

Inhalt

Vorwort	15
Abkürzungsverzeichnis	17
I Grundlagen	21
1 Das informationelle Selbstbestimmungsrecht – Historie	21
2 Hintergrund und Ziele zur DS-GVO	24
3 Besondere Bedeutung der Patientendaten im Krankenhaus...	25
II Zentraler Grundsatz der Verarbeitung	26
1 Verbot mit Erlaubnisvorbehalt gem. DS-GVO	26
2 »Verarbeitung« als neuer Oberbegriff	27
3 Verhältnis zwischen ärztlicher Schweigepflicht und Datenschutz	27
III Datenschutznormen/-regelungen	30
1 Übersicht über die Regelungen	30
2 EU Datenschutz-Grundverordnung (DS-GVO)	31
2.1 Persönlicher Anwendungsbereich	31
2.2 Kirchliche Krankenhausträger	32
2.3 Sachlicher Anwendungsbereich	33
2.4 Besondere Datenkategorien (Gesundheitsdaten)	33
2.5 Fazit zur Zulässigkeit der Verarbeitung von Gesundheitsdaten unter der DS-GVO	35
3 Bundesdatenschutzgesetz (BDSG)	35
4 Fazit zur DS-GVO und zum BDSG als Befugnisnormen	37
5 Bereichsspezifische Bundesregelungen	38
6 Landesrechtliche Regelungen	39
6.1 Landeskrankenhausgesetze	39
6.2 Bereichsspezifische Landesregelungen	41
6.3 Landesdatenschutzgesetze (LDSG)	41
7 Übersicht: Anwendbarkeit Gesetz je nach Trägerschaft	44
8 Auflistungen vorhandener Befugnisnormen speziell für Krankenhäuser	45

IV	Einwilligungen	51
1	Einsichtsfähigkeit	51
2	Kirchliche Krankenhausträger	52
3	Hintergrund – »besonders sensible Daten«	53
4	Gesetzliche Grundlagen	53
5	Verbot mit Erlaubnisvorbehalt, Art. 9 DS-GVO	54
6	Sanktionen	54
7	Weitergeltung bereits eingeholter Einwilligungserklärungen	55
8	Anforderungen insgesamt – <i>Checkliste</i>	57
V	Ärztliche Schweigepflicht	67
1	Allgemeines	67
2	Grundlagen der Verschwiegenheitspflicht	67
3	Tatbestandsvoraussetzungen des § 203 StGB	69
	3.1 Geschütztes Rechtsgut	69
	3.2 Täterkreis	69
	3.3 Fremdes Geheimnis	98
	3.4 Kenntnis im Rahmen der ärztlichen Funktion	99
	3.5 Unbefugtes Offenbaren	99
4	Gesetzliche Offenbarungsbefugnisse oder -verpflichtungen ...	100
5	Einwilligung des Patienten	102
6	Wahrnehmung berechtigter Interessen	102
7	Rechtfertigender Notstand	103
8	Verhalten bei Verdacht auf Straftaten	105
	8.1 Berechtigung zur Anzeige	105
	8.2 Pflicht zur Anzeige	106
9	Verhalten bei Verdacht auf Kindesmisshandlung	108
	9.1 Schwerwiegende lebensbedrohliche Verletzungen ...	108
	9.2 Feststellung aktueller und älterer Verletzungen	110
	9.3 »Typischer Spielunfall«	110
	9.4 Bundeskinderschutzgesetz	111
	9.5 Mitteilungspflichten gegenüber den Krankenkassen ...	112
	9.6 Rechtliche Grundlage für eine Einschaltung des Jugendamtes	112
	9.7 Rechtliche Grundlage für eine Einschaltung der Polizei	113
	9.8 Inhalt der Anzeige	115
	9.9 Dokumentation	115
VI	Durch die DS-GVO bedingte Änderungen	117
1	Informationspflichten gegenüber Patienten im Krankenhausbereich auf der Grundlage der Art. 12 ff. DS- GVO	119
	1.1 Kirchliche Krankenhausträger	119
	1.2 Rechtliche Grundlagen	120

