Inhaltsverzeichnis

1 Einführung Datenschutz in der ärztlichen Praxis 1
Joachim Schütz

1.1 Grundzüge des Datenschutzrechts und rechtliche Rahmenbedingungen – 1
1.2 Begrifflichkeiten (Art. 4 DS-GVO, insbesondere Gesundheitsdaten, Verarbeitungsbegriff) – 2
1.2.1 Personenbezogene Daten – 2
1.2.2 Verarbeitung – 3
1.2.3 Einschränkung der Verarbeitung – 5
1.2.4 Pseudonymisierung – 5
1.2.5 Dateisystem – 5
1.2.6 Verantwortlicher – 6
1.2.7 Auftragsverarbeiter – 6
1.2.8 Empfänger – 7
1.2.9 Dritter – 8
1.2.10 Einwilligung – 9
1.3 Anliegen des Datenschutzes (Art. 1 DS-GVO, inklusive Grundrechtsschutz: Art. 7, 8 GRCh; Recht auf informationelle Selbstbestimmung) – 10
1.3.1 Art. 1 Abs. 1 DS-GVO – 10
1.3.2 Art. 1 Abs. 2 DS-GVO – Schutz von Grundrechten und Grundfreiheiten – 10
1.3.3 Art. 1 Abs. 3 DS-GVO – Grundsatz des freien Datenverkehrs – 11
1.4 Besonderheiten des Datenschutzes für Ärztinnen und Ärzte – 11
1.4.1 Gesundheitsdaten, Berufsgeheimnis und ärztliche Schweigepflicht – 11
1.4.2 Datenschutzrechtliche Kernregelungen – 12
1.4.3 Die Rolle der Aufsichtsbehörden – 12
1.5 Berufsgeheimnis und Schweigepflicht im Lichte des Datenschutzrechts – 13
1.6 Betroffenenrechte – Allgemeine Hinweise – 13

2 Anwendungsbereich der Datenschutzregelungen (DS-GVO/BDSG) 15
Bernd Halbe, Jan Ippach

2.1 Sachlicher und räumlicher Schutzbereich der DS-GVO (Art. 2 und 3 DS-GVO) – 15
2.1.1 Sachlicher Schutzbereich der DS-GVO – 15
2.1.2 Räumlicher Schutzbereich der DS-GVO – 16
2.2 Verhältnis der DS-GVO zu nationalen Datenschutzregelungen („Öffnungsklauseln") – 17
2.3 Arzt als Adressat der DS-GVO – 17
2.3.1 Arzt als Verantwortlicher nach Art. 4 Nr. 7 DS-GVO – 17
2.3.2 Arzt als Auftraggeber nach Art. 4 Nr. 8 DS-GVO – 18

Bibliografische Informationen
http://d-nb.info/1181226864

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

2.3.3 Merkposten: Gemeinsame Verarbeitung (Art. 26 DS-GVO) – 18
2.4 Verhältnis zur ärztlichen Schweigepflicht (§ 1 Abs. 2 Satz 3 BDSG – „Parallelität") – 19

3 Grundprinzipien der Datenverarbeitung 21
Carsten Dochow
3.1 Rechtmäßigkeitsprinzip – 21
3.2 Verarbeitung nach Treu und Glauben – 22
3.3 Verhältnismäßigkeitsgrundsatz – 23
3.4 Transparenzprinzip – 23
3.5 Beteiligung des Betroffenen – 25
3.6 Zweckbindungsgrundsatz – 25
3.7 Erforderlichkeit, Datenminimierung und Speicherbegrenzung – 26
3.8 Richtigkeit der Daten – 28
3.9 Technische und organisatorische Sicherungen – 29
3.10 Grundsatz der Verantwortlichkeit – 29
3.11 Rechenschaftspflicht – 30
3.12 Unabhängige Datenschutzkontrolle – 31

