

Inhaltsverzeichnis

Abkürzungsverzeichnis	27
Einführung	37
A. Chancen	38
B. Risiken	39
C. Spannungsfeld legitimer Interessen	40
D. Interessenausgleich mit Hindernissen	41
E. Lösbarkeit de lege lata oder nur de lege ferenda?	42
F. Gegenstand und Gang der Untersuchung	43
I. Gegenstand der Betrachtung	43
II. Gang der Untersuchung	44
Kapitel 1: Allgemeine Grundsätze	47
A. Begriffliche Vorfragen	47
I. Big Data und Big-Data-Anwendungen	47
1. Ansätze zur Begriffsdefinition	48
a) Schnelle Auswertung großer Mengen heterogener Daten	48
b) Weitere technische Definitionsansätze	49
c) Big-Data-Anwendungen	50
d) Andere Definitionsversuche	52
2. Verortung gegenüber künstlicher Intelligenz	52
3. Zusammenfassung und verbleibende begriffliche Unschärfe	54
II. Gesundheitsdaten	55
1. Grundlegendes Begriffsverständnis, Art. 4 Nr. 15 DS-GVO	55
a) Kumulative Tatbestandsmerkmale der Definitionsnorm	56
aa) Personenbezug	56
bb) Gesundheitsbezug	56

cc) Information über Gesundheitszustand	56
b) ErwG 35 der DS-GVO und EuGH: weites Verständnis	57
c) Abgrenzung zu anderen Datenkategorien des Gesundheitssektors	58
aa) Genetische Daten, Art. 4 Nr. 13 DS-GVO	59
bb) Sozialdaten und Leistungsdaten i.S.d. Sozialdatenschutzrechts	59
cc) Weitere verwandte Begriffe	61
d) Zwischenfazit	62
2. Überflüssigkeit der Differenzierung von Datenkategorien wegen Big Data?	63
a) Problem: Enthüllung von Gesundheitsinformationen durch Masse nicht-sensibler Daten	64
b) Lösungsansatz: Erfassung mittelbarer Gesundheitsbezüge bei gleichzeitiger Begrenzung	65
aa) Figur mittelbarer Gesundheitsdaten	66
bb) Ansätze zur Begrenzung der Reichweite des Gesundheitsdatenbegriffs	67
(1) Subjektive Theorie: „Auswertungsabsicht“	68
(2) Objektive Theorie: „Verwendungszusammenhang“	68
(3) Dritter Ansatz: Ablehnung der Begrenzung	69
(4) Bewertung	70
3. Fazit zum Gesundheitsdatenbegriff und Big Data	71
B. Anwendungsszenarien für Big Data mit Gesundheitsdaten	72
I. Vielfältige potenzielle Datenquellen im Gesundheitsbereich	73
II. Verschiedene Einsatzmöglichkeiten in der Forschung	75
III. Big-Data-Anwendungen in der Behandlungssituation	78
IV. Gesetzliche und private Krankenversicherung	81
V. Public Health und staatliche Stellen	83
VI. Big-Tech und sonstige private Akteure	85
Kapitel 2: Grundrechtliche Rahmenbedingungen im Mehrebenensystem	89
A. Bedeutung der Grundrechte für Big-Data-Anwendungen	90

B. Nebeneinander der Grundrechtsordnungen im Mehrebenensystem	92
I. Einfluss der EMRK	92
II. Weiter Anwendungsbereich der GRCh insbesondere im Datenschutzrecht	94
III. Verbleibender Raum der mitgliedstaatlichen Grundrechte	95
1. Exklusive Wirkung der GRCh mangels mitgliedstaatlicher Umsetzungsspielräume	96
2. Doppelte Grundrechtsbindung im Übrigen	97
a) Spielräume für mitgliedstaatliche Schutzstandards	
nach der Rechtsprechung des EuGH	97
b) Die Bestimmung des Determinierungsgrads	99
c) Vermeintliche Annäherung des BVerfG an den EuGH	99
3. Prüfungsvorbehalte des BVerfG	101
a) Der Solange-II-Vorbehalt	102
b) Kompetenzkontrolle	102
c) Identitätskontrolle	103
4. Bedeutung für den Grundrechtsschutz im Gesundheitsdatenschutzrecht	104
a) DS-GVO als Verordnung mit Hybridcharakter	104
b) Unterschiedliche Grundrechtsbindung je nach Zulässigkeitstatbestand	105
aa) Zulässigkeitstatbestände mit Gestaltungsspielräumen	105
bb) Keine doppelte Grundrechtsbindung bei wiederholtem Wortlaut	106
cc) Zulässigkeitstatbestände ohne Gestaltungsspielräume	107
dd) Zwischenfazit	108
IV. Zusammenfassung und weiterhin offene Fragen	108
C. Das Datenschutzgrundrecht des unionalen Primärrechts	110
I. Rechtsquellen	110
1. Charta-Grundrechte als Anknüpfungspunkt	110
2. Das Verhältnis von Art. 7 und Art. 8 GRCh	111
a) Lex-specialis-Konstellation nach deutschem Grundrechtsverständnis	112
b) Der Ansatz des EuGH	112
c) Fazit	114

