

C. Bake, B. Blobel, P. Münch (Hrsg.)

Handbuch Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen

Spezielle Probleme des Datenschutzes und der Datensicherheit im Bereich des Gesundheits- und Sozialwesens (GSW) in Deutschland

3. überarbeitete und erweiterte Auflage 2009

DATAKONTEXT

Handbuch Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen

**Spezielle Probleme des Datenschutzes und der Datensicherheit im Bereich des
Gesundheits- und Sozialwesens (GSW) in Deutschland**

Teil I: Datenschutz

inhaltlich erarbeitet und redaktionell bearbeitet von

Christian Bake

v. Bodelschwingsche Anstalten Bethel, Bielefeld

Holger Koch

Fachberater für Datenschutz und Datensicherheit, Mixdorf

David Koeppel

Datenschutzbeauftragter der Vivantes GmbH, Berlin

Dr. Peter Münch

Datenschutzberater und -beauftragter, Vorstandsmitglied der GDD, Hamm

Barbara Tietze

Diakonisches Werk der Ev.-Luth. Landeskirche Sachsens e.V., Radebeul

Inhalt

Einleitung	11
1.1 Problemstellung	11
1.2 Wozu soll diese Schrift dienen?	12
Zur Problemstellung Datenschutz	15
2.1 Grundsätzliches	15
2.2 Datenschutzgesetzgebung	16
2.3 Einordnung des Geltungsbereiches	18
Der Datenschutzbeauftragte	19
3.1 Bestellung	19
3.2 Rechte und Pflichten	20
3.3 Aufgaben	20
Datenschutz und besonderes Berufsgeheimnis	23
4.1 Einleitung	23
- 4.1.1 Berufsgeheimnis und Anzeigepflichten	23
4.1.2 Zeugnisverweigerungsrecht und Beschlagnahmeyerbpt.	24
4.1.3 Entbindung von der Schweigepflicht	25
4.1.4 Anordnung einer Untersuchung	26
4.1.5 Internationale Kooperation	26
4.2 Zulässigkeit der Datenverarbeitung	26
4.2.1 Dokumentationspflicht	26
4.2.2 Verbot mit Erlaubnisvorbehalt	27
4.2.3 Zweckbindung	27
4.2.4 Erforderlichkeit	27
4.2.5 Datenvermeidung und Datensparsamkeit	28
4.3 Pflichten der verantwortlichen Stelle	28
4.3.1 Erheben	29
Erheben bei Leistungserbringern	30
Erheben bei Leistungsträgern	34
4.3.2 Speichern	34
Speichern bei Leistungserbringern	35
Speichern bei Leistungsträgern	38
4.3.3 Verändern	38
4.3.4 Übermitteln und Offenbaren	38
Übermitteln durch Leistungserbringer	40
Übermitteln durch Leistungsträger	49
4.3.5 Sperren	49
Sperren bei Leistungserbringern	50
Sperren bei Leistungsträgern	51

4.3.6	Löschen.	51
	Löschen bei Leistungserbringern.	52
	Löschen bei Leistungsträgern.	54
4.3.7	Nutzen.	54
	Nutzen bei Leistungserbringern.	55
	Nutzen durch Leistungsträger.	56
4.4	Rechte der Betroffenen.	56
4.4.1	Grundsätze.	56
4.4.2	Rechte des Betroffenen.	57
4.4.3	Benachrichtigung.	59
4.4.4	Auskunft und Akteneinsicht.	59
4.4.5	Berichtigung, Sperrung und Löschung.	61
4.4.6	Widerspruchsrecht.	61
4.4.7	Schadensersatz.	62
4.4.8	Anrufung eines Datenschutzbeauftragten.	62
4.4.9-	Klage - Strafrechtlicher Schutz des Betroffenen.	62
4.5	Datenschutzorganisation.	63
4.5.1	Datenschutzordnung.	63
4.5.2	Verfahrensübersicht.	64
4.5.3	Auftragsdatenverarbeitung und Outsourcing.	65
4.5.4	Akten und Archive.	65
	Allgemeine Anforderungen.	65
	Besonderheiten elektronischer Archive.	66
	Formanforderungen an Dokumente.	68
4.5.5	Automatisierte Informationssysteme.	70
	Allgemeines.	70
	Datenarten.	70
	Die Struktur automatisierter Informationssysteme.	72
	Folgerungen für automatisierte Informationssysteme.	73
4.5.6	Web-Auftritt nach TMG und Datenschutzerklärung.	73
4.5.7	Telekommunikation.	76
	Private Patientenkommunikation.	76
	Private Mitarbeiterkommunikation.	77
	Dienstliche Kommunikation.	77
4.5.8	Videoüberwachung und Videomonitoring.	79
	Videoüberwachung im Gesundheits- und Sozialwesen.	79
	Überwachung öffentlich zugänglicher Räume.	79
	Videoüberwachung in nichtöffentlich zugänglichen Räumen.	81
	Medizinisch indizierte Videoüberwachung (Monitoring).	81
	Videoüberwachung am Arbeitsplatz.	82
4.5.9	Dienstleistungen durch Fremdfirmen.	82
	Dienstleistungen durch externe Leistungserbringer.	83
	Mikroverfilmung und Datenspeicherung durch Dienstleister.	83
	Externe Patientenarchive.	84

