Inhaltsverzeichnis

1 Grundsätzliches zum Schutz von Daten 13

1.1 Der Begriff „Daten“ 15
1.2 Der Begriff „Algorithmus“ 16
1.3 Der Begriff „Information“ 17
1.4 Zusammenspiel von „Daten“, „Algorithmen“ und „Informationen“ 17

2 Der Gesetzesdschungel im Bereich des Schutzes von Daten 21

2.1 Das Medizinprodukterecht 22
2.2 Das Patientengeheimnis/die ärztliche Schweigepflicht 23
2.3 Das Datenschutzrecht 23
2.4 Das Wettbewerbsrecht 24
2.5 Das Zivilrecht 24
2.6 Das Strafrecht 25
2.7 Das Straf-/Zivilprozessrecht 26
2.8 Das öffentliche Recht 26
2.9 Das Steuerrecht/das Handelsrecht 27
2.10 Das Sozialrecht 27

3 Die DSGVO als Revolution oder Evolution?! – Richtlinie vs. Verordnung und Auswirkungen auf das nationale Recht 29

3.1 Die EU-Datenschutzrichtlinie 29
3.2 Die DSGVO und das nationale Recht 31

4 Hauptakteure beim Datenschutz – Betroffener/Verantwortlicher 33

4.1 Betroffener 33
4.2 Verantwortlicher 34
4.2.1 Verantwortlicher/Geheimnisträger 35
4.2.2 Einzelpraxen 36
4.2.3 Gemeinschaftspraxen 36
4.2.4 Praxisgemeinschaften 37

4.2.5 Medizinische Versorgungszentren 38
4.2.6 Krankenhäuser 38
4.2.7 Belegärzte 39
4.2.8 Ermächtigte Krankenhausärzte 40
4.2.9 Betriebsärzte 40

5 Anwendungsbereich der DSGVO (Wann ist das Datenschutzrecht/die DSGVO zu beachten?) 43

5.1 Einführung 43
5.2 Sachliche Anwendbarkeit der DSGVO 44
5.2.1 Personenbezug der Daten 44
5.2.2 Verarbeitung 45
5.2.3 Automatisierte Datenverarbeitung 45
5.2.4 Datenverarbeitung in einem „Dateisystem“ 46
5.2.5 Ausnahmen bei der Anwendung 46
5.2.6 Schlussfolgerung 46

6 Relevante Begrifflichkeiten 49

6.1 Personenbezogene Daten 50
6.2 Datenverarbeitung 54
6.3 Pseudonymisierung 56
6.4 Dateisystem 60

7 Allgemeine Prinzipien beim Schutz von Patientendaten 63

7.1 Allgemeines 63
7.2 Rechtmäßigkeit 67
7.3 Treu und Glauben/Fairness 68
7.4 Transparenz 70
7.5 Zweckbindung 71
7.6 Datenminimierung 73
7.7 Speicherbegrenzung 74
7.8 Richtigkeit 75
7.9 Integrität und Vertraulichkeit 76
7.10 Rechenschaftspflicht 77

8 Legitimationen zur Verarbeitung von Patientendaten in einer Arztpraxis 79

8.1 Allgemeines 79
8.2 Wichtige Rechtsgrundlagen für die Verarbeitung von Patientendaten 80
8.2.1 Verarbeitung zum Schutz lebenswichtiger Interessen bei Einwilligungsunfähigkeit des Patienten 81
8.2.2 Verarbeitung zur Geltendmachung/Verteidigung von Rechtsansprüchen 81
8.2.3 Verarbeitung zu Behandlungszwecken u.V.m. 83
8.2.4 Verarbeitung aufgrund des Interesses der öffentlichen Gesundheit 86
8.2.5 Verarbeitung zu Forschungszwecken 87
8.2.6 Verarbeitung von genetischen Daten 88
8.3 Einwilligung des Patienten 89
8.3.1 Freiwilligkeit/Kopplungsverbot 90
8.3.2 Bestimmtheit der Einwilligung 91
8.3.3 Informiertheit des Betroffenen 92
8.3.4 Unmissverständlichkeit der Einwilligungserteilung 94
8.3.5 Form der Einwilligungserklärung 94
8.3.6 Widerrufbarkeit der Einwilligung 95
8.3.7 Zwingende Notwendigkeit einer Einwilligung durch Gesetz 96
8.3.8 Einwilligung von Minderjährigen 97

9 Rechte der Patienten 101

9.1 Allgemeines 101
9.2 Transparenzpflicht 103
9.3 Informationspflicht bei Direkterhebung 108
9.4 Informationspflicht bei Dritterhebung 113
9.5 Auskunftsrecht des Patienten 115
9.6 Erfüllung des Auskunftsanspruchs in der Praxis 119
9.7 Einsichtsrecht 120
9.8 Berichtigung 123

9.9 Aufbewahrung und Löschung von Daten 126
9.10 Recht auf Einschränkung der Verarbeitung/Sperrung 132
9.11 Mitteilungspflicht über Berichtigung, Löschung oder Sperrung 135
9.12 Recht auf Datenübertragbarkeit 137

