

Inhaltsübersicht

Vorwort	VII
Inhaltsverzeichnis	XI
§1 <i>Einführung</i>	1
A. Daten in der Dauerschleife	1
B. Datenprivatrecht	4
C. Regulatorisches und ermöglichendes Privatrecht	8
D. Problemaufriss und Aufbau der Untersuchung	12
Teil 1: Technische und ökonomische Grundlagen	23
§2 <i>Technische Grundlagen moderner Informationsverarbeitungssysteme</i>	25
A. Tracking-Instrumente	25
B. Künstliche Intelligenz: Techniken maschinellen Lernens	29
C. Das Internet der Dinge	37
D. Konvergenzprozesse: Auf dem Weg zum <i>Internet of Everything</i>	43
§3 <i>Technisch-ökonomische Problemstellungen und rechtliche Herausforderungen</i>	47
A. Erste rechtliche Herausforderung: Multirelationalität vernetzter Datenanalyse	47
B. Zweite rechtliche Herausforderung: Ambivalenz vernetzter Datenerhebung und -verarbeitung	56
C. Dritte rechtliche Herausforderung: Ermöglichung der Durchsetzung heterogener Datenschutzpräferenzen	76
D. Leitfälle und Leitfragen für die weiteren Teile der Arbeit	77
E. Ergebnisse von §3	82

Teil 2: Datenschutzrecht und allgemeines Privatrecht	85
§ 4 <i>Vernetzte Datenerhebung und -analyse im Datenschutzrecht</i>	87
A. Datenschutzrechtliche Grundlagen	87
B. Ermöglichende Strukturen im Datenschutzrecht	159
C. Regulatorische Strukturen im Datenschutzrecht	270
D. Ergebnisse von § 4	309
§ 5 <i>Vernetzte Datenerhebung und -analyse im allgemeinen Privatrecht</i> ...	313
A. Zum Verhältnis von unio-nalem Datenschutzrecht und mitgliedstaatlichem Privatrecht	314
B. Ermöglichende Strukturen im allgemeinen Privatrecht	343
C. Regulatorische Strukturen im allgemeinen Privatrecht	397
D. Ergebnisse von § 5	538
 Teil 3: Reformperspektiven	 545
§ 6 <i>Präferenzverwirklichung durch Technikgestaltung</i>	547
A. Autonomie, Informiertheit und Datenschutzpräferenzen	548
B. Minimierung von Datenschutzrisiken durch Technik	553
C. Entscheidungsunterstützung durch Recht	577
D. Ergebnisse von § 6	655
 Teil 4: Schluss	 657
§ 7 <i>Lösungsansätze für die drei rechtlichen Herausforderungen, de lege lata und de lege ferenda</i>	659
A. Erste rechtliche Herausforderung: Multirelationalität von Daten	659
B. Zweite rechtliche Herausforderung: Ambivalenz von Nutzen und Risiken	662
C. Dritte rechtliche Herausforderung: Heterogenität von Datenschutzpräferenzen	666
§ 8 <i>Wesentliche Ergebnisse der Arbeit in zehn Thesen</i>	669
Literaturverzeichnis	673
Sachregister	741

Inhaltsverzeichnis

Vorwort	VII
Inhaltsübersicht	IX
§1 <i>Einführung</i>	1
A. Daten in der Dauerschleife	1
B. Datenprivatrecht	4
C. Regulatorisches und ermöglichendes Privatrecht	8
D. Problemaufriss und Aufbau der Untersuchung	12
I. Regulierende und ermöglichende Strukturen im Datenprivatrecht	12
II. Kurzüberblick über die drei Hauptteile der Arbeit	15
1. Technische und ökonomische Grundlagen (Teil 1)	16
2. Datenschutzrecht und allgemeines Privatrecht (Teil 2)	17
3. Reformperspektiven (Teil 3)	20
Teil 1: Technische und ökonomische Grundlagen	23
§2 <i>Technische Grundlagen moderner Informationsverarbeitungssysteme</i>	25
A. Tracking-Instrumente	25
I. Cookies	26
II. Fingerprinting-Techniken	28
III. Sonstige eindeutige Kennungen	28
B. Künstliche Intelligenz: Techniken maschinellen Lernens	29
I. Begriffe	29
II. Strategien und Modelle maschinellen Lernens	31
1. Lernstrategien	31
a) Überwachtes Lernen (<i>supervised learning</i>)	31
b) Verstärkungslernen (<i>reinforcement learning</i>)	33
c) Unüberwachtes Lernen (<i>unsupervised learning</i>)	33
2. Maschinelles Lernen als Optimierungsproblem: Tiefe neuronale Netze	34
III. Technische Autonomie, Daten und Inferenzen	35

