

Inhaltsübersicht

Vorwort	V
Inhaltsverzeichnis	XIII
A. Einführung	1
B. Grundlagen	5
I. Strukturwandel durch big data und AI	5
1. Big data	5
2. Soziale und ökonomische Funktion entscheidend für die rechtliche Strukturierung	6
3. Datenzugang und Datenqualität als Bottleneck	7
4. Angestammte und neuartige Geschäftsmodelle auf unterschiedlichen Marktebenen und mit marktübergreifender Relevanz	9
5. Allgemeingültige Definition von big data und AI weder möglich noch notwendig	11
II. Die immaterialgüter- und datenschutzrechtliche Perspektive: Drei Phasen im Rahmen typischer big data-Sachverhalte	14
1. Ausgangspunkt	14
2. Potenziell relevante materielle und immaterielle Rechtsobjekte in typischen big data-Prozessen	16
III. Identifizierbare Probleme der Datenökonomie und mögliche Lösungsansätze	22
1. Verlagerung und Spezifizierung der Diskussion um die Regulierung der Datenökonomie in den letzten Jahren	22
2. Grundlegende Zielsetzungen	25
3. Konkrete Probleme und immaterialgüterrechtliche Forschungsherausforderungen	30
4. Bedeutung der immaterialgüterrechtlichen Perspektive: „Hin- und Herwandern“ des Blicks	37

C. Der urheberrechtliche Rahmen der Datenwirtschaft	
de lege lata und de lege ferenda	41
I. Überblick	41
II. Urheberrechtlicher Schutz für kreative und investorische Leistungen in der Datenwirtschaft	42
1. Urheberrecht und Leistungsschutz an Datenbanken	42
2. Urheberrechtlicher Computerprogrammschutz	115
III. Bereichsübergreifende Anpassung der allgemeinen urheberrechtlichen Schrankenregelungen an die Belange und Besonderheiten der Datenwirtschaft, insbesondere Text- und Data-Mining	121
1. Die neuen Text- und Data-Mining-Schranken der DSM-RL und bestehender weiterer Reformbedarf	121
2. Unzureichende Absicherungen gegen die Umgehung von Ausnahmen und Schranken in der InfoSoc-RL	125
3. Zusammenfassung und Reformbedarf	126
D. Der patentrechtliche Rahmen der Datenwirtschaft	
de lege lata und de lege ferenda	127
I. Zusätzliche Anreize für Schaffung und Offenlegung wertvoller Datensätze	128
II. Datenformate, Schnittstellen und Rolle des Patentrechts	130
III. Zugang zu Patentlizenzen im Bereich technischer Standards (standardessentielle Patente)	132
IV. Zusammenfassung und Reformbedarf	135
E. Die Relevanz der Trade Secrets-RL für die europäische Datenwirtschaft de lege lata und de lege ferenda	137
I. Schutzgegenstand	138
1. Weite Definition des Geschäftsgesheimnisses	138
2. Anknüpfungspunkte in typischen big data- und Industrie 4.0-Sachverhalten	141
3. Zusammenfassung	155
II. Schutzsubjekt: Inhaberschaft des Geschäftsgesheimnisses	156
1. Ausgangspunkt: Vage Legaldefinition	156
2. Lösungsvorschläge zur rechtssicheren Konkretisierung des Rechtsinhabers	157

	<i>Inhaltsübersicht</i>	IX
III.	Schutzwirkung	163
1.	Grundsatz der Informations(zugangs)freiheit: Rechtmäßiger Erwerb, rechtmäßige Nutzung und Offenlegung	163
2.	Schutz vor bestimmten Verletzungshandlungen	168
IV.	Ausnahmen	177
1.	Abwägung mit dem Recht der freien Meinungsäußerung und der Informationsfreiheit	177
2.	Whistleblowing-Ausnahme	178
3.	Sonstige legitime Interessen	181
V.	Flexible Durchsetzungsvorschriften	182
VI.	Zusammenfassung und Reformbedarf	184
F.	Datenschutz und DSGVO	191
I.	Ausgangspunkt: Freier Datenverkehr vs. Schutz des Einzelnen . .	193
1.	Regelungsziele der Datenschutzgrundverordnung	194
2.	Datenschutzrecht als Ausschließlichkeitsrecht für personenbezogene Daten?	197
II.	Spannungsverhältnis zwischen big data und Datenschutz	199
1.	Veränderte Verarbeitungsprozesse durch big data	199
2.	Datenschutzrechtliche Interessenslage bei big data	201
III.	Anwendungsbereich der DSGVO in big data-Sachverhalten	205
1.	Gegenstand: Verarbeitung personenbezogener Daten	205
2.	Besondere Arten personenbezogener Daten	209
3.	Anonymisierte Daten	214
IV.	Grenzüberschreitender Datenverkehr	227
1.	Territorialer Anwendungsbereich der DSGVO	227
2.	Voraussetzungen der DSGVO für den Datentransfer in Drittstaaten	230
V.	An der Datenverarbeitung Beteiligte:	
	Verantwortliche – Auftragsverarbeiter – Betroffene	239
1.	Verantwortlicher vs. Betroffener	239
2.	Gemeinsame Verantwortlichkeit (Joint Controllership)	240
VI.	Grundvoraussetzung: Rechtmäßigkeit der Datenverarbeitung . . .	247
1.	Erforderlichkeit der Festlegung einer spezifischen Verarbeitungsgrundlage	247
2.	Einwilligung des Betroffenen	248
3.	Berechtigte Interessen des Verantwortlichen	275
4.	Möglichkeiten der Zweckänderung einer Datenverarbeitung . .	282
5.	Zusammenfassung und Reformbedarf	291