4 Rechtliche Grundlagen der Verarbeitung von Gesundheitsdaten 33
4.1 Grundsystematik und Regelungen für die Verarbeitung von Gesundheitsdaten im Überblick – 33
Carsten Dochow
4.1.1 Grundsystematik des Gesundheitsdatenschutzrechts – 33
4.1.2 Überblick zu den Erlaubnisgründen für die Verarbeitung von Gesundheitsdaten – 35
4.2 Allgemeine Rechtsgrundlagen für die Verarbeitung von Gesundheitsdaten – 38
Carsten Dochow
4.2.1 Verarbeitung im Bereich der Arbeitsmedizin, Gesundheitsvorsorge und ärztlichen Behandlung – 39
4.2.2 Verarbeitung zur Erfüllung von Pflichten aus dem Sozialrecht und Verwaltung von Systemen und Diensten im Gesundheitsbereich – 42
4.2.3 Verarbeitung zur Erfüllung spezieller Pflichten im öffentlichen Gesundheitsinteresse – 44
4.2.4 Verarbeitung im erheblichen öffentlichen Interesse – 45
4.2.5 Verarbeitung zum Schutz lebenswichtiger Interessen bei Einwilligungsunfähigkeit des Betroffenen – 46
4.2.6 Verarbeitung zur Wahrung von Rechtsansprüchen – 48
4.2.7 Verarbeitung zu anderen Zwecken (§ 24 BDSG) – 50
4.3 Bereichsspezifische Vorschriften – 51
Carsten Dochow
4.3.1 Arzneimittel (klinische Prüfungen) – 52
4.3.2 Bestattungswesen – 52
4.3.3 Betäubungsmittel – 52
4.3.4 Forschung – 53
4.3.5 Infektionsschutz – 53
4.3.6 Insolvenzverfahren – 54

4.3.7 Kinderschutz – 54
4.3.8 Krebsregister – 55
4.3.9 Medizinprodukte (klinische Prüfungen) – 55
4.3.10 Personenstandswesen – 55
4.3.11 Psychiatrie, Maßregelvollzug – 55
4.3.12 Statistik – 56
4.3.13 Strahlenschutz und Röntgen – 56
4.3.14 Transfusionswesen – 58
4.3.15 Unfallversicherung – 59
4.3.16 Vertragsarztrecht, gesetzliche Krankenversicherung – 59
4.4 Spezielle Rechtsgrundlagen im vertragsärztlichen Bereich – 60
Jürgen Schröder
4.4.1 Vertragsärztliche Abrechnung – 60
4.4.2 Qualitätssicherung und -prüfung – 60
4.4.3 Dokumentationssammlung Ärzte/Überweisungen – 61
4.4.4 Anfragen von Krankenkassen – 61
4.4.5 Behandlungsfehlerunterstützung – 62
4.4.6 Meldung von Krankheitsursachen und drittverursachten Schäden – 62
4.4.7 Versichertenstammdatenmanagement – 62
4.5 Einwilligung – 62
Carsten Dochow
4.5.1 Bedeutung und Kritik an der Rechtsfigur der Einwilligung – 63
4.5.2 Verhältnis zu gesetzlichen Grundlagen für die Datenverarbeitung – 64
4.5.3 Verhältnis zum Behandlungsvertrag – 66
4.5.4 Voraussetzungen einer wirksamen Einwilligung – 66
4.5.5 Fazit und Checkliste für die wirksame Einwilligung – 77
4.5.6 Muster Datenschutz-Einwilligungserklärung – 77
4.6 Zusammenfassung der Grundlagen für die Datenverarbeitung in der Arztpraxis – 79
Carsten Dochow

5 Auftragsverarbeitung – der Arzt als Verantwortlicher 81
Joachim Schütz
5.1 Allgemeines zur Auftragsverarbeitung – 81
5.2 Besonderheiten in der ärztlichen Praxis – 81
5.2.1 Sozialdatenschutz – 81
5.2.2 Schweigepflicht und Datenschutz – 82
5.2.3 Besonderheiten der Offenbarungsbefugnis bei der Auftragsdatenverarbeitung – Belehrungspflichten – 83
5.2.4 Datenschutzrechtliche Verpflichtung nach Art. 28 Abs. 3b DS-GVO – 83
5.3 Auftragsverarbeitung und Auftragsverarbeiter – 83
5.4 Die richtige Auswahl – 85
5.5 Vertragliche Regelungen – 85
5.5.1 Vertragsgegenstand (Art. 28 Abs. 3 Satz 1 DS-GVO) – 86
5.5.2 Weisungsgebundenheit (Art. 28 Abs. 3 Satz 2 Buchst. a DS-GVO) – 86

