

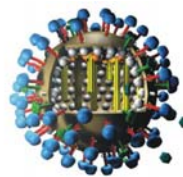
## Umsetzung gesetzlicher Anforderungen im Bereich IT-Sicherheit und Datenschutz in kleinen und mittleren Unternehmen

Klaus Foitzick  
Geschäftsführer  
net integration Informationsmanagement GmbH,  
Volljurist, ISO 27001 Auditor

München 25.6.2008

### Basisinformation

- Das „**mooresche Gesetz**“ sagt aus, dass sich die Anzahl an Transistoren auf einem handelsüblichen Prozessor alle achtzehn Monate verdoppelt.
- Dies wird auch voraussichtlich die nächsten 20 Jahre so bleiben.
- Behält das „**mooresche Gesetz**“ Recht, so haben in einem Prozessor in 20 Jahren ca. 1 Million mal so viele Transistoren Platz wie heute.
- Aktuell haben Transistoren eine Länge von ca. 50 nm und sind etwa so groß wie ein **Influenzavirus**.



Grafik und Daten aus Wikipedia, 2008

## Was bedeutet dies für uns?



- Wir stehen mit der Entwicklung im Bereich der Informationstechnologie ganz am Anfang.
- IT-Systeme werden Menschen zunehmend in allen Bereichen unterstützen. Z.B.
  - Medizin (z.B. Ambient Assisted Living) **Software as a Service**
  - Kommunikationstechnologie **hat**
  - Branchen- und Bürosoftware **steigenden Marktanteil**

**Der Umfang sensibler Daten von Menschen und Unternehmen in digitaler Form wird dramatisch steigen. Vertraulichkeit, Integrität und Verfügbarkeit sind ein Muss.**

## Dies darf nicht passieren!



The screenshot shows the website **wiwo.de** on Monday, 23.06.2008. The main article is titled "Ex-Vorstände Hultsch und Klinkhammer waren informiert" and "Neue Affäre: Telekom hörte Telefonkunden ab". The article text states: "Die Deutsche Telekom räumt nach der bekannt gewordenen Ausspionierung von Journalisten und eines Aufsichtsrats einen neuen Abhörskandal ein. Wie aus vertraulichen Protokollen, Aufzeichnungen und Briefen hervorgeht, die der WirtschaftsWoche sowie dem ZDF vorliegen, hat das Unternehmen vom 12. bis 16. Dezember 1996 insgesamt rund 120 Telefongespräche von Telefonkunden überwacht - ohne Einschaltung der Staatsanwaltschaft und ohne richterliche Anordnung." The article has 4 comments and 17 ratings. On the right, there is an advertisement for Cisco with the text "Alle Mitarbeiter sind jederzeit erreichbar. Mehr dazu -> welcome to the human network. CISCO". Below the ad is a section "Köpfe der Wirtschaft" featuring René Obermann (Deutsche Telekom AG) and Dr. phil. Ron Sommer (Deutsche Telekom (ehemals)). The browser status bar at the bottom shows "Internet | Geschützter Modus: Inaktiv" and a zoom level of 100%.

## Gesetzliche Regelungen für Unternehmen



Bundesdatenschutzgesetz	Rechtsgrundlage für die Verarbeitung personenbezogener Daten
Telekommunikationsgesetz	Kommunikation über elektronische Medien wie E-Mail und Telefon
GoBS, GoB, GdpdU, GmbHG, AktG, HGB, „EuroSOX“	<ul style="list-style-type: none"> <li>• Archivierung steuerlich relevanter Daten,</li> <li>• interne Kontrollsysteme,</li> <li>• Mitwirkungspflichten,</li> <li>• IT-Sicherheitskonzept,</li> <li>• Risikokonzept</li> </ul>
Viele weitere, auch branchenspezifische, Gesetze und Regelungen	

## Gelten diese Regelungen für KMUs



Gelten alle diese Regelungen auch für kleine und mittlere Unternehmen?

Was sind kleine und mittlere Unternehmen?

## Was sind KMUs?



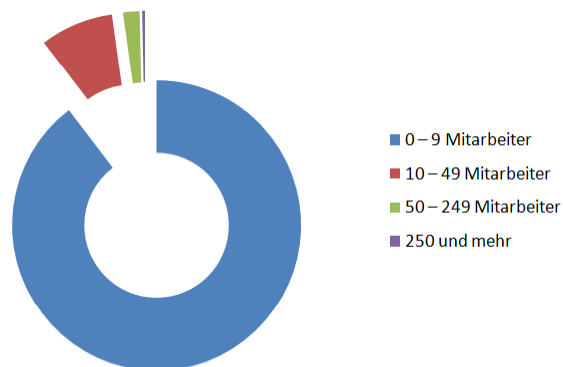
Die Kommission der Europäischen Union empfiehlt folgende Definition:

**Kleine und mittlere Unternehmen (KMU)** ist die Sammelbezeichnung für Unternehmen, die definierte Grenzen hinsichtlich Beschäftigtenzahl, Umsatzerlös oder Bilanzsumme nicht überschreiten.