II. Anwendungsbereich: personenbezogene Daten	114
III. Verarbeitungsvorgang als Eingriff	115
IV. Rechtfertigung: kein pauschaler Ausschluss von Big Data	116
1. Allgemeine Rechtfertigungsanforderungen	116
2. Big Data im Konflikt mit Zweckbindung und Datenminimierung	118
3. Zwischenfazit: Auflösbarkeit der Zielkonflikte	119
V. Weitere Gewährleistungen	119
VI. Fazit	120
 D. Das Recht auf informationelle Selbstbestimmung der deutschen Verfassung	 120
I. Entwicklung	121
II. Schutzbereich und Eingriff	122
III. Strenger Parlamentsvorbehalt	124
IV. Kriterien der Verhältnismäßigkeitsprüfung und Big Data	126
V. Weitere Gewährleistungen	127
VI. Fazit	128
 E. Weitere relevante Grundrechtspositionen	 128
I. Gesundheitsschutz im Konflikt mit Privatheitsinteressen	128
II. Die Forschungsfreiheit als möglicher Gegenpol zum Datenschutz	130
III. Sonstige Grundrechtspositionen in der Abwägung	131
 F. Zusammenfassung der grundrechtlichen Vorgaben für Big Data im Gesundheitsbereich	 132
 Kapitel 3: Anwendbarkeit des Datenschutzrechts auf Big-Data- Applikationen	 135
 A. Weitreichender räumlicher Anwendungsbereich	 135
 B. Begriffe der Automatisierung und Verarbeitung	 137
I. Verarbeitung	137
II. Grad der Automatisierung	139
III. Bedeutung für Big-Data-Anwendungen	139
 C. Grundlegendes zum Kernkriterium des Personenbezugs	 140
I. Kontinuität zum Personenbezugsbegriff der DSRL	141
II. Tatbestandsmerkmale der Personenbeziehbarkeit von Daten	143
1. Informationen und Daten	143

2. Natürliche Personen	145
3. Bezug zu einer natürlichen Person	146
a) Sachdaten mit oder ohne Bezug zu einer Person	147
b) Allgemeine statistische und aggregierte Aussagen	148
c) Inhalts-, Zweck- oder Ergebniselement	148
d) Eingeschränkte Bedeutung für Big Data	149
4. Identifiziertheit oder Identifizierbarkeit der Person	149
a) Identifizierbarkeit als Risikobewertung	150
aa) Erwägungsgründe als Anknüpfungspunkt der Auslegung	151
bb) Uneinheitlicher Umgang mit Restrisiken in Literatur und Aufsicht	152
cc) Grenzziehung ohne Fehlertoleranz als Schwäche des Konzepts	154
b) Maßstab der Risikobewertung	155
aa) Objektiv-dynamischer Maßstab für technische Identifizierungsmittel	156
bb) Objektiver Maßstab für allgemein verfügbares Wissen	158
cc) Subjektives Element: Spezialwissen Dritter	159
dd) Nur objektives oder auch subjektives Identifizierungsinteresse als Maßstab?	161
III. Anonymität und Pseudonymisierung	162
1. Anonymität und Anonymisierung	163
a) Anonymität als Gegenbegriff zur Personenbezogenheit	163
b) Technologieneutralität auch bei Anonymisierungsverfahren	164
2. Pseudonymisierung und Verschlüsselung	166
3. Sonderfall Hash-Verfahren	168
IV. Zwischenfazit	170
D. Leistungsfähigkeit des Personenbezugsmodells auch für Big Data	172
I. Re-Identifizierung durch Big Data in der Realwelt	173
1. De-anonymisierende Spezifika von Big-Data-Anwendungen	173
2. Weiterhin relevante klassische Re-Identifizierungsszenarien	174

