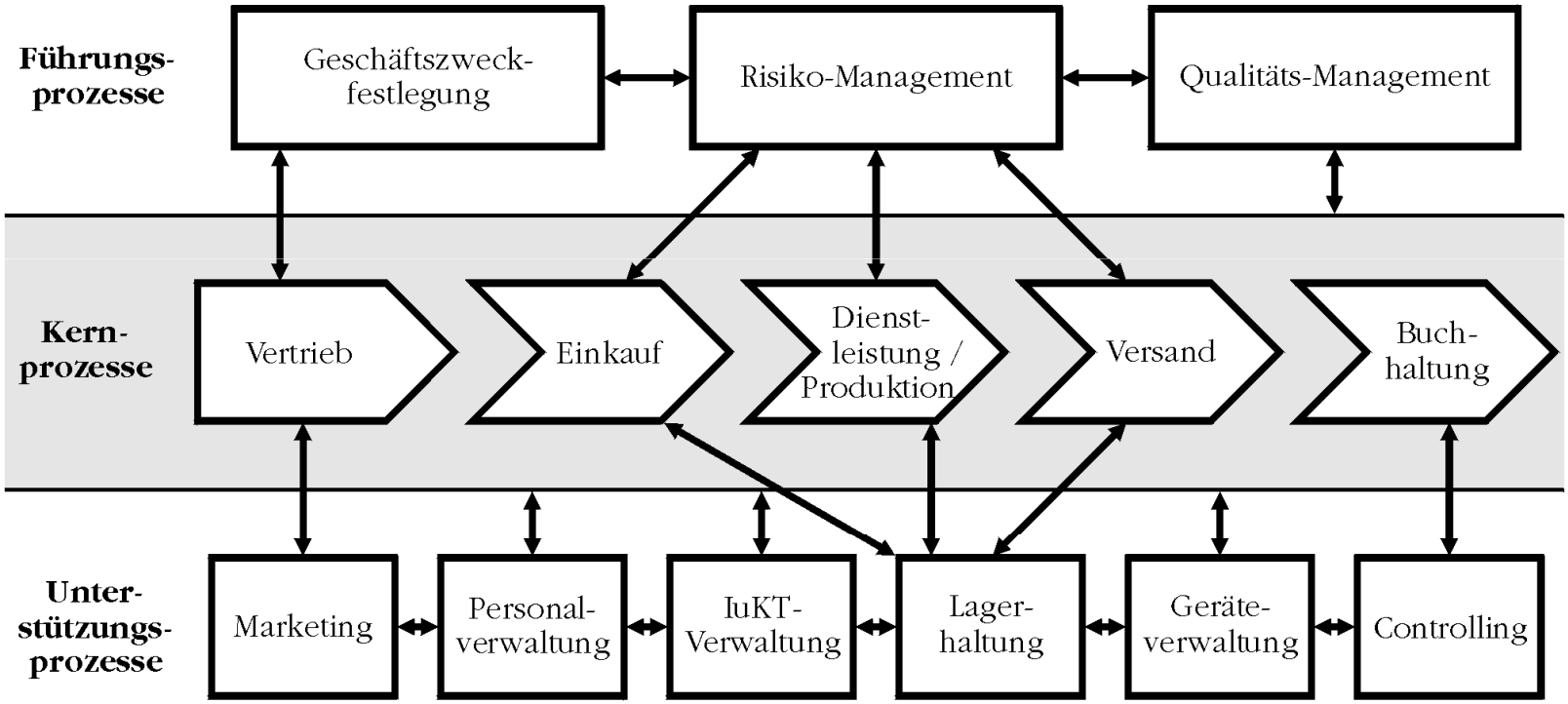
Kundendatenschutz

- **Kunden** der Unternehmen können sein:
  - **juristische Personen** (Kapitalgesellschaften, Mehrpersonengesellschaften, Personenvereinigungen)
  - **natürliche Personen** (Einpersonengesellschaften, Privatpersonen)
- Datenschutz in der BRD nur für natürliche Personen relevant!
- Vertreter juristischer Personen werden i.d.R. als juristische Person „gewertet“, sofern es nicht um die Person als solche geht

→ bei Kundendatenverwaltung ist zu ermitteln, ob Datenschutz überhaupt relevant ist

