

Inhaltsverzeichnis

Einführung	
<i>Thorsten Kingreen/Jürgen Kühling</i>	25
Teil 1: Grundlagen – Allgemeiner Teil	
<i>Jürgen Kühling/Christian Seidel</i>	29
A. Der Begriff der Gesundheitsdaten	30
I. Personenbezogene Daten	31
II. Gesundheitsdaten	34
1. Angaben über die Gesundheit gemäß § 3 Abs. 9 BDSG	34
2. Sozialdaten	38
a) Definition und Beispiele	38
b) Regelungssystematik des Sozialdatenschutzes	40
c) Anwendungsbereich im Rahmen dieses Buches	40
d) Zusammenfassung	41
3. Leistungsdaten	42
4. Abgrenzung zu anderen gesundheitsdatenschutzrelevanten Begriffen	44
III. Legaldefinition der Gesundheitsdaten im Entwurf der DSGVO	45
IV. Resumée	48
B. Problemaufriss und Überblick über Kategorien beteiligter Akteure	50
I. Allgemeine Problematik der multipolaren Grundstruktur	50
II. Gesteigerte Komplexität am Beispiel des Gesundheitswesens	50
1. Trias: „Patient – Leistungserbringer – Leistungsträger“	50
2. Beteiligte Entitäten in der Sphäre des Patienten/ Versicherten	51
3. Beteiligte Entitäten auf Leistungserbringerseite	52
4. Beteiligte Entitäten auf Leistungsträgerseite	53
III. Vergleichende Akteursbetrachtung in weiteren Referenzgebieten	54

C. Regelungsstrukturen des einfachgesetzlichen Datenschutzrechts	56
I. Allgemeine Steuerungsvorgaben zur Identifikation der einschlägigen Rechtsquelle	56
1. Abgrenzung allgemein/bereichsspezifisch	56
2. Abgrenzung öffentlich/nicht-öffentlich	58
3. Einfluss der Kompetenzverteilung im Grundgesetz	60
II. Allgemeines Datenschutzrecht	62
1. System und Aufbau des BDSG	62
2. Wesentliche Begriffsbestimmungen	64
a) Personenbezogene Daten und Betroffener	64
b) Gesundheitsdaten als besondere Arten personenbezogener Daten	65
c) Umgang mit personenbezogenen Daten im Gesundheitsbereich	67
aa) Erheben	68
bb) Verarbeiten	69
(1) Speichern	69
(2) Verändern	70
(3) Übermitteln	70
(4) Sperren	72
(5) Löschen	72
cc) Nutzen	73
dd) Automatisierte Verarbeitung und nicht automatisierte Datei	73
3. Wesentliche Regelungsgrundsätze	74
a) Verbot mit Erlaubnisvorbehalt	74
b) Zweckbindung und Erforderlichkeit	75
c) Transparenz	76
d) Datenvermeidung und Datensparsamkeit	76
4. Zulässigkeit des Datenumgangs	78
a) Überblick über die Zulässigkeitstatbestände	78
aa) Nicht-öffentlicher Bereich	79
bb) Öffentlicher Bereich	81
b) Besonderheiten beim Umgang mit sensiblen Daten	82
aa) Nicht-öffentlicher Bereich	82
(1) Datenumgang für eigene Geschäftszwecke (§ 28 Abs. 6 BDSG)	82
(2) Gesundheitsbereich (§ 28 Abs. 7 BDSG)	84

(3) Übermittlung oder Nutzung bei Zweckänderung (§ 28 Abs. 8 BDSG)	85
(4) Privilegierte Organisationen (§ 28 Abs. 9 BDSG)	85
(5) Datenumgang zum Zweck der Übermittlung	86
bb) Öffentlicher Bereich	86
5. Verantwortliche Stelle und Dritter	88
6. Auftragsdatenverarbeitung	91
7. Einwilligung	94
a) Rechtsnatur	95
b) Wirksamkeitsvoraussetzungen	96
aa) Freiwilligkeit	96
bb) Informiertheit	100
cc) Bestimmtheit	100
dd) Besonderheiten bei sensiblen Daten i.S.d. § 3 Abs. 9 BDSG, insbesondere Gesundheitsdaten	101
c) Formale Wirksamkeitsvoraussetzungen	102
aa) Abgabe	102
bb) Form	102
cc) Besondere Hervorhebung	103
d) Widerruf	104
8. Betroffenenrechte	105
a) Benachrichtigung	105
b) Auskunft	106
c) Korrekturpflichten und sonstige Rechte des Betroffenen	108
9. Datenschutzkontrolle	110
a) Institutionelle Komplexität als Abbild der materiell- rechtlichen Komplexität	110
b) BfDI	111
c) LDSB für öffentliche Entitäten auf Landesebene	112
d) Aufsichtsbehörden für den Privatbereich	113
a) Meldepflichten	116
b) Vorabkontrolle	117
c) Behördlicher/betrieblicher DSB	118
10. Sanktionen	122
11. Landesrecht	124

