UIMC®

DR. VOSSBEIN GMBH & CO KG

**U**nternehmens- und
**I**nformations- **M**anagement
**C**onsultants

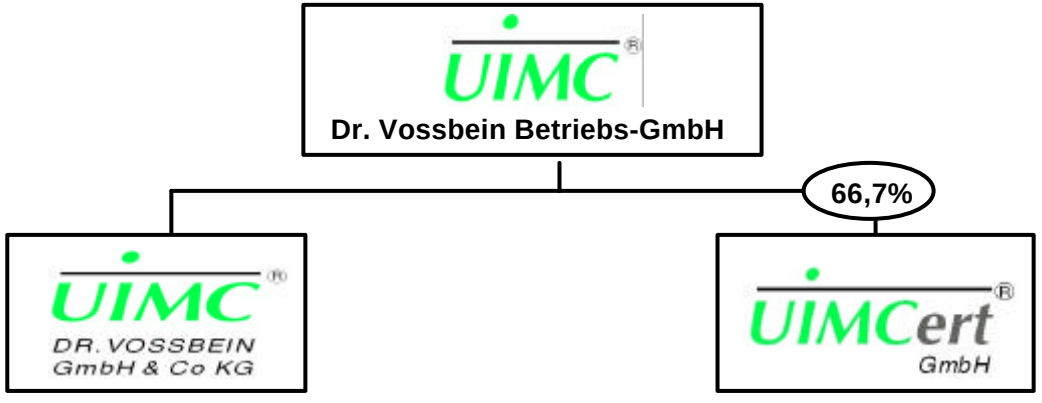
# Datenschutzmanagement und IT-Sicherheitsmanagement - zwei eng verbundene Aufgabengebiete

**Dr. Jörn Voßbein**

Internet: www.uimc.de

Nützenberger Str. 119
42115 Wuppertal

Telefon: (0) 202 - 265 74 - 0
Telefax: (0) 202 - 265 74 - 19
E-Mail: consultants@uimc.de




## Beratung

- Beratung in den Bereichen:
  - IV-Management und IV-Sicherheit
  - Datenschutz
  - Externe Datenschutzbeauftragung
  - Organisation und Unternehmensmanagement
- Durchführung von Seminaren
- Anwendung von Analyse- und Beratungstools

## Zertifizierung

- Durchführung von Auditierungsprozessen
- Erteilen von Zertifikaten auf der Basis von Auditierungsergebnissen
- Durchführung von Seminaren und Fortbildungsvorhaben
- Akkreditiert beim ULD (Datenschutz) und bei der TGA (BS7799-2: IT-Sicherheitsmanagement)

# Gesetzliche Bestimmungen zum Datenschutz

- **Bundesdatenschutzgesetz (BDSG)**
- Landesdatenschutzgesetze (z. B. LDSG NW)
- Bereichsspezifische DS-Gesetze: z. B.
  - Gesundheitsdatenschutzgesetz (GDSG NW)
  - Tele-Gesetze
- Sonstige Gesetze
  - Sozialgesetzbuch (SGB V)
  - § 203 StGB

u. a.

# Zielrichtung des BDSG

**§1 Zweck und Anwendungsbereich des Gesetzes**

(1) Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

# Wenn Gesetze in das Recht auf informationelle Selbstbestimmung des einzelnen eingreifen, gelten folgende Grundregeln:

- → Nur das erforderliche Minimum an Daten kann verlangt werden.
- → Die Daten dürfen nur für den Zweck verwendet werden, für den sie erhoben oder erfaßt wurden.
- → Auch bei der Organisation und dem Verfahren des Umgangs mit personenbezogenen Daten muss auf die Rechte des einzelnen Rücksicht genommen werden.

# Unterstützung der IT-Sicherheit durch den Datenschutz

# Zusammenhang Datenschutz und IT-Sicherheit

- Einhaltung der technisch-organisatorischen Maßnahmen
- Realisierung der Rechte der Betroffenen
- Realisierung der Datensparsamkeit und Datenvermeidung
- Revisionsfähigkeit von Systemen
- Beeinflussung der ordnungsgemäßen Einsatzumgebung
- Förderung und Einsatz von Privacy Enhancing Technology
- Ausarbeitung von datenschutzspezifischen Protection Profiles

# Aufgaben des Datenschutzbeauftragten

- **Überwachung bei der Führung von Übersichten**

- **Überwachung der ordnungsgemäßen Anwendung der DV-Programme**

- Beratende Mitwirkung bei der Auswahl der mit der Datenverarbeitung beschäftigten Personen