5.5.3 Vertraulichkeitsverpflichtung (Art. 28 Abs. 3 Satz 2 Buchst. b DS-GVO) – 86
5.5.4 Schutzmaßnahmen gemäß Art. 32 Abs. 3 Satz 2 Buchst. c DS-GVO – 86
5.5.5 Recht zur Begründung von Unterauftragsverhältnissen (Art. 28 Abs. 2, Abs. 3 Satz 2 Buchst. d DS-GVO) – 87
5.5.6 Gewährleistung der Betroffenenrechte (Art. 28 Abs. 3 Satz 2 Buchst. e DS-GVO) – 87
5.5.7 Unterstützung bei der Erfüllung der Anforderungen nach Art. 32–36 DS-GVO – 87
5.5.8 Unterstützung zur Nachweiserbringung (Art. 28 Abs. 3 Satz 2 Buchst. h DS-GVO) – 87
5.5.9 Kontrollrechte (Art. 28 Abs. 3 Satz 2 Buchst. h DS-GVO) – 88
5.5.10 Umgang mit Daten nach Beendigung der Verarbeitung (Art. 28 Abs. 3 Satz 2 Buchst. g DS-GVO) – 88

6 Verzeichnis von Verarbeitungstätigkeiten (VvV) 89
Marlis Hübner
6.1 Wesentliche Rechtsgrundlagen nach der DS-GVO – 89
6.2 Zweck der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten – 89
6.3 Pflicht zur Erstellung des Verzeichnisses von Verarbeitungstätigkeiten – 90
6.4 Inhalt des Verzeichnisses von Verarbeitungstätigkeiten – 91
6.4.1 Inhalt des Verzeichnisses von Verarbeitungstätigkeiten des Verantwortlichen gemäß Art. 30 Abs. 1 DS-GVO – 91
6.4.2 Inhalt des Verzeichnisses von Verarbeitungstätigkeiten des Auftragsverarbeiters gemäß Art. 30 Abs. 2 DS-GVO – 95
6.4.3 Rechtsfolgen bei Verstößen – 97

7 Datenschutz-Folgenabschätzung 99
Carsten Dochow
7.1 Definition und Bedeutung – 99
7.2 Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung – 100
7.2.1 Hintergrund: „Hohes Risiko" bei der geplanten Datenverarbeitung – 100
7.2.2 Fälle der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung – 102
7.3 Durchführung der Datenschutz-Folgenabschätzung – 110
7.3.1 Inhalt einer Datenschutz-Folgenabschätzung – 110
7.3.2 Ablauf: Schritte einer Datenschutz-Folgenabschätzung – 110
7.3.3 Verantwortlichkeit für Datenschutz-Folgenabschätzung und Einbeziehung des Datenschutzbeauftragten – 112
7.3.4 Ergebnis der Datenschutz-Folgenabschätzung – 113
7.4 Konsultation der Aufsichtsbehörde – 114
7.5 Gemeinsame Datenschutz-Folgenabschätzung – 114
7.6 Matrix zur Dokumentation der Datenschutz-Folgenabschätzung – 115

8 Betrieblicher Datenschutzbeauftragter in der Arztpraxis 117
Carsten Dochow
8.1 Allgemeines und Bedeutung des betrieblichen Datenschutzbeauftragten – 117
8.2 Pflicht zur Benennung eines Datenschutzbeauftragten – 118
8.2.1 Hintergründe zur Benennungspflicht – 118
8.2.2 Fälle der Pflicht zur Benennung eines Datenschutzbeauftragten – 120
8.2.3 Fazit zu Gesundheitseinrichtungen – 128
8.2.4 Benennung eines internen oder externen Datenschutzbeauftragten – 129
8.2.5 Publizität: Veröffentlichung und Meldung der Kontaktdaten des Datenschutzbeauftragten – 130
8.2.6 Nachweis durch formale Benennung und Möglichkeit der Befristung? – 131
8.3 Rechte und Stellung des Datenschutzbeauftragten – 133
8.3.1 Weisungsfreiheit und Unabhängigkeit – 133
8.3.2 Benachteiligungsverbot, Schutz vor Kündigung und Abberufung – 134
8.3.3 Frühzeitige Beteiligung, Unterstützung und Ressourcen – 134
8.3.4 Besondere Stellung im Betrieb – 135
8.4 Qualifikation und Aufgaben des Datenschutzbeauftragten – 136
8.4.1 Qualifikation – 136
8.4.2 Aufgaben – 137
8.5 Datenschutzbeauftragter und Verschwiegenheit – 139
8.6 Haftung des Datenschutzbeauftragten – 140
8.7 Folgen bei Verstößen („Fehler-Checkliste") – 141