D. Überformende Vorgaben des EU-Sekundärrechts	125
I. Allgemeine Datenschutzrichtlinie 95/46/EG	125
1. Prägung des nationalen Rechts	125
a) Grundlagen	125
b) Stand der Harmonisierung im Lichte des „ASNEF“- Urteils des EuGH	126
aa) Weitgehende Vollharmonisierung	126
bb) Notwendigkeit eines sinnvollen Konkretisierungskonzepts	128
cc) Unmittelbare Wirkung der Richtlinie	129
2. Vorsteuernde Elemente mit Blick auf den Gesundheitsdatenschutz	130
a) Umgang mit sensiblen Daten – Konkretisierungsspielraum für Mitgliedstaaten	130
b) Sonderproblem der Auftragsdatenverarbeitung	131
aa) Abgrenzung zur Funktionsübertragung	132
bb) Richtlinienvorgaben hinsichtlich der Modalitäten	134
cc) Einordnung der Einschaltung privater Abrechnungsstellen im Gesundheitsbereich als zentraler Anwendungsfall	134
dd) Sonderfall Unterauftragsverhältnis	136
II. Bevorstehende Änderungen durch die neue Datenschutz- Grundverordnung	138
1. Grundlagen	138
a) Zentrale materiell-rechtliche und prozedurale Änderungen	138
b) Zentrale institutionelle Änderungen	139
c) Ausgestaltungsspielräume der Mitgliedstaaten	142
2. Legaldefinition Gesundheitsdaten und genetische Daten	143
3. Auftragsdatenverarbeitung	144
4. Dispens vom Verarbeitungsverbot für sensible Daten und Verarbeitungsbefugnis	148
5. Einwilligung	151
III. Exkurs: Geringe komplementäre Bedeutung des Völkerrechts	152
1. Leitlinien der UN/OECD-Leitlinien	153
2. Datenschutz-Konvention des Europarats	153

E. Grundrechtliche Steuerungsvorgaben	155
I. Unionsgrundrechtliche Vorgaben	155
1. Vertrag von Lissabon	156
a) Art. 7 EU-Charta	156
b) Art. 8 EU-Charta	157
aa) Verhältnis zu Art. 7 EU-Charta	157
bb) Schutzbereich und Eingriff	158
cc) Rechtfertigung	158
dd) EuGH-Urteil zum biometrischen Reisepass	160
2. Resümée und Ausblick	161
II. Exkurs: Vorgaben aus der EMRK	162
1. Art. 8 EMRK	162
2. Wertungen des EGMR	163
III. Deutsche Grundrechte als Steuerungsparameter	164
1. Grundrechte in ihrer abwehrrechtlichen Dimension	164
a) Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG)	164
aa) Grundlagen und Schutzbereich	164
bb) Abwägungstopoi	165
(1) Allgemein	165
(2) Spezifisch gesundheitsrechtliche Dimension	166
(a) Strukturelle Sensibilität	166
(b) Dauerhafte Merkmalskompromittierung	166
cc) Bestimmtheit und Normenklarheit	167
(1) Grundlagen	167
(2) Spezifische Problematik im Gesundheitsrecht	167
dd) Wichtige verfassungsrechtliche Entscheidungen	168
(1) Bürger/Bürger-Verhältnis	169
(2) Bürger/Staat-Verhältnis	169
b) Recht auf Wissen/Recht auf Nichtwissen	171
c) Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	174
aa) Grundlagen	174
bb) Die „E-Card“ als gesundheitsrechtliches Anwendungsfeld?	174
d) Gegenläufige Grundrechtspositionen	176

