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

Vorlesung im Sommersemester 2008

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

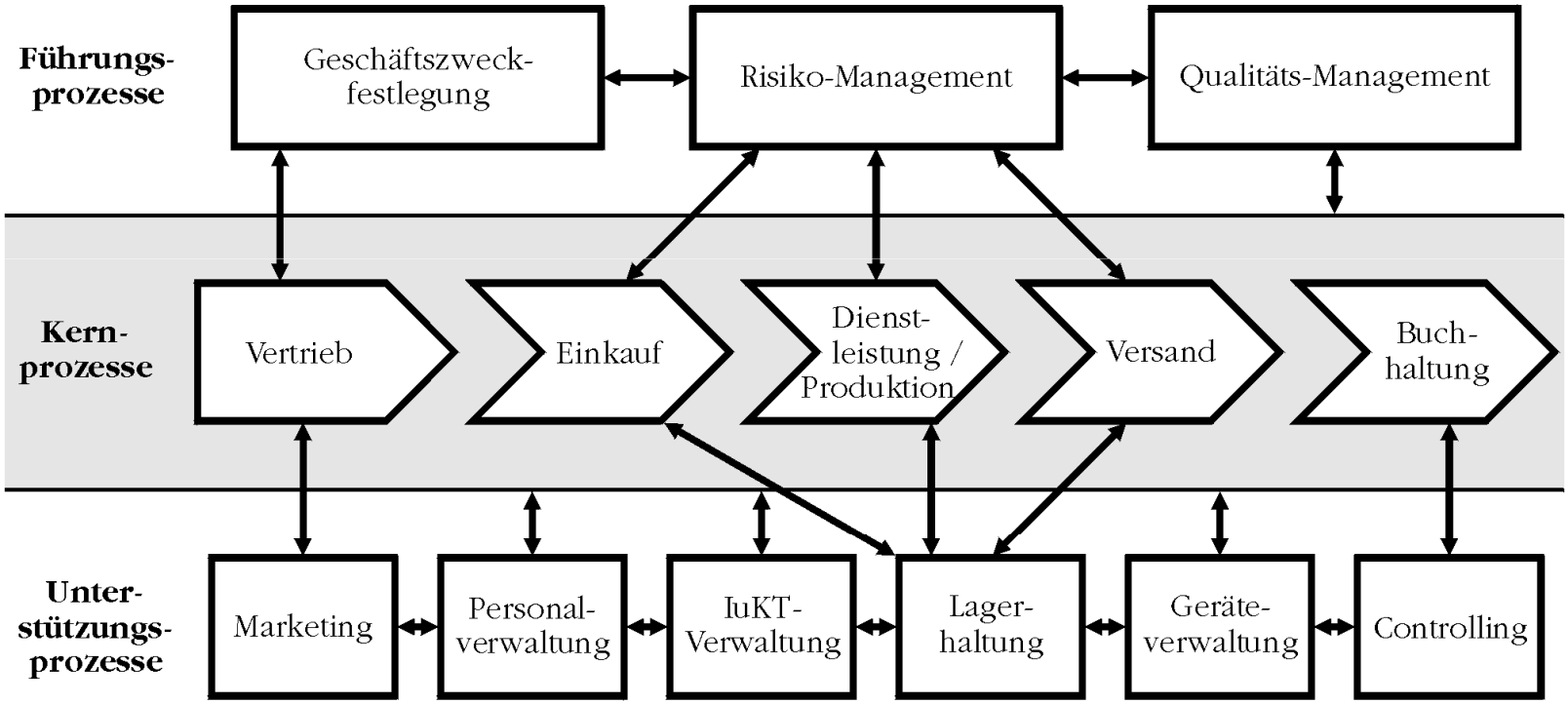
Kundendatenschutz

- **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

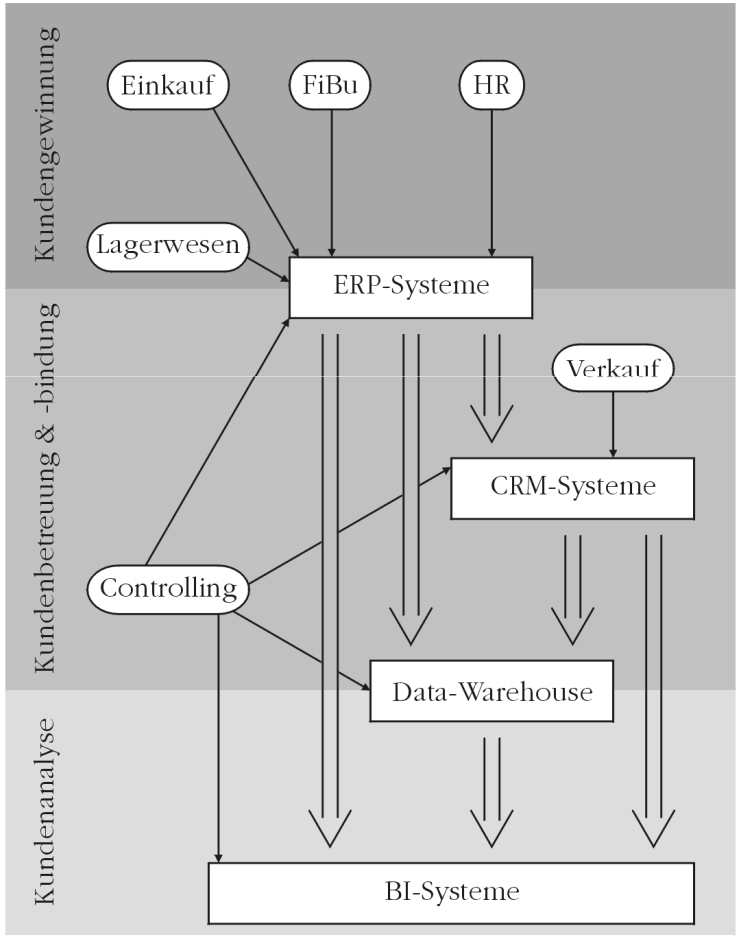
Unternehmensprozesse



Kundendatenverwaltung (1)

- **Vertrieb** befasst mit:
  - Werbung (→ Kundengewinnung)
    → vertragsähnliches Vertrauensverhältnis
  - Bestandspflege (→ Kundenbindung)
    → Vertragsverhältnis
- **Finanzbuchhaltung** befasst mit:
  - Verwaltung der Zahlungsströme
    → Vertragsverhältnis
  - Umgang mit Zahlungsverzug
    → Vertragsverhältnis
- Besonderheiten:
  - **Mitarbeiter** als Kunden → Vertragsverhältnis
  - **RFID** zur Warenkennzeichnung kann zu personenbezogenem Datum mutieren! → vertragsähnliches Vertrauensverhältnis

Kundendatenverwaltung (2)



Kundengewinnung (1)

- Erhebung von **Interessentendaten** (z.B. via Web-Formular unter Beachtung von Telemedienrecht)
- Abgabe einer „**invitatio ad offerendum**“
