

## Technische und organisatorische Maßnahmen

Wenn die Erhebung zulässig ist, müssen für die Speicherung und Verarbeitung weitere Anforderungen erfüllt werden:

=> Technische und organisatorischen Maßnahmen nach § 9 BDSG

=> Die 8 Gebote (Anhang zu § 9 BDSG)

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

## Zutrittskontrolle

- Sicherheitsschlösser mit Schlüsselregelung
- verschlossene Türen bei Abwesenheit
- Fenstersicherung (Erdgeschoss)
- Festlegung von Sicherheitsbereichen
- Zutrittsberechtigungsregelung
- Ausweisleser
- Protokollierung der Zu- und Abgänge
- Zutrittsregelungen für betriebsfremde Personen
- Empfang
- Codeschloss

# Zugangskontrolle

- Tastatursicherung durch Schloss
- Identifizierung und Authentifizierung
- Begrenzung der Fehlversuche
- Protokollierung
- Systemverwalterbefugnisse / -protokollierung
- Dunkelschaltung des Bildschirms mit Passwortschutz
- Firewall

# Zugriffskontrolle

- Berechtigungskonzept
- Identifizierung und Authentifizierung
- Verschlüsselung
- Aufbewahrung in verschließbaren Schränken – „Data Safes“
- gesonderte Aufbewahrung der Sicherungsdisketten

## Weitergabekontrolle

- Kennzeichnung der Datenträger
- Verschlüsselung von Daten auf Datenträgern
- Bestandsverzeichnis und Bestandskontrolle der Datenträger
- Festlegung der zur Abgabe von Datenträgern berechtigten Personen
- Festlegung des Empfängerkreises
- Regelungen für den Transport von Datenträgern
- Kryptographische Verschlüsselung der übertragenen Daten
- Fernwartungskonzept

# Eingabekontrolle

- Identifizierung und Authentifizierung
- Protokollierung aller Eingaben / Veränderungen

# Auftragskontrolle

- Schriftliche Festlegung der Weisungen / Vertrag
- Kontrolle der Einhaltung beim Auftragnehmer

# Verfügbarkeitskontrolle

- Betriebsbereitschaft
- Notfallkonzept
- Notfall-Rechenzentrum
- Unterbrechungsfreie Stromversorgung (USV)
- Brandmelder
- Datensicherung
- Zusätzliche Sicherungskopien mit Lagerung an besonders geschützten Orten



## Trennungsgebot

d.h. gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Gewährleistung der Zweckbindung)

Bei der Volkszählung 1987: strenges Abschottungsgebot  
BDSG 2001: Physische oder logische Trennung

# Rechtlicher Rahmen der Software-Entwicklung

- 1 Betriebsverfassungsgesetz (BetrVG) vom 23.7.2001
- 2 Datenschutzgesetz (BDSG vom 23.5.2001)
- 3 Tele- und Mediendienste - Rechtsgrundlagen**
- 4 Arbeitsschutzgesetz (ArbSchG vom 27.9.1996)
- 5 Bildschirmarbeitsverordnung (BildscharbV vom 4.12.96)
- 6 Normen (DIN, EN, ISO), Richtlinien (VDI)

# Telekommunikationsdienst oder Tele- bzw. Mediendienst



## TK- oder Teledienst

TKG gilt für Telekom-  
munikations-Dienstlei-  
stungen, d.h. das  
gewerbliche Angebot  
von Telekommunikation  
einschließlich des Ange-  
bots von Übertragungs-  
wegen für Dritte

## TK- oder Teledienst

Teledienste im Sinne von Absatz 1 sind insbesondere

1. Angebote im Bereich der Individualkommunikation (z.B. Telebanking, Datenaustausch),
2. Angebote zur Information oder Kommunikation, soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht  
(Datendienste, zum Beispiel Verkehrs-, Wetter-, Umwelt- und Börsendaten, Verbreitung von Informationen über Waren und Dienstleistungsangebote),
3. Angebote zur Nutzung des Internets oder weiterer Netze,
4. Angebote zur Nutzung von Telespielen,
5. Angebote von Waren und Dienstleistungen in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit (§ 2 Teledienste Gesetz TDG)

# Tele- oder Mediendienst

## Teledienste

elektronische Informations- und Kommunikationsdienste, die für eine individuelle Nutzung bestimmt sind.