1.3	Hintergrund	120
1.4	Zeitpunkt der Information	120
1.5	Form und Darstellung der Information	121
1.6	Notwendige Informationen im Einzelnen	123
1.7	Mögliche Ausnahmen von der Informationspflicht? ...	135
1.8	Verstöße und Sanktionen gegen die Informationspflicht	137
1.9	Stationärer Bereich – <i>Musterformulierung</i>	137
1.10	Institutsambulanzen/MVZ – <i>Musterformulierung</i>	147
2	Auskunftsrecht gemäß Art. 15 DS-GVO	156
2.1	Kirchliche Krankenhausträger	156
2.2	Rechtslage vor Geltungsbeginn der DS-GVO	157
2.3	Informationspflichten vs. Auskunftsrecht	157
2.4	Stufen des Auskunftsrechts	157
2.5	Antragstellung formlos, ohne Angabe eines Grundes	159
2.6	Frist für die Auskunftserteilung	159
2.7	Ausnahmen vom Auskunftsrecht	160
2.8	Beachtung Rechte Dritter	161
2.9	Grenzen des Auskunftsrechts	162
2.10	Form der Auskunftserteilung	163
2.11	Umsetzung im Krankenhausbereich	166
2.12	Kosten	168
2.13	Rechtsfolgen bei Verstoß	169
3	Recht auf Löschung / Recht auf »Vergessenwerden« gemäß Art. 17 DS-GVO / § 21 DSGVO / § 19 KDG	170
3.1	Pflicht zur Löschung personenbezogener Daten	171
3.2	Pflicht zur Löschung nicht nur auf Verlangen des Betroffenen	175
3.3	Ausnahmen von der Pflicht zur Löschung gemäß Art. 17 Abs. 3 DS-GVO / § 21 Abs. 3 DSGVO / § 19 Abs. 3 KDG	175
3.4	Beschränkung des Lösungsanspruchs nach § 35 BDSG neue Fassung	179
3.5	Kirchliche Besonderheiten	180
3.6	Fazit	181
3.7	Nachberichtspflichten gemäß Art. 19 DS-GVO / § 23 DSG-EKD / § 21 KDG	181
3.8	Recht auf »Vergessenwerden« gemäß Art. 17 Abs. 2 DS-GVO / § 21 Abs. 2 DSGVO / § 19 Abs. 2 KDG ...	182
3.9	Sanktionen	182
4	Recht auf Datenübertragbarkeit gem. Art. 20 DS-GVO	183
4.1	Kirchliche Krankenhausträger	183
4.2	Entstehungsgeschichte und Ziele	184
4.3	Anwendungsbereich und Sinn und Zweck	185
4.4	Bereichsausnahme	185

	4.5	Fazit	187
5		Widerspruchsrecht gemäß Art. 21 DS-GVO / § 25 DSGVO / § 23 KDG	187
	5.1	Widerspruch gegen Verarbeitungen zur Wahrnehmung öffentlicher Aufgaben oder zur Wahrung berechtigter Interessen (Art. 21 Abs. 1 DS-GVO)	188
	5.2	Widerspruch gegen Direktwerbung (Art. 21 Abs. 2 und 3 DS-GVO)	192
	5.3	Widerspruch gegen Verarbeitungen zu Forschungszwecken (Art. 21 Abs. 6 DS-GVO)	193
	5.4	Pflicht zum Hinweis auf das Widerspruchsrecht nach Art. 21 Abs. 1 und 2 DS-GVO (Art. 21 Abs. 4 DS-GVO)	194
	5.5	Sanktionen	195
	5.6	Kirchliche Besonderheiten	196
6		Verarbeitung von personenbezogenen Daten zu einem anderen Zweck	197
	6.1	Zulässigkeit der Weiterverarbeitung zu einem anderen Zweck	197
	6.2	Informationspflichten bei einer Weiterverarbeitung zu einem anderen Zweck	201
7		Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO	210
	7.1	Kirchliche Krankenhausträger	211
	7.2	Verantwortlichkeit	211
	7.3	Einzuhaltende Grundsätze gem. Art. 5 Abs. 1 DS-GVO	212
	7.4	Für wen wird die Rechenschaftspflicht statuiert? Beweislast?	213
	7.5	Zeitpunkt und Dauer der Nachweisbarkeit?	213
	7.6	Sanktionen	213
	7.7	Umsetzbarkeit im Krankenhausbereich	214
	7.8	Zwischenfazit	215
	7.9	Datenschutzkonzept – <i>Beispiel</i>	215
8		Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO / § 31 DSGVO / § 31 KDG	228
	8.1	Inhalte des Verzeichnisses (Art. 30 Abs. 1 DS-GVO) ...	228
	8.2	Unterschiede zwischen früherem Verfahrensverzeichnis nach BDSG und jetzigem Verzeichnis von Verarbeitungstätigkeiten nach der DS-GVO	229
	8.3	Befreiung von der Verzeichnispflicht (Art. 30 Abs. 5 DS-GVO)	230
	8.4	Sanktionen	230
	8.5	Kirchliche Besonderheiten	230