- Einkauf (Adresshandel) oder Nutzung (Lettershop) von **listenmäßig** zusammengefassten Daten (Zugehörigkeit zu einer Personengruppe, Berufs- / Branchen- / Geschäftsbeziehung, Namen, Titel, akademische Grade, Anschrift, Geburtsjahr) nach § 28 Abs. 3 Nr. 3 BDSG i.V.m. § 29 BDSG
  ~ 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 **Veröffentlichungen**

→ **Angabe der Quelle bei Speicherung erforderlich!**

Kundengewinnung (2)

- bei **Werbung** außerdem zu beachten: [siehe insb. 3. Übung]
  - ° unlautere Werbung (Kaltaquise am Telefon, unverlangte Werbung per Fax/E-Mail...) → UWG
  - ° SPAM → TMG
  - ° Widerspruchsrecht des Betroffenen → BDSG (z.B. via Robinsonliste beim Direktmarketing)
  - ° Einwilligung (elektronisch → TMG; sonst → BDSG)
  - ° Auswertung von Todesanzeigen wäre sittenwidrig!

→ Datenschutz und Verbraucherschutz konvergieren

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

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)

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 Adressdaten zum Forderungseinzug säumiger Zahler an Inkassounternehmen ist der Betroffene hinzuweisen!
- Übermittlung von Angaben zur Zahlungsunfähigkeit bzw. -unwilligkeit zur Wahrung berechtigter Interessen Dritter zulässig! (§ 28 Abs. 3 Nr. 1 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