9 Arzt/Praxis als Arbeitgeber 145
Bernd Halbe/Joachim Schütz
9.1 Allgemeine Grundsätze zum Schutz der Beschäftigten – 145
9.2 Beschäftigtendatenschutz – 145
9.2.1 Erlaubnistatbestand für die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses – § 26 Abs. 1 BDSG – 146
9.2.2 Erlaubnis durch Einwilligung – § 26 Abs. 2 BDSG – 148
9.2.3 Aufdeckung von Straftaten – § 26 Abs. 1 Satz 2 BDSG – 149
9.2.4 Verarbeitung von besonderen Kategorien personenbezogener Daten – § 26 Abs. 3 BDSG – 149
9.2.5 Sachlicher und persönlicher Geltungsbereich – § 26 Abs. 7 und 8 BDSG – 150
9.3 Betroffenenrechte der Beschäftigten – 150
9.4 Unterrichtung und Verpflichtung von Beschäftigten des Verantwortlichen und des Auftragsverarbeiters auf das Datengeheimnis – 151

10 Rechte von Patienten (Betroffenenrechte) 153
Jürgen Schröder
10.1 Informationspflichten – 153
10.1.1 Allgemeines – 153
10.1.2 Inhalt der Information – 153
10.1.3 Form, Nachweis und Zeitpunkt der Information – 155
10.2 Auskunftsrechte – 156
10.2.1 Antrag auf Auskunftsrecht – 156
10.2.2 Umfang des Auskunftsrecht – 156
10.2.3 Form, Frist und Kosten der Auskunftserteilung – 157
10.2.4 Grenzen der Auskunftserteilung – 157
10.3 Rechte auf Berichtigung, Löschung und Einschränkung der Verarbeitung – 158
10.3.1 Recht auf Berichtigung – 158
10.3.2 Recht auf Löschung – 159
10.3.3 Recht auf Einschränkung der Verarbeitung – 159
10.4 Recht auf Datenübertragbarkeit – 159
10.5 Widerspruchsrecht – 160

11 Ärztliche Schweigepflicht 161
Bert-Sebastian Dörfer
11.1 Einleitung – 161
11.2 Rechtsgrundlagen – 161
11.3 Gegenstand und Reichweite der Schweigepflicht – 162
11.4 Adressaten der Schweigepflicht – 163
11.5 Einschränkungen der Schweigepflicht – 163
11.5.1 Schweigepflichtentbindung durch Einwilligung – 163
11.5.2 Gesetzliche Offenbarungspflichten – 164
11.5.3 Gesetzliche Offenbarungsbefugnisse – 165
11.5.4 Weitere Erlaubnisgründe – 167

12 Sicherheit der Verarbeitung und praxisinterne Datenschutzrichtlinie 169
Jakob Strüve
12.1 Einleitung – 169
12.2 Technisch-organisatorische Maßnahmen zur Umsetzung der Datensicherheit in der Praxis – 170
12.2.1 Zugangskontrolle – 170
12.2.2 Zugriffskontrolle – 172
12.2.3 Transportkontrolle – 173
12.2.4 Verfügbarkeitskontrolle – 173
12.2.5 Trennungskontrolle – 174
12.2.6 Organisationskontrolle – 174
12.2.7 Kontrolle der Vorgaben – 174
12.2.8 Maßnahmen nach § 22 Abs. 2 BDSG – 175