VII.	Betroffenenrechte	294
1.	Allgemeine Vorgaben für die Betroffenenrechte	295
2.	Betroffenenrechte – entgrenzte Pflichten oder Verhältnismäßigkeit?	295
3.	Auskunftsrecht	296
4.	Recht auf Löschung („Recht auf Vergessenwerden“)	307
5.	Recht auf Berichtigung	315
6.	Datenportabilität gemäß Art. 20 DSGVO	315
7.	Zusammenfassung und Reformbedarf	351
VIII.	Risikobasierter Ansatz der DSGVO – Chance oder Bürde für big data?	353
1.	Allgemeine Pflicht zur Datenschutzfolgenabschätzung?	354
2.	Privacy by design und privacy by default – Umsetzbarkeit bei big data?	358
3.	Technische und organisatorische Maßnahmen als Mittel der Risikominimierung?	362
4.	Berücksichtigung der Unternehmensgröße?	363
5.	Zusammenfassung und Reformbedarf	364
IX.	DSGVO und „Künstliche Intelligenz“: Verbot der automatisierten Einzelentscheidung	364
1.	Voraussetzung: Ausschließlich auf automatisierter Datenverarbeitung beruhende Entscheidung	365
2.	Unmittelbare rechtliche Wirkung oder vergleichbare erhebliche Beeinträchtigung	366
3.	Erlaubnistatbestände des Art. 22 Abs. 2 DSGVO	369
4.	Umfang der Informations- und Auskunftspflichten bei automatisierten Einzelentscheidungen	370
5.	Zusammenfassung und Reformbedarf	375
X.	Datenschutzverstöße: Remedies – Enforcement – Accountability	379
1.	Grundproblem 1: Zentralisierte Verantwortlichkeit bei dezentralisierter Verarbeitung	380
2.	Grundproblem 2: Inkohärente Bewertung durch mitgliedstaatliche Datenschutzbehörden	381
3.	Anspruch auf Schadensersatz bei Datenschutzverstößen	381
4.	Bußgelder und sonstige Sanktionen für Datenschutzverstöße	383
5.	Privatrechtliche Durchsetzung der DSGVO?	384
XI.	Bereichsspezifische Sonderregeln des Datenschutzrechts, insbesondere ePrivacy-RL	389
XII.	Ausblick: Funktionale Schwächen der angestammten Datenschutzkonzeption und mögliche alternative Lösungsansätze	391

1. Überlegungen zu weitergehenden Rechten zum Schutz der Privatsphäre?	391
2. Vertragsrecht als Lösung	394
XIII. Zusammenfassung und Reformbedarf	401
G. Reformperspektive: Immaterialgüter- und datenschutzrechtliche Probleme, Trends und Building Blocks für die Datenökonomie	409
I. Möglicher Überschutz und Transaktionskosten	409
1. Anreizgedanke für Datenproduktion und effiziente Datendissemination als inhärente Grenze des Schutzgegenstands	409
2. Funktionale Grenzen zentralisierter Ausschließlichkeitsrechte in big data-Szenarien und besondere Bedeutung des Vertragsrechts	411
3. Schutzrechtsüberschneidung als Problem für Datenzugang . . .	414
4. Trend <i>de lege ferenda</i> : Sinkende Schutzfristen und langfristig wachsende Bedeutung von Registerrechten	417
II. Flexible Hybride zwischen Ausschließlichkeitsrecht und verhaltensbezogener Regelung: Begrenzte Drittirkung vertraglicher Vereinbarungen als Paradigma für die Datenökonomie?	420
1. Kommerzialisierung von Daten und der immaterialgüterrechtliche und datenschutzrechtliche Rahmen . .	420
2. Qualifizierte Drittirkung vertraglicher Vereinbarungen in Anlehnung an den Geschäftsgeheimnisschutz?	422
3. Mögliche lauterkeitsrechtliche Ansätze <i>de lege lata</i> und <i>de lege ferenda</i> ?	426
III. Neue Zugangsrechte in der Datenökonomie, Datenportabilität und die Schnittstelle zum Immaterialgüter- und Datenschutzrecht . .	428
1. Verlagerung der Diskussion in Richtung (bereichsspezifischer) Zugangsrechte	428
2. Die Unterscheidung von Zugangsrechten und Nutzungsmöglichkeiten und -rechten	429
3. Relevante Szenarien für Zugangsrechte und die Schnittstelle zum Immaterialgüterrecht hinsichtlich der Nutzungsregelung . .	435
4. Portabilität und Interoperabilität	457
Literaturverzeichnis	461
Sachregister	495