Typ	Beschäftigte		Umsatzerlös (Mio €)		Bilanzsumme (Mio €)
Mittlere Unternehmen	< 250	und	≤ 50	oder	≤ 43
Kleine Unternehmen	< 50	und	≤ 10	oder	≤ 10
Kleinstunternehmen	< 10	und	≤ 2	oder	≤ 2

KMU-Definition: Empfehlung der Kommission vom 6. Mai 2003

## Verteilung der Unternehmensgrößen in Deutschland



Statistisches Bundesamt, Statistisches Jahrbuch 2007

Gelten diese Regelungen für KMUs



Ja,  
die gesetzlichen Regelungen müssen, bis auf  
geringe Ausnahmen, auch durch kleine und  
mittlere Unternehmen erfüllt werden.

Aber, die Verhältnismäßigkeit muss gewahrt  
bleiben.

Wichtigste Aufgaben



Bundesdaten- schutzgesetz (BDSG)	<ul style="list-style-type: none"> <li>• Bestellung Datenschutzbeauftragter § 4g</li> <li>• Verpflichtung /Schulung der Mitarbeiter § 5</li> <li>• (Vorab-)kontrolle sensibler Systeme</li> <li>• Verzeichnisse § 4g</li> <li>• Technische und org. Maßnahmen § 9</li> </ul>
Telekommunikations- gesetz (TKG)	Regelungen für die E-Mail- und Internetnutzung
GoBS, GoB, GdgdU, GmbHG, AktG, HGB	<ul style="list-style-type: none"> <li>• Archivierung steuerlich relevanter Daten,</li> <li>• internes Kontrollsystem,</li> <li>• Risikomanagement</li> </ul>

# Datenschutzrechtliche Anforderungen

(ein Auszug)

## Grundlagen des Datenschutzes

### **Erlaubnisvorbehalt**

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses **Gesetz** oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene **eingewilligt** hat. § 4 BDSG, §§ 28 ff BDSG

## Welche Pflichten ergeben sich aus dem Bundesdatenschutzgesetz? (ein Auszug)



- Datenvermeidung und Datensparsamkeit § 3a
- Meldepflichten § 4d
- Verpflichtung der Mitarbeiter auf das Datengeheimnis § 5
- Bestellung eines Datenschutzbeauftragten (ab meist 9 Mitarbeitern mit EDV-Arbeitsplätzen § 4f, soweit keine besonderen personenbezogenen Daten vorliegen)
- Unterstützung des Datenschutzbeauftragten bei seinen Aufgaben § 4g
- Auskunfts-, Löschungs-, Sperrungspflichten §§ 19 ff
- Spezielle Pflichten der Auftragsdatenverarbeitung § 11

## Wie müssen Daten nach BDSG geschützt werden?



### Die 8 Gebote des Datenschutzes §9 BDSG i.V.m. Anlage

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungsgebot

Personaldaten



Kundendaten

## Wo finden Sie Hilfe?



- Bestellung eines Datenschutzbeauftragten sowie seine Pflichten  
<http://www.bsi.de/gshb/baustein-datenschutz/dokumente/b01005.pdf>
- Verfahrensverzeichnis  
<http://www.bitkom.org/de/publikationen/38336.aspx>
- Spezielle Pflichten der Auftragsdatenverarbeitung § 11  
<http://www.bitkom.org/de/publikationen/38336.aspx>
- Übermittlung personenbezogener Daten - Inland, EU-Länder, Drittländer  
<http://www.bitkom.org/de/publikationen/38336.aspx>
- Datenschuttschulung der IHK-Akademie  
<http://akademie.muenchen.ihk.de/akademie/base/inhalte/startseite.html>



## Anforderungen aus dem Telekommunikationsrecht (ein kleiner Auszug)

## Regelungen im TKG: Private Mailnutzung



Durch die geduldete private Nutzung der Internetdienste (WWW / MAIL) in einem Firmennetz fällt dieses in den Anwendungsbereich des Fernmeldegeheimnisses. (§ 88ff TKG)



### Folge:

Jede Änderung des Inhalts einer Nachricht, Vorenthalten (Spamschutz) oder administrativer Einblick (Umleitung durch Administrator, ungeregelte Vertretung etc.) kann zu einer Strafbarkeit nach § 206 STGB führen. Daher sollte der Umgang mit der privaten Nutzung dringend geregelt werden.