C.	Das Internet der Dinge	37
I.	Vier Charakteristika von IoT-Geräten	39
II.	Vier Schichten des IoT	41
D.	Konvergenzprozesse: Auf dem Weg zum <i>Internet of Everything</i>	43
§3	<i>Technisch-ökonomische Problemstellungen und rechtliche Herausforderungen</i>	47
A.	Erste rechtliche Herausforderung: Multirelationalität vernetzter Datenanalyse	47
I.	Techno-physische Vernetzung: Internet der Dinge	47
II.	Ökonomische Folgerungen: Daten als Gegenleistung	49
1.	Daten als funktionales Geldäquivalent	49
a)	Austausch ohne monetäre Gegenleistung	50
b)	Wertschöpfung an Daten	51
aa)	Optimierung von Modellen	51
bb)	Daten als Input für Modelle	51
cc)	Datenhandel	52
2.	Systematisierung: Kategorien von Daten als Gegenleistung	53
a)	Datenbasiertes Grundmodell	53
aa)	Vollkommen datenfinanzierte Modelle	53
bb)	Freemium-Modelle	53
b)	Monetäres Grundmodell	54
aa)	Rabattmodelle	54
bb)	Data on top-Modelle	54
III.	Die Multirelationalität von personenbezogenen Daten	55
B.	Zweite rechtliche Herausforderung: Ambivalenz vernetzter Datenerhebung und -verarbeitung	56
I.	Potenzial	57
1.	Individuelle Ebene	57
a)	Präferenzenerfüllung	57
b)	Zeitersparnis	57
c)	Kaufkraftsteigerung	58
2.	Sozialer Nutzen	58
II.	Datenschutzrechtliche Risiken	58
1.	Vier Typen von Marktversagen	59
a)	Informationsasymmetrie: Mangelnde Kenntnis der Datenverarbeitung	60
aa)	Informationsüberlastung	60
bb)	Rationale Ignoranz	61
b)	Verhaltensökonomische Effekte bei der Datenbewertung	62
c)	Negative Externalitäten durch Kollektiveffekte	64
aa)	Adverse Inferenz	65
bb)	Ähnlichkeitsbasierte Inferenz	66

d)	Unschärfe des Datenpreissignals	67
e)	Zusammenfassung zum Marktversagen	70
2.	Soziale Risiken	70
a)	Verhaltens- und Freiheitsverengung (<i>chilling effects</i>)	71
b)	Unentziehbarkeit	73
c)	Mangelndes Bewusstsein der Datenerhebung	74
d)	Diskriminierung	75
C.	Dritte rechtliche Herausforderung: Ermöglichung der Durchsetzung heterogener Datenschutzpräferenzen	76
D.	Leitfälle und Leitfragen für die weiteren Teile der Arbeit	77
I.	Drei paradigmatische Leitfälle	77
1.	Datenweiterleitung an Drittunternehmen	77
2.	Datenerhebung durch Drittanbieter (<i>third-party tracking</i>)	79
3.	Datenerhebung bei Dritten	80
II.	Leitfragen	81
E.	Ergebnisse von § 3	82
Teil 2: Datenschutzrecht und allgemeines Privatrecht		85
§ 4	Vernetzte Datenerhebung und -analyse im Datenschutzrecht	87
A.	Datenschutzrechtliche Grundlagen	87
I.	Rechtsgrundlagen des Datenschutzrechts im Kurzüberblick	88
1.	Europäische Ebene	88
a)	DS-GVO	88
b)	ePrivacy-Instrumente	89
c)	Sonstige Instrumente	90
2.	Nationale Ebene	91
a)	BDSG	92
b)	UWG	92
c)	Sonstige Regelungen	93
II.	Anwendbarkeit der DS-GVO	93
1.	Territoriale Anwendbarkeit	93
a)	Art. 3 Abs. 1 DS-GVO: Niederlassungsprinzip	94
aa)	Der Begriff der Niederlassung	95
bb)	Verarbeitung im Rahmen der Tätigkeit der Niederlassung	96
b)	Art. 3 Abs. 2 DS-GVO: Marktortprinzip	98
aa)	Art. 3 Abs. 2 lit. a DS-GVO: Marktangebot	99
(1)	Dienstleistung oder Ware	100
(2)	Spezifisches Angebot	100
bb)	Art. 3 Abs. 2 lit. b DS-GVO: Verhaltensbeobachtung	102

