

Peter Münch

# **Technisch-organisatorischer Datenschutz**

- Leitfaden für Praktiker -

4. überarbeitete und erweiterte Auflage 2010

**DATAKONTEXT**

# Inhaltsverzeichnis

<b>Vorwort</b> .....	11
<b>1. Ziele des technisch-organisatorischen Datenschutzes</b> .....	15
1.1 Einführung.....	15
1.2 Der wachsende Stellenwert der Datensicherheit in der Informationsgesellschaft.....	19
1.3 Störungen im Datenverarbeitungsprozess.....	33
1.3.1 Begriffliche Einordnung.....	33
1.3.2 Fahrlässig herbeigeführte Störungen.....	36
1.3.3 Vorsätzliche Störungen (Computerkriminalität).....	38
1.3.4 Technische Störungen und Störungen durch „höhere Gewalt“.....	54
1.3.5 Zusammenfassende Aussagen.....	58
1.4 Datensicherheit im Spiegel der Gesetzgebung.....	61
1.5 Grundanforderungen an vertrauenswürdige IT-Systeme..	85
1.6 Bewertung und Zertifizierung vertrauenswürdiger IT-Systeme.....	97
<b>2. Datensicherheitsmanagement im Kontext mit datenschutzrechtlichen Anforderungen</b> .....	109
2.1 Risikomanagement.....	109
2.1.1 Gesetzlicher Hintergrund und Eigeninteresse.....	109
2.1.2 Angemessenheitsprinzip.....	117
2.1.3 Datensicherheitsstrategie.....	121
2.1.4 Risikoanalyse.....	125
2.2 Datensicherheitskonzeption und-richtlinien.....	151
2.3 Dokumentationssicherheit.....	169
2.4 Maßnahmen zur Erhaltung und Verbesserung des Datensicherheitsniveaus.....	173
2.5 Revision der Datensicherheit.....	179
2.6 Restrisikoabdeckung durch Versicherung.....	189
2.7 Kosten und Nutzen der Datensicherheit.....	193
2.8 Organisatorische Regelungen.....	201
2.8.1 Personelle Aspekte.....	201
2.8.2 Aufbauorganisation.....	213
2.8.3 Ablauforganisation.....	215
2.8.4 Organisatorische Aspekte beim Einsatz neuer Software ..	221
2.8.5 Das Problem der Auswahl geeigneter und angemessener Sicherheitsmechanismen.....	233

<b>3.</b>	<b>Schlüsseltechnologien in der Informationsverarbeitung mit Datensicherheitsbezug</b> .....	241
3.1	Internet/Intranet/Extranet .....	241
3.2	Cloud Computing .....	255
3.3	Internet-Telefonie: Voiceover IP (VoIP) .....	259
3.4	Verschlüsselungstechniken .....	263
3.5	Elektronische Signatur .....	279
3.6	Mobile Funknetze .....	291
3.7	Chipkartentechnologie .....	297
3.8	Radio Frequenz Identifikation (RFID) .....	303
3.9	Biometrische Verfahren .....	307
3.10	Videotechnik .....	315
<b>4.</b>	<b>Verfahren zum technisch-organisatorischen Datenschutz</b> .....	323
4.1	Technische und organisatorische Maßnahmen zur Zutrittskontrolle .....	323
4.2	Technische und organisatorische Maßnahmen zur Zugangskontrolle .....	331
4.3	Technische und organisatorische Maßnahmen zur Zugriffskontrolle .....	345
4.3.1	Zugriffskontrolle im standardisierten Sinne .....	346
4.3.2	Zugriffskontrolle bei und nach der Speicherung .....	353
4.4	Technische und organisatorische Maßnahmen zur Weitergabekontrolle .....	361
4.4.1	Weitergabekontrolle bei elektronischer Übertragung .....	362
4.4.2	Weitergabekontrolle beim Datenträgertransport .....	377
4.4.3	Weitergabekontrolle bei der Übermittlung personenbezogener Daten .....	380
4.5	Technische und organisatorische Maßnahmen zur Eingabekontrolle .....	383
4.6	Technische und organisatorische Maßnahmen zur Auftragskontrolle .....	391
4.7	Technische und organisatorische Maßnahmen zur Verfügbarkeitskontrolle .....	395
4.7.1	Objektsicherungsmaßnahmen .....	397
4.7.2	Sichere Versorgung .....	400
4.7.3	Datenbestandssicherung .....	405
4.7.4	Hardware- und Softwaresicherung .....	420
4.8	Technische und organisatorische Maßnahmen zur Durchsetzung des Trennungsgebotes .....	425
4.9	Schutz gegen Schaden stiftende Software .....	429

<b>Glossar</b> .....	449
<b>Literaturverzeichnis</b> .....	473
<b>Namens- und Stichwortverzeichnis</b> .....	491

