

**Interface!brunch**

**Datenschutz und Datensicherheit**

**am 29. März 2007 bei CBXNET**

**Wolf-Ingo Wengel (Dipl.-Ing. FH)**  
**Datenschutzbeauftragter**



**GESELLSCHAFT FÜR DATENSCHUTZ  
UND DATENSICHERUNG e.V.**

# 1. Rechtliche Grundlagen

## Das Volkszählungsurteil des BVerfG (1983)

„Recht auf informationelle Selbstbestimmung“

Siehe Grundgesetz

Artikel 1: Die Würde des Menschen ist unantastbar

Artikel 2: Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit

## Europäische Datenschutzrichtlinie

wirksam seit 24.10. 1995 (für EU Mitgliedsstaaten)

Umsetzungszeitraum. drei Jahre (24.10. 1998)

Deutschland: neues BDSG seit 23.5. 2001 (!)

## Das Bundesdatenschutzgesetz (BDSG)

Gliederung in sechs Abschnitte

§§ 1-11: allgemeine Bestimmungen

(Schutzzweck, Anwendungsbereich, Begriffsdefinitionen)

§§ 12-26: öffentliche Stellen

(Rechtsgrundlagen, Rechte des Betroffenen, Bundesdatenschutzbeauftragter)

§§ 27-38a: nichtöffentliche Stellen

(Rechtsgrundlagen, Rechte des Betroffenen, Aufsichtsbehörde)

§§ 39-42: Sondervorschriften

(Forschung, Berufs- und Amtsgeheimnisse,

DSB für Medien des Bundesrechtes: DLF, DW)

§§ 43,44: Schlußvorschriften

(Straf - und Bußgeldtatbestände)

§§ 45-46: Übergangsvorschriften

(Anpassungsfristen laufender Verwendungen, Weitergeltung von Begriffsdefinitionen)

„NICHTÖFFENTLICHE STELLEN“:

Personen und Personenmehrheiten, die rechtlich selbständig sind.

personenbezogene Daten :

Einzelangaben über persönliche oder sachliche Verhältnisse

*Persönlich*: Name, Adresse, Familienstand, Geburtsdatum, Staatsangehörigkeit,

Konfession, Krankheiten.....

*Sachlich*: Einkommen, Versicherung, Eigentumsverhältnisse, KFZ, Steuer....

AUFSICHTSBEHÖRDE:

§ 38 BDSG: Bundesländer (einige Regelungen auf Länderebene abweichend)

Das Teledienstschutzgesetzes (TDDSG) und das  
Telekommunikationsgesetz (TKG)

TRANSPORTSCHICHT (Telekommunikation) **TKG**

DIENSTEBENE (Teledienst) **TDDSG**

INHALTSEBENE (allg. Recht) **BDSG** ggf. Landesdatenschutzgesetze

Datenübermittlung innerhalb Europas

GRUNDLAGE: Europäische Datenschutzrichtlinie 95/46 EG – gilt für:

- Übermittlung in andere EU-Mitgliedsstaaten
- Übermittlung in andere Vertragsstaaten des europäischen Wirtschaftsraumes (Norwegen, Island, Lichtenstein)
- Organe und Einrichtungen der EU

(wie Inlandsübermittlung - §§ 4, 28-30 BDSG)

Datenübermittlung in Drittstaaten

- Zulässigkeit gem. §§ 4, 27 ff BDSG prüfen
- angemessenes Datenschutzniveau beim Drittlandempfänger prüfen

Wenn das angemessenes Datenschutzniveau nicht gegeben sein sollte ist eine Übermittlung zulässig bei Einwilligung des Betroffenen bzw. Datenschutzgarantien (Vertragslösung, Konzernrichtlinien)  
Das BDSG macht keine Aussagen, WANN ein angemessenes DS-Niveau vorliegt.

Gemäß EU-DSRL (Art. 25 Abs. 6) gibt es ein angemessenes DS-Niveau für Argentinien, Guernsey, Isle of Man, Schweiz, Kanada (z.T !)

Hilfestellung zur Beurteilung eines angemessenen Datenschutzniveaus  
[http://europa.eu.int/comm/internal\\_market/privacy/index\\_de.htm](http://europa.eu.int/comm/internal_market/privacy/index_de.htm).