13 Verletzung des Schutzes personenbezogener Daten („Datenpannen") 177
Jakob Strüve
13.1 Einführung und allgemeiner Überblick zu den Regelungen – 177
13.1.1 Vorliegen eines Datenschutzvorfalls – 177
13.1.2 Maßnahmen beim Vorliegen eines Datenschutzvorfalls – 178
13.1.3 Vorliegen einer Verletzung des Schutzes der personenbezogenen Daten – 178
13.1.4 Verstöße gegen den Schutz der personenbezogenen Daten – 179
13.1.5 Keine Verletzung des Schutzes personenbezogener Daten – 179
13.2 Art. 33 DS-GVO – Mitteilung an die datenschutzrechtliche Aufsicht – 179
13.2.1 Durchführung der Meldung – 179
13.2.2 Vorliegen der Kenntnis beim Verantwortlichen – 180
13.2.3 Verzögerte Meldung – 180
13.2.4 Unterlassen der Meldung – 181
13.3 Art. 34 DS-GVO – Benachrichtigung des Betroffenen – 181
13.3.1 Zu erteilende Informationen bei der Benachrichtigung – 181
13.3.2 Art und Weise der Benachrichtigung – 182
13.3.3 Unterlassen der Benachrichtigung – 182
13.3.4 Vorliegen eines voraussichtlich hohen Risikos – 182
13.4 Einbindung des Datenschutzbeauftragten bei der Meldung und Benachrichtigung – 183
13.5 Dokumentationspflichten im Zusammenhang mit dem Datenschutzvorfall – 183
13.6 Maßnahmen im Vorfeld – 183
13.7 Folgen einer unterlassenen Meldung und Benachrichtigung – 184
13.8 Beweisverwertungsverbote – 184

14 Sanktionen und Haftung 187
Bernd Halbe/Jan Ippach
14.1 Überblick – 187
14.2 Sanktionsmaßnahmen nach der DS-GVO – 187
14.2.1 Geldbuße – 187
14.2.2 Weitere aufsichtsbehördliche Abhilfemaßnahmen – 188
14.2.3 Datenschutzverstoß durch Praxismitarbeiter oder externen Auftragsverarbeiter – 188
14.2.4 Umfang und Grenze der Sanktionsmöglichkeit – 188
14.3 Sanktionsmöglichkeiten nach nationalem Recht (BDSG) – 189
14.4 Schadenersatz und Haftung – 189

15 Umgang mit der Aufsichtsbehörde 191
Marlis Hübner
15.1 Unabhängige Aufsichtsbehörden – 191
15.2 Aufklärung und Beratung durch die Aufsichtsbehörde? – 192
15.3 Weitere Aufgaben und Befugnisse der Aufsichtsbehörde – 193
15.3.1 Weitere Aufgaben der Aufsichtsbehörde – 193
15.3.2 Befugnisse der Aufsichtsbehörde – 195
15.4 Beschränkung der Befugnisse der Aufsichtsbehörde nach § 29 Abs. 3 BDSG – 199

16 Anhang: Muster **203**
Muster 1: Datenschutz-Einwilligungserklärung – 204
Muster 2: Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO – 206
Muster 3: Arztpraxis – Verzeichnis von Verarbeitungstätigkeiten (Bayerisches Landesamt für Datenschutzaufsicht) – 212
Muster 4: Verzeichnis von Verarbeitungstätigkeiten (Kassenärztliche Bundesvereinigung) – 213
Muster 5: Matrix zur Dokumentation der Datenschutz-Folgenabschätzung – 216
Muster 6: Urkunde zur Benennung einer/s internen betrieblichen Datenschutzbeauftragten – 217
Muster 7: (Widerrufliche) Einwilligungserklärung zur Nutzung von Bildaufnahmen des Mitarbeiters auf der Homepage der Arztpraxis – 219
Muster 8: Informationen zur Datenverarbeitung gemäß Art. 13 DS-GVO zum Arbeitsvertrag – 220
Muster 9: Verpflichtung zur Vertraulichkeit und zur Wahrung datenschutzrechtlicher Bestimmungen nach der DS-GVO – 222
Muster 10: Einfache Passwortrichtlinie – 224
Muster 11: Praxisinterne Datenschutzrichtlinie – Verzeichnis der allgemeinen technisch-organisatorischen Maßnahmen – 225
Muster 12: Verpflichtungserklärung zur Wahrung des Datengeheimnisses und der Schweigepflicht – 227
Muster 13: Meldung an die datenschutzrechtliche Aufsicht – 228
Muster 14: Zu erteilende Informationen bei der Benachrichtigung – 229
Muster 15: Dienstanweisung – Richtlinie zum Umgang mit Verstößen und über die Zusammenarbeit mit Aufsichtsbehörden – 230
Muster 16: Patienteninformation zum Datenschutz – 231

Literaturverzeichnis **233**

Stichwortverzeichnis **235**