2. Sachliche Anwendbarkeit	103
a) Grundtatbestand: Art. 2 Abs. 1 DS-GVO	103
aa) Personenbezogene Daten	104
(1) Bezug zu einer Person	104
(2) Identifizierbarkeit einer konkreten Person	105
(a) Grundsätzliche Kriterien	105
(aa) (Re-)Identifizierungsstrategien	106
(bb) Die Rechtssache <i>Breyer</i>	107
(cc) Der 26. Erwägungsgrund der DS-GVO: Illegale Re-Identifizierung	108
(dd) Folgerungen	110
(b) Anwendung auf die drei Leitfälle	111
(aa) Datenweiterleitung an Dritte (personalisierte Werbung)	112
α. Namenlose Profile	112
β. Machine-to-machine-Kommunikation ...	113
(bb) Datenerhebung durch Dritte (<i>third-party tracking</i>)	114
(cc) Datenerhebung bei Dritten	117
(3) Ergebnis zu personenbezogenen Daten	117
(4) Regelung nicht personenbezogener Daten	117
bb) Spezifische Verarbeitungsformen	119
(1) Ganz oder teilweise automatisierte Verarbeitung ...	119
(2) Speicherung oder Speicherungsabsicht in Dateisystem	119
b) Ausnahmen: Art. 2 Abs. 2–3 DS-GVO	120
aa) Kein Anwendungsbereich des Unionsrechts, Art. 2 Abs. 2 lit. a DS-GVO	120
(1) Die Fälle <i>Österreichischer Rundfunk</i> und <i>Lindqvist</i> – Argumente des EuGH und Kritik	121
(2) Der Anwendungsbereich des Unionsrechts nach der DS-GVO	123
(a) Die klassischen Kriterien der Eröffnung des Anwendungsbereichs des Unionsrechts	124
(b) Die partielle Fortgeltung der EuGH-Rechtsprechung	125
(aa) Fortgeltung des Falls <i>Österreichischer Rundfunk</i>	125
(bb) Keine Fortgeltung des Falls <i>Lindqvist</i>	126
(3) Folgerungen	126
bb) Weitere Ausnahmen	127
3. Ergebnis zur Anwendbarkeit der DS-GVO	128
III. Datenschutzrechtliche Grundkonzepte	128

1. Stufen datenschutzrechtlicher Verantwortlichkeit in vernetzten Umgebungen	129
a) Relevanz der Bestimmung der Verantwortlichkeit	129
b) Typen von Verantwortlichkeit	130
aa) Alleinige Verantwortlichkeit	130
bb) Gemeinsame Verantwortlichkeit	130
cc) Zwischenstufen: Die Rechtssache <i>Wirtschaftsakademie Schleswig-Holstein</i>	132
dd) Anwendung auf die drei Leitfälle	133
(1) Datenerhebung durch Drittanbieter (<i>third-party tracking</i>)	133
(a) Die Rechtsprechung des EuGH	133
(aa) Kriterien	133
a. Cookies: Nochmals <i>Wirtschaftsakademie Schleswig-Holstein</i> ..	133
β. Social Plug-Ins: Die Rechtssache <i>Fashion ID</i>	136
(bb) Rechtsfolgen	137
a. Geltung der DSRL (Altfälle)	137
β. Art. 26 Abs. 3 DS-GVO	137
(b) Plädoyer für eine abgestufte Verantwortung im Rahmen der DS-GVO	138
(aa) Kriterien	138
(bb) Rechtsfolgen	140
a. Notwendigkeit einer teleologischen Reduktion	141
β. Subsidiäre Anwendung von §275 Abs. 1 oder 2 BGB	141
γ. Konsequenzen für einzelne Betroffenenrechte	143
(2) Datenübermittlung an Drittunternehmen (personalisierte Werbung)	143
(a) Werbenetzwerke (<i>ad exchanges</i>)	144
(b) Weiterleitung im Internet der Dinge	145
(3) Datenerhebung bei Dritten	145
c) Datenschutzrechtliche Störerhaftung als dritte Kategorie? ..	146
d) Ergebnis zur Verantwortlichkeit	148
2. Grundsätze der Datenverarbeitung	148
a) Rechtscharakter der Grundsätze	148
b) Die Grundsätze des Art. 5 Abs. 1 DS-GVO im Einzelnen ...	150
aa) Art. 5 Abs. 1 lit. a Var. 1 DS-GVO: Legalität	150
bb) Art. 5 Abs. 1 lit. a Var. 2 DS-GVO: Treu und Glauben (<i>fairness</i>)	150