Datenübermittlung in die USA

Weitgehend fehlende Datenschutzvorschriften, EU: „kein angemessenes DS-Niveau“  
Seit 27.7.2000: Safe-Harbor-Principles (Übereinkommen EU mit US-Handelsminist.)

US-Unternehmen können Safe Harbor freiwillig beitreten.

Liste beigetretener Unternehmen abrufbar unter:

[web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list](http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list)

## 2. betrieblicher Datenschutz

### Der betriebliche Datenschutzbeauftragte

#### AUFGABEN

- Überwachung der ordnungsgemäßen Anwendung der IT-Programme
- Vorabkontrolle von automatisierten Verarbeitungen
- Auskunft über Verfahren der DV (Verfahrensverzeichnis) – auf Antrag
- Beschwerden von Betroffenen nachgehen (Mitarbeiter, Kunden, Lieferanten...)
- Schulung der relevanten Mitarbeiter
- Beratung der Unternehmensleitung
- Mitwirkung bei Betriebsvereinbarungen o.ä.
- Mitwirkung bei der Vertragsgestaltung (Rechenzentren, Fernwartung, Entsorgung)

#### STELLUNG IM BETRIEB

- unmittelbar dem Vorstand / der GF unterstellt
- weisungsfrei in Ausübung seiner Funktion als DSB
- darf wg. Erfüllung seiner Aufgaben nicht benachteiligt sein
- Verschwiegenheitspflicht

#### WER (welches Unternehmen) MUSS EINEN DSB BESTELLEN

- mind. 10 Personen verarbeiten automatisiert Daten
- unabhängig von Mitarbeiterzahl bei Pflicht zur Vorabkontrolle oder Meldepflicht

#### VORAUSSETZUNGEN FÜR DIE BESTELLUNG EINES DSB

Fachkunde (Kenntnisse in: IT, BWL, Recht, Organisation, Revision, Kommunikation)

Zuverlässigkeit (keine Interessenkonflikte, persönl. Integrität)

NICHT bestellt werden dürfen z.B. Leiter IT, Leiter Personal, Geschäftsführung  
BESTELLT werden dürfen z.B. MA aus Revision, Organisation, Rechtsabteilung

FUNKTIONSFORMEN: Vollzeit, Extern – ggf. nebenberuflich

#### Vorteile eines externen Datenschutzbeauftragten – speziell für kmU's

- Effektive und zuverlässige Umsetzung der Aufgaben eines DSBs
- Transparente Kostenplanung / kalkulierbare Kosten durch Beratervertrag
- Befristeter Vertrag mit einem externen DSB, statt eines besonderen Kündigungsschutzes bei einem internen DSB
- Kostensenkung durch Outsourcing. Die eigenen Mitarbeiter können sich Ihren Kernaufgaben widmen
- Keine (zusätzlichen) Kosten für Aus- und Weiterbildung
- Vermeidung innerbetrieblicher Interessenskonflikte
- Unvoreingenommenheit des externen DSBs gegenüber der Sache und der Firma
- Keine „Betriebsblindheit“
- Synergieeffekte“ durch Praxiserfahrungen aus anderen Unternehmen

### 3. Datenschutz-Praxis

DATENVERARBEITUNGSPHASEN pb Daten

Erhebung, Verarbeitung, Nutzung

Speichern, Verändern, Übermitteln, Sperren, Löschen

#### DV für eigene Geschäftszwecke

Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichem Vertrauensverhältnis

VERTRÄGE: Arbeitsvertrag, Kaufvertrag, Werkvertrag, Dienstvertrag

Vertragsähnl. VERTRAUENSVERHÄLTNISSE:

Geschäftsanhörung / Bewerbung

Mitgliedschaftsverhältnisse

Geschäftsführung ohne Auftrag (§§ 677 ff. BGB)

Gefälligkeitsverhältnisse

*Dazu können auch Daten Dritter zählen*

Problemfelder:

- Bonitätsdaten (z.B. bei Kreditverträgen)
- Rennlisten
- Werturteile über Kunden oder Angestellte
- Leistungs- und Verhaltensdaten

Erhebung, Verarbeitung und Nutzung von pb Daten ist nur zulässig, soweit das BDSG (oder eine andere Rechtsvorschrift) dies erlaubt oder anordnet ODER der Betroffene eingewilligt hat.

