Datenschutz/Datensicherheit

1. **Datenschutz – Datensicherheit: Abgrenzungen zu TKG – TMG**
2. **Begriffsabgrenzungen**
3. **Historie des Datenschutz**
4. **Ziele des Datenschutzes**
5. **Begriffsdefinitionen**
6. **BDSG - Grundsätze**
7. **Zulässigkeit des Datenumgangs**
8. **Rechte und Pflichten (u. a. der Betroffenen)**
9. **Risiken**
10. **Datensicherheit / 8 Gebote**
11. **Büroalltag**
12. **Grundsätze**
    - **ordnungsgemäßer DV**
    - **der Auftragsbindung**
    - **der Kontrollierbarkeit**
    - **der Transparenz**
    - **der Funktionssicherheit**

DS-1

Als **Datenschutz** (*engl.: data privacy; protection of data privacy*) bezeichnet man die Gesamtheit der gesetzlichen und betrieblichen Maßnahmen zum Schutz der Rechte von Personen vor Verletzung der Vertraulichkeit und der Sicherheit des Informationshaushaltes.
(Quelle: Hansen, S. 457 ff.)

Beispiel:
Bibliothek: Eine Person geht regelmäßig in die B., um Zeitungen zu lesen und um sich Bücher auszuleihen, für die Weiterbildung und zur Unterhaltung.
Im Laufe der Jahre sammelt sich daher eine beträchtliche Menge von Daten über ihre Person in der Datenbank des Bibliotheksverwaltungssystems an.
Ihre Pünktlichkeit und Unpünktlichkeit beim Zurückgeben von Büchern könnte auf ihre Zuverlässigkeit, die Auswahl der Zeitungen, Berichte und Bücher auf ihre politische Einstellung, ihre Freizeitliteratur auf ihre Hobbies und ihre Bildungsliteratur auf ihr berufliches Engagement schließen lassen.
Alle Daten zusammen könnten ein relativ genaues Persönlichkeitsprofil abgeben.
Es könnte aber auch sehr verzerrt sein, z.B. wenn die Person diese Bibliothek nur für Ganz bestimmte Literaturrecherchen verwendet und sonst aus einer anderen Bibliothek Ihre Literatur bezieht. Auf die Interpretation der Daten hat die Person i. a. keinen Einfluss.
So kann durch eine Indiskretion eines Bibliotheksangestellten durchaus Schaden er-Wachsen, dessen Ursache für die Person rätselhaft ist.

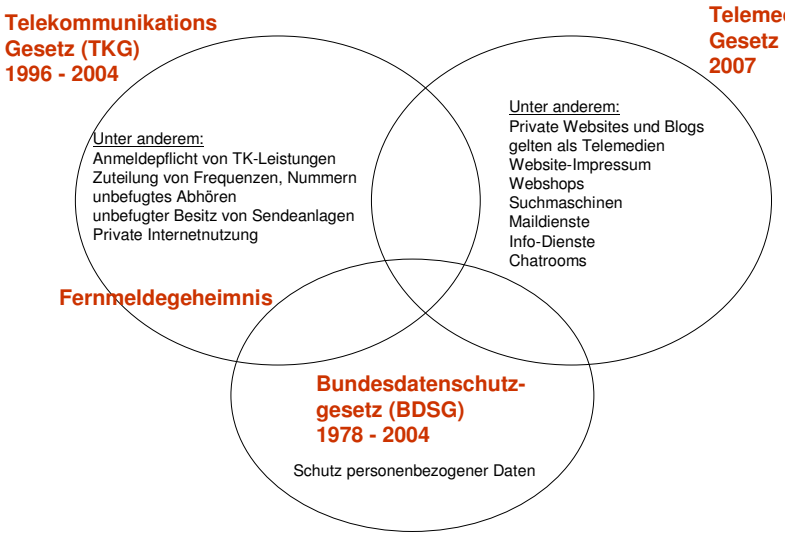
DS-2

Datenschutz
- → heftige und kontroverse Meinungsäußerungen!
- → Thema „Der große Bruder“ aus dem Roman „1984“ von George Orwell
- → Auseinandersetzungen zwischen Arbeitgebern und Gewerkschaften um betriebliche Personalinformations-systeme (PIS)
- → stetiges Nachhinken möglicher juristischer und technischer Maßnahmen des Datenschutzes und der Datensicherung hinter neuen Informationstechnologien (Telefonüberwachung, Zugriff zu privaten PC über das Web)