3. Zunehmende Automatisierung und Einbeziehung unstrukturierter Daten	176
II. Datenschutzrechtliche Einordnung	176
1. Von Anfang an identifizierbare Daten	177
2. Nachträglich wieder identifizierbare Daten und damit einhergehende Probleme	178
a) Innovationsbedingte Re-Identifizierung	178
b) Informationsbedingte Re-Identifizierung	179
c) Prüfpflicht außerhalb des Anwendungsbereichs des Datenschutzrechts	179
d) Verbleibende Probleme bei Veröffentlichungen von Daten	179
e) Mögliche Lösungswege	180
f) Zwischenfazit	182
3. Schwächen alternativer Ansätze	182
III. Ergebnis zur Leistungsfähigkeit des Personenbezugsmodells	184
E. Ausnahmen vom Anwendungsbereich	185
I. Haushaltsausnahme	186
II. Strafverfolgung und -vollstreckung sowie Gefahrenabwehr in diesen Bereichen	187
III. Sozialdatenschutz als im Anwendungsbereich des Unionsrechts liegende Materie	188
IV. Fazit: Ausnahmen ohne Bedeutung für Big Data	189
F. Ergebnis zur Anwendbarkeit des Datenschutzrechts auf Big-Data-Anwendungen	190
Kapitel 4: Die Datenschutzgrundsätze des Art. 5 DS-GVO und Big Data – ein Widerspruch?	193
A. Funktionsweise der Datenschutzgrundsätze der DS-GVO	193
B. Für Big Data unproblematische Grundsätze	195
C. Zweckbindung mit variablen Anforderungen	196
I. Funktionsweise des Art. 5 Abs. 1 lit. b DS-GVO	196
II. Zielkonflikt zu der Funktionsweise von Big Data	197

III. Verbleibende Räume für Big-Data-Anwendungen	198
1. Breit gefasste Zweckfestlegung (Broad Consent)	199
a) Allgemeine Anforderungen an die Ausdifferenzierung des Zwecks	199
aa) Bedeutung bei Einwilligungen und anderen Zulässigkeitstatbeständen	200
bb) DS-GVO: explizite Zweckfestlegung	200
cc) Allgemeine Vorgaben der unionalen Aufsicht zur Zweckfestlegung	201
dd) Klare Fälle zu unspezifischer Zwecke	201
b) Ausnahmsweise Verwendung generischer Zwecke im Forschungskontext	202
aa) Auslegungsbedürftigkeit: Widersprüchliche Aufsichtspraxis	203
bb) Wortlaut	204
cc) Systematik	205
dd) Historisch-genetische Gesichtspunkte	206
(1) Broad Consent als Wille des Gesetzgebers nach ErwG 33 der DS-GVO	206
(2) Einschränkende Bedingungen des ErwG 33 der DS-GVO	207
ee) Teleologische und unionsgrundrechtskonforme Auslegung	208
(1) Verbietet das Datenschutzgrundrecht Broad Consent bei Gesundheitsdaten?	209
(2) Forschungsfreiheit und Gesundheitsschutz als Argumente für Broad Consent	211
(3) Dynamische Einwilligung als unzulängliche Alternative für die Forschung	212
(4) Altruistisches Handeln als Ausübung von Selbstbestimmung	213
(5) Information über Zweckoffenheit zur Sicherstellung der Freiwilligkeit	215
ff) Auslegungsergebnis: Broad Consent in Forschung umfassend zulässig	215

