



**Peter Schaar**

# **Der multipel vernetzte Mensch – eine neue Sicht auf den Datenschutz**

**Berlin Open '09**

**22.Juni 2009**



- Technisches Umfeld
  - Monolithische Großrechnerwelt
  - Zentral organisierte Rechenzentren
  - Closed Shop-Betrieb/Lochkarten
  - Kaum Vernetzung
- Regelungsziele
  - Schutz personenbezogener Daten
  - Verhinderung von Datenmissbrauch
- Regelungsmechanismen
  - Verbot/Erlaubnis
  - „Zehn Gebote“ der Datensicherheit
  - Meldepflichten



# Datenschutz 1983

- Technisches Umfeld
  - Großrechner ergänzt um „mittlere Datentechnik“ und erste PCs
  - Rechenzentren als Dienstleister
  - Automatisierte Abrufverfahren
  - „Neue Medien“ (Bildschirmtext)
- Regelungsziele
  - Recht auf informationelle Selbstbestimmung
  - Schutz personenbezogener Daten
  - Verhinderung von Datenmissbrauch
- Regelungsmechanismen
  - Verbot/Erlaubnis
  - „Zehn Gebote“ der Datensicherheit
  - Meldepflichten



- Technisches Umfeld
  - Weltweite Vernetzung
  - Internet als Basistechnologie
  - Vielfältige Organisationsformen/Geschäftsmodelle
  - Miniaturisierte, vielfältige Informationstechnik
- Regelungsziele
  - Recht auf informationelle Selbstbestimmung
  - Schutz personenbezogener Daten
  - Verhinderung von Datenmissbrauch
- Regelungsmechanismen
  - Verbot/Erlaubnis
  - „Acht Gebote“ der Datensicherheit
  - Meldepflichten



# Heutiges Datenschutzrecht (Ziele)

- Recht auf informationelle Selbstbestimmung
  - Schutz personenbezogener Daten
- Schutz der Privatsphäre
  - Absolut geschützter Kernbereich der Privatsphäre
- Verhinderung von Datenmissbrauch
  - § 9 BDSG
  - „Acht Gebote“ (Zutrittskontrolle, Zugangskontrolle, ...)



# Datenschutzrecht (Schutzobjekt)

- Personenbezogene Daten

„Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“

- Direkter Personenbezug
- Indirekter Personenbezug

Nicht geschützt: (faktisch) Anonyme Daten



# Datenschutzrecht (Rollenmodell)

- Klar definierte Rollen
  - Betroffener
    - Person, der die Daten zuzuordnen sind
  - Verantwortliche Stelle
    - Verarbeitet personenbezogene Daten „für sich selbst“
  - Auftragnehmer
    - Handelt im Auftrag der verantwortlichen Stelle
  - Dritter
    - Rest der Welt, auch Empfänger von Daten



# Heutiges Datenschutzrecht (Regelungsansätze)

- Verbot mit Erlaubnisvorbehalt
- Zulässigkeitsvoraussetzungen
  - Gesetzliche Befugnis
  - Einwilligung des Betroffenen
- Grundsätze
  - Erforderlichkeit
  - Zweckbindung
  - Transparenz
  - Betroffenenrechte (Auskunft, Sperrung, Löschung)
  - Gewährleistung der Datensicherheit





# Beobachtungen



- Miniaturisierung/Internet/Mobilfunk/GPS
- Verknüpfung unterschiedlicher Technologien
- Ubiquitous-/Grid-/Cloud-Computing
- Unbegrenzte Speicherkapazitäten
- Digitale Freizügigkeit (Beispiel Soziale-Netzwerke)
- Persönlichkeitsprofile
- Neue Geschäftsmodelle (z.B. Outsourcing)
- Internationale Vernetzung
- Elektronische Mensch-Maschinen-Schnittstellen



# Paradigmenwechsel der Datenverarbeitung

## Konventionelle Datenverarbeitung

- Ortsgebundene Datenverarbeitung
- Rechenzentren
- Wenig mobil
- „close shop“-Betrieb
- kaum vernetzt
- manuelle Datenerhebung
- Bürger nie selbst Datenverarbeiter

## Allgegenwärtigen Datenverarbeitung

- nicht ortsgebunden
- hoch flexibel
- Aggregation im Rechenzentren
- sehr mobil
- ungesteuert
- sehr vernetzt
- automatische Datenerhebung
- Bürger ist selbst Datenverarbeiter



# Technische Schutzziele –heute

**IT-Grundschutz**  
(Grundschutz = Datenschutz + X)

**Verfügbarkeit**

**Integrität**

**Vertraulichkeit**

**Systeme/Systemkomponenten/Verfahren**



- Technologischer Datenschutz in vernetzten Systemen ist mehr als IT-Sicherheit
- Anforderungen
  - Transparenz für den Betroffenen
  - Anonymität
  - Unbeobachtbarkeit
  - Profilbildung verhindern
- Sonst: Persönliche Entfaltung nicht möglich
- Anpassungsdruck, Duckmäusertum



# Schutzziele und vernetzte Technik

Schutzziele heute

Notwendige Schutzziele

zum Teil ausgeblendet beim Grundschutz!



- Verantwortlichkeit des Einzelnen für seine Daten wächst; bewusster Umgang mit der Preisgabe von persönlichen Informationen
- Informationelle Selbstbeschränkung von Staat und Wirtschaft
- Diskriminierungsfreie Entscheidungsmöglichkeiten; Anonymität muss (wenn gewünscht) gewahrt bleiben
- Umfassende Transparenz: Information, Benachrichtigung
- Privacy-Technologien schützen die Privatsphäre



- Datenschutz bereits bei der Normung, Zertifizierung und Systemdesign
- Aufgepfropfter Datenschutz „second best“ („end of the pipe“)
- Data protection by default
- Kontextbezogener Schutz (Sensibilität der Daten Anwendungsbereich, Missbrauchsinteresse)
- Risikoadäquanz
- Gewährleistungspflicht der Anbieter
- Keine Abwälzung der Verantwortung auf Anwender/ Nutzer





- Einführung einer Zertifizierung nicht nur gemäß IT-Sicherheit, sondern auch gemäß DATENSCHUTZ
- Zertifizierung von Verfahren durch Audits
  - Schutzprofile: Grundsteine datenschutzgerechter Lösungen
  - Anforderungen und Verfahren zur Vergabe von Datenschutzgütesiegeln gesetzlich vorgeben
- Verifikation des Datenschutzes durch Nutzer



# Noch Fragen?