2. Schutzpflichtendimension	177
a) Grundlagen der Schutzpflichtendogmatik im Datenschutzrecht	177
b) Technische und organisatorische Maßnahmen	179
aa) Verfassungsrechtliche Vorgaben für die Bestimmung von Technikstandards und Rechtsprechung des BVerfG	179
bb) Beispiel E-Card	181
cc) Beispiel Gendiagnostik	182
3. Einwilligung	182
Teil 2: Bereichsspezifisches Gesundheitsdatenschutzrecht	186
A. Gesundheitswesen	
<i>Philipp Kircher</i>	186
I. Das Urteil des BSG vom 10.12.2008	186
II. Rechtsbeziehungen und Datenströme in der Krankenversicherung	187
1. Private Krankenversicherung	187
2. Gesetzliche Krankenversicherung	188
III. Verfassungsrechtliche Kompetenzverteilung	190
1. Sozialversicherung	191
2. Private Krankenversicherung	191
3. Leistungserbringung	192
IV. Überblick über die einfach-rechtlichen Rechtsgrundlagen	196
1. Bundesrecht	196
2. Landesrecht	197
3. Kirchliches Datenschutzrecht	198
V. Identifikation der einschlägigen Rechtsquelle	198
1. Normativer Ausgangspunkt: Das Bundesdatenschutzgesetz	199
a) Öffentliche Stellen	199
aa) Öffentliche Stellen des Bundes	199
bb) Öffentliche Stellen der Länder	199
b) Nicht-öffentliche Stellen	200
2. Die Subsidiarität des Bundesdatenschutzgesetzes	200
a) Landesrecht (§ 1 Abs. 2 Nr. 2 BDSG)	201
b) Bundesrecht (§ 1 Abs. 3 S. 1 BDSG)	202
aa) Vorrang des Sozialdatenschutzrechts	202

bb)	Strafrechtlicher Geheimnisschutz	204
c)	Verschwiegenheitspflichten (§ 1 Abs. 3 S. 2 BDSG)	204
aa)	§ 203 StGB als Pflicht zur Geheimniswahrung	205
bb)	Verhältnis Strafrechtlicher Geheimnisschutz und sonstige Verschwiegenheitspflichten	206
cc)	Sozialgeheimnis	207
d)	Vorrang von Geheimnispflichten nach § 28 Abs. 7 BDSG	208
e)	Kirchliches Datenschutzrecht und andere Rechtsvorschriften	209
3.	Subsidiarität des Sozialdatenschutzes	210
a)	Sozialdatenschutz und fachspezifische Bücher des SGB	211
b)	Sozialdatenschutz und Geheimnispflichten	212
VI.	Zusammenschau	213
VII.	Datenschutz in der Behandlungssituation (Leistungserbringer)	216
1.	Ärzte	217
a)	Datenumgang durch den Arzt und seine Gehilfen	218
b)	Datenübertragung an andere Leistungserbringer	220
aa)	Mitbehandelnde Ärzte	220
bb)	Hausarzt/Facharzt bzw. sonstiger Leistungserbringer und hausarztzentrierte Versorgung (GKV)	220
cc)	Hausarzt/Facharzt bzw. sonstiger Leistungserbringer (PKV)	222
dd)	Konzile und Supervision	223
ee)	Ärztetzwerke	223
ff)	Integrierte Versorgung nach § 140a SGB V	224
gg)	Strukturierte Behandlungsprogramme	225
c)	Einbeziehung Dritter/Outsourcing	227
aa)	Callcenter	228
bb)	EDV-Systemadministration in der Praxis durch Dritte	229
cc)	Abrechnung unter Einbeziehung Dritter (PKV)	230
d)	Abrechnung von Leistungen in der GKV	233
aa)	Abrechnung in der Regelversorgung	234
bb)	Abrechnung ohne Beteiligung der KV	235