Beispiele:

- Access Provider
- Electronic Banking
- Datenbankabruf (redaktionelle Gestaltung)
- Warenbestellungen
- Fahrplanauskünfte

## Mediendienste

elektronische Verteildienste und solche, bei denen die redaktionelle Gestaltung zur Meinungsbildung im Vordergrund steht. Sie richten sich an die Allgemeinheit.

Beispiele:

- Zeitungen / Zeitschriften
- redaktionell bearbeitete Newsletter  
z.B. Angebote von Reiseunternehmen  
mit Informationen zur Geschichte und Politik eines Landes
- Pressemitteilungen online

# Rechtlicher Rahmen der Software-Entwicklung

- 1 Betriebsverfassungsgesetz (BetrVG) vom 23.7.2001
- 2 Datenschutzgesetz (BDSG vom 23.5.2001)
- 3 Tele- und Mediendienste - Rechtsgrundlagen
- 4 Arbeitsschutzgesetz (ArbSchG vom 27.9.1996)**
- 5 Bildschirmarbeitsverordnung (BildscharbV vom 4.12.96)**
- 6 Normen (DIN, EN, ISO), Richtlinien (VDI)**

## **Arbeitsschutzgesetz vom 27.9.1996**

### **§ 5 Beurteilung der Arbeitsbedingungen**

Arbeitgeber muss ermitteln, welche Schutzmaßnahmen notwendig sind

### **§ 6 Dokumentation**

Maßnahmen und ihre Überprüfung müssen dokumentiert werden

### **§ 11 Arbeitsmedizinische Vorsorge**

Arbeitgeber muss auf Wunsch arbeitsmedizinische Untersuchung veranlassen

### **§ 12 Unterweisung**

Arbeitgeber muss über Sicherheit und Gesundheitsschutz unterweisen



# **Bildschirmarbeitsverordnung vom 4.12.1996**

## **§ 2 Begriffsbestimmungen**

was ist ein Bildschirm? was ist ein  
Bildschirmarbeitsplatz?

## **§ 3 Beurteilung der Arbeitsbedingungen**

Sicherheits- und Gesundheitsbedingungen insbesondere  
hinsichtlich einer möglichen Gefährdung des Sehvermögens  
sowie körperlicher Probleme und psychischer Belastungen  
sind zu ermitteln und zu beurteilen.

## **§ 4 Anforderungen an die Gestaltung (Anhang)**

# Bildschirmarbeitsverordnung vom 4.12.1996

## § 5 Täglicher Arbeitsablauf

Bildschirmarbeit ist durch andere Tätigkeiten oder Pausen zu unterbrechen

## § 6 Untersuchung der Augen und des Sehvermögens vor Antritt, danach regelmäßig, bei Auftritt von Sehbeschwerden

# **DIN EN ISO 9241 Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten**

## *Teil Titel*

- 1 Allgemeine Einführung  
DIN EN ISO (2/02)
- 2 Anforderungen an die Arbeitsaufgaben - Leitsätze  
DIN EN ISO (6/93)
- 3 Anforderungen an visuelle Anzeigen  
DIN EN ISO (8/93)
- 4 Anforderungen an die Tastatur  
DIN EN ISO (1/99)
- 5 Anforderungen an Arbeitsplatzgestaltung und  
DIN EN ISO (8/99) Körperhaltung