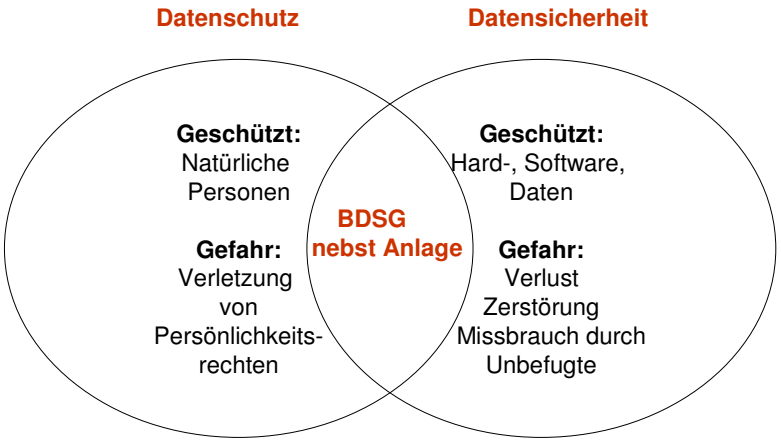
Datensicherung → „Die Gesamtheit der Maßnahmen, die Daten in ihrem Bestand, ihrer Form und ihrem Inhalt vor gewollten oder ungewollten Störungen durch Menschen oder Umwelt sowie vor unbefugter Einsicht schützen sollen.“

Datenschutzvorschriften existieren seit Jahren:
Arzt-, Steuer-, Bank-, Postgeheimnis; Gesetz über das Kreditwesen, Arbeits-Förderungs-, Berufsbildungs-, Betriebsverfassungsgesetz u.a.

Begriffsabgrenzung



Begriffsabgrenzung



Historie des Datenschutzes

1970	Das Hessische Datenschutzgesetz (**das erste Datenschutzgesetz der Welt**)
1973	Das Schwedische Datenschutzgesetz
1977	Das Kanadische Datenschutzgesetz (Human Rigths Act)
1978	Das Französische Gesetz über die elektronische Datenverarbeitung Das Dänische Gesetz über die Register der Behörden und die privaten Register Das Norwegische Gesetz über Personendatenregister Das Österreichische Datenschutzgesetz
1978	Das Bundesdatenschutzgesetz **(BDSG)** ab 1.1.1978 in Kraft
1991	Novellierung des Bundesdatenschutzgesetzes
1995	**Die EG-Datenschutzrichtlinie**
	Novellierung des Bundesdatenschutzgesetzes
Mai 2004	Umsetzungsfrist

Ziele des Datenschutzes

1. Vermeidung der Verletzung der Persönlichkeitsrechte **(§1 Abs.1 BDSG)**

   Jeder Mitarbeiter
   ist
   Bürger, Kunde, Arbeitnehmer…
   Betroffener

2. **Gewährleistung** des
   „Recht(s) auf informationelle Selbstbestimmung“ (1984)

3. **Abwehr** von Gefahren des Missbrauchs von Daten

4. Gebot zur **Datenvermeidung** und **Datensparsamkeit**

Ziele des Datenschutzes

§ 1 Absatz 1 BDSG

Zweck des Datenschutzrechtes ist es, den ***Einzelnen*** davor zu schützen, dass er durch den Umgang mit seinen **personenbezogenen Daten** in seinem Persönlichkeitsrecht beeinträchtigt wird

Wer ist der Einzelne?

Mitarbeiter
Bewerber
Mitarbeiter aus Fremdfirma
Kunde
Interessent
Besucher

Begriffsdefinitionen

personenbezogene Daten

sind Einzelangaben zu - persönlichen oder
- sachlichen

Verhältnissen einer bestimmten oder bestimmbaren Person (Betroffener)

§3 Abs.1 BDSG

Einzelangaben zu persönlichen Verhältnissen

sind
- Name
- Anschrift
- Familienstand
- Geburtsdatum
- Staatsangehörigkeit
- Konfession
- Beruf
- Vereinszugehörigkeit
- Krankheiten / Gesundheitszustand
- arbeitsrechtliche Beurteilungen etc.