c) Auswirkung von Broad Consent auf Big-Data-Anwendungen	216
aa) Datenintegrationszentren deutscher Universitätskliniken	217
bb) Unzulässig unspezifische Verarbeitungszwecke bei Wearables	218
2. Die Möglichkeit der Zweckänderung in der DS-GVO	219
a) Strittige Rechtsfolge der Zweckvereinbarkeit	220
aa) Vereinbarkeitstest als Zulässigkeitstatbestand	220
bb) Vereinbarkeit nur als Aussage über Einhaltung der Zweckbindung	221
cc) Einordnung und Bewertung	222
(1) Missglückter Regelungsansatz	222
(2) Restriktivere Ansicht überzeugt	222
(3) Erhebliche Rechtsunsicherheit bei der anderen Ansicht	223
dd) Zwischenfazit	223
b) Zweckänderung zu privilegierten Zwecken	223
aa) Fiktion der Zweckvereinbarkeit	224
bb) Umfang der Privilegierung	224
(1) Statistische Zwecke im Sinne der DS-GVO	225
(2) Der Forschungsbegriff der DS-GVO	226
cc) Weitere Anforderungen an die privilegierte Zweckänderung	227
c) Erhöhte Anforderungen an Zweckänderungen im Übrigen	227
aa) Vereinbarkeits- oder Kompatibilitätstest nach Art. 6 Abs. 4 DS-GVO	228
bb) Erhebliche Unschärfe der Kriterien	228
d) Bedeutung für Big-Data-Anwendungen	229
aa) Zulässige zweckändernde Verarbeitung von Versorgungsdaten	230
(1) Datentransparenz als Ausgangspunkt für Big-Data-Anwendungen	230
(2) Zweckänderungsvoraussetzungen der DS-GVO für die Datentransparenz	232
(3) Zur anderen Ansicht	233

(4) Zwischenergebnis zum Beispiel der Datentransparenz	234
bb) Rechtswidrige Zweckänderung bei Gesundheits-Apps und in anderen kommerziellen Szenarien	234
IV. Fazit zum Verhältnis von Zweckbindung und Big (Health) Data	235
1. Forschungsfreundliche Ausrichtung des Zweckbindungsgrundsatzes	235
2. Geringere Spielräume im sonstigen Gesundheitsbereich	236
3. Sachgemäßer Rechtsrahmen mit Durchsetzungsdefiziten	237
D. Datenminimierung als Verbot unverhältnismäßig großer Datenmengen	238
I. Funktionsweise des Art. 5 Abs. 1 lit. c DS-GVO	239
1. Datenminimierung als Ausprägung des Verhältnismäßigkeitsprinzips	239
2. Historischer Hintergrund	240
3. Bedeutung für datenschutzrechtlich Verantwortliche	241
II. Zielkonflikt zu Big Data	242
III. Verbleibende Spielräume für Big-Data-Anwendungen	243
1. Abhängigkeit vom Verarbeitungszweck	243
2. Spielräume des Verhältnismäßigkeitsprinzips	244
a) Erforderlichkeit und Angemessenheit der Verarbeitung großer Datenmengen im Einzelfall	244
b) Keine Absolutheit der Kriterien in der Rechtsprechung des EuGH	245
c) Für Forschung oder Versorgung notwendige große Datenmengen	246
IV. Fazit zur Datenminimierung: Beschränkung von Big Data ohne Totalverbot	247
E. Ergebnis zu den Datenschutzgrundsätzen und Big Data	249
I. Ausreichende Spielräume im materiellen Recht	249
II. Nachschärfungsbedarf in Rechtsprechungs- und Aufsichtspraxis	250

Kapitel 5: Zulässigkeit big-data-basierter Verarbeitung von Gesundheitsdaten	253
A. Zulässigkeitstatbestände der DS-GVO und deren Spielräume für Big Data	254
I. Eigenständige Verarbeitungstatbestände im unionalen Sekundärrecht	255
1. Eingeschränkte Bedeutung des Art. 6 Abs. 1 UAbs. 1 DS-GVO für den Untersuchungsgegenstand	255
a) Der Streit um das Verhältnis von Art. 6 und 9 DS-GVO	256
b) Keine Ergebnisrelevanz des Streits	257
c) Zwischenfazit	258
2. Untauglichkeit des Vereinbarkeitstests des Art. 6 Abs. 4 DS-GVO als Rechtsgrundlage	258
3. Einzelfallbezogener Tatbestand des Art. 9 Abs. 2 lit. c DS-GVO	259
4. Selbst veröffentlichte Daten als legale Datenquelle nach Art. 9 Abs. 2 lit. e DS-GVO	260
a) Voraussetzungen der Norm für Big-Data- Anwendungen	260
b) Veröffentlichte Daten aus sozialen Netzwerken als Big- Data-Quelle?	261
c) Beispiel Depressionserkennung mit Social-Media- Bildern	262
d) Fazit	263
5. Datenverarbeitung aufgrund eines (Behandlungs-)Vertrages nach Art. 9 Abs. 2 lit. h Var. 3 i.V.m. Abs. 3 DS-GVO	263
a) Doppelfunktion als eigenständiger Zulässigkeitstatbestand und als Öffnungsklausel	264
b) Voraussetzungen des Zulässigkeitstatbestandes	265
aa) Verarbeitungszwecke des Art. 9 Abs. 2 lit. h DS-GVO	265
bb) Behandlungsvertrag	265
cc) Erforderlichkeit	266
dd) Berufsgeheimnisträger	266
c) Zulässige behandlungsunterstützende Anwendungen	266
d) Grenzen des Zulässigkeitstatbestandes	267