- **Bekanntgabe der Vorschriften an die mit der Datenverarbeitung beschäftigten Personen und deren Schulung**

# Aufgaben des Datenschutzbeauftragten

- Verpflichtung auf das Datengeheimnis im Sinne des § 5 BDSG

- **Beratung über technische und organisatorische Maßnahmen**

- **Erarbeitung und Pflege eines Datenschutz-Handbuches**

- Kontrolle und Wahrung der Rechte Betroffener

- Aus- und Weiterbildung des Datenschutzbeauftragten

- Erstellen eines Tätigkeitsberichtes

# Vorteilsfaktoren des Datenschutzes

- Gesetzliche Forderung
- „Weisungsfreiheit“
- Hierarchische Positionierung des DSB
- Öffentlichkeitswirksamkeit von DS-Problemen
- Möglichkeit der Stilllegung durch Aufsichtsbehörden
- Pflicht zur Vorabkontrolle

➔ DS als Argumentationshilfe

# Gesetzliche Folgen von Datenschutzverletzungen

§44 BDSG (Straftaten):

Datenverarbeitung gegen Entgelt oder um jemanden zu schädigen.
Freiheitsstrafe bis zu 2 Jahren oder Geldstrafe

§43 BDSG (Ordnungswidrigkeiten):

Datenverarbeitung entgegen den Vorschriften des BDSG.

Geldstrafe bis zu 25.000 Euro

# Das Datenschutz-Managementsystem

# Datenschutz-Managementsystem (Aufbauorganisatorische Lösungen zur Sicherstellung des Datenschutzes)

- Datenschutzbeauftragter und –koordinatoren
- Datenschutz-Managementteam
- Datenschutz am Arbeitsplatz (Mitarbeiterpflichten im Datenschutz)
- Kooperation mit Mitarbeitervertretungen
- Aufbauorientierte Datenschutzregelsysteme (Handbücher und Einzelregelungen)

# Organisatorische Hilfsmittel

## Das Datenschutzhandbuch

## Ziele des Datenschutzhandbuchs

Zusammenfassung der datenschutzbezogenen organisatorischen Regelungen-Einarbeitungshilfe für neue Mitarbeiter
Entscheidungsgrundlage und -hilfe in Datenschutzfragen

# Organisatorische Hilfsmittel

## Struktur des Datenschutzhandbuchs

## Inhalte

- Übergeordnete Regelungen
- aufbauorganisatorische Regelungen
- ablauforganisatorische Regelungen
- bereichsspezifische Regelungen
- formale Regelungen

Das Datenschutzhandbuch sollte möglichst Teil eines IT-Sicherheitshandbuches sein.

# Datenschutz-Prozessorganisation (Ablauforganisatorische Lösungen zur Sicherstellung des Datenschutzes)

- Ablauforientierte Datenschutzregelsysteme (Handbücher und Einzelregelungen)
- Datenschutzrelevante Organisationslösungen
- Verfahren zur Be- und Verarbeitung personenbezogener Daten

# Datenschutztechnische Lösungen und solche technischen, die den Datenschutz unterstützen

- Technisch-organisatorische Maßnahmen (TOMs)
- Einsatz von PET
- Physische und umgebungsbezogene Sicherheit

# Technische und organisatorische Maßnahmen zum Datenschutz

Anlage § 9 BDSG:

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die [...] innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

# Technische und organisatorische Maßnahmen zum Datenschutz

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

⇒

# Technische und organisatorische Maßnahmen zum Datenschutz

## -Zutrittskontrolle-

*Gesetzestext:*

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen , mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

*Anmerkungen:*

Damit ist der räumliche Zutritt gemeint. Z. B. der Zutritt zu einem Raum, in dem einige DV-Anlagen mit sensiblen personenbezogenen Daten stehen.

# Technische und organisatorische Maßnahmen zum Datenschutz

## -Zugangskontrolle-

*Gesetzestext:*

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

*Anmerkungen:*

Damit ist der Zugang zu den einzelnen DV-Anlagen selbst gemeint. Z. B. das Einloggen bzw. Eindringen in eine DV-Anlage.

# Technische und organisatorische Maßnahmen zum Datenschutz

## -Zugriffskontrolle-

*Gesetzestext:*

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungs-systems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

# Technische und organisatorische Maßnahmen zum Datenschutz

## -Weitergabekontrolle-

*Gesetzestext:*

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenüber-tragung vorgesehen ist.