Inhaltsverzeichnis

Vorwort	V
Inhaltsübersicht	VII
A. Einführung	1
B. Grundlagen	5
I. Strukturwandel durch big data und AI	5
1. Big data	5
2. Soziale und ökonomische Funktion entscheidend für die rechtliche Strukturierung	6
3. Datenzugang und Datenqualität als Bottleneck	7
4. Angestammte und neuartige Geschäftsmodelle auf unterschiedlichen Marktebenen und mit marktübergreifender Relevanz	9
5. Allgemeingültige Definition von big data und AI weder möglich noch notwendig	11
II. Die immaterialgüter- und datenschutzrechtliche Perspektive: Drei Phasen im Rahmen typischer big data-Sachverhalte	14
1. Ausgangspunkt	14
2. Potenziell relevante materielle und immaterielle Rechtsobjekte in typischen big data-Prozessen	16
a) Erste Phase: Datenbeschaffung (gegebenenfalls inkl. Datenvalidierung)	17
b) Zweite Phase: Datenanalyse (gegebenenfalls inkl. Datenvalidierung)	19
c) Dritte Phase: Umgang mit den Ergebnissen der Analyse (inkl. Präsentation)	21
III. Identifizierbare Probleme der Datenökonomie und mögliche Lösungsansätze	22
1. Verlagerung und Spezifizierung der Diskussion um die Regulierung der Datenökonomie in den letzten Jahren	22

2. Grundlegende Zielsetzungen	25
a) Wirksamer Wettbewerb und Wahrung von Privatautonomie	26
b) Innovationsförderung	27
c) Wahrung grundrechtlich besonders geschützter Rechtspositionen	28
d) Wahrung öffentlicher Interessen	29
3. Konkrete Probleme und immaterialgüterrechtliche Forschungsherausforderungen	30
a) Möglicher Überschutz und Transaktionskosten	31
b) Mögliche Schwächen des derzeitigen rechtlichen und technischen Rahmens für den Zugang zu und die Teilung von Daten	32
aa) Institutionen für wettbewerbsbasierte Datenverbreitung und -nutzung	32
bb) Technische und organisatorische Standards für die Datenverarbeitung und Schnittstelle für Datenaustausch (Infrastrukturebene)	33
c) Neue bereichsspezifische Zugangsrechte in der Datenökonomie und Datenportabilität	35
4. Bedeutung der immaterialgüterrechtlichen Perspektive: „Hin- und Herwandern“ des Blicks	37
 C. Der urheberrechtliche Rahmen der Datenwirtschaft	
de lege lata und de lege ferenda	41
I. Überblick	41
II. Urheberrechtlicher Schutz für kreative und investorische Leistungen in der Datenwirtschaft	42
1. Urheberrecht und Leistungsschutz an Datenbanken	42
a) Allgemeine Voraussetzungen	42
b) Urheberrechtlicher Datenbankwerkschutz	46
aa) Besondere Schutzworaussetzung: Eigene geistige Schöpfung	46
bb) Schutzmumfang und Schranken	52
(1) Datenbankstruktur als Schutzgegenstand: Begrenzung auf strukturrelevante Nutzungen	52
(2) Technisch notwendige Vervielfältigung der Datenbankstruktur als Voraussetzung der Datennutzung	53
(3) Nutzung der Datenbankstruktur und resultierende Probleme für die Datenwirtschaft	54

(a) Problem: Urheberpersönlichkeitsrechte, insbesondere Entstellungsschutz sowie Änderungsverbot	55
(b) Problem: Datenbankstruktur als Industriestandard und Reformbedarf auf der Ebene des Schutzgegenstands?	56
(c) Problem: Herstellung von Interoperabilität und Datenportabilität und Reformbedarf im Bereich der Schranken	58
cc) Zusammenfassung und Reformbedarf	59
c) Datenbankschutz sui generis	62
aa) Besondere Schutzworaussetzung: Wesentliche Investition	62
(1) Wesentlichkeitskriterium als de minimis-Schwelle . .	62
(2) Investitionen in das „Beschaffen“ der Datenbankinhalte	64
(a) Restriktive Interpretation der Kommission und der überwiegenden Literatur	64
(b) Gebotene teleologische Interpretation der Abgrenzungskriterien „Beschaffen“ vs. „Erzeugen“ (teleologischer BHB/Hill-Test)	65
(c) Typische Szenarien in der Datenwirtschaft	68
(aa) Zurverfügungstellung von Daten insbesondere durch Nutzer von Dienstleistungen (<i>volunteered data</i>)	68
(bb) Betriebsdaten im engeren Sinne und Datenerhebung bei Gelegenheit des Betriebs einer Maschine im weiteren Sinne (<i>observed data</i>)	69
(cc) Derivative Daten (<i>inferred data</i>)	72
(dd) Metadaten	74
(ee) Alternative Gestaltungsmodelle	75
(3) Weitere Anknüpfungspunkte für berücksichtigungsfähige Investitionen in typischen big data-Sachverhalten	76
(4) Ausschluss typischer big data-Datenbanken nach der spin off-Theorie?	78
(5) Zusammenfassung und Reformbedarf	80
bb) Ausschließlichkeitsrechte des Datenbankherstellers . . .	82
(1) Weite Auslegung der „Entnahme“ oder „Weiterverwendung“	82