→ Aber: Einpersonengesellschaften nicht immer leicht zu erkennen

Unternehmensprozesse



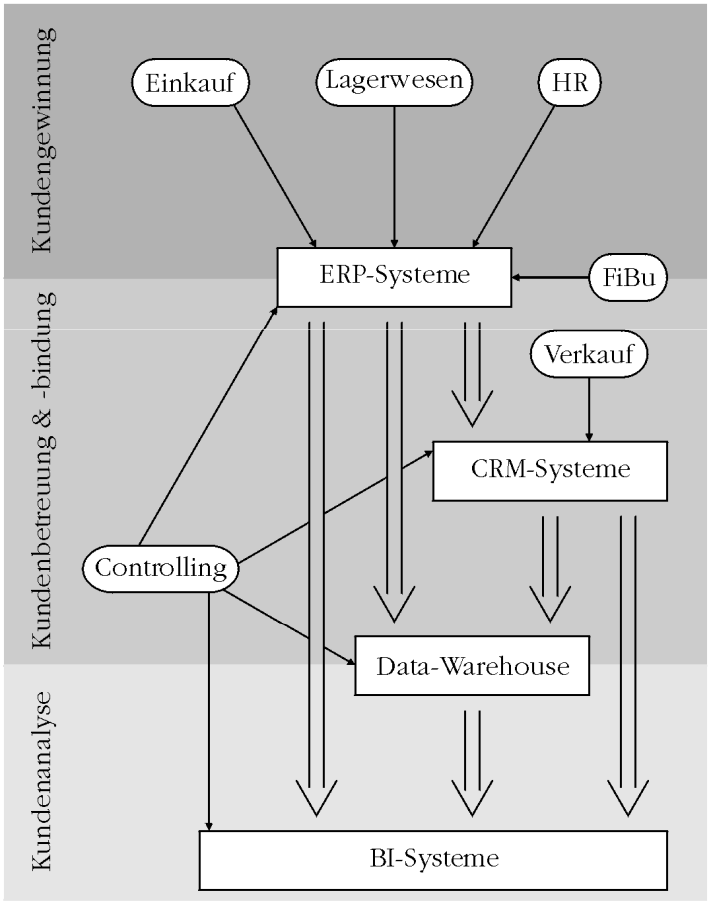
Kundendatenverwaltung (1)

- **Vertrieb** befasst mit:
  - Werbung (→ Kundengewinnung)
    → rechtsgeschäftsähnliches Schuldverhältnis
  - Bestandspflege (→ Kundenbindung)
    → rechtsgeschäftliches Schuldverhältnis (z.B. Kaufvertrag)
- **Finanzbuchhaltung** befasst mit:
  - Verwaltung der Zahlungsströme (→ Kundenbetreuung)
    → rechtsgeschäftliches Schuldverhältnis
  - Umgang mit Zahlungsverzug (→ Kundenbetreuung)
    → rechtsgeschäftliches Schuldverhältnis
- **Versand** befasst mit:
  - Versand bestellter Güter an Kunden (→ Kundenbetreuung)
    → rechtsgeschäftliches Schuldverhältnis

Kundendatenverwaltung (2)

- Besonderheiten:
  - **Mitarbeiter** als Kunden → rechtsgeschäftliches Schuldverhältnis → besondere Anforderung der Datentrennung!
  - **RFID** zur Warenkennzeichnung kann zu personenbezogenem Datum mutieren! → rechtsgeschäftsähnliches Schuldverhältnis
- Eingesetzte **Systeme** (teilweise übergreifend integriert):
  - Enterprise Resource Planning System (**ERP-System**) zur Verwaltung der Güter-, Abrechnungs- und Finanzströme inkl. Betriebsdatenerfassung (BDE)
  - Customer Relationship Management System (**CRM-System**) zur Verwaltung der Kundenhistorie und Werbekampagnen
  - Data Warehouse Systeme zur Kundendatenaufbereitung und Datenqualitätssicherung
  - Business Intelligence System (**BI-System**) zu Analyse und Reporting der Kundendaten

Kundendatenverwaltung (3)



Kundengewinnung (1)