# Technische und organisatorische Maßnahmen zum Datenschutz

## -Eingabekontrolle-

*Gesetzestext:*

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

# Technische und organisatorische Maßnahmen zum Datenschutz

## -Auftragskontrolle-

*Gesetzestext:*

Es ist zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

# Technische und organisatorische Maßnahmen zum Datenschutz

## -Verfügbarkeitskontrolle-

*Gesetzestext:*

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

*Anmerkungen:*

Schutz vor Wasserschäden, Blitzschlag oder Stromausfall

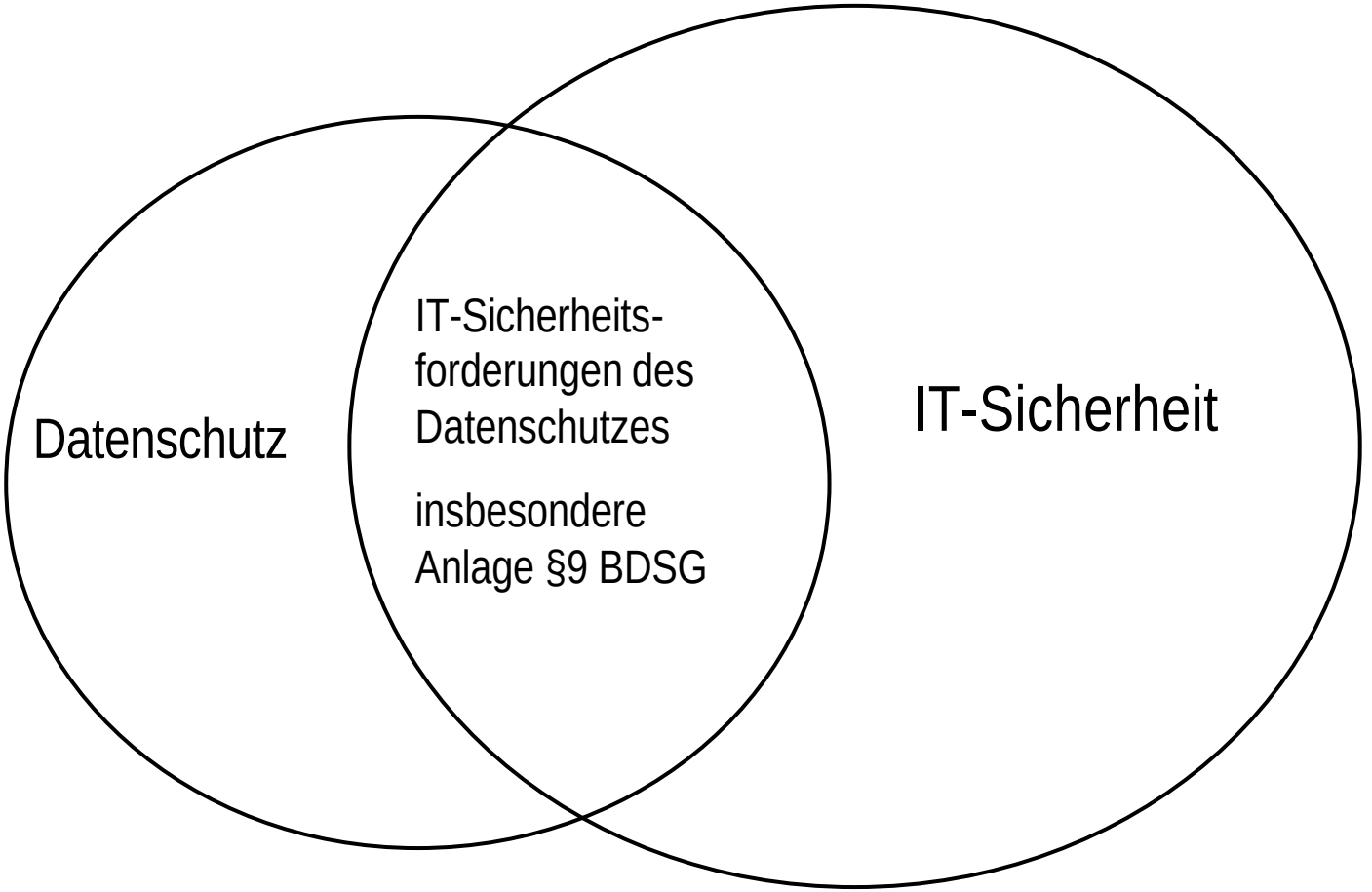
# Technische und organisatorische Maßnahmen zum Datenschutz