cc)	Datenübertragung zur Prüfung späterer Leistungsgewährung	236
e)	Abrechnung von Leistungen in der GKV unter Einbeziehung Dritter	236
aa)	Kritische Würdigung des BSG- Urteils vom 10.12.2008	237
bb)	Gesetzgeberische Reaktion auf das Urteil des BSG vom 10.12.2008	241
cc)	Einbindung nach § 295a SGB V	242
dd)	Ambulante spezialfachärztliche Abrechnung nach § 295 Abs. 5 SGB V	244
2.	Weitere Leistungserbringer	245
a)	Apotheker	245
b)	Hebammen	248
c)	„Sonstige Leistungserbringer“	248
3.	Krankenhäuser	248
a)	Krankenhausverwaltung als Gehilfen	249
b)	Abrechnung im Krankenhaus	249
aa)	Allgemeine Krankenhausbehandlung	249
bb)	Ambulante Versorgung	250
cc)	Einbindung Dritter in die Abrechnung	250
dd)	Ambulante Notfallversorgung	250
4.	Datenschutz bei „Vertragspartnern auf Leistungserbringerseite“	250
5.	Datenschutz beim öffentlichen Leistungserbringer	252
6.	Mitteilung von Krankheitsursachen und drittverursachten Gesundheitsschäden	252
7.	Qualitätssicherung bei Leistungserbringern	254
8.	Ergebnisse	256
VIII.	Datenschutz im Gesundheitswesen (Sozialdaten)	256
1.	Allgemeiner Sozialdatenschutz	257
a)	Zulässigkeit des Datenumgangs	257
aa)	Zulässigkeitsdreiklang / Zweckbindung / Erforderlichkeit	258
bb)	Gesundheitsdaten im Sozialdatenschutzrecht	258
b)	Sozialdatenschutz und bereichsspezifische Sozialdatenschutzregelungen	259
2.	Gesetzliche Krankenversicherung	259
a)	Krankenkassen	260

b) Kassen(zahn)ärztliche Vereinigungen	261
3. Einzelprobleme	262
a) Auskunftsbegehren der Krankenkassen	262
b) Abrechnungsstrukturen	263
c) Finanzierung und Korporatismus	264
d) Gesundheitsfonds und Risikostrukturausgleich	264
e) Qualitätssicherung	266
f) Prüfverfahren	268
aa) Wirtschaftlichkeitsprüfung nach § 106 SGB V	269
bb) Abrechnungsprüfung nach § 106a SGB V	270
cc) Stationäre Qualitäts- und Wirtschaftlichkeitsprüfung nach § 113 SGB V	270
dd) Prüfungen durch den medizinischen Dienst der Krankenversicherung (MDK)	271
g) E-Health	272
h) Die elektronische Gesundheitskarte	273
i) Modellvorhaben	274
4. Vereinzelt Anwendbarkeit des SGB V auf private Krankenversicherer	274
5. Ergebnisse	275
IX. Fazit	276
B. Familie	
<i>Nicolaj Torbohm</i>	278
I. Familie als sozialer und genetischer Tatbestand	278
II. Der Schutz familienrelevanter Gesundheitsdaten	279
1. Schutz durch das BDSG	279
a) Anwendbarkeit	279
b) Übermittlung durch öffentliche Stellen und nicht- öffentliche Stellen	281
2. Schutz durch ärztliches Berufsrecht und die ärztliche Schweigepflicht	284
III. Schutz familienbezogener genetischer Daten	286
1. Schutz durch das GenDG	287
a) Anwendbarkeit und Verhältnis zu anderen Datenschutzregelungen	287
b) Materiell-rechtliche Bestimmungen	289
aa) Diagnostische Untersuchungen	290
bb) Prädiktive Untersuchungen	290

cc)	Vorgeburtliche genetische Untersuchungen	292
c)	Prozedurale Schutzmechanismen	298
aa)	Beratung, Aufklärung, Einwilligung und Widerruf	298
bb)	Aufbewahrungsfristen und Vernichtung der Ergebnisse	302
cc)	Empfehlung der Drittberatung	304
2.	Schutz durch sonstige Rechtsquellen	312
3.	Referenzgebiete	313
a)	Vaterschaftstests	313
aa)	Einleitung	313
bb)	Das Vaterschaftsaufklärungsverfahren, § 1598a BGB	315
cc)	Anforderungen an die genetische Untersuchung, § 17 GenDG	317
dd)	Auskunftspflicht aus Treu und Glauben, § 242 BGB	320
(1)	Anspruch des (Schein)Vaters auf Auskunft über die Person des mutmaßlich biologischen Vaters	320
(2)	Anspruch des biologischen Vaters auf Auskunft über die Person des rechtlichen Vaters	322
(3)	Anspruch des Kindes auf Auskunft über seine genetische Abstammung	322
ee)	Fazit und Kritik	323
b)	Präimplantationsdiagnostik	324
aa)	Einleitung	324
bb)	Überblick über § 3a EsSchG	326
cc)	Organisationsrechtliche und materiell-rechtliche Regelungen	328
(1)	Die Ethikkommissionen	328
(2)	Die PID-Zentren	332
dd)	Prozedurale Regelungen	334
(1)	Das Verfahren in den Ethikkommissionen und ihre Prüfungscompetenz	334
(2)	Aufklärung und Beratung	335
(3)	Datenschutz	336
ee)	Prozessuale Fragen	340