	Datenträgervernichtung	84
	DV-Dienstleistungen und DV-Wartung im Krankenhaus	85
	Fernwartung der Krankenhaussoftware	85
	Telekommunikation	85
4.5.10	Datenschutzaudit	86
	Gesetzlicher Rahmen	86
	Zielstellungen und Verfahren	86
	Konzeptionelle Überlegungen und Wege	88
4.5.11	Datenschutzrelevante betriebliche Regelungen	89
4.6	Spezielle Regelungen	90
4.6.1	Kirchlicher Datenschutz	90
	Gesetzliche Regelungen	90
	Historie des kirchlichen Datenschutzes	90
	Vergleich des DSG-EKD mit dem BDSG	91
	Verordnungen im Bereich der evangelischen Kirche	93
	Bereichsspezifische Regelung für Patientendaten	93
	Datenschutzregelungen der Katholischen Kirche	94
4.6.2	Sozialdatenschutz	94
	Besonderheiten beim Sozialdatenschutz	95
	Übermittlungsbefugnisse für Sozialdaten	96
	Datenschutz in der Krankenpflege	97
	Datenschutz in Alten- und Pflegeheimen	98
	Sozialdatenschutz in der Kinder- und Jugendhilfe	98
4.7	Versorgungsformen	99
4.7.1	Integrierte Versorgungsformen	99
	Grundlegendes	99
	Einverständnis und Rechte des Patienten	100
	Informationssysteme für die integrierte Versorgung	101
	Medizinische Versorgungszentren (MVZ)	101
	Strukturierte Behandlungsprogramme	102
	Kooperationen	103
	Integrierte Versorgung mit Beteiligung von Pflegeeinrichtungen	104
	Portale	104
4.7.2	Prävention und Vorsorgesysteme	106
4.7.3	Personalisierte Versorgung	107
4.8	Medizinische Forschung	108
4.8.1	Allgemeines und gesetzliche Grundlagen	108
4.8.2	Klinische Studien	110
4.9	Qualitätsmanagement in der Gesundheitseinrichtung	111
4.9.1	Qualitätsmanagement als einrichtungsinterne Aufgabe	111
4.9.2	Verpflichtung zur Qualitätssicherung in der Krankenversorgung	112
4.9.3	Verpflichtung zur Qualitätssicherung in der Pflegeversicherung	112
5	Technische und organisatorische Maßnahmen	115
5.1	Umsetzung technisch-organisatorischer Maßnahmen	115

5.1.1	Grundsätzliches	.115
5.1.2	Zutrittskontrolle	.118
5.1.3-	Zugangskontrolle	.118
5.1.4	Zugriffskontrolle	.119
5.1.5	Weitergabekontrolle	.120
5.1.6	Eingabekontrolle	.120
5.1.7	Auftragskontrolle	.121
5.1.8	Verfügbarkeitskontrolle	.121
5.1.9	Trennungsgebot	.122
5.1.10	Vorabkontrolle	.123
5.2	Notfall- und Katastrophenmanagement im Krankenhaus	.124
5.2.1	Notfallmanagement	.125
5.2.2	Katastrophenmanagement	.126
5.2.3	Katastrophenplan	.127
5.2.4	Nach einer Katastrophe	.127
6	Literatur und Referenzen zum Datenschutz	c129
		.131
	Mitwirkende an diesem Buch	281

Handbuch Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen

**Spezielle Probleme des Datenschutzes und der Datensicherheit im
Bereich des Gesundheits- und Sozialwesens (GSW)
in Deutschland**