(2) Begrenzung des Schutzgegenstands auf wesentliche Teile einer Datenbank	84
cc) Inhaberschaft des <i>sui generis</i> -Rechts	85
(1) Ausgangspunkt: Der Begriff des Datenbankherstellers und die vage Konkretisierung in Erwägungsgrund 41 S. 2 Datenbank-RL	85
(2) Resultierender Reformbedarf: Primat des Vertragsrechts	88
dd) Schranken (Ausnahmen) des Datenbankherstellerrechts	91
(1) Fehlende Kohärenz mit dem allgemeinen Urheberrecht	92
(2) Fehlende systematische Kohärenz mit dem Datenbankurheberrecht und Sonderproblem bei public sector information (PSI)	93
(3) Zusammenfassung und Reformbedarf	95
ee) Schutzdauer	96
(1) Angemessenheit der fünfzehnjährigen Schutzfrist	96
(2) Begründung einer eigenen Schutzdauer für Neuinvestitionen	96
(a) Ausgangspunkt und Begriff der Neuinvestitionen	96
(b) Schutzmfang des <i>sui generis</i> -Rechts an der „veränderten“ Datenbank	97
(3) Verbleibende Probleme und Lösungsmöglichkeiten de lege ferenda	98
(a) Ewigkeitsschutz bei dauernd aktualisierten Datenbanken	98
(b) Nachweis- bzw. Nutzungsschwierigkeiten bei Teiländerungen	98
ff) Umwandlung des <i>sui generis</i> -Schutzrechts in ein Registerrecht	100
(1) Vorschläge zur Umwandlung in ein Registerrecht und kritische Bewertung	100
(2) Möglichkeiten der praktischen Umsetzung	104
(a) Beschreibung und Glaubhaftmachung des Datenbankinhalts	104
(b) Hinterlegung des gesamten Datenbankinhalts	105
(c) Hinterlegung des Hashwerts (kryptographischer Zeitstempeldienst)	106
(d) Vorzugswürdige praktische Umsetzung und Grenzen	108
gg) Verhältnis zu lauterkeitsrechtlichem Leistungsschutz in den Mitgliedstaaten	110

hh) Verallgemeinerung: Abgrenzung zu anderen Rechtsinstrumenten	112
ii) Zusammenfassung und Reformbedarf	112
2. Urheberrechtlicher Computerprogrammschutz	115
a) Schutzworaussetzungen und Schutzgegenstand	115
b) Schutzmfang: Persönlichkeitsrechte und Verwertungsrechte	118
c) Schranken (Ausnahmen) vom urheberrechtlichen Schutz für Computerprogramme	119
III. Bereichsübergreifende Anpassung der allgemeinen urheberrechtlichen Schrankenregelungen an die Belange und Besonderheiten der Datenwirtschaft, insbesondere Text- und Data-Mining	121
1. Die neuen Text- und Data-Mining-Schranken der DSM-RL und bestehender weiterer Reformbedarf	121
2. Unzureichende Absicherungen gegen die Umgehung von Ausnahmen und Schranken in der InfoSoc-RL	125
a) Umgehung durch technische Schutzmaßnahmen (TPM)	125
b) Umgehung der Ausnahmen durch privatautonome Gestaltungen	125
3. Zusammenfassung und Reformbedarf	126
 D. Der patentrechtliche Rahmen der Datenwirtschaft de lege lata und de lege ferenda	127
I. Zusätzliche Anreize für Schaffung und Offenlegung wertvoller Datensätze	128
II. Datenformate, Schnittstellen und Rolle des Patentrechts	130
III. Zugang zu Patentlizenzen im Bereich technischer Standards (standardessentielle Patente)	132
IV. Zusammenfassung und Reformbedarf	135
 E. Die Relevanz der Trade Secrets-RL für die europäische Datenwirtschaft de lege lata und de lege ferenda	137
I. Schutzgegenstand	138
1. Weite Definition des Geschäftsgeheimnisses	138
2. Anknüpfungspunkte in typischen big data- und Industrie 4.0-Sachverhalten	141
a) Einzeldatum	142
b) Datensets	144

