Grundlagen des Datenschutzes und der IT-Sicherheit (4)

Vorlesung im Sommersemester 2007
an der Universität Ulm
von Bernhard C. Witt

Grob-Gliederung zur Vorlesung

Topics zum Datenschutz:
- Geschichte des Datenschutzes

→ **Datenschutzrechtliche Prinzipien**
- Vertiefung in ausgewählten Bereichen
- Verwandte Gebiete zum Datenschutz

Topics zur IT-Sicherheit:
- Einflussfaktoren zur IT-Sicherheit
- Mehrseitige IT-Sicherheit
- Risiko-Management
- Konzeption von IT-Sicherheit

Prinzipien des Datenschutzes

- Subsidiarität
- Verbot mit Erlaubnisvorbehalt
- Zweckbindung
- Transparenz
- Vorrang der Direkterhebung
- Verhältnismäßigkeit
- Datensparsamkeit
- Kontrollprinzip vs Lizenzprinzip

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 **Verfahrensverzeichnis**
- **Nachvollziehbarkeit** von durchgeführten 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

- 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)

Prinzip der Datensparsamkeit

- Anforderung zur Gestaltung der eingesetzten IT-Systeme
- Vermeidung des Personenbezugs, sofern dieser nicht unbedingt erforderlich ist
- Verwendung datenschutzfreundlicher Techniken
- Ermöglichung anonymer und unbeobachteter Nutzung von Telemedien

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

Grob-Gliederung zur Vorlesung

Topics zum Datenschutz:

- Geschichte des Datenschutzes
- Datenschutzrechtliche Prinzipien

→ **Vertiefung in ausgewählten Bereichen**

- Verwandte Gebiete zum Datenschutz

Topics zur IT-Sicherheit:

- Einflussfaktoren zur IT-Sicherheit
- Mehrseitige IT-Sicherheit
- Risiko-Management
- Konzeption von IT-Sicherheit

Datenschutzrechtliche Vertiefung

- Allgemein gültige Regelungen
- Datensicherheit
- Kundendatenschutz (Wahlthema)
- Datenschutz bei Sicherheitsbehörden (Wahlthema)

Allgemein gültige Regelungen (1)

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!

Allgemein gültige Regelungen (2)

Zulässigkeit der Datenverarbeitung durch:

- Einwilligungserklärung [Anforderungen siehe 1. Übung]
- Rechtsvorschrift

Verpflichtung auf das **Datengeheimnis** auch über Beschäftigungsdauer hinaus

Grundsätze: [siehe auch datenschutzrechtliche Prinzipien]

- Direkterhebung beim Betroffenen
- Zweckbindung erhobener Daten
- Datensparsamkeit
- Beachtung des Schutzbedarfs
- technische + organisatorische Vorkehrungen zum Datenschutz
- Kontrolle durch Datenschutzbeauftragte

Allgemein gültige Regelungen (3)

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

Allgemein gültige Regelungen (4)

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

Aus dem Alltag eines DSB

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

Datensicherheit (1): Begriffsdefinitionen (1)

Definition 4: Sicherheit

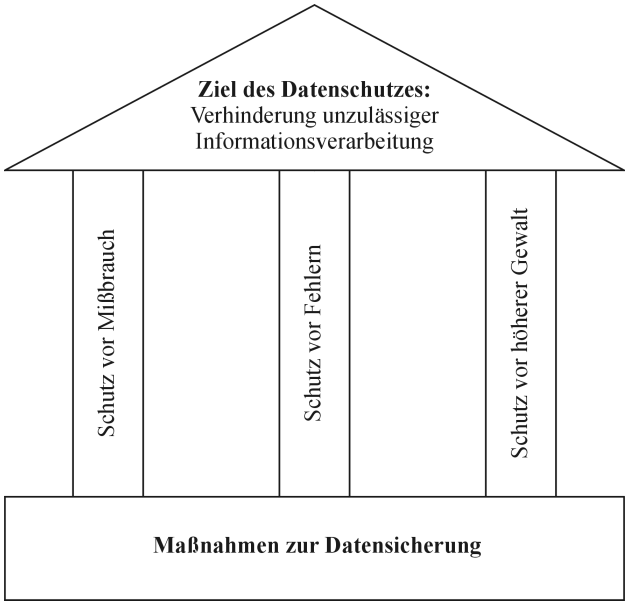
Abwesenheit von Gefahren

Definition 5: Datensicherung

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

→ Datensicherung zielt insb. auf **Ausfallsicherheit** ab!

Datensicherheit (2): Verhältnis Datenschutz zu Datensicherung



Datensicherheit (3): Begriffsdefinitionen (2)

Definition 6: 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

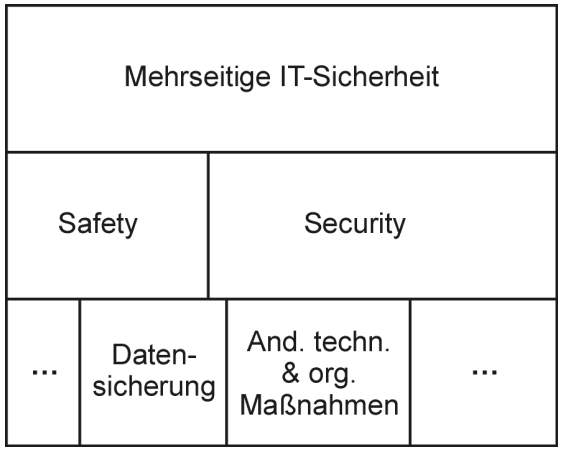
→ Verlässlichkeit und Beherrschbarkeit der IT-Systeme

→ Sicherheit der Systeme und vor den Systemen

Datensicherheit (4): Abgrenzungen

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

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



Datensicherheit (5): Abgrenzungen

Zusammenhang zwischen mehrseitiger IT-Sicherheit und Datenschutz:

- Überschneidung bei der Verarbeitung personenbezogener Daten
- Schwerpunkt liegt auf Security