e) Zusammenfassung	268
6. Einwilligung in eine Big-Data-Datenverarbeitung nach Art. 9 Abs. 2 lit. a DS-GVO	268
a) Allgemeine Kritik an der Einwilligung	269
b) Informiertheit	270
aa) Allgemeine Voraussetzungen	271
bb) Problem der Informiertheit bei Big Data	272
(1) Konfliktsituation: Vollständigkeit vs. Lesbarkeit	272
(2) Lösungsansatz	273
(a) Zulässige Vereinfachungen	273
(b) Adäquate Informationsdarstellung	275
cc) Zwischenfazit zur Informiertheit	276
c) Ausdrückliche Willensbekundung	276
d) Zweckbestimmtheit der Einwilligung	278
aa) Allgemeine Voraussetzungen	278
bb) Zielkonflikt von Ergebnisoffenheit bei Big Data und Zweckbestimmtheit	279
(1) Broad Consent bei Datenverarbeitung zu Forschungszwecken	279
(2) Notwendigkeit mehrerer Einwilligungserklärungen im Übrigen	279
e) Freiwilligkeit beim Einsatz von Big-Data-Anwendungen	280
aa) Problem des Ungleichgewichts	282
bb) Beispiel: Big-Data-Anwendungen in der staatlichen Pandemiebekämpfung	283
(1) Big-data-basierte staatliche Kontaktnachverfolgung in der Pandemie	284
(2) Freiwilliges Zusatzangebot zum App-Download in der Pandemie	284
cc) Relatives Koppelungsverbot bei nicht erforderlichen Datenverarbeitungen	285
dd) EuGH: Unfreiwilligkeit bei scheinbarer Koppelung und Beweislast des Verantwortlichen	288

ee)	Alternativangebote zu an Einwilligungen gekoppelte Leistungen	289
	(1) Koppelung bei gleichwertigen Alternativangeboten des Verantwortlichen	289
	(2) Koppelung bei Alternativangeboten auf dem freien Markt	290
	(3) Bezahlmodelle als Alternative zur Datenverarbeitung	291
	(a) Stand der datenschutzrechtlichen Diskussion	292
	(b) Stellungnahme	293
	(4) Bezahlmodelle auch bei Gesundheitsdaten und Big Data?	295
	(a) Argumente gegen die einwilligungsbasierte Kommerzialisierbarkeit von Gesundheitsdaten	296
	(b) Selbstbestimmung als Argument für gewollte Kommerzialisierung	297
	(c) Umgang mit betroffenen Personen, die auf Dienste angewiesen sind	298
	(d) Einschränkungen der Bestimmtheit und Informiertheit	299
ff)	Beispiele: marktmächtige Unternehmen als Verantwortliche	300
gg)	Zwischenfazit zur Freiwilligkeit	302
f)	Praktische Untauglichkeit der Einwilligung bei Sekundärdaten	303
g)	Ergebnis zur Einwilligung	304
7.	Zwischenfazit	306
II.	Weite Ausgestaltung der Öffnungsklauseln im Gesundheitssektor	307
1.	Öffnungsklausel zur Einwilligung, Art. 9 Abs. 2 lit. a DS-GVO	307
	a) Reichweite des Ausschlussrechts der Mitgliedstaaten	308
	b) Modifikation der Einwilligungsbedingungen durch die Mitgliedstaaten	308
	c) Bedeutung für Big-Data-Anwendungen	309