Teil II: Datensicherheit

PD Dr. Bernd Blobel

Universitätsklinikum Regensburg, eHealth Competence Center

Inhalt

Einführung	145
1.1 Veränderungen in Struktur und Funktion des GSW.	146
1.2 Rechtliche Basisprinzipien für die Verarbeitung	147
1.3 Kommunikation: Gefahren, Bedrohungen, Schutzobjekte.	148
1.4 Modellierung von sicheren Informationssystemen.	149
1.5 Verantwortlichkeiten und organisatorische Maßnahmen.	151
1.6 Empfohlene Sicherheitsinfrastruktur.	152
1.7 Ausblick	153
Sicherheits-Policy.	155
2.1 Das Domänenmodell.	155
2.2 Systemkomponenten.	156
2.2.1 Kommunikationspartner.	157
2.2.2 Kommunikationsinhalte.	157
2.2.3 Kommunikationsinfrastruktur.	158
2.2.4 Kommunikationsdienste	158
Sicherheitsmodelle.	159
3.1 Das allgemeine Sicherheitsmodell.	159
3.2 Sicherheits-Schichtenmodell.	160
Allgemeine Sicherheitsdienste.	163
4.1 Sicherheitsservices.	163
4.1.1 Integrität	163
4.1.2 Verbindlichkeit	163
4.1.3 Vertraulichkeit	163
4.1.4 Verfügbarkeit	163
4.2 Sicherheitsmechanismen.	164
4.2.1 Ciphertext	164
4.2.2 Verschlüsselung	164
4.2.3 Hashing	164
4.2.4 Digitale Signatur.	164
4.3 Algorithmen und Protokolle.	165
4.3.1 Symmetrische Verfahren.	166
DES.	166
3DES.	167
IDEA.	167
AES und Rijndael.	167
4.3.2 Asymmetrische Verfahren.	168
RSA	168
ElGamal.	168
DSA und DSS.	168

Kommunikationssicherheit	171
5.1 Sicherheitsdienste	171
5.1.1 Identifikation und Authentifikation	171
5.1.2 ID-Management und Biometrie	171
5.1.3 Zugriffskontrolle	172
5.1.4 Notariatsfunktionen	172
5.2 Normalisierung von Daten	173
5.3 Lösungskonzepte	173
5.3.1 Kommunikation über sichere Kanäle	174
5.3.2 Kommunikation sicherer Objekte	174
Anwendungssicherheit	177
6.1 , Autorisierung	177
6.2 Zugriffskontrolle	177
6.2.1 Geschlossene Systeme	178
6.2.2 Offene Systeme	178
6.2.3 Mandatory Access Control	178
6.2.4 Discretionary Access Control	179
6.2.5 Management von Zugriffskontroll-Konzepten	180
Rollenbasierte Zugriffskontroll-Konzepte	180
Regelbasierte Zugriffskontroll-Konzepte	181
Klassifikation von Informationen	182
6.2.6 Zugriffsmatrizen	182
6.2.7 Rollen- und Regelkonzepte im Gesundheitswesen	183
Strukturelle bzw. organisatorische Rollen	183
Funktionsbezogene Rollen	183
6.3 Notariats-Funktionen	184
6.4 Audit	184
6.5 Key Backup	184
6.5.1 Key Recovery	184
6.5.2 Key Escrow	185
6.5.3 Probleme der Key-Backup-Verfahren	185
Sicherheitsbezogene Basis-Szenarien	187
7.1 Nutzer-Management	187
7.2 Nutzer-Authentifizierung	188
7.3 Konsens des informierten Patienten	188
7.4 Audit	189
7.5 Initialisierung der Kommunikation	189
7.6 Informationsanforderung	190
7.7 Zugriffskontrolle	190
7.8 Bereitstellung der Information	191
7.9 Übertragung der Information	191