aa) Kommerzieller Wert	144
bb) Ausschluss belangloser Informationen	145
cc) Geheimer Charakter	146
dd) Angemessene Geheimhaltungsmaßnahmen	149
ee) Zusammenfassung	151
c) Algorithmen	151
d) Neuronale Netze und separat gespeicherte Gewichtungsmatrizen	153
e) Private Blockchains	153
f) Software-Implementierungen	153
g) „Negative Informationen“	154
3. Zusammenfassung	155
II. Schutzsubjekt: Inhaberschaft des Geschäftsgeheimnisses	156
1. Ausgangspunkt: Vage Legaldefinition	156
2. Lösungsvorschläge zur rechtssicheren Konkretisierung des Rechtsinhabers	157
a) Rechtssicherheit durch privat- und parteiautonome Regelungen	157
b) Fakultative Registrierung im „Geheimnisschutzregister“	159
III. Schutzwirkung	163
1. Grundsatz der Informations(zugangs)freiheit: Rechtmäßiger Erwerb, rechtmäßige Nutzung und Offenlegung	163
2. Schutz vor bestimmten Verletzungshandlungen	168
a) Rechtswidriger Erwerb	169
b) Rechtswidrige Nutzung oder Offenlegung	170
c) Erwerb, Nutzung und Offenlegung durch Dritte – Begrenzte Drittewirkung	174
d) Rechtsverletzende Produkte	176
IV. Ausnahmen	177
1. Abwägung mit dem Recht der freien Meinungsäußerung und der Informationsfreiheit	177
2. Whistleblowing-Ausnahme	178
3. Sonstige legitime Interessen	181
V. Flexible Durchsetzungsvorschriften	182
VI. Zusammenfassung und Reformbedarf	184
 F. Datenschutz und DSGVO	191
I. Ausgangspunkt: Freier Datenverkehr vs. Schutz des Einzelnen	193
1. Regelungsziele der Datenschutzgrundverordnung	194
a) Schutz personenbezogener Daten	194

	<i>Inhaltsverzeichnis</i>	XIX
b)	Gewährleistung freien Datenverkehrs	195
2.	Datenschutzrecht als Ausschließlichkeitsrecht für personenbezogene Daten?	197
II.	Spannungsverhältnis zwischen big data und Datenschutz	199
1.	Veränderte Verarbeitungsprozesse durch big data	199
2.	Datenschutzrechtliche Interessenlage bei big data	201
	a) Interessen der Wettbewerber auf Datenmärkten	201
	b) Interessen der Marktgegenseite (Kunden und Verbraucher) . .	203
	c) Interessen der Öffentlichkeit bzw. Allgemeinheit	204
III.	Anwendungsbereich der DSGVO in big data-Sachverhalten	205
1.	Gegenstand: Verarbeitung personenbezogener Daten	205
	a) Begriff der personenbezogenen Daten	205
	b) Pseudonymisierung und Verschlüsselung	208
2.	Besondere Arten personenbezogener Daten	209
	a) Grundsatz des Verarbeitungsverbots	210
	b) Einwilligung in die Verarbeitung besonderer Arten personenbezogener Daten	211
	c) Ausnahme vom Verarbeitungsverbot: Öffentlich zugänglich gemachte Daten	213
3.	Anonymisierte Daten	214
	a) Vorgaben der DSGVO zur Anonymisierung	215
	b) Probleme der Anonymisierung bei big data	216
	aa) Gefahr der Re-Identifizierung	216
	bb) Folgen nachträglicher Identifizierung bzw. unzureichender Anonymisierung	217
	c) Probleme rein technischer Anonymisierungsverfahren . . .	218
	d) Weitergehende technische und organisatorische Maßnahmen – best practices und Standards	219
	e) Rechts- und Interessenausgleich: Widerlegliche Vermutung der Anonymisierung	219
	aa) Vergleichbare Ansätze weltweit	220
	bb) Umsetzung in der EU	222
	cc) Interimslösungen für Anonymisierung	224
	f) Art. 11 DSGVO als Ansatzpunkt?	224
	g) Ausnahmetatbestand für vorübergehende Datenspeicherung zu Anonymisierungszwecken?	225
	h) Zusammenfassung und Reformbedarf	225
IV.	Grenzüberschreitender Datenverkehr	227
1.	Territorialer Anwendungsbereich der DSGVO	227