**Wird die Privatnutzung der Dienste Mail und WWW im Unternehmen nicht ausdrücklich verboten, ist eine Einwilligung (schriftlich) für die notwendigen administrativen unternehmerischen Tätigkeiten durch die Benutzer notwendig, soweit dieser die Dienste privat nutzen möchte.**

## Wo finden Sie Hilfe im Internet?



- **Leitfaden zur privaten Nutzung von E-Mail und Internet**  
<http://www.bitkom.org/de/publikationen/38336.aspx>

## Anforderungen aus den handelsrechtlichen und steuerrechtlichen Regelungen

### Regelung zur Archivierung

**Faustregel:**

Alle Daten des Rechnungswesens (**steuerlich relevante Daten**), die einmal beim Steuerpflichtigen auf einem maschinell verwertbaren Datenträger gespeichert waren, sind auch in dieser Form vorzuhalten, damit sie durch die Finanzbehörde maschinell ausgewertet werden können.

„Steuerlich relevant“ sind Daten immer dann, wenn sie für die Besteuerung des Steuerpflichtigen von Bedeutung sein können. Eine (elektronisch übersandte) E-Mail stellt ein **originär** digitales Dokument dar, das für den Datenzugriff im Originalformat maschinell auswertbar vorgehalten werden muss.  
(„FAQ“ des BMF, Stand 2007)

## Wie müssen die Daten archiviert werden?



### Revisionsicherheit

Anforderungen an die elektronischen Archivierungssysteme, die in Deutschland den Anforderungen des Handelsgesetzbuches (§§ 239, 257 HGB), der Abgabenordnung (§§ 146, 147 AO), den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) und weiteren steuerrechtlichen und handelsrechtlichen Vorgaben entsprechen müssen:

Ordnungsmäßigkeit	Dokumentation des Verfahrens
Vollständigkeit	Sicherung vor Verlust
Sicherheit des Gesamtverfahrens	Nutzung nur durch Berechtigte
Einhaltung der Aufbewahrungsfristen	Schutz vor Veränderung und Verfälschung
Nachvollziehbarkeit	Prüfbarkeit

## Organisatorische Steuerungsaufgaben



Ab einer bestimmten Unternehmensgröße muss sich die Geschäftsleitung über die Organisation ihrer

- strategischen Aufgaben
- konzeptionellen Aufgaben und
- operativen Aufgaben

Gedanken machen.

## Organisatorische Steuerungsaufgaben



### **Strategische Aufgaben**

1. Sicherstellung einer bedarfs- und rechtskonformen IT-Nutzung
2. Bestellung eines betrieblichen Datenschutzbeauftragten

### **Konzeptionelle Aufgaben**

1. Einführung / Aktualisierung des Sicherheitskonzepts
2. Regelungen beim Zugang von externen Dritten
3. Professionelle Beschaffung von IT-Systemen und Durchführung von IT-Projekten
4. Sicherung von Vertraulichkeit und Geheimhaltung

## Organisatorische Steuerungsaufgaben



### **Operative Aufgaben**

1. Ordnungsgemäße Abbildung der wirtschaftlichen Verhältnisse des Unternehmens in der Buchführung
2. Datenschutzrechtliche Konformität sicherstellen
3. Einsatz von SPAM- und Viren-Filtern abwägen
4. Regelung für die Nutzung von E-Mail und Internet am Arbeitsplatz
5. Verhinderung von Schädigung Dritter durch firmeneigene IT, insbesondere virenfreier Daten-/Datenträgeraustausch
6. Durchführung regelmäßiger Backups
7. Verwendung lizenzierter Software

## Wo finden Sie Hilfe im Internet?



• [http://www.bitkom.org/files/documents/BITKOM\\_Leitfaden\\_Matrix\\_der\\_Haftungsrisiken-V1.1f.pdf](http://www.bitkom.org/files/documents/BITKOM_Leitfaden_Matrix_der_Haftungsrisiken-V1.1f.pdf)