8	Sicherheitsinfrastrukturen	193
8.1	Trusted Third Party	193
8.2	Public Key Infrastructure	194
8.3	Sichemeitstoken	194
9	Spezielle Architekturen	195
9.1	Zentralrechner	195
9.2	Dezentrale Architekturen	196
9.2.1	Client-Server-Architekturen	196
9.2.2	Netzwerkzentrierte Architekturen	196
9.2.3	Netzwerkdienste	196
9.2.4	Netzwerkprotokolle	196
	Internet	197
	Intranet	197
9.3	Drahtlose Übertragung (WLAN)	197
9.4	Gesundheitskarte (nach BMGS)	199
9.4.1	Einführung	200
9.4.2	Konzeption der Gesundheitskarte	200
9.4.3	Gesundheitskarte und Datenschutzaspekte	201
9.5	Elektronischer Arztausweis	202
9.6	Rahmenarchitektur und Infrastruktur	203
10	Intrusion Protection und Firewalls	205
10.1	Was ist eine Firewall?	205
10.2	Anforderungen an eine Firewall	205
10.3	Leistungsbereich einer Firewall	205
10.4	Firewall-Konzepte	206
10.4.1	Statische und dynamische Paketfilter auf IP-Ebene	206
10.4.2	Gateways auf der Anwendungsebene	207
10.4.3	Circuit Level Gateways	208
10.4.4	Stateful Inspection	208
10.5	Firewall-Architekturen	209
10.5.1	Screening Router	209
10.5.2	Dual/Three/Multi Homed Host	210
10.5.3	Screened Host	211
10.5.4	Screened Subnet	211
10.5.5	Mischtechniken	212
10.6	Demilitarisierte Zone (DMZ)	212
10.7	Empfehlung für ein Firewall-Konzept	212
10.8	Neuere Elemente einer Firewall	213
10.9	Wartung einer Firewall	213
10.10	Entscheidungsreihenfolge bei Firewall-Projekten	214
10.11	Personal bzw. Desktop-Firewalls	214

10.12	Zukünftige, Entwicklungen	215
10.13	Intrusion Protection	215
10.14	Weiterführende Informationen	216
11	Viren und andere Schaden stiftende Software	217
11.1	Was ist ein Computervirus	217
11.2	Aufbau eines Computervirus	217
11.2.1	Reproduktionsteil	217
11.2.2	Erkennungsteil	217
11.2.3	Schadensteil	218
11.2.4	Bedingungsteil	218
11.2.5	Tarnungsteil	218
11.3	Grundtypen von Computerviren	218
11.3.1	Boot-Viren	218
11.3.2	File-Viren	218
11.3.3	„Stealth“ oder „Tarnkappen“-Viren	219
11.3.4	Makro-Viren	219
11.4	Grundtypen von Schaden stiftender Software	219
11.4.1	Wurm	219
11.4.2	Hintertür (Backdoor)	220
11.4.3	Trojanische Pferde	220
11.5	Häufigkeit des Auftretens von Schäden	220
11.6	Hauptangriffsziele von Viren	222
11.7	Vorbeugende Maßnahmen	222
11.8	Abwehrmaßnahmen	223
11.8.1	Virensuchprogramme	223
11.8.2	Prüfsummen (CRC) - Programm	223
11.9	Gesetzliche Aspekte	223
11.10	Weiterführende Informationen	224
12	Anwendungen	225
12.1	Informations- und Dokumentationssysteme	225
12.1.1	Elektronische Gesundheitsakte	225
12.1.2	De-Identifikation von Gesundheitsinformationen	226
12.2	Archive	227
12.3	Register	228
12.4	Wartung bzw. Fernwartung	229
13	Literatur und Referenzen zur Datensicherheit	231
13.1	Literaturverzeichnis	231
13.2	Weitergehende Referenzen im WWW	236
13.3	Standards zu Datenschutz und Datensicherheit	237
13.3.1	Architekturstandards	237
13.3.2	Modellierungs- und Methodologiestandards	237

13.3.3	Kommunikationsstandards	239
13.3.4	Infrastrukturstandards	242
13.3.5	Privacy-Standards	242
13.3.6	Safety-Standards	243
13.3.7	Token-Standards	244
13.3.8	Qualitätssicherungsstandards	244
13.3.9	Policy-Standards	245
13.3.10	Terminologie- und Ontologiestandards	245
13.3.11	ID-Managementstandards	246
14	Anlagen zu Datenschutz und Datensicherheit auf der CD	247
14.1	Hauptverzeichnis	247
14.2	Teil A - Verzeichnis der Anlagen, auf die im Text des Handbuchs verwiesen wurde	247
14.3	Teil B - Verzeichnis der GQD-Mitteilungen	250
14.4	Teil C - Verzeichnis der Gerichtsentscheide	251
14.5	Teil D - Verzeichnis der Veröffentlichungen zu speziellen Themen	256
14.6	Teil E - Verzeichnis der BSI-Kurzinformationen	257
14.7	Literaturempfehlungen	259
14.8	Abkürzungsverzeichnis	269
	Index	277
	Mitwirkende an diesem Buch	281