## -Trennungsgebot-

*Gesetzestext:*

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

# Möglichkeiten der Integration beider Managementsysteme


Datenschutz
IT-Sicherheits-
forderungen des
Datenschutzes
insbesondere
Anlage §9 BDSG
IT-Sicherheit

# BS 7799/ISO-IEC 17799

- Vorgänger: BS 7799:1995 im Gegensatz zur BS 7799:1999
- Anderer Name: Code of practice for Information security management (kurz: Code of practice, CoP)
- Anwendungsbereich: Organisationen mit und ohne Erwerbscharakter und Organisationen der öffentlichen Hand (Organisationsbegriff des BS 7799), in Industrie und Handel und in großen, mittleren und kleinen Organisationen

# BS 7799/ISO-IEC 17799

- Gültig: ab 15 Mai 1999
- Der BS 7799 besteht aus zwei Teilen
- Teil 1 (BS 7799-1:1999) Leitfaden zum Management von Informationssicherheit, ca. 95 Seiten
- Teil 2 (BS 7799-2:1999) Spezifikation für Managementsysteme für Informationssicherheit, ca. 25 Seiten

# BS 7799/ISO-IEC 17799

- 1. Teil, der direkt als Grundlage des Tools dient. In diesem werden **Empfehlungen** ausgesprochen.

- Im 2. Teil sind die **Anforderungen** für die Schaffung, Implementierung und Dokumentation von Managementsystemen für Informationssicherheit festgelegt.

- 109 übergeordnete Sicherheitsanforderungen und 600 bis 800 verschiedene Maßnahmenpakete zu ihrer Abdeckung.

- Kapitel 1 und 2: *Anwendungsbereich* und *Begriffe und Definitionen* in dem BS 7799

# Beschränkung des BS 7799/ISO-IEC 17799

- Nicht alle Maßnahmen sind für jede Situation relevant
- Keine Berücksichtigung von Beschränkungen aus spezifischen Gesichtspunkten heraus
- Möglichkeit der Ergänzung durch weitere Richtlinien
- BS 7799 kann als Grundlage für z. B. die Entwicklung einer Unternehmenspolitik herangezogen werden

# IT-Sicherheit unter BS 7799

## Der Umfang des IT-Sicherheits-Audit gem. BS 7799

- Sicherheitspolitik
- Organisation der Sicherheit
- Einstufung und Kontrolle der Werte
- Personelle Sicherheit
- Physische und umgebungsbezogene Sicherheit
- Management der Kommunikation und des Betriebs
- Zugangskontrolle
- Systementwicklung und -wartung
- Management des kontinuierlichen Geschäftsbetriebs
- Einhaltung der Verpflichtungen