**Schutzwürdig ist ALLES, wo ein persönliches Interesse Betroffener besteht.**

#### Auftragsdatenverarbeitung (ADV)

Die verantwortliche Stelle bedient sich einer Stelle, die **weisungsabhängig** pb Daten erhebt, verarbeitet oder nutzt.

Beispiele: Rechenzentrum als Dienstleister, Datenerfassungsbüros, Direktmarketing

#### Funktionsübertragung (Abgrenzung zur ADV)

Es wird nicht nur eine weisungsabhängige DV-Hilfsfunktion ausgeführt, sondern die übergebenen Daten werden zur Erfüllung weiterer (eigener) Aufgaben oder Funktionen benötigt.

Beispiele: ext. Lohnbuchhaltung, Personalverwaltung, Inkasso

## 4. techn.- organisatorische Maßnahmen

### Einteilung der Telekommunikation in Unternehmen

#### TRANSPORTSCHICHT

(Telekommunikation) **TKG**

pb Daten: Quelle, Datum, Zeit, Dauer, Anschluss, Zielnummer, Datenmenge

#### DIENSTEBENE

(Teledienst) **TDDSG**

pb Daten: Seiten im web, Verweildauer, feste IP's,

#### INHALTSEBENE

(allg. Recht) **BDSG** ggf. Landesdatenschutzgesetze

pb Daten: Inhalt von Gespräch oder E-mail, kommunizierte Daten, downloads

Die dienstliche / berufliche Nutzung z.B. des Internet fällt nicht in den Anwendungsbereich des TDDSG

Umkehrschluss: die erlaubte private Nutzung fällt darunter.

Wenn der Arbeitgeber private Telekommunikation erlaubt, wird er gegenüber dem Arbeitnehmer zum Anbieter.

(Der Betriebsrat regelt Arbeitnehmerbelange, NICHT private Belange!)

Erlaubnis: ausdrücklich oder konkludent

Ausdrücklich: Arbeitsvertrag, Erklärung des AG, Betriebsvereinbarung

Konkludent: „betriebliche Übung“ (Praxis) - mind. ½ Jahr in Gebrauch

Beispiel: in einem Betrieb ist das private Telefonieren grundsätzlich gestattet.

Später wird ein betriebliches E-mail-System eingeführt. Es kann daraus geschlossen werden, dass die private Nutzung des E-mail-Systems erlaubt ist.

### **Es gibt derzeit in Deutschland (noch) keine höchstrichterliche Rechtssprechung zur Internetnutzung !**

Eine einmal gegebene uneingeschränkte Erlaubnis lässt sich (für AG) nur sehr schwer wieder rückgängig machen .....!

Lösungen:

IT- und Kommunikationskonzept des Unternehmens sollte alle mögliche „Fälle“ berücksichtigen und entsprechende Vorkehrungen beinhalten.

Beispiele:

Einrichtung privater E-mail Accounts

Vorwahl von speziellen Codes

## Videüberwachung

geschlossene, betriebliche Räume (BAG)

AG und ggf. BR haben das allgemeine Persönlichkeitsrecht des AG zu beachten

öffentlich zugängliche Räume (§ 6b BDSG)

Beobachtung (in Echtzeit) z.B. Eingangsbereiche, Schalterhallen, Zaunanlagen d.h Wahrnehmung des Hausrechtes oder berechtigter Interessen für konkrete Zwecke.

Verarbeitung und Nutzung ist im Rahmen des Erforderlichen zulässig.

Es besteht eine Informationspflicht (erkennbar machen, dass überwacht wird, wer dies tut, Benachrichtigung bei Identifizierung)

Löschung: unmittelbar, wenn der Zweck erreicht ist. (in der Regel zwischen 24 Stunden und einer Woche, Praxis ca. drei Tage) (§ 6b Abs. 3 + 4 BDSG)

Spezialfall: verdeckte Videoüberwachung

gem. BAG (Urteil vom 27.3.2003) ist die Zulässigkeit gegeben wenn:

- ein konkreter Verdacht einer strafbaren Handlung oder eine andere schwere Verfehlung zu Lasten des AG vorliegt
- weniger einschneidende Maßnahmen ausgeschöpft sind
- die (verd.) Videoüberwachung das einzig verbleibende Mittel ist
- die (verd.) Videoüberwachung insgesamt nicht unverhältnismäßig ist

## EHUG

Am 1. Januar 2007 trat das „Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister“ (EHUG) in Kraft. Es gilt für alle im Handelsregister eingetragenen Unternehmen.