IV. Fazit	342
C. Datenschutz in der medizinischen Forschung	
<i>Nicolaj Torbohm</i>	344
I. Einleitung	344
II. Einfachgesetzliche Datenschutzbestimmungen	344
1. Schutz durch das BDSG	345
a) Forschungsklauseln im BDSG	345
aa) Verarbeitung und Nutzung durch Forschungseinrichtungen	346
bb) Datenerhebung und weitere Verarbeitung zu Forschungszwecken	348
b) Forschung auf Grundlage einer Einwilligung des Betroffenen	350
2. Schutz durch die LDSGe	352
3. Beispiele bereichsspezifischer Regelungen	353
a) Art. 27 Abs. 4 BayKrG	353
b) § 11 BayKRG	356
c) § 40 Abs. 2a i.Vm. § 42 Abs. 2a AMG	357
III. Forschung mit besonderen Arten von Daten	358
1. Forschung mit Sozialdaten	358
a) Forschung durch die Sozialversicherungsträger	358
b) Forschungsvorhaben der Krankenkassen und der Kassenärztlichen Vereinigungen	361
c) Forschung durch andere Institutionen	363
2. Forschung mit genetischen Daten und das Problem der Biobanken	364
IV. Fazit und Ausblick auf die Harmonisierung des Datenschutzrechts durch eine europäische Datenschutz- Grundverordnung	369
D. Private Versicherungsverträge	
<i>Julia Washausen</i>	372
I. Einleitung	372
II. Erheben von Daten beim Versicherungsnehmer	373
1. Anzeigepflichten des Versicherungsnehmers	373
a) Vorvertragliche Datenerhebung	373
aa) Verpflichtung zur Anzeige gefahrerheblicher Umstände, § 19 VVG	373

bb) Besonderheiten bei der Risikoprüfung in der privaten Krankenversicherung	375
b) Gefahrerhöhung, § 23 VVG	376
c) Datenerhebung im Leistungsfall, §§ 30, 31 VVG	377
aa) Anzeigepflicht des Versicherungsnehmers	377
bb) Aushändigung von Krankenunterlagen	378
d) Informationspflichten des Versicherers	379
2. Genetische Untersuchungen	380
a) Verbot nach § 18 Abs. 1 S. 1 GenDG	380
b) Verlangen bzw. Entgegennahme von Dritten	383
c) Ausnahme, § 18 Abs. 1 S. 2 GenDG	384
d) Anzeige von (Vor-)Erkrankungen, § 18 Abs. 2 GenDG	385
3. Weitere Schritte der Datenverarbeitung	385
III. Datenerhebung bei Dritten	386
IV. Beteiligung von Dritten	390
1. Beteiligung Dritter an der Risiko- und Leistungsprüfung	390
a) Versicherungsvermittler	390
b) Beauftragung von externen Dienstleistern	392
c) Einsatz von Detektiven	393
d) Warn- und Hinweisdatenbank der Versicherungswirtschaft	393
e) Datenschutzrechtliche Zulässigkeit	394
aa) Abweichung vom Grundsatz der Direkterhebung	394
bb) Auftragsdatenverarbeitung, § 11 BDSG	395
cc) § 28 BDSG	397
dd) § 29 BDSG	400
2. Datenweitergabe innerhalb verbundener Unternehmen	401
3. Datenübermittlung an Rückversicherer	402
4. Einwilligung in die Datenverarbeitung	403
V. Fazit	406
E. Arbeitsleben	
<i>Julia Washausen</i>	408
I. Rechtsgrundlagen	408
1. Vorschriften des BDSG	409
2. AGG und BGB	410
II. Kollektivrecht und Betriebsrat	411
1. Betriebsvereinbarungen und Tarifverträge	411