(1) Rechtsbereichsübergreifende Fairness jenseits von Transparenz	151
(2) Inhaltliche Ausfüllung	152
cc) Art. 5 Abs. 1 lit. a Var. 3 DS-GVO: Transparenz	154
dd) Art. 5 Abs. 1 lit. b DS-GVO: Zweckbindung	155
ee) Art. 5 Abs. 1 lit. c DS-GVO: Datenminimierung	156
ff) Art. 5 Abs. 1 lit. d-f DS-GVO: Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit	158
c) Zusammenfassung zu den Grundsätzen der Datenverarbeitung	159
B. Ermöglichende Strukturen im Datenschutzrecht	159
I. Die Einwilligung und ihre Schranken: Reibungspunkte zwischen Privatautonomie und Regulierung	161
1. Ermöglichungscharakter	161
2. Zum Verhältnis von Einwilligung und Vertrag	162
3. Grundtatbestand: Art. 6 Abs. 1 lit. a DS-GVO	164
a) Allgemeiner Begriff der Einwilligung, Art. 4 Nr. 11 DS-GVO	165
aa) Unmissverständlichkeit	165
(1) Grundsatz: Ausdrücklich oder konkludent	165
(a) Dimensionen der Unmissverständlichkeit	165
(aa) Aktives Tun	165
(bb) Gesonderte Einwilligung	167
(b) Anwendung auf die drei Leitfälle	170
(aa) Datenweiterleitung an Dritte (personalisierte Werbung)	170
(bb) Datenerhebung durch Dritte (<i>third-party tracking</i>)	171
(cc) Datenerhebung bei Dritten	171
(2) Ausnahme: Nur ausdrücklich	172
bb) Bestimmtheit	172
cc) Informiertheit	174
(1) Transparenz	175
(2) Erkenntnismöglichkeit	176
(3) Anwendung auf die drei Leitfälle	177
(a) Datenweiterleitung an Dritte	177
(b) Datenerhebung durch Dritte	178
(c) Datenerhebung bei Dritten	179
dd) Freiwilligkeit	180
(1) Klares Ungleichgewicht und mangelnde Alternativen	180
(2) Gesonderte Einwilligung?	181
(3) Kopplungsverbot, Art. 7 Abs. 4 DS-GVO	181
(a) Erforderlichkeit zur Vertragserfüllung	182

(aa)	Verhältnis zu Art. 6 Abs. 1 lit. b DS-GVO . . .	182
(bb)	Drei Lesarten	183
α.	Ökonomischer Erforderlichkeitsmaßstab	183
β.	Objektiver Erforderlichkeitsmaßstab	184
γ.	Subjektiver Erforderlichkeitsmaßstab	185
(b)	Abhängigkeit der Vertragserfüllung von der Einwilligung	186
(aa)	Die Relevanz der Marktmacht	187
α.	Literaturansichten	187
β.	Stellungnahme: Marktmacht als gewichtiger indirekter Bewertungsfaktor	188
(bb)	Dienst gegen monetäre Zahlung als zumutbare Alternative	189
(c)	Rechtsfolge: Widerlegliche Vermutung	190
(aa)	Widerlegung durch funktional äquivalentes Marktangebot	191
(bb)	Widerlegung durch hypothetische wirksame Leistungspflicht	192