Begriffsdefinitionen

Einzelangaben zu sachlichen Verhältnissen

beziehen sich auf
- Besitzverhältnisse
- Eigentumsverhältnisse
- Einkommen
- vertragliche Beziehungen zu Dritten (z.B. Versicherungen)
- Vertragskonditionen
- Steuern etc.

Besondere Datenarten (sensitive Daten) § 3 Abs. 9

alle Angaben über :
- die rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder philosophische Überzeugungen
- Gewerkschaftszugehörigkeit
- Gesundheit
- Sexualleben etc.

Begriffsdefinitionen

Automatisierte Verarbeitung ist
die Erhebung, Verarbeitung oder Nutzung von Daten
unter Einsatz von **Datenverarbeitungsanlagen.**

Nicht automatisierte Datei ist
jede Sammlung personenbezogener Daten, die gleichartig aufgebaut ist **und** nach bestimmten Merkmalen zugänglich ist **und** ausgewertet werden kann.

Pseudonymisieren ist
das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffen auszuschließen oder wesentlich zu erschweren.

Anonymisieren ist
das Ersetzen von Daten einer Person in der Art, dass diese nicht mehr der Person zugeordnet werden können. (Datenvermeidung)

Begriffsdefinitionen

Datenumgang umfasst das
Erheben, *Verarbeiten* und Verwenden (Nutzen) von Daten **§3 Abs.4**

Erheben ist
das Beschaffen von Daten über den Betroffenen

Verarbeiten umfasst das
- Speichern
- Verändern
- Übermitteln
- Sperren und
- Löschen von Daten

BDSG – Grundsätze

Ziel: Nicht Verhinderung einer Verarbeitung, sondern Kontrolle der DV

Grundsätze:

- **Relevanz:** Es dürfen nur Daten ermittelt und verarbeitet werden, die relevant (d.h. wesentlich) in Bezug auf den Betriebszweck des Auftraggebers sind
- **Publizität:** Als individuelle Publizität wurde das Auskunftsrecht des Betroffenen über seine Daten verankert (-> Register)
- **Richtigkeit:** Diesem Grundsatz entsprechend hat der Betroffene ein Recht darauf, falsche Daten richtig stellen zu lassen und unzulässigerweise ermittelte Daten löschen zu lassen
- **Weitergabebeschränkung:** Als zentraler Teil einer Datenverwendungskontrolle geht es hier um Einschränkungen der Übermittlung sowie um Regelungen, unter welchen Voraussetzungen Datenbanken verknüpft werden dürfen
- **Trennung der Funktionen:** Die informationstechnische Durchführung (-> Service-RZ) wird getrennt von der Funktion des Auftraggebers, der die rechtliche Verantwortung für die Anwendungen trägt
- **Verpflichtung zu Datensicherungsmaßnahmen**
- **Statuierung einer eigenen Geheimhaltungspflicht** (Datengeheimnis)
- **Schaffung eigener Kontrollorgane** (Datenschutzbeauftragte)
- **Internationaler Datenverkehr** (Kontrolle grenzüberschreitender Datenverkehr)

Zulässigkeit des Datenumgangs

§ 4 Abs. 1

Die **Erhebung, Verarbeitung und Nutzung** personenbezogener Daten ist nur zulässig, soweit

- das **BDSG** oder
- eine andere Rechtsvorschrift dies erlaubt oder
- der Betroffene eingewilligt hat.

andere Rechtsvorschriften im Sinne von **§ 4 Absatz 1 BDSG** sind dem Bundesrecht ***nachrangige*** Rechtsvorschriften, wie etwa

- Landesrecht
- kommunales Recht
- Betriebsvereinbarungen

Zulässigkeit des Datenumgangs

gemäß

§ 1 Absatz 3 Satz 1 BDSG

gehen andere Rechtsvorschriften des Bundes den Vorschriften dieses Gesetztes (BDSG) vor, soweit sie auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind.