- Erhebung von **Interessentendaten** (z.B. via Web-Formular unter Beachtung vom Telemedienrecht)
- Webseite als „**invitatio ad offerendum**“ → Angebot durch Kunde
- Einkauf (Adresshandel) oder Nutzung (Lettershop) von **listen-mäßig** zusammengefassten Daten (Zugehörigkeit zu einer Personengruppe, Berufs- / Branchen- / Geschäftsbezeichnung, Namen, Titel, akademische Grade, Anschrift, Geburtsjahr) zum Zweck der Werbung nach § 28 Abs. 3 Nr. 1 BDSG mit Abwägung ~ Auszug aus Melderegister gem. jeweiligem Meldegesetz (Gruppenauskunft ohne Angabe der Staatsangehörigkeit, Geschlecht und evtl. relevante gesetzliche Vertreter bzw. einfache Melderegisterauskunft mit Titel und Geburtsjahr)
- Auswertung von **allgemein zugänglichen Quellen**

→ **Angabe der Quelle (Herkunft) bei Speicherung erforderlich!**

Kundengewinnung (2)

- bei **Werbung** außerdem zu beachten:
  - ° unlautere Werbung (Kaltakquise am Telefon, Mitteilung per Fax/E-Mail... jeweils ohne Einwilligung) → § 7 II UWG
  - ° SPAM → § 6 TMG & § 7 II Nr. 4 UWG
  - ° Widerspruchsrecht des Betroffenen → § 28 IV BDSG (z.B. via Robinsonliste beim Direktmarketing)
  - ° Einwilligung (§ 13 II TMG bzw. §§ 4a oder 28 IIIa BDSG)
  - ° Auswertung von Todesanzeigen wäre sittenwidrig!

→ Datenschutz und Verbraucherschutz konvergieren

- Bei Erhebungen personenbezogener Daten via Telemedien sind die **Impressumpflichten** (§ 5 TMG) zu beachten
- Abgabe einer **Visitenkarte** begründet zwar rechtsgeschäftsähnliches Schuldverhältnis, berechtigt aber noch nicht zur Werbung (→ Kontext beachten!)

Kundenbetreuung (1)

- zur Vertragsabwicklung Erhebung, Verarbeitung oder Nutzung personenbezogener Daten i.d.R. unerlässlich
- **Formen** der Kundenbindung:
  - produkt-/dienstleistungsbezogene Folgeaufträge
  - Rabatt-Systeme (z.B. Kundenkarten)
  - gezielte Ansprache der Kunden (auch unter Berücksichtigung „weicher“ Informationen)
  - Einrichtung von Warndateien vor „faulen“ Kunden
- **Umsetzung** mittels:
  - Customer-Relationship-Management-Systeme (CRM)
  - Data-Mining / Data-Warehousing (z.B. mittels Business Intelligence Tools oder Online Analytical Processing)
  - Call-Center zur Kundenbetreuung (aber § 201 StGB!)

→ **i.d.R. Vorabkontrolle (insb. wg. Profilbildung) erforderlich!**

Kundenbetreuung (2)

- **Zweckbestimmung** der Vertragsbeziehung berücksichtigen!
- **Löschungsfristen** & **Sperrungsanforderungen** berücksichtigen!
- Problem: Manche Datenbanken „kennen“ keine Löschung wg. **Datenqualität**
- **Perspektivwechsel** bei CRM-Systemen oder Data Warehouses auch bei Vertretern juristischer Personen möglich → Grenzen setzen!
- **Anreicherung** von CRM-Systeme kontrollieren!

Finanzstromüberwachung

- ggf. fallen neben Barzahlungen oder EC-Kartenzahlungen auch Lastschriftermächtigungen, Kreditkartenzahlungen, eCash-Zahlungen oder Kundenkredite an
  → Vielzahl zu prüfender Formulare & Zahlungssysteme
  → Zweckbestimmung beachten
- auf Übermittlung von Daten säumiger Zahler zum Forderungseinzug an Inkassounternehmen ist der Betroffene hinzuweisen!
- Datenübermittlung an Auskunfteien dagegen nur unter bestimmten Voraussetzungen zulässig (§ 28a BDSG)
- Abschätzung künftiger Zahlungsfähigkeit mittels Scoring nur mit anerkannten Verfahren (§ 28b BDSG)
- Finanzbuchhaltung i.d.R. in Enterprise-Resource-Planning-Systemen (ERP-Systemen) integriert!
- Archivierung unter Berücksichtigung von GoBS & GDPdU