a) Weitreichende Geltung der DSGVO für Stellen außerhalb der EU	227
b) Einschränkung der Reichweite auf Ebene der Betroffenenrechte	228
2. Voraussetzungen der DSGVO für den Datentransfer	
in Drittstaaten	230
a) Angemessenheitsbeschluss	231
b) Geeignete Garantien	232
aa) Standardvertragsklauseln (SCC)	233
bb) Binding Corporate Rules (BCR)	235
cc) Codes of conduct	235
dd) Zertifizierung	236
c) Ausnahmetatbestände des Art. 49 DSGVO:	
Beschränkte Reichweite	237
aa) Ausdrückliche Einwilligung in den Datentransfer	237
bb) Zur Vertragserfüllung erforderlicher Datentransfer und zwingendes berechtigtes Interesse	238
d) Bewertung und Folgerungen	239
V. An der Datenverarbeitung Beteiligte:	
Verantwortliche – Auftragsverarbeiter – Betroffene	239
1. Verantwortlicher vs. Betroffener	239
2. Gemeinsame Verantwortlichkeit (Joint Controllership)	240
a) Voraussetzungen der gemeinsamen Verantwortlichkeit	242
b) Folge der gemeinsamen Verantwortlichkeit: Klar abgegrenzte Verantwortungsbereiche?	243
c) Abgrenzung der gemeinsamen Verantwortlichkeit von der Auftragsverarbeitung	245
d) Weitere Konstellationen	246
VI. Grundvoraussetzung: Rechtmäßigkeit der Datenverarbeitung	247
1. Erforderlichkeit der Festlegung einer spezifischen Verarbeitungsgrundlage	247
2. Einwilligung des Betroffenen	248
a) Bedeutung der Einwilligung	248
b) Grundproblem: Einwilligung bei multipolaren Strukturen	250
c) Voraussetzungen einer wirksamen Einwilligung im Datenschutzrecht	252
aa) Freiwilligkeit der Einwilligung	252
(1) Unterschiedliche Auslegung der Freiwilligkeit in den Mitgliedstaaten	252

(2) Spannungsverhältnis zwischen Freiwilligkeit der Einwilligung und Vertragsrecht: „Dienste gegen Daten“	253
(a) Hintergrund	253
(b) Freiwilligkeit der Einwilligung bei „Diensten gegen Daten“?	256
(c) Andere Verarbeitungsgrundlagen für Fälle von „Diensten gegen Daten“?	258
(d) Bewertung und Folgerungen	260
bb) Bestimmtheit der Einwilligung	260
cc) Informierte Einwilligung	261
dd) Unmissverständlichkeit der Einwilligung	263
ee) Abgrenzung der Einwilligung von erforderlicher Datenverarbeitung gemäß Art. 6 Abs. 1 lit. b DSGVO	264
ff) Bewertung und Folgerungen	267
d) AGB-rechtliche Kontrolle der Einwilligungserklärung	268
e) Widerruf der Einwilligung	269
f) Zusammenfassung und Reformbedarf	273
3. Berechtigte Interessen des Verantwortlichen	275
a) Bedeutung der Interessenabwägung	275
b) Struktur der Interessenabwägung	276
c) Interessenabwägung im engeren Sinne	277
aa) Interessen des Verantwortlichen	277
bb) Interessen des Betroffenen	278
d) Widerspruchsrecht des Betroffenen	279
e) Bewertung und Folgerungen	280
4. Möglichkeiten der Zweckänderung einer Datenverarbeitung	282
a) Exkurs: Spannungsverhältnis zwischen Grundsätzen des Datenschutzes und big data	282
b) Zweckbindung vs. Zweckänderung	283
aa) Einwilligung in die Zweckänderung der Datenverarbeitung	285
bb) Erlaubte Zweckänderung bei Kompatibilität der Verarbeitungszwecke	285
cc) Privilegierung der Zweckänderung bei Forschungszwecken bzw. statistischen Zwecken	287
c) Bewertung und Folgerungen	290
5. Zusammenfassung und Reformbedarf	291
VII. Betroffenenrechte	294
1. Allgemeine Vorgaben für die Betroffenenrechte	295

2. Betroffenenrechte – entgrenzte Pflichten oder Verhältnismäßigkeit?	295
3. Auskunftsrecht	296
a) Reichweite des Auskunftsrechts	296
aa) Nur Auskunft oder Recht auf Kopie?	296
bb) Erforderlicher Umfang der Auskunft	299
cc) Sonderfall: Auskunft bei automatisierten Entscheidungen, insbesondere Scoring	300
b) Einschränkungen des Auskunftsrechts bei Datenverarbeitung zu Forschungszwecken	301
c) Einschränkung des Auskunftsrechts durch Interessenabwägung	301
aa) Geschäftsgeheimnisschutz vs. Auskunftsinteresse des Berechtigten	302
bb) Rechte des geistigen Eigentums vs. Auskunftsinteresse des Berechtigten	304
cc) Auskunftsinteresse bei Daten Dritter?	304
dd) Auskunftsinteresse bei nicht identifizierbaren Betroffenen?	305
ee) Folgen für Auskunftserteilung	305
d) Bewertung und Folgerungen	306
4. Recht auf Löschung („Recht auf Vergessenwerden“)	307
a) Recht auf Löschung – Pflicht zur Löschung	307
b) Technische Alternativen zur Löschung?	308
c) Einschränkungen der Löschpflicht des Verantwortlichen	310
d) Sonderfall: Recht auf Löschung bzw. Vergessenwerden bei Suchmaschinen	311
e) Löschpflichten und „künstliche Intelligenz“	313
5. Recht auf Berichtigung	315
6. Datenportabilität gemäß Art. 20 DSGVO	315
a) Vom Portabilitätsrecht betroffene Datenverarbeitungen	315
b) Sinn und Zweck des Portabilitätsrechts	316
c) Gegenstand des Portabilitätsrechts: Bereitgestellte Daten	318
d) Form der zu portierenden Daten	320
aa) Strukturiertes, gängiges und maschinenlesbares Format	320
bb) Spezialfall: Datenübermittlung an andere Anbieter	321
e) Technische Umsetzungsansätze für das Portabilitätsrecht	322
f) Bestehende Ansätze für die praktische Umsetzung des Portabilitätsrechts	324
aa) Mittel zur effektiven Durchsetzung des Portabilitätsrechts	325
(1) Art. 20 DSGVO als Marktverhaltensregelung	325
(2) Übertragbarkeit des Portabilitätsrechts	326