8.6	Konkrete Darstellung einzelner Verarbeitungstätigkeiten im Verzeichnis	231
8.7	Ergebnis	234
9	Informationspflichten bei Datenschutzverletzungen	235
9.1	Meldepflicht gegenüber den Aufsichtsbehörden (Art. 33 DS-GVO / § 32 DSGVO / § 33 KDG)	236
9.2	Meldepflicht gegenüber der betroffenen Person (Art. 34 DS-GVO / § 33 DSGVO / § 34 KDG)	245
10	Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO / § 34 DSGVO / § 35 KDG	252
10.1	Pflicht zur Durchführung einer DSFA	252
10.2	Inhalt einer DSFA	253
10.3	Ausnahmetatbestand des Art. 35 Abs. 10 DS-GVO / § 34 Abs. 7 DSGVO / § 35 Abs. 9 KDG	255
10.4	Sanktionen	257
10.5	Verbändeübergreifende Praxishilfe	257
10.6	Positivlisten der Aufsichtsbehörden	257
11	Datenschutzerklärung auf der Homepage	262
11.1	Rechtslage vor bzw. bis zum 25.05.2018	262
11.2	Rechtslage ab dem Geltungsbeginn der DS-GVO	266
11.3	Auswirkungen auf das »Impressum«	273
12	Konzernprivileg	276
13	Gemeinsame Verantwortlichkeit gemäß Art. 26 DS-GVO / § 29 DSGVO / § 28 KDG	278
14	Facebook-Fanpages	280
15	Bußgeldkatalog der Aufsichtsbehörden	282

VII	Verwendung von Patientendaten innerhalb des Krankenhauses – Fallbeispiele	284
1	Krankenhausverwaltung	284
1.1	Abrechnung erbrachter Leistungen	284
1.2	Bewertung und Abrechnung des Bereitschaftsdienstes	285
1.3	Allgemeine Organisations- und Kontrollzwecke	286
2	Behandlung im Team / Zuziehung weiterer Ärzte/Gehilfen des Arztes	287
3	Medizinprodukteberater	288
4	Postöffnung im Krankenhaus	290
5	Mitschneiden von Telefongesprächen	292
6	Videüberwachung in nicht öffentlich zugänglichen Patientenzimmern	293
6.1	Allgemeine rechtliche Überlegungen	293
6.2	Medizinische/Ethische Argumente für und gegen Videüberwachungen	294
6.3	Ausnahmeregelung in Nordrhein-Westfalen	296
6.4	Möglicher datenschutzrechtlicher Verstoß	297

6.5	Mögliche Verwirklichung des Straftatbestandes § 201a Abs. 1 StGB	297
6.6	Mögliche Grundrechtsverletzung	299
6.7	Fazit zu Videoüberwachungen	300
7	Aktive Benachrichtigung von Angehörigen	302
8	Auskunft an der Pforte / am Telefon	303
9	Auskunft über den Gesundheitszustand	304
10	Beschriftung von Zimmertür und Krankenbett	304
11	Patientenarmband	305
12	Mithören von Gesprächen zwischen Behandlungspersonal und Patienten durch Dritte	306
13	Auskunft über Mitpatienten	308
14	Auskunft über Ärzte und nichtärztliche Mitarbeiter	308
15	Einsichtnahmerecht des Patienten in die Krankenunterlagen	309
15.1	Rechtliche Grundlagen des Einsichtnahmerechtes des Patienten	310
15.2	Frühere Einschränkungen des Einsichtnahmerechtes durch den BGH	310
15.3	Entscheidung des BVerfG zum Maßregelvollzug	312
15.4	Landesrechtliche Regelungen	313
15.5	Regelung in § 630g BGB auf Bundesebene	314
15.6	Vermittlung der Einsichtnahme durch einen Arzt.	315
15.7	Praktischen Handhabung	316
15.8	Weitere Grenzen der Einsichtnahme	316
15.9	Keine Unterlagen über die interne Organisation	317
15.10	Verhältnis des Rechts auf Einsichtnahme gem. § 630g BGB und des Rechts auf Auskunft gem. Art. 15 DS-GVO	319
16	Herausgabe von Krankenunterlagen an den Patienten	329
16.1	Grundsätzlich keine Originale	330
16.2	Anfertigung von Kopien	331
16.3	Höhe der Kopierkosten	331
16.4	Höhe der Kopierkosten bei elektronischen Akten	332
16.5	Kopierkosten – Vorleistungspflicht des Patienten	333
16.6	Keinen Anspruch auf Zusendung	334
16.7	Eidesstattliche Versicherung	335
16.8	Beglaubigte Kopien	335
16.9	Keine Unterlagen über die interne Organisation des Krankenhauses	335
17	Einsichtnahmerecht von Angehörigen und Erben	336
17.1	Einsichtnahmerecht von Angehörigen und Erben – <i>früher</i>	337
17.2	Einsichtnahmerecht von Angehörigen und Erben – <i>heute</i>	337
18	Einsichtnahmerecht in Obduktionsberichte	343