Dabei ist gleichgültig, ob die Spezialregelung im Hinblick auf das datenschutzrechtliche Schutzniveau hinter dem BDSG zurückbleibt oder ob es höher ansetzt:

gemeint sind hier etwa:
- arbeitsrechtliche Vorschriften
- handelsrechtliche Vorschriften
- Sozialgesetze
- Steuergesetze

Zulässigkeit des Datenumgangs

im Rahmen der Verarbeitung **sensitiver Daten** sind engere Voraussetzungen an die Zulässigkeit der Datenverarbeitung gestellt

§ 28 BDSG

fasst die Zulässigkeitstatbestände einer Datenverarbeitung als Mittel für die Erfüllung eigener Geschäftszwecke zusammen

Zulässigkeit des Datenumgangs

gemäß **§ 28 Absatz 1 BDSG** ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig,

→
wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient

►Abwicklung Mitgliedschaftsverhältnis
Arbeitsverhältnis

Rechte + Pflichten

Mitarbeiter

Einhaltung der Datenschutzregelungen (intern, extern)

- Schutz vor unberechtigtem Zugriff
- Keine unzulässige Weitergabe an Dritte
- Information des Vorgesetzten und DSB

Führungskräfte

Verpflichtung aller auf das Datengeheimnis

- Keine unzulässige Weitergabe an Dritte
- Schulung
- Arbeitsanweisungen
- Kontrollen
- Vertragsgestaltung
- Info des DSB
- Einschaltung des DSB
- Dokumentationspflicht

Rechte der Betroffenen

- **Auskunft** §34

- **Benachrichtigung** über §35
  - Tatsache der Speicherung (bei erstmaliger Speicherung)
  - Art der gespeicherten Daten
  - Zweckbestimmung der Erhebung
  - Verarbeitung oder Nutzung
  - Name und die Anschrift des Unternehmens
  - Kategorien der Empfänger (bei Weitergabe von Daten)

ABER:
eine Benachrichtigung ist insbesondere dann nicht erforderlich, wenn der Betroffene auf andere Weise Kenntnis von der Sicherung hat
- so etwa bei bestehenden Vertrags- oder vertragsähnlichen Vertrauens-verhältnissen

oder
- wenn der Betroffene seine Daten selbst mitgeteilt hat.

Rechte der Betroffenen

- **Berichtigung** §35
  - soweit die Daten unrichtig sind

- **Löschung** §35
  - Nr.1
    wenn die Speicherung der Daten unzulässig ist
  - Nr. 2
    wenn es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit, über Gesundheit oder das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verarbeitenden Stelle nicht bewiesen werden kann

Rechte der Betroffenen

- **Sperrung** §35

  das Recht auf Sperrung - **§ 35 Absatz 3 BDSG** tritt an die Stelle der Löschung, soweit

  Nr. 1
  im Falle des **§ 35 Absatz 2 Nr. 3 BDSG** einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen

  Nr. 2
  Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden

  Nr.3
  eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist

Rechte der Betroffenen

- **Widerspruch** §35
  - führt zur Unzulässigkeit der Datenverarbeitung, soweit eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen Situation daran überwiegt

- **Schadensersatz** §7

Risiken

Computerviren

Hacker

Mitarbeiter (unwissend oder fahrlässig)

Geschäftspartner

Dienstleister (z.B. Putzkräfte)

Fehler/Fahrlässigkeit in IT-Sicherheit

Unwissenheit

etc.

Datensicherheit nach § 9 BDSG

Ziele:

Verfügbarkeit
kein Datenverlust

Authentizität
Echtheit
Sicherstellung des Autors

Integrität
Vollständigkeit
keine Änderung durch Unbefugte

Datensicherheit / 8 Gebote

§6 BDSG: Sicherheitsmaßnahmen zur Erfüllung des Datenschutzes

Realisierbar durch:	
Zutrittskontrolle (Raum)	Unbefugten ist der Zutritt zu verwehren
Zugangskontrolle (IS)	Unbefugten ist die Nutzung zu verwehren
Zugriffskontrolle (Berechtigung)	Unbefugten Mitarbeitern ist der Zugriff zu verwehren
Weitergabekontrolle (Kommunikation)	Schutz bei Transport und Speicherung
Eingabekontrolle (Person)	Gewährleistung einer nachträglichen Überprüfung und Feststellung
Auftragskontrolle (Fremdaufträge)	Entsprechend der Weisung des Auftraggebers
Verfügbarkeitskontrolle (Verlust)	Schutz vor Zerstörung und Verlust
Trennungsgebot (Zweck)	Gewährleistung von Zweckunterscheidung

Zu: Datensicherheit / 8 Gebote

Zutrittskontrolle:
Ausweisleser/ Schlüssel
Anmeldung beim Pförtner
Kameraüberwachung des Geländes

Zugangskontrolle:
Passwortschutz (Verwehrung des Zugangs von Unbefugten)
Abmeldung des Rechners
Verschlüsselung