### Leitfaden Matrix der Haftungsrisiken der BITKOM

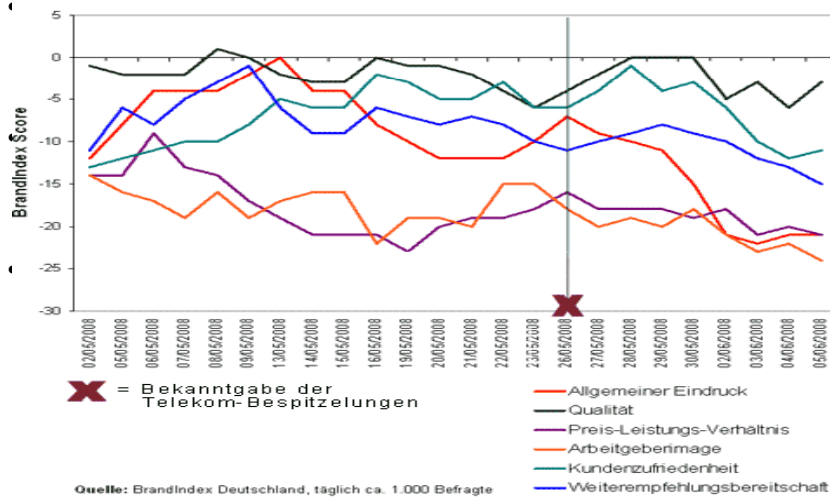
#### 2.1 Strategische Aufgaben

Nr.	Pflicht bzw. Regelungs-/ Handlungsbedarf	Verantwortlichen		Persönliche Haftung ggü.	Rechtsgrundlagen der Pflicht bzw. des Regelungs-/ Handlungsbedarfs	Potentielle Schäden und sonstige Nachteile für das Unternehmen bei Pflichtverletzung bzw. Nichtregulierung	Ansprüche Dritter (z.B. Kunden, Betroffene)	Anmerkungen sowie ausgewählte Entscheidungen
		Verantwortl. Unternehmen	Verantwortl. Einzelne					
1.	Sicherstellung eines bedarfs- und rechtskonformen IT-Nutzung				<ul style="list-style-type: none"> <li>Gesellschaftsrecht § 91 II AktG § 43 GmbHG</li> <li>(KonTraG)</li> <li>Gesellschaftsrecht § 116 AktG</li> <li>(KonTraG)</li> </ul>	<ul style="list-style-type: none"> <li>Unternehmensverluste durch Ausfall der Systeme</li> <li>Insolvenz</li> <li>Verunsicherung der Unternehmenskredite</li> <li>OgU Verlust von Versicherungsschutz für das Unternehmen</li> <li>Imageschaden nach Verlust von personenbezogenen Daten aufgrund von Sicherheitslücken</li> </ul>	<ul style="list-style-type: none"> <li>Schadenersatz</li> </ul>	<ul style="list-style-type: none"> <li>Siehe Erläuterungen in der Einleitung zu Kapitel 2</li> <li>Bietet ein Unternehmen über seinen Internetauftritt auch seine Produkte oder Dienstleistungen an, muss es verlässliche gesetzliche Pflichten beachten. Verstöße sind sanktionsbewehrt, zu diesem Themenkomplex siehe BITKOM-Prüfungsausschuss „Zweckbindungsgeschäft“ (Juni/Juli, März 2008)</li> <li>Der Aufsichtsrat hat zu kontrollieren, ob der Vorstand alle erforderlichen Maßnahmen im Rahmen des Risikomanagements getroffen hat. Führt er diese Kontrolle unzureichend aus und treten erhebliche Schäden, insbesondere Insolvenz, ein, haftet auch der Aufsichtsrat persönlich</li> <li>Haftung nur bei mangelnder Kontrolle (BöGH, NJW 1997, 4840 (Odermann))</li> </ul>
2.	Bestellung eines betrieblichen Datensicherheitsbeauftragten				<ul style="list-style-type: none"> <li>Datenschutzrecht § 41, I und II BDSG</li> </ul>	<ul style="list-style-type: none"> <li>Bußgeld bis zu 25.000 EUR</li> </ul>		<ul style="list-style-type: none"> <li>Eine Bestellung ist unverzüglich erforderlich wenn vier oder mehr Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beauftragt sind.</li> <li>Die Bestellung sollte dabei schriftlich erfolgen.</li> </ul>

## Lohnen sich die Investitionen?



### Imagedimensionen der Deutschen Telekom



Vielen Dank



## Kontakt Daten:

### Systemhaus

Klaus Foitzick  
Geschäftsführer

net integration  
Informationsmanagement GmbH

Potdamer Straße 3  
80802 München

Tel: +49 89 381 980  
Fax: +49 89 381 98 – 150  
Web: [www.netintegration.de](http://www.netintegration.de)  
E-Mail: [foitzick@netintegration.de](mailto:foitzick@netintegration.de)

### Rechenzentrum

Klaus Foitzick  
Geschäftsführer

Global Access  
Internet Services GmbH

Potdamer Straße 3  
80802 München

Tel: +49 89 92 40 20  
Fax: +49 89 92 40 2-150  
Web: [www.global.de](http://www.global.de)  
E-Mail: [foitzick@global.de](mailto:foitzick@global.de)

ISO 9001 und 27001 zertifiziert