2. Rolle des Betriebsrates bei der Datenverarbeitung	413
a) Datenverarbeitung durch den Betriebsrat	413
b) Betriebsrat als Datenschutzbeauftragter	414
III. Datenerhebung	415
1. Eignungsfeststellung	415
a) Fragen des Arbeitgebers	416
b) Backgroundchecks	418
c) Ärztliche, psychologische und genetische Untersuchungen	419
aa) Rolle des Betriebsarztes	419
bb) Ärztliche, psychologische Untersuchungen	421
cc) Genetische Untersuchungen vor und nach Beschäftigungsbeginn	422
dd) Arbeitsmedizinische Vorsorgeuntersuchungen	424
(1) Ärztliche Untersuchungen nach der ArbMedVV und anderen Vorschriften	424
(2) Zulässigkeit genetischer Untersuchungen zur arbeitsmedizinischen Vorsorge	426
(3) Regelungen des BDSG zur Gesundheitsvorsorge	427
2. Arbeitsunfähigkeit des Arbeitnehmers	427
a) Entgeltfortzahlung bei Krankheit	427
b) Schwangerschaft	429
c) Kranken-/Rückkehrgespräche	430
d) Betriebliches Eingliederungsmanagement	430
e) Einsatz von Detektiven	432
IV. Aufbewahrung von Daten: die Personalakte	433
V. Rechte des Arbeitnehmers	434
VI. Öffentlicher Dienst	435
1. Anwendbarkeit der §§ 28 Abs. 2 Nr. 2 und 32-35 BDSG	436
2. Vorrangige Regelungen	437
VII. Fazit	439

Teil 3: Schlussfolgerungen	
<i>Thorsten Kingreen und Jürgen Kühling</i>	440
A. Befund	440
I. Zentrifugaltendenzen im Datenschutzrecht	440
II. Erkenntnisse aus einzelnen Anwendungsfeldern des Gesundheitsdatenschutzrechts	442
1. Gesundheitswesen	442
2. Familie	445
3. Forschung	446
4. Versicherungswesen	447
5. Arbeitsleben	449
B. Rekonstruktion der verfassungsrechtlichen und -dogmatischen Grundlagen des Datenschutzrechts	450
I. Die Reichweite des Parlamentsvorbehalts im Datenschutzrecht	451
1. Konzeptionelle Rückbesinnung auf eine sinnvolle Verrechtlichungsverpflichtung	452
a) Qualifizierter Parlamentsvorbehalt: Notwendigkeit klarer und bestimmter Normen	452
b) Anforderungen an die Normenbestimmtheit und Bereichsspezifität als Quelle des Verrechtlichungsschubs	453
c) Parlamentsvorbehalt auch im Unionsrecht?	456
d) Fazit: begrenzter Anwendungsbereich des qualifizierten Parlamentsvorbehalts	457
2. Wertungswidersprüche zwischen Datenschutz- und Gesundheitsrecht	458
3. Konsequenzen für die Gesetzgebung im Gesundheitsdatenschutzrecht	460
a) Faktische Entgrenzung des qualifizierten Gesetzesvorbehalts im Datenschutzrecht	460
b) Begrenzte Notwendigkeit bereichsspezifischer Regeln	461
c) Weitergehende Reintegration datenschutzrechtlicher Regeln in BDSG und LDSGe	463
d) Begrenzung der Regelungsgehalte in bereichsspezifischen Regeln und Verweise auf BDSG und LDSGe	464

e) Verbesserung der bereichsspezifischen Regeln selbst – Paradigma Abrechnung von Gesundheitsleistungen	465
4. Schlussfolgerungen für die Interpretation des Parlamentsvorbehalts im Gesundheitsdatenschutzrecht	467
II. Verteilung der Gesetzgebungskompetenzen	468
1. Das Problem des fehlenden umfassenden Kompetenztitels auf Bundesebene	468
2. Angemessene Kompetenzausstattung auf Unionsebene	471
C. Ausblick	472
Literaturverzeichnis	475