19	Auskünfte gegenüber den Eltern minderjähriger Patienten ...	344
19.1	Einwilligungsfähigkeit als Abgrenzungskriterium	345
19.2	Einwilligungsfähiger Minderjähriger	346
19.3	Rechtsprechung	347
19.4	Fazit zur Rechtsprechung	349
19.5	Gesamtfazit	350
20	Kopieren von Ausweisen	352
20.1	Fotokopieren, Fotografieren und Einscannen	354
20.2	Einwilligung	354
20.3	Berechtigte Interessen bei Nicht-Einwilligung	354

VIII Verwendung von Patientendaten außerhalb des Krankenhauses (Übermittlung an Dritte) – Fallbeispiele

1	Übermittlung von Patientendaten zwischen Krankenhäusern und Hausärzten/Vor-/Nach-/Weiter-/Mitbehandlern	355
1.1	Gesetzliche Grundlage – Hausarzt	356
1.2	Hausarzt – Musterformulierung	358
1.3	Umfang der Datenübermittlung – Hausarzt	361
1.4	Anwendbarkeit auf Notfallpatienten – Hausarzt	361
1.5	Widerruf der Einwilligung – Hausarzt	362
1.6	Übermittlung an Vor-/Weiter-/Nachbehandler	362
1.7	Landesverträge gem. § 115 Abs. 2 Nr. 2 SGB V	364
1.8	Regelungen in Landeskrankenhausesetzen	365
1.9	Definition des Hausarztes	366
1.10	Empfehlung	367
1.11	Sonstige Vor-/Weiter-/Nachbehandler – <i>Muster</i>	368
1.12	Checkliste zu Hausärzten und sonstigen Vor-/Nach-/Weiterbehandlern	372
1.13	Abgrenzung zu Mitbehandlern	374
2	Externe Datenverarbeitung	375
2.1	Beispiele und Grundlagen externer Datenverarbeitung	375
2.2	Auftragsverarbeitung	376
2.3	Externe Abrechnung	384
2.4	Externe Schreibbüros	391
2.5	Fernwartung von EDV-Systemen	392
3	Herausgabe von Krankenunterlagen an Rechtsanwälte und andere vom Patienten Beauftragte	393
4	Auskünfte gegenüber privaten Versicherungen	393
4.1	Unternehmen der privaten Krankenversicherung	393
4.2	Unwirksamkeit pauschaler Schweigepflichtentbindungserklärungen	402
4.3	Empfehlung	405
4.4	Übertragbarkeit o. g. Grundsätze unter der Maßgabe der DS-GVO	406
4.5	Sonstige private Versicherungen	406

5	Staatsanwaltschaft und Polizei	406
5.1	Auskünfte gegenüber Strafverfolgungsbehörden	407
5.2	Durchsuchung und Beschlagnahme	412
6	Herausgabe von Krankenunterlagen an Gerichte	421
7	Einsicht in Krankenunterlagen durch den Rechnungshof	423
8	Arbeitgeber bzw. Dienstherr des Patienten	425
9	Weitergabe von Patientendaten an interessierte Firmen	426
10	Datenübermittlung an Seelsorger	426
11	Auskunft an Versorgungsämter	428
12	Auskunft an das Bundeskartellamt	430
13	Auskunft an das Finanzamt	431
IX	Übermittlung von Patientendaten an Sozialversicherungsträger und MDK	432
1	Datenübermittlung an die gesetzlichen Krankenkassen	432
1.1	Datenübermittlung gemäß § 301 SGB V	432
1.2	Datenübermittlung gemäß § 294a Abs. 1 SGB V	442
1.3	Datenübermittlung und Informationspflicht gemäß § 294a Abs. 2 SGB V	458
1.4	Bestimmungen aus dem vertragsärztlichen Bereich ...	463
2	Datenübermittlung an den MDK.....	464
2.1	Allgemeines	464
2.2	Einzelfallüberprüfung gemäß §§ 275 ff. SGB V.....	464
2.3	Exkurs: Klageverfahren, Verjährung	469
3	Entlassmanagement	469
X	Übermittlung von Patientendaten an Unfallversicherungsträger	477
1	Allgemeines	477
2	§§ 199 und 201 SGB VII als Rechtsgrundlage	478
3	Umfang der Datenübermittlung	479
4	Zeitpunkt der Überprüfung	480
5	Handlungsempfehlung für Krankenhäuser	481
XI	Dokumentation und Archivierung	483
1	Allgemeines	483
1.1	Archivierung im Krankenhaus	484
1.2	Externe Archivierung	484
1.3	Dauer der Aufbewahrung der Dokumentation	486
1.4	Datenschutzkonforme Vernichtung	489
2	Archivierungsformen	492
2.1	Mikroverfilmung	492
2.2	Digitale Dokumentation und Archivierung	493
2.3	Digitale Archivierung von Röntgenbildern	507