## Kapitel 3: Sicherheitspolitik

3.1.Informationssicherheitspolitik

## Kapitel 3: Datenschutzpolitik

3.1 Datenschutzpolitik

## Kapitel 4: Organisation der Sicherheit

4.1 Infrastruktur der Informationssicherheit

4.2 Sicherheit bei dem Zugang durch Fremdunternehmen

4.3 Outsourcing

## Kapitel 4: Organisation des Datenschutzes

4.1 Infrastruktur des Datenschutzes

4.2 Datenschutz bei dem Zugang durch Fremd-unternehmen

4.3 Outsourcing

## Kapitel 5: Einstufung und Kontrolle der Werte

5.1 Zurechenbarkeit für Werte

5.2 Einstufung von Informationen

## Kapitel 5: Einstufung und Kontrolle der Werte von personenbezogenen Daten

5.1 Zurechenbarkeit für Werte

5.2 Einstufung von personenbezogenen Daten

## Kapitel 6: Personelle Sicherheit

6.1 Sicherheit bei der Stellenbeschreibung und bei der Bereitstellung von Ressourcen

6.2 Benutzerschulung

6.3 Verhalten bei Sicherheitsvorfällen und Störungen

## Kapitel 6: Personeller Datenschutz

6.1 Datenschutz bei der Stellenbeschreibung und bei der Bereitstellung von Ressourcen

6.2 Benutzerschulung

6.3 Verhalten bei Datenschutzvorfällen und Störungen

## Kapitel 7: Physische und umgebungsbezogene Sicherheit

7.1 Sicherheitszonen

7.2 Sicherheit der Geräte

7.3 Allgemeine Maßnahmen

## Kapitel 7: Physische und umgebungsbezogene Sicherheit

7.1 Sicherheitszonen

7.2 Sicherheit der Geräte

7.3 Allgemeine Maßnahmen

## Kapitel 8: Management der Kommunikation und des Betriebs

8.1 Betriebsverfahren und -verantwortlichkeiten

8.2 Systemplanung und -abnahme

8.3 Schutz vor bösartiger Software

8.4 Interne Organisation (housekeeping)

## Kapitel 8: Management der Kommunikation und des Betriebs

8.1 Betriebsverfahren und -verantwortlichkeiten

8.2 Systemplanung und -abnahme

8.3 Schutz vor bösartiger Software

8.4 Haushaltsorganisation

## Kapitel 8: Management der Kommunikation und des Betriebs

8.5 Netzwerkmanagement

8.6 Umgang mit und Sicherheit von Datenträgern

8.7 Austausch von Informationen und Software

## Kapitel 8: Management der Kommunikation und des Betriebs

8.5 Netzwerkmanagement

8.6 Umgang mit Datenschutz bei Datenträgern

8.7 Austausch von Informationen und Software

## Kapitel 9: Zugangskontrolle

9.1 Geschäftsanforderungen an die Zugangskontrolle

9.2 Verwaltung der Zugriffsrechte der Benutzer

9.3 Verantwortung der Benutzer

9.4 Netzzugriffskontrolle

## Kapitel 9: Zugangskontrolle

9.1 Geschäftsanforderungen an die Zugriffskontrolle

9.2 Verwaltung der Zugriffsrechte der Benutzer

9.3 Verantwortung der Benutzer

9.4 Netzzugriffskontrolle

## Kapitel 9: Zugangskontrolle

9.5 Kontrolle des Betriebssystemzugriffs

9.6 Zugriffskontrolle für Anwendungen

## Kapitel 9: Zugangskontrolle

9.5 Kontrolle des Betriebssystemzugriffs

9.6 Zugriffskontrolle für Anwendungen

## Kapitel 9: Zugangskontrolle

9.7 Überwachung des Systemzugriffs und der Systembenutzung

9.8 Mobile Computing und Telearbeit

## Kapitel 9: Zugangskontrolle

9.7 Überwachung des Systemzugriffs und der Systembenutzung

9.8 Mobile Computing und Telearbeit

9.10 Protokollauswertung

## Kapitel 10: Systementwicklung und -wartung

10.1 Sicherheitsanforderungen an Systeme

10.2 Sicherheit in Anwendungssystemen

10.3 Kryptographische Maßnahmen

## Kapitel 10: Systementwicklung und -wartung

10.1 Datenschutzanforderungen an Systeme

10.2 Datenschutz in Anwendungssystemen

10.3 Kryptographische Maßnahmen

## Kapitel 10: Systementwicklung und -wartung

10.4 Sicherheit von Systemdateien

10.5 Sicherheit bei Entwicklungs- und Supportprozessen

## Kapitel 10: Systementwicklung und -wartung

10.4 Datenschutz bei Systemdateien

10.5 Datenschutz bei Entwicklungs- und Supportprozessen

10.6 Qualitäts- und Revisionsanforderungen

## Kapitel 11: Management des kontinuierlichen Geschäftsbetriebs

11.1 Aspekte zur Aufrechterhaltung des Geschäftsbetriebs

## Kapitel 11: Management des kontinuierlichen Geschäftsbetriebs

11.1 Aspekte zur Aufrechterhaltung des Geschäftsbetriebs

## Kapitel 12: Einhaltung der Verpflichtungen

12.1 Einhaltung gesetzlicher Verpflichtungen

12.2 Überprüfungen der Sicherheitspolitik und der Einhaltung technischer Normen

## Kapitel 12: Einhaltung der Verpflichtungen

12.1 Einhaltung gesetzlicher Verpflichtungen

12.2 Überprüfung der Sicherheitspolitik und der Einhaltung technischer Normen

12.3 Überlegungen zum Systemaudit

# Zertifizierung des Datenschutzmanagementsystems des Heilig-Geist-Hospitals Bingen gemäß BS 7799-2

Als Zertifizierungsgrundlage dient der Standard BS7799-2, der international als Standard zur Zertifizierung des Managements der Sicherheit von Informations-Systemen sowie Informations-Teil-Systemen, wie dem Datenschutz-Management-System, genutzt wird.

Gegenstand der Auditierung und Zertifizierung ist das Heilig-Geist-Hospital Bingen als Verantwortliche Datenverarbeitende Stelle im Hinblick auf die Ordnungsmäßigkeit des Datenschutz-Management-Systems gemäß der Datenschutzgesetzgebung.