Verzeichnis von ergänzenden Checklisten, Mustern,  
Hinweisen und Gesetzen

<b>Dateiname</b>	<b>Inhalt</b>
	<b>1. Checklisten</b>
CHE01 .doc	Checkliste zur Prüfung der technischen und organisatorischen Maßnahmen gemäß Anlage zu § 9 Satz 1 BDSG (Beispiel: AB Mittelfranken/Bayern/Hamburg)
CHE02.doc	Checkliste zur Gewährleistung der Verfügbarkeit
CHE03.doc	Checkliste zur Gewährleistung der Vertraulichkeit
CHE04.doc	Checkliste zur Gewährleistung der Ordnungsmäßigkeit
CHE05.doc	Checkliste Zugangskontrolle
CHE06.doc	Checkliste: Zugriffskontrolle bei SAP R/3
CHE07.doc	Checkliste: Auswahl von Zutrittskontrollereinrichtungen
CHE08.doc	Checkliste zur Auswahl einer Firewall
CHE09.doc	Orientierungshilfe und Checkliste zur Protokollierung
CHE10.doc	Checkliste zur Vorabkontrolle gemäß § 4d (5, 6) BDSG
CHE11 .doc	Orientierungshilfe und Checkliste Outsourcing
CHE12.doc	Checkliste Auftragsdatenverarbeitung
CHE13.doc	Checkliste zur Einrichtung von rechnergestützten Heimarbeitsplätzen
CHE14.doc	Checkliste zur Beurteilung von Bildschirmarbeitsplätzen
CHE15.doc	Checkliste: Telemediendienste
CHE16.doc	Checkliste: Datensicherheit für Entscheider
CHE17.doc	Checkliste für IT-Sicherheitsüberprüfungen durch externe Berater
CHE18.doc	Checkliste: Sicherheitsbewusstsein
CHE19.doc	Checkliste: Ausscheiden von Mitarbeitern
CHE20.doc	Checkliste: Schutz gegen Innentäter
CHE21 .doc	Checkliste: Computer forensische Untersuchung

## Inhaltsverzeichnis

### 2. Muster

MUS01.doc	Muster: Sicherheitskonzeption eines Unternehmens
MUS02.doc	Muster: Datensicherheitsordnung eines Unternehmens
MUS03.doc	Muster: Richtlinie für den ordnungsgemäßen Einsatz aller Betriebsarten von APC
MUS04.doc	Muster: Richtlinien für die Arbeit an PC-Arbeitsplätzen
MUS05.doc	Muster: Katastrophen- und Wiederanlaufplan
MUS06.doc	Muster: Richtlinie zur Nutzung mobiler Datenträger
MUS07.doc	Muster: Sicherheitsrichtlinie zur Smartcard-Anwendung
MUS08.doc	Muster: Nutzung privilegierter netzgebundener APC
MUS09.doc	Mustermerkblatt: Sicherer Umgang mit APC
MUS10.doc	Muster: Merkblatt zur Verwendung von Benutzererkennung und Passwort
MUS11 .doc	Muster: Richtlinie zur Zugriffskontrolle (Berechtigungen)
MUS12.doc	Muster: Richtlinie für Telearbeiter/innen
MUS13.doc	Muster: Merkblatt Datenschutz und Datensicherheit bei tragbaren PCs
MUS14.doc	Muster: Merkblatt Datenschutz und Datensicherheit bei Telefax
MUS15.doc	Muster: Merkblatt für eine sichere E-Mail-Nutzung
MUS16.doc	Muster: Ordnung zur Vernichtung von Datenträgern
MUS17.doc	Muster: Benutzerordnung Internet
MUS18.doc	Muster: Postordnung eines Unternehmens
MUS19.doc	Muster: Verpflichtung auf das Fernmeldegeheimnis
MUS20.doc	Muster einer betrieblichen Datenschutzordnung
MUS21 .doc	Muster: Verfahrensübersicht nach §§ 4e, 4g (2) BDSG
MUS22.doc	Musterdienstvereinbarung: Internet am Arbeitsplatz
MUS23.doc	Muster: Betriebsvereinbarung E-Mail und Internet (unter Verbot privater Nutzung)
MUS24.doc	Muster einer Betriebsvereinbarung Videokameraeinsatz
MUS25.doc	Muster: Betriebsvereinbarung zum Einsatz von Videotechnik am Arbeitsplatz
MUS26.doc	Muster: Betriebsvereinbarung ISDN-TK-Anlage
MUS27.doc	Muster: Verfahrensanweisung ISDN-TK-Anlage
MUS28.doc	Muster: Aufgabenbeschreibung eines IT-Sicherheitsbeauftragten
MUS29.doc	Muster: Allumfassende Verpflichtungserklärung
MUS30.doc	Muster: Vereinbarung zur Überlassung Transportabler