# **DIN EN ISO 9241 Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten**

*Teil Titel*

6 Leitsätze für die Arbeitsumgebung  
DIN EN ISO (3/01)

7 Anforderungen an visuelle Anzeigen bez. Reflexionen  
DIN EN ISO (12/98)

8 Anforderungen an Farbdarstellungen  
DIN EN ISO (4/98)

9 Anforderungen an Eingabemittel, ausgen. Tastaturen  
DIN EN ISO (3/02)

# **DIN EN ISO 9241 Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten**

*Teil Titel*

10 Grundsätze der Dialoggestaltung  
DIN EN ISO (7/96)

11 Anforderungen an die Gebrauchstauglichkeit - Leitsätze  
DIN EN ISO (1/99)

12 Informationsdarstellung  
DIN EN ISO (8/00)

13 Benutzerführung  
DIN EN ISO (8/00)

# **DIN EN ISO 9241 Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten**

*Teil Titel*

14 Dialogführung mittels Menüs  
DIN EN ISO (12/00)

15 Dialogführung mittels Kommandosprachen  
DIN EN ISO (8/99)

16 Dialogführung mittels direkter Manipulation  
DIN EN ISO (3/00)

17 Dialogführung mittels Bildschirmformularen  
DIN EN ISO (4/00)

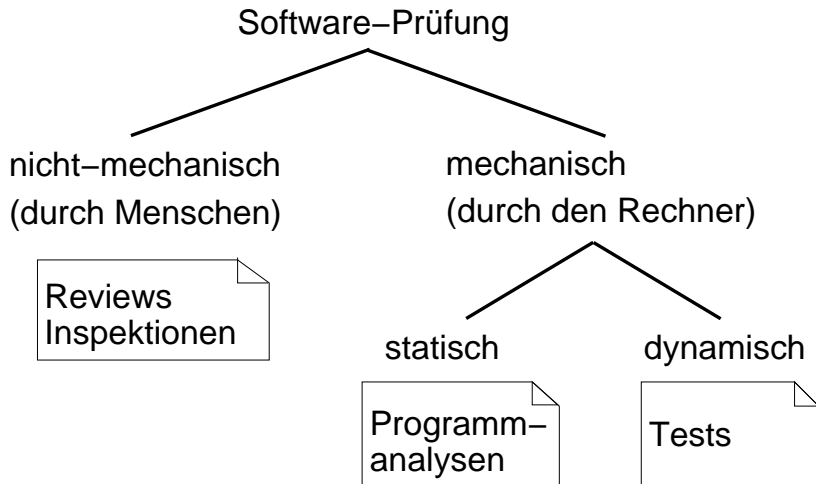
## 1 Reviews

- Software-Prüfungen
- Reviews
- Ablauf von Reviews
- Review-Regeln
- Review-Checklisten
- Review-Varianten
- Fallen und Gegenmittel

- Bedeutung der Prüfung für die Anforderungsspezifikation kennen
- Anforderungsspezifikation prüfen können



- Validierung: Are we doing the right thing?
  - Prüfung, ob das, was entwickelt wird, gewünscht ist.
- Verifikation: Are we doing the thing right?
  - Prüfung, ob der Entwicklungsschritt x richtig durchgeführt wurde.



| das Dokument ...                     | ... ist prüfbar durch |      |
|--------------------------------------|-----------------------|------|
|                                      | Inspektion            | Test |
| Lastenheft                           | X                     |      |
| Pflichtenheft                        | X                     |      |
| Systementwurf                        | X                     |      |
| Definition der Daten und Algorithmen | X                     |      |
| Benutzerhandbuch                     | X                     |      |
| Testdaten                            | X                     |      |
| Code                                 | X                     | X    |
| Anleitungen etc.                     | X                     |      |

## Prinzip

- Eine Software-Einheit wird (dezentral) von mehreren Gutachtern inspiziert;
- in einer gemeinsamen Sitzung werden die Mängel zusammengetragen und dokumentiert.

## Ziel

- Fehler zu finden,
- **nicht**, die Fehler auch zu beheben.
  - Fehlerbehebung ist ein separater Arbeitsschritt, den der Entwickler im Allgemeinen wieder ohne Mitwirkung Dritter durchführt.