bb) Übertragungs- und Exporttools	327
cc) Personal Information Management-Systeme und user centric approach	327
dd) Single sign on-Dienste	330
ee) Branchenspezifische Lösungen und Datentreuhändermodelle	331
ff) Datenverwertungsgesellschaften und gerätebasierte Datenverwaltung	332
gg) Bewertung und Folgerungen: Bedeutung von Datenintermediären	333
g) Einschränkung des Portabilitätsrechts durch Interessenabwägung	333
aa) Herausgabe von Daten Dritter?	333
bb) Geschäftsgeheimnisschutz vs. Interesse des Betroffenen	335
cc) Rechte des geistigen Eigentums vs. Interesse des Betroffenen	336
dd) Nutzungsziel als Abgrenzungskriterium für die herauszugebenden Daten?	338
ee) Weitere Einschränkungen des Portabilitätsrechts?	339
h) Datenportabilität gemäß Art. 16 Abs. 4 Digitale Inhalte-RL .	339
i) Verallgemeinerungsfähigkeit des Rechts auf Datenportabilität?	342
j) Bewertung und Folgerungen	347
7. Zusammenfassung und Reformbedarf	351
VIII. Risikobasierter Ansatz der DSGVO – Chance oder Bürde für big data?	353
1. Allgemeine Pflicht zur Datenschutzfolgenabschätzung?	354
a) Erforderlichkeit einer Datenschutzfolgenabschätzung	354
b) Kriterien für die Risikobewertung	355
c) Leitlinien der Datenschutzbehörden	356
d) Problem: Zentralisierte Risikobewertung bei dezentralisierter Datenverarbeitung	357
e) Bewertung und Folgerungen	358
2. Privacy by design und privacy by default – Umsetzbarkeit bei big data?	358
3. Technische und organisatorische Maßnahmen als Mittel der Risikominimierung?	362
4. Berücksichtigung der Unternehmensgröße?	363
5. Zusammenfassung und Reformbedarf	364
IX. DSGVO und „Künstliche Intelligenz“: Verbot der automatisierten Einzelentscheidung	364

1.	Voraussetzung: Ausschließlich auf automatisierter Datenverarbeitung beruhende Entscheidung	365
2.	Unmittelbare rechtliche Wirkung oder vergleichbare erhebliche Beeinträchtigung	366
	a) Allgemeine Anforderungen an rechtliche Wirkung und erhebliche Beeinträchtigung	366
	b) Einzelfälle rechtlicher Wirkung und erheblicher Beeinträchtigung	367
3.	Erlaubnistatbestände des Art. 22 Abs. 2 DSGVO	369
4.	Umfang der Informations- und Auskunftspflichten bei automatisierten Einzelentscheidungen	370
	a) Offenlegung von Algorithmen und Formeln?	370
	b) Offenlegung konkret getroffener Einzelentscheidung?	372
	c) Erforderlichkeit geeigneter Maßnahmen und Garantien	373
5.	Zusammenfassung und Reformbedarf	375
	a) Verbot automatisierter Einzelentscheidungen im System der DSGVO	375
	b) Keine datenschutzrechtlichen Offenlegungspflichten	376
	c) Algorithmenregulierung: Kein primärer Gegenstand des Datenschutzrechts	376
X.	Datenschutzverstöße: Remedies – Enforcement – Accountability .	379
1.	Grundproblem 1: Zentralisierte Verantwortlichkeit bei dezentralisierter Verarbeitung	380
2.	Grundproblem 2: Inkohärente Bewertung durch mitgliedstaatliche Datenschutzbehörden	381
3.	Anspruch auf Schadensersatz bei Datenschutzverstößen	381
4.	Bußgelder und sonstige Sanktionen für Datenschutzverstöße	383
5.	Privatrechtliche Durchsetzung der DSGVO?	384
	a) Durchsetzung im Wege des Rechts des unlauteren Wettbewerbs?	384
	b) Durchsetzung im Wege des Kartellrechts?	386
XI.	Bereichsspezifische Sonderregeln des Datenschutzrechts, insbesondere ePrivacy-RL	389
XII.	Ausblick: Funktionale Schwächen der angestammten Datenschutzkonzeption und mögliche alternative Lösungsansätze	391
1.	Überlegungen zu weitergehenden Rechten zum Schutz der Privatsphäre?	391
2.	Vertragsrecht als Lösung	394
	a) Bedeutung des AGB-Rechts	394
	b) Transparenz als allgemeiner Wertungsmaßstab	394