Verändert bzw. angepasst wurden die nachfolgenden Paragraphen:

Handelsgesetzbuch § 37a Abs. 1, §125 Abs.1, Satz 1

Aktienengesetz § 80 Abs.1, Satz 1

GmbH-Gesetz § 35a Abs.1, Satz 1

Genossenschaftsgesetz § 25 a

indem auf >Geschäftsbriefe< die Formulierung „gleichviel welcher Form“ eingefügt wurde.

Das betrifft somit E-mails, Faxe, Postkarten oder andere Schreiben, die Geschäftsbriefe ersetzen, wie z.B. Auftragsbestätigungen, Angebote oder Bestellformulare(Karten).

Die gesetzliche Änderung macht (leider) keine Aussagen zu Kleingewerbetreibenden wie z.B. GbR's, die nicht im Handelsregister eingetragen sind. Eine Änderung des § 15b der Gewerbeordnung (GewO) im o.g. Sinne erfolgte nicht.

Das Handelsgericht kann fehlende Angaben auf Geschäftsbriefen mit Zwangsgeld ahnden.

Ob allerdings auch eine wettbewerbsrechtliche Abmahnung für fehlende Angaben gerechtfertigt sein könnte, ist derzeit gerichtlich nicht geklärt

## 5. IT – Sicherheit

Daten sind verschiedenen Bedrohungen ausgesetzt

Organisatorische Mängel	z.B. fehlende Regelungen
Höhere Gewalt	z.B. Blitzschlag, Hochwasser
Menschliches Versagen	z.B. Fehlbedienung
Technisches Versagen	z.B. Festplattencrash
Vorsätzliche Handlungen	z.B. Hackerangriff auf Passwortdatei

Sehr oft werden die tatsächlichen Bedrohungen subjektiv falsch eingeschätzt

<u>Schäden durch</u>	<u>befürchtet</u>	<u>tatsächlich</u>
Viren	43%	19%
Java	9%	0%
AxiveX	17%	0%
Phys. Einbruch	11%	1%
Missbrauch von Schutzrechten	20%	70%

Quelle:Meta Group Deutschland GmbH

### Die am meisten verbreiteten Angriffsmethoden

Angriffe auf Passworte  
(Raten, Ausspionieren, Passwortknacker ,Brute Force Attacken)

Pishing „password - fishing“  
(gefälschte Bank-mails, gefälschte websites mit PIN-Eingabe)

Laufzeitfehler provozieren  
(Buffer Overflows, undefinierte Zustände durch Ausnutzung von Softwarefehlern)

Sniffing  
(Netzwerkkarten manipulieren zum mitlesen aller Datenpakete – lokal oder im Internet durch umkonfigurierten Router oder Funknetz (W-LAN) mitlesen, wenn unverschlüsselt)

Spoofing  
(vortäuschen einer falschen Identität – IP, DNS, Mail)

Spamming  
(Überflutung von E-mail-Accounts – z.T. bis zur Überlastung von Servern/Netzen)

Denial of Service (DoS) d.h. Überlastung von Servern  
(immer neue Dienste starten oder Verbindungsanforderungen – SYN-Flooding)

Ausnutzung von Schwachstellen  
(durch ein bestimmtes Datenpaket stürzt ein Server sofort ab – z.B. „ping of death“)

destruktive Programme  
(Viren -benötigen Wirt-, Würmer, Trojaner)

*Aber die einfachste und meist erfolgreichste Angriffsmethode ist:*

SOCIAL ENGINEERING  
d.h. das systematische aushorchen von Mitarbeitern oder IT-Administratoren !

Anforderungen an die IT-Sicherheit für pb Daten gem. BDSG

Zutrittskontrolle

Zugangskontrolle

Zugriffskontrolle

Verfügbarkeitskontrolle

Eingabekontrolle

Weitergabekontrolle

Auftragskontrolle

Gewährleistung getrennter Verarbeitung

RISIKOMANAGEMENT

Mit relativ geringem Aufwand ist bereits ein hoher Sicherheitsstand erreichbar.  
Eine weitere Erhöhung des Aufwandes erhöht die Sicherheit nur noch gering.

**IT-Sicherheit ist eine Führungsaufgabe, denn sie muss  
„von oben“ initiiert und verantwortet werden.**

---