**Muster (Fortsetzung)**

- MUS31.doc Muster: Freigabeprotokoll
- MUS32.doc Muster: Vertragsinhalt Auftragsdatenverarbeitung (ADV)- 1. Version (GDD)
- MUS33.doc Mustervertrag Auftragsdatenverarbeitung (ADV) - 2. Version (RP Darmstadt)
- MUS34.doc Mustervertrag Auftragsdatenverarbeitung (ADV) - 3. Version (BITKOM)
- MUS35.doc Mustervertrag zur Übernahme und Vernichtung von Datenträgern
- MUS36.doc Mustervertrag Fernwartung
- MUS37.doc Muster: Hinweis für Vertrag abschließende Fachabteilungen zur ADV
- MUS38.doc Muster: Vorgabe von IT-Sicherheitsanforderungen bei Auftragsdatenverarbeitung
- MUS39.doc Muster: Prüfformular für Auftragnehmer gem. § 11 BDSG
- MUS40.doc Muster: Vertrag über automatisierte Abrufverfahren gemäß § 10 BDSG

**3. Hinweise**

- HIN01 .pdf Inhaltliche Anforderungen an eine Verfahrensübersicht nach den Vorstellungen einer Aufsichtsbehörde
- HIN02.pdf Empfehlungen zur Verwendung privater Heim-PC für dienstliche Zwecke
- HIN03.pdf Empfehlungen für den Betrieb einer Firewall
- HIN04.doc Hinweise zur Gestaltung einer Richtlinie „Zutrittskontrolle“
- HIN05.pdf Hinweise zur Vorbereitung und Durchführung von Mitarbeiterschulungen
- HIN06.pdf Tools für Datenschutzbeauftragte
- HIN07.pdf Hinweise zum sicheren Umgang mit öffentlichen Schlüsseln
- HIN08.pdf Datenschutzgerechte Behandlung von defekten Festplatten
- HIN09.pdf BW: Hinweise zum Datenschutz Nr. 31 (Datenschutzbeauftragte)
- HIN10.pdf BW: Hinweise zum Datenschutz Nr. 33 (Wartung; Betriebsrat; § 5)
- HIN11 .pdf BW: Hinweise zum Datenschutz Nr. 40 (Video; internationaler Datenverkehr)

### Hinweise (Fortsetzung)

HIN12.pdf	Hinweise zur datenschutzgerechten Datenträgervernichtung nach DIN 32757
HIN13.pdf	Orientierungshilfe Datensicherheit bei USB-Geräten
HIN14.pdf	Wie wird Interoperabilität von PKI gewährleistet?
HIN15.pdf	Hinweise zur Auswahl einer USV-Anlage
HIN16.pdf	Hinweise zur sicheren Nutzung von VoIP
HIN17.pdf	Hinweis: Sicherheitsstandard für Kreditkartendaten
HIN18.pdf	Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz
HIN19.pdf	Arbeitspapier zu Datenschutzaspekten digitaler Zertifikate und PKI

### 4. Verschiedenes

VER01.doc	Der DES-Algorithmus: Ein Übungsbeispiel
VER02.doc	Selbsttest: Kryptoanalyse eines Buchstabencodes
VER03.pdf	Sammlung relevanter Gerichtsentscheide
VER04.pdf	Arbeitshilfe: IT-Sicherheitskriterien im Vergleich
VER05.pdf	IT-Sicherheitsprodukte (Produkt/Hersteller)
VER06.pdf	Störungen und daraus resultierende Schäden (Kosten)
VER07.pdf	Datenschutzgerechte Datenträgerentsorgung
VER08.pdf	Multiple-Choice-Fragen zur Selbstkontrolle
VER09.pdf	Lösungen zu VER08.pdf

### 5. Gesetze

GES01 .pdf	Bundesdatenschutzgesetz (BDSG) - nichtamtliche Volltextversion
GES02.pdf	Telekommunikationsgesetz (TKG), Auszug
GES03.pdf	Signaturgesetz (SigG)
GES04.pdf	Telemediengesetz (TMG)
GES05.pdf	9. Staatsvertrag für Rundfunk und Telemedien (Ausz.)
GES06.pdf	Zugangskontrolldiensteschutzgesetz (ZKDSG)
GES07.pdf	Telekommunikationsüberwachungsverordnung (TKÜV)
GES08.pdf	Kommentar zum § 7 des neuen Gesetzes gegen den unlauteren Wettbewerb (UWG)
GES09.pdf	Änderung des § 203 Strafgesetzbuch
GES10.pdf	Änderung Strafgesetzbuch (Computerkriminalität) mit Kommentar und Hinweisen
GES11 .pdf	Auszug aus dem Urheberrechtsgesetz