10 Anforderungen an die Erhebung von Patientendaten/ die Behandlungsdokumentation 141

11 Verarbeitungsverzeichnis 147

11.1 Allgemeines 147
11.2 Der Wortlaut des Art. 30 und des Erwägungsgrunds 82 147
11.3 Zielsetzung/Zweck(e) des Verarbeitungsverzeichnisses 150
11.4 Datenverarbeitungstätigkeiten in einer Arztpraxis 152
11.5 Die Rechenschaftspflicht und das Verarbeitungsverzeichnis 155
11.6 Schriftlich oder digital? 156
11.7 Inhalt des Verarbeitungsverzeichnisses 158
11.7.1 Namen und Kontaktdaten 158
11.7.2 Bezeichnung und Kurzbeschreibung des Prozesses 159
11.7.3 Zwecke der Verarbeitung 160
11.7.4 Kategorien betroffener Personen und personenbezogener Daten 161
11.7.5 Kategorien von Empfängern 162
11.7.6 Übermittlungen in Drittländer 163
11.7.7 Speicherdauer 165
11.7.8 Technische und organisatorische Maßnahmen 166
11.8 Verpflichtung zur Erstellung des Verzeichnisses 167
11.9 Ausnahmen von der Verpflichtung zur Führung des Verarbeitungsverzeichnisses 170

12 Sicherheit der Datenverarbeitung – Risiko 173

12.1 Grundsätzliche Pflichten zur Einhaltung des Datenschutzes 174
12.1.1 „Risiken für Rechte und Freiheiten von natürlichen Personen“ 175
12.1.2 Rechte und Freiheiten natürlicher Personen 176

12.1.3 Begriff des Risikos ... 177
12.1.4 Risikobeurteilung ... 179
12.2 Sicherheit der Verarbeitung ... 191
12.2.1 Pseudonymisierung ... 196
12.2.2 Verschlüsselung ... 197
12.2.3 Die „klassischen" Ziele der Informationssicherheit ... 201
12.2.4 Maßnahmen zur Erfüllung der datenschutzrechtlichen Prinzipien ... 210
12.3 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ... 216

13 Verletzung des Schutzes von Daten/Meldepflichten ... 221

13.1 Meldepflicht an die Aufsichtsbehörde ... 223
13.2 Meldepflicht an den Betroffenen ... 225

14 Pflicht zur Vornahme einer Datenschutzfolgenabschätzung ... 229

14.1 Einführung in die Datenschutzfolgenabschätzung ... 229
14.2 Pflicht zur Durchführung ... 230
14.3 Verpflichteter zur DSFA = Der Verantwortliche ... 231
14.4 Verarbeitungsvorgang ... 232
14.5 Erforderlichkeit der Durchführung ... 233
14.6 Inhalt der DSFA und ihrer Dokumentation ... 234
14.7 Zeitpunkt der Durchführung einer DSFA ... 235
14.8 Konkrete Durchführung einer DSFA ... 236
14.9 Konsultation der Aufsichtsbehörde ... 239

15 Datenschutzbeauftragter – Pflicht zur Bestellung/Aufgaben etc. ... 241

15.1 Wann muss ein DSB bestellt werden? ... 241
15.2 Welche Anforderungen muss ein DSB erfüllen? ... 246
15.3 Welche Aufgaben muss ein DSB erfüllen? ... 249

16 Empfehlungen zur Umsetzung des Schutzes von Daten in der Praxis ... 251

16.1 Allgemeines zum technischen und organisatorischen Schutz von (Patienten-)Daten ... 251
16.2 Räumliche Ausgestaltung und Praxisorganisation ... 252

16.3 Sicherheitsvorkehrungen bei externer elektronischer Kommunikation ... 256
16.3.1 Pflichten bei der elektronischen Kommunikation ... 257
16.3.2 Übermittlung und Empfang via Fax ... 259
16.3.3 Übermittlung und Empfang via E-Mail ... 260
16.3.4 Einsatz mobiler Geräte wie Smartphones und Apps ... 261
16.4 Der „Praxisauftritt" im Netz ... 265

17 Verarbeitung von Daten bei Einschaltung Externer ... 273

17.1 Empfänger ... 275
17.2 Gemeinsam für die Verarbeitung Verantwortliche ... 276
17.2.1 Allgemeines zur gemeinsamen Verarbeitung ... 277
17.2.2 Gemeinsame Entscheidung über Zwecke und Mittel der Verarbeitung ... 280
17.2.3 Gemeinsame Vereinbarung/Vertrag ... 281
17.2.4 Haftung ... 284
17.2.5 Besondere Verpflichtungen gemeinsam Verantwortlicher ... 285
17.3 Auftragsverarbeiter/Auftragsverarbeitung ... 286
17.3.1 Typische Merkmale einer Auftragsverarbeitung ... 288
17.3.2 Problematik der Verwendung von vom Auftragsverarbeiter vorbereiteten Standardverträgen ... 292
17.3.3 Besondere Auswahl des Auftragsverarbeiters ... 294
17.3.4 Ärztliche Verschwiegenheitspflicht vs. Auftragsverarbeitung ... 296
17.3.5 Folgen bei Verstößen ... 297
17.3.6 Vertrag mit dem Auftragsverarbeiter (Inhalt) ... 297
17.4 Übermittlung an einen weiteren Verantwortlichen ... 325
17.5 Abgrenzungsfragen ... 326

18 Aufsichtsbehörden bei Berufsgeheimnisträgern und ihre Befugnisse ... 331

18.1 Befugnisse der Aufsichtsbehörde ... 332
18.2 Einschränkung ... 335

19 Verstöße gegen die DSGVO/den Schutz von Daten und drohende Sanktionen 341

19.1 Haftung und Recht auf Schadensersatz 343
19.2 Verhängung von (verhältnismäßigen) Bußgeldern 345
19.3 Sanktionen (Datenschutzstrafrecht) 349
19.4 Weitere Möglichkeiten/Maßnahmen, die bei Verstoß gegen die DSGVO drohen 351

20 Nützliche Internetadressen 353

Nachwort des Verfassers 355

Stichwortverzeichnis 358