2. Regelungen für Leistungsträger nach Art. 9 Abs. 2 lit. b DS-GVO	310
a) Niedrigschwellige Anforderungen der Öffnungsklausel	311
b) Bedeutung für Big-Data-Anwendungen	311
3. Regelungen für die Leistungserbringer nach Art. 9 Abs. 2 lit. h i.V.m Abs. 3 DS-GVO	312
a) Anforderungen der Öffnungsklausel an mitgliedstaatliches Recht	312
b) Konsequenzen für den Untersuchungsgegenstand	313
4. Rechtsetzungsbefugnis in Bezug auf die öffentliche Gesundheit i.S.v. Art. 9 Abs. 2 lit. i DS-GVO	313
a) Voraussetzungen der Öffnungsklausel	314
b) Big-data-spezifische Implikationen	314
5. Regelungen für die Forschung, Art. 9 Abs. 2 lit. j DS-GVO	315
6. Regelungen bei einem erheblichen öffentlichen Interesse gemäß Art. 9 Abs. 2 lit. g DS-GVO?	316
7. Zusätzliche Bedingungen oder Beschränkungen nach Art. 9 Abs. 4 DS-GVO	316
a) Streit um die Reichweite der Öffnungsklausel	317
b) Konsequenzen für Big-Data-Anwendungen	317
8. Zwischenfazit zu den Spielräumen der Mitgliedstaaten bei Big-Data-Anwendungen	318
III. Fazit zum unionssekundärrechtlichen Zulässigkeitsrahmen für Big Data	319
B. Möglichkeit bereichsspezifischen Unionsrechts	320
I. Sekundärrecht de lege lata mit Berührungspunkten zum Gesundheitsdatenschutzrecht	320
1. Klinische Prüfungen	321
2. Infektionsdatenschutz	322
3. Das neue Datenrecht der EU	323
II. Harmonisierungsperspektive de lege ferenda am Beispiel des europäischen Datenraums	325
1. Die zwei Stoßrichtungen des EHDS-VO-E	326
2. Doppelte kompetenzielle Abstützung	328
3. Potenzial zur persönlichkeitsrechtskonformen Schaffung großer Datensätze	328
4. Ähnlichkeit zu bestehenden Ansätzen	329

5. Ergänzung der Zweckänderungsregelung der DS-GVO	330
6. Verbleibende Risiken bei großen Datensammlungen	331
III. Fazit zum bereichsspezifischen Unionssekundärrecht	331
 C. Spielräume für Big Data innerhalb des deutschen Gesundheitsdatenschutzrechts	332
I. (Fehlende) Systematik des deutschen Gesundheitsdatenschutzrechts	333
1. Zersplittete Gesetzgebungskompetenzen	333
a) Lediglich ungeschriebene Bundeskompetenzen	333
b) Datenschutzrechtliche Kompetenzen im Gesundheitswesen	334
aa) Regelungsbefugnis auf der Leistungsträgerseite	335
bb) Kompetenz bei Datenverarbeitungen durch die Leistungserbringer	335
cc) Strittiger Sonderfall des kirchlichen Gesundheitsdatenschutzrechts	336
c) Weitere Kompetenzverteilung im Gesundheitsdatenschutzrecht	338
d) Zwischenfazit	339
2. Unübersichtliche Vielfalt an Gesetzestexten	339
a) Allgemeines Datenschutzrecht auf Bundes- und Landesebene	340
b) Vielfältiges und heterogenes bereichsspezifisches Recht	340
aa) Das Sozial- und Privatversicherungsdatenschutzrecht	340
bb) Datenschutzgesetzgebung für Krankenhäuser	343
cc) Vielfältige Gesetze für die Forschung mit Gesundheitsdaten	343
dd) Vielzahl weiterer gesundheitsdatenschutzrechtlicher Regelungen	344
ee) Kirchliches Datenschutzrecht	345
c) Parallel zu beachtende Verschwiegenheitspflichten	345
3. Entwicklung der Gesetzgebung	346
a) Anpassung an die DS-GVO	347
b) Fortentwicklung des Sozialdatenschutzrechts im Rahmen der Digitalisierung des Gesundheitswesens	348
c) Zwischenfazit zu den deutschen Reformbestrebungen	350