Zugriffskontrolle:
Passwort
Protokollierung
Firewall

Weitergabekontrolle:
Verschlüsselung
Protokolle (an welche Stellen…)
Absicherung der Übertragungswege

Zu: Datensicherheit / 8 Gebote

Eingabekontrolle:
Berechtigungsvergabe
Menügestaltung
Kontrolle (welche Daten zu welcher Zeit von wem in DV eingegeben)

Auftragskontrolle:
Sorgfältige Auswahl des Auftragnehmers
Einhaltung der Weisungen des Auftraggebers
Kontrolle der Auftragnehmer

Verfügbarkeitskontrolle:
Katastrophenvorsorge
ordnungsgemäße Sicherungen

Trennungskontrolle:
logische Trennung
Abgrenzung der Verarbeitungszwecke

Büroalltag

Datengeheimnis §5
Alle Mitarbeiter, die mit der Verwendung personenbezogener Daten beschäftigt sind, sind auf das Datengeheimnis zu verpflichten.

Hierzu zählen auch Teilzeitkräfte, Auszubildende, Mitglieder des Betriebsrats.

Alle Mitarbeiter sind zu informieren und zu schulen, damit sie eine Sensibilität für personenbezogene Daten ihrer Kunden, Kollegen etc. und ihrer eigenen personenbezogenen Daten entwickeln können

und damit sie

Ideen zur Verbesserung des Datenschutzes und der Datensicherheit kreieren können.

Grundsätze ordnungsgemäßer DV

"Es ist **Pflicht des Kaufmanns**, Bücher zu führen und die dafür geltenden Vorschriften einzuhalten **(§ 238 HGB, § 140 AO).** Werden bestimmte Buchführungsaufgaben auf die DV verlegt, hat er dafür zu sorgen, dass die DV die Vorschriften in gleicher Weise erfüllt."

Grundsatz der Auftragsbindung

Dazu gehören:

- → alle Geschäftsvorfälle (GV) müssen autorisiert sein
- → für alle bilanzwirksamen GV müssen die Grundfunktionen der Buchführung (Beleg-, Grundbuch- und Kontofunktion) erfüllt sein
- → die Anforderungen der Vollständigkeit, Zeitgerechtigkeit, Klarheit und Richtigkeit müssen eingehalten werden
- → die Belege und Bücher müssen für Prüfungszwecke lesbar und verfügbar sein
- → die verwendeten Nachweismedien müssen über die Aufbewahrungsfrist dauerhaft sein

Grundsatz der Kontrollierbarkeit

Dazu gehören:

- →Zulässigkeitskontrollen beim Benutzerzugriff
- →Fehlerkontrollen bei der Dateneingabe
- →Abstimmkontrollen bei der Datenbestandsführung
- →Abwicklungskontrollen über den Tagesbetrieb, die Betriebssystemverwaltung, die Dateiverwaltung
- →Schutzmaßnahmen gegen die Verfälschung von Daten und Programmen

Grundsatz der Transparenz

Dazu gehören:

- →alle für ein Verfahren relevanten Angaben über Dateneingaben und -ausgaben, Speicherung, Verarbeitung und Übertragung von Daten zu dokumentieren
- →die Dokumentation ist übersichtlich zu gliedern
- →die Dokumentation soll eindeutig und aktuell sein
- →über die vorgeschriebene Aufbewahrungsfrist soll auch die Entwicklungsgeschichte nachgewiesen werden
- →Dokumentationen über buchhalterische Verfahren sind nach **§ 257 HGB** und **§ 147 AO** aufzubewahren (10 Jahre)

Grundsatz der Funktionssicherheit

dazu gehören:

→Schutz vor Zerstörung durch räumliche Sicherungsmaßnahmen
→Speicherung der Daten / Programme auf dauerhaften Datenträgern
→verlässliches Datensicherungssystem zur Gewährleistung der Verfügbarkeit gemäß Aufbewahrungspflicht
→Schutz der Daten / Programme vor Manipulationen (z.B. Funktionstrennung zwischen EDV-Betrieb, Datenverwaltung, Betriebssystemverwaltung, Programmverwaltung, Programmierung)
→angemessener Versicherungsschutz für Gefahren und Schadenspotential
→Überwachung der Sicherungs- und Kontrollmaßnahmen durch eine Revision