XII	Formen der Datenübermittlung	509
1	Datenübermittlung per Telefax	509
2	Datenübermittlung per E-Mail	510
3	Telemedizin	512
4	Nutzung von Messenger-Diensten im Krankenhaus	516
4.1	Juristische Anforderungen	517
4.2	Datenschutz und Schweigepflicht	517
4.3	Technische Datenschutzerfordernngen	518
4.4	Orientierung an den Anforderungen des »branchenspezifischen Sicherheitsstandards (B3S) für Krankenhäuser« bei der Nutzung mobiler Endgeräte	520
4.5	Nutzungsszenarien	521
4.6	Keine Primärdokumentation	521
4.7	Auswahl eines Messenger-Dienstes für den Betrieb ...	522
4.8	Betriebliche Nutzung eines Messenger-Dienstes gestattet?	522
4.9	Umsetzung in Form einer Dienstanweisung, individuellen Vereinbarung oder Betriebsvereinbarung	523
4.10	Zur Verfügung gestellte Dienst-Mobiltelefone auch privat nutzbar?	524
4.11	Benutzerkreis	524
XIII	Der betriebliche Datenschutzbeauftragte im Krankenhaus unter Maßgabe der DS-GVO / des DSGVO-EKD / des KDG	525
1	Pflicht zur Benennung eines betrieblichen Datenschutzbeauftragten	526
1.1	Krankenhäuser in öffentlicher Trägerschaft	526
1.2	Krankenhäuser in privater Trägerschaft	526
1.3	Krankenhäuser in kirchlicher Trägerschaft	528
1.4	Interner oder externer Datenschutzbeauftragter möglich	528
1.5	Ergebnis	529
2	Konzerndatenschutzbeauftragter	529
3	Anforderungsprofil	531
4	Aufgaben und Stellung des Datenschutzbeauftragten	531
4.1	Aufgaben des Datenschutzbeauftragten	531
4.2	Stellung des Datenschutzbeauftragten	533
5	Schutz und Haftung des Datenschutzbeauftragten	534
5.1	Schutz	534
5.2	Haftung	535
6	Beendigung der Tätigkeit des Datenschutzbeauftragten	537
7	Veröffentlichung und Mitteilung der Kontaktdaten	538
8	Umgang mit bestehenden Bestellungen	539
9	Rechtsfolgen bei Verstößen	540

XIV	Einzelfälle	541
1	Datenschutz und HIV-Infektionen	541
2	Forschung mit Patientendaten	544
3	Warnungen vor »Krankenhauswanderern«	548
4	Übergabe der Patientenkartei bei einer Praxisaufgabe	549
5	Datenschutzrechtliche Vorgaben bei der Schließung eines Krankenhauses	552
5.1	Fortbestehen der gesetzlichen Aufbewahrungsfristen	552
5.2	Dauer der Aufbewahrung	553
5.3	Zuständigkeit für die Aufbewahrung	553
5.4	Form der Aufbewahrung	554
5.5	Sonderfall der Insolvenz	554
6	Schweigepflicht des Betriebsarztes gegenüber dem Arbeitgeber	555
6.1	Allgemeine arbeitsmedizinische Vorsorgeuntersuchungen	556
6.2	Spezielle arbeitsmedizinische Vorsorgeuntersuchungen	556
6.3	Datenweitergabe an den Arbeitgeber	557
7	Umgang mit Betäubungsmitteln	559
	Anhang	561
	Anhang 1: Rechtliche Rahmenbedingungen für den Einsatz von Krankenhausinformationssystemen	561
	Anhang 2: Szenarien zulässigen Datenaustauschs zwischen stationären und ambulanten Leistungserbringern	575
	Literaturverzeichnis	582
	Stichwortverzeichnis	587