4. Zusammenfassung zur Systematik des deutschen Gesundheitsdatenschutzrechts	350
II. Big-Data-Tauglichkeit des deutschen allgemeinen Gesundheitsdatenschutzrechts	351
1. Tatbestände des § 22 BDSG	352
a) Tatbestandsvoraussetzungen des § 22 Abs. 1 Nr. 1 lit. b BDSG	353
b) Normwiederholung	353
c) Geringe Spezifität	354
d) Zweiteilung des allgemeinen Datenschutzrechts	355
e) Konsequenzen für Big-Data-Anwendungen aa) Stärken des technologienutralen Ansatzes bb) Umgang mit verbleibender Rechtsunsicherheit	356
2. Zweckänderungsvorschriften der §§ 23 f. BDSG	357
a) Zweckänderungen durch private Stellen	358
b) Zweckänderungen durch staatliche Akteure	358
c) Zwischenfazit	359
3. Tatbestand des § 27 Abs. 1 S. 1 BDSG für die Forschung	359
a) Allgemeine Voraussetzungen	359
b) Verortung im Regelungsgefüge des Forschungs- und Gesundheitsdatenschutzrechts	360
c) Implikationen für die big-data-basierte Forschung mit Gesundheitsdaten aa) Zweckänderung und Anwendbarkeit auf große Datenmengen bb) Problem erheblicher Rechtsunsicherheit cc) Beispielhafte Veranschaulichung des ambivalenten Ergebnisses	361
4. Fazit zum BDSG	365
III. Bereichsspezifisches deutsches Gesundheitsdatenschutzrecht und Big Data	366
1. Datenschutzrechtliche Aspekte deutscher Sozialgesetzgebung	366
a) Hypertrophie, Komplexität und Rechtsunsicherheit	366
b) Stets gegebene Einwilligungsmöglichkeit aa) Unmittelbare Anwendung der DS-GVO bb) Einwilligungsregelungen im allgemeinen Sozialrecht	367
368	368

cc) Deklaratorische Verweise auf die Einwilligung im SGB V	369
dd) Zwischenfazit	369
c) Unübersichtliche Datenzugangsmöglichkeiten für Forschung	370
aa) Datenzugang für Forschende nach dem SGB X	370
bb) Forschungsnutzung nach §§ 287 und 287a SGB V	371
cc) Zwischenergebnis zu den Forschungsdatenzugängen	372
d) Datenspenden nach § 363 SGB V	373
e) Datentransparenz nach den §§ 303a ff. SGB V	374
aa) Eingeschränkte Big-Data-Tauglichkeit der Regelungen	375
bb) Notwendigkeit der vollen Ausschöpfung der Möglichkeiten der §§ 303a ff. SGB V	376
(1) Das strenge Sicherheitskonzept der Datentransparenzvorschriften	376
(2) Grundrechtskonformität	377
(3) Praxistaugliche Nutzung der rechtlichen Möglichkeiten	378
f) Fazit zum Sozialdatenschutzrecht	379
2. Weitere Aspekte bereichsspezifischer Gesetzgebung	380
a) Krankenhauspezifische Landesregelungen	381
b) Krankenhäuser in kirchlicher Trägerschaft	382
c) Infektionsdatenschutzrecht	383
IV. Big-Data-Anwendungen und ärztliche Schweigepflicht	385
V. Fazit zum nationalen Gesundheitsdatenschutzrecht und Big Data	387
1. Zum allgemeinen deutschen Gesundheitsdatenschutzrecht	387
2. Zum bereichsspezifischen Gesundheitsdatenschutzrecht	388
D. Ergebnis zur Zulässigkeit von Big-Data-Anwendungen nach dem deutsch-unionalen Gesundheitsdatenschutzrecht	388
I. Zur unionalen Ebene	389
II. Zur mitgliedstaatlichen Ebene	390