Kundendatenanalyse

- Auswertung von Kundendaten anhand vorhandenen Datenmaterials, das ggf. um weitere Daten „angereichert“ wird
- Analysetools, die hierzu zum Einsatz kommen:
  - **Business Intelligence Systeme** liefern Reportingdaten (→ Dash-Board mit Drill-Down-Funktion)
  - **Data Warehouses** liefern Langzeitanalysen & Korrelationen (→ Data-Mining)
  - **Scoring-Systeme** liefern Persönlichkeitsbilder (→ Abgrenzung zur automatisierten Einzelentscheidung)
- Kundendatenanalyse dient stets der (Kauf-) Verhaltens- oder (Kaufkraft-) Leistungskontrolle → **Vorabkontrolle** erforderlich!

Ergebnis Kundendatenschutz

- **Grundsätze** des Kundendatenschutzes:
  - Berücksichtigung der Herkunft von Kundendaten
  - Transparenz gegenüber dem Kunden
  - Widerspruchsrecht bei der Bewerbung von Kunden
- Wertschöpfungsprozesse grundlegend für **Verfahren**:
  - Kundengewinnung (Vertrieb, Marketing, Finanzbuchhaltung → ERP-Systeme)
  - Kundenbetreuung (Vertrieb, Versand, Finanzbuchhaltung, Call Center → CRM-Systeme)
  - Kundendatenanalyse (Vertrieb, Finanzbuchhaltung, Einkauf → BI-Systeme & Data-Warehousing)
- je mehr mit Kundendaten durchgeführt wird, desto eher ist eine **Vorabkontrolle** erforderlich

Mediendatenschutz: Schichtenmodell

Anzuwendendes Datenschutzrecht abhängig von zu betrachtender Schicht (≠ ISO-OSI-Referenzmodell):

- Transfer = technische Kommunikationsabwicklung
- Dienst = Kommunikationsart
- Inhalt = Kommunikationsinhalt

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

Mediendatenschutz: Einordnungen (1)

- **Telekommunikation** = technischer Vorgang des Aussendens, Übermittelns & Empfangens von Signalen mittels TK-Anlagen (§ 3 Nr. 22 TKG)
- **TK-Anlagen** = technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können (§ 3 Nr. 23 TKG)
- Alle Mediendienste (Telekommunikationsdienst bzw. Telemediendienst) nutzen die Transportebene
- Ausstrahlung via **Web** an Allgemeinheit (Broadcast-Funktion) über Rundfunkstaatsvertrag im TMG geregelt; andere Web-Dienste dagegen i.d.R. elektronischer Informations- bzw. Kommunikationsdienst (Telemediendienst)

Mediendatenschutz: Einordnungen (2)

- **Voice over IP** = Telefonie mittels verbindungsloses Netzwerk-protokoll
  → Einordnung derzeit noch strittig, sofern nicht ein eigenes VoIP-Netz aufgebaut / verwendet wird (sog. „Next Generation Network“), da dann nachweislich mit eigener Kontrollmöglich-keit für VoIP-Anbieter betrieben
  → aufgrund des funktionsbezogenen Verwendungszwecks (Telefonie!) jedoch vorzugsweise als TK-Dienst einzuordnen
- **E-Mail** = Telemediendienst, zumal dieser Dienst nur unter Aus-nutzung einer umfassenderen Kommunikationsumgebung (zum Erstellen, Darstellen, Speichern, Verwalten etc.) möglich ist; Einstufung als elektronischer Geschäftsbrief führt insbesondere zu Aufbewahrungspflichten

Mediendatenschutz: Einordnungen (3)

- Eine rein dienstliche Nutzbarkeit von Mediendiensten „befreit“ vom Fernmeldegeheimnis (§ 3 Nr. 10 TKG & § 11 I TMG)
- Selbst bei gestatteter oder geduldeter Privatnutzbarkeit von Mediendiensten ist Abruf & Verbreitung beleidigender, rassistischer, sexistischer, gewaltverherrlichender oder pornographischer Inhalte untersagt und vom Anbieter kontrollierbar
- Ebenso darf ein Verstoß gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen durch Anbieter kontrolliert werden
- Einzelverbindungsnachweise (z.B. für Handy-Nutzung) bedürfen der Einwilligung durch Nutzer bzw. deren Betriebs-/Personalrat (§ 99 I TKG)