c) Wechselspiel zwischen datenschutzrechtlichen Vorgaben und Vertragsbedingungen	395	
d) Standardverträge und Selbstverpflichtung	395	
e) Weitergehender Lösungsansatz: Personal information management-Systeme und datenschutzrechtliches Lizenzvertragsrecht	397	
XIII. Zusammenfassung und Reformbedarf	401	
 G. Reformperspektive: Immateriagüter- und datenschutzrechtliche Probleme, Trends und Building Blocks für die Datenökonomie		409
I. Möglicher Überschutz und Transaktionskosten	409	
1. Anreizgedanke für Datenproduktion und effiziente Datendissemination als inhärente Grenze des Schutzgegenstands	409	
2. Funktionale Grenzen zentralisierter Ausschließlichkeitsrechte in big data-Szenarien und besondere Bedeutung des Vertragsrechts	411	
3. Schutzrechtsüberschneidung als Problem für Datenzugang	414	
4. Trend de lege ferenda: Sinkende Schutzfristen und langfristig wachsende Bedeutung von Registerrechten	417	
II. Flexible Hybride zwischen Ausschließlichkeitsrecht und verhaltensbezogener Regelung: Begrenzte Drittewirkung vertraglicher Vereinbarungen als Paradigma für die Datenökonomie?	420	
1. Kommerzialisierung von Daten und der immateriagüterrechtliche und datenschutzrechtliche Rahmen	420	
2. Qualifizierte Drittewirkung vertraglicher Vereinbarungen in Anlehnung an den Geschäftsgeheimnisschutz?	422	
a) Grenzen des bestehenden Geschäftsgeheimnisschutzes und Vorschläge bzw. Modelle für eine Ausdehnung des Prinzips begrenzter Drittewirkung	422	
b) Bestehendes zivilrechtliches Instrumentarium (insbesondere § 241 Abs. 2 BGB)	423	
3. Mögliche lauterkeitsrechtliche Ansätze de lege lata und de lege ferenda?	426	
III. Neue Zugangsrechte in der Datenökonomie, Datenportabilität und die Schnittstelle zum Immateriagüter- und Datenschutzrecht	428	
1. Verlagerung der Diskussion in Richtung (bereichsspezifischer) Zugangsrechte	428	
2. Die Unterscheidung von Zugangsrechten und Nutzungsmöglichkeiten und -rechten	429	

a) Grundsatzüberlegung: Nur indirekte Relevanz des Immaterialgüterrechts bezüglich Zugangsregimes	429
b) Besonderheiten bei Geschäftsgeheimnissen und Bedeutung des bestehenden kartellrechtlichen Rahmens	431
c) Verbleibende Bedeutung des Immateriagüterrechts als Leitbild für Ausgestaltung nachfolgender Nutzungsmöglichkeiten . .	435
3. Relevante Szenarien für Zugangsrechte und die Schnittstelle zum Immateriagüterrecht hinsichtlich der Nutzungsregelung . .	435
a) Relevante Szenarien für Zugangs- und Nutzungsregimes	435
b) Schnittstelle zum Immateriagüterrecht, insbesondere Datenbankschutzrecht sui generis	438
aa) Berücksichtigung auf der Ebene von Schutzzvoraussetzungen und Schutzgegenstand	438
bb) Fallgruppen spezifischer Zugangsinteressen trotz grundätzlich bestehenden immateriagüterrechtlichen Schutzbedarfs	439
(1) Zugangs- und Portabilitätsrechte betreffend individual level use data für „berechtigte Nutzer“ von smart devices	440
(a) Regelung der Mindestrechte des „rechtmäßigen Nutzers“ im digitalen Urheberrecht als bestehende funktionale Entsprechung	440
(b) Folgerung hinsichtlich der Portabilität auf der Nutzungsebene: In der Regel keine zusätzliche Vergütung bei individual level data berechtigter Nutzer	443
(c) Zwingende sektorspezifische Zugangs- und Portabilitätsrechte für berechtigte Nutzer?	444
(d) Zusammenfassung und Reformbedarf in der Datenbank-RL	446
(2) Zugangs- und Nutzungsrechte betreffend komplette Datenstrukturen oder Datensets für Wettbewerber (aggregated data)	448
(a) Grundsätzlich mit verhandelter Vergütung (Zwangslizenz, liability rule)	448
(b) Zwangslizenzen auf kartellrechtlicher Grundlage	449
(c) Neue Zwangslizenzregelung für sui generis- geschützte sole source Datenbanken in der Datenbank-RL	451

(d) Nutzungsumfang und FRAND-Vergütung	453
(e) Gegenlizenzen (Kreuzlizenzen)	454
(f) Zugangsansprüche bei geheimen Informationen	455
4. Portabilität und Interoperabilität	457
Literaturverzeichnis	461
Sachregister	495