Kapitel 6: Weitere datenschutzrechtliche Anforderungen an Big-Data-Anwendungen	391
A. Verantwortlichkeit und Auftragsverarbeitung bei arbeitsteiligen oder dezentralen Datenverarbeitungen	391
I. Möglichkeiten der Verantwortungsverteilung	392
1. Gemeinsame Verantwortung nach dem Verständnis des EuGH	392
2. Getrennte alleinige Verantwortung	395
3. Auftragsverarbeitung	395
4. Zwischenfazit	396
II. Konsequenzen für Big-Data-Anwendungen im Gesundheitsbereich	397
1. Handlungsbedürfnis und -möglichkeit Verantwortlicher	397
2. Bewertung des Effekts auf Big-Data-Anwendungen	398
B. Rechte der betroffenen Person und Big Data	399
I. Allgemeine Voraussetzungen	399
II. Schwierigkeit bei großen Datenmengen	401
1. Erklärungsbedürftigkeit komplexer Anwendungen	401
2. Große Datenmengen im Randbereich zur Anonymität	401
3. Ansatzpunkte für eine ausgewogene Eingrenzung der Betroffenenrechte bei Big Data	402
a) Weitreichende spezielle Ausnahmen	403
b) Art. 11 DS-GVO als Einschränkung der Betroffenenrechte	403
aa) Art. 11 Abs. 1 DS-GVO und die Informationspflichten	403
bb) Art. 11 Abs. 2 DS-GVO und die Art. 15 ff. DS-GVO	404
III. Fazit zum Verhältnis der Betroffenenrechte zu Big Data	404
C. Systemdatenschutz, Datensicherheit und Datenschutz-Folgenabschätzung	405
I. Anwendbarkeit auf Big Data	406
II. Flexibilität für Verantwortliche	407
III. Ergebnis: Keine innovationshemmende Wirkung	408
D. Aufsicht, Sanktionen und Schadenersatz	408
I. Bußgeldrahmen für Big-Data-Anwendungen	408

II. Schadenersatzforderungen vieler betroffener Personen	410
III. Effekt der Haftungsrisiken auf Big-Data-Anwendungen	411
IV. Wirkung des gegenwärtigen institutionellen Ansatzes	412
1. Weitestgehend funktionale Kooperation auf EU-Ebene	412
2. Weniger stark ausgeprägte nationale Kooperation	413
a) Öffentlichkeitsarbeit im informellen Gremium der DSK	414
b) Zuständigkeitsbündelung ohne gesetzlich vorgeschriebene Kooperation	414
c) Sonderfall länderübergreifender Gesundheitsforschung	415
d) Zwischenfazit zum deutschen institutionellen Datenschutz	416
V. Zusammenfassung zur Aufsicht und Rechtsdurchsetzung	417
 Kapitel 7: Zusammenfassung der Ergebnisse und gesetzgeberischer Handlungsbedarf	419
A. Unionale Ebene	419
I. DS-GVO nachbessern – sinnvoll und realistisch?	419
1. Funktionales Recht de lege lata bei zutreffender Auslegung	419
a) Personenbezugsbegriff ohne genormte Anonymisierung und allgemeines Re-Identifizierungsverbot	420
b) Festhalten am Gesundheitsdatenbegriff	421
c) Keine Abkehr von den Datenschutzgrundsätzen	421
d) Für die Behandlung erforderliche Big-Data-Anwendungen	422
e) Einwilligungsbasierte Zulässigkeit in sinnvollem Maße	422
f) Keine Innovationsfeindlichkeit der weiteren Rahmenbedingungen	423
g) Beibehaltung der Technologieneutralität und Abbau von Unsicherheiten durch Aufsicht und Rechtsprechung	423
2. Sinnvolle Fortentwicklungen	424
a) Abbau der Öffnungsklauseln	424
b) Präzisierungsbedarf bei der Rechtsfolge der Zweckänderungsvorschriften	426

c) Detailoptimierung des Aufsichtskooperationsrahmens	427
3. Geringe kurzfristige Realisierungswahrscheinlichkeit	427
II. Schaffung von speziellem gesundheitsdatenschutzrechtlichem Sekundärrecht	428
B. Mitgliedstaatliche Ebene	428
I. Breite Möglichkeiten <i>de lege lata</i>	429
II. Abbau verbleibender Rechtsunsicherheiten	430
III. Anpassungsbedarf im deutschen Recht	431
1. Komplexitätsreduktion im Sozialdatenschutzrecht	432
2. Vereinheitlichung der Regelungen für Forschung und Krankenhäuser	433
a) Problem uneinheitlicher Vorschriften	433
b) Sinnvolle Zentralisierung des einfachgesetzlichen Rechts	434
Folgerungen und Ausblick	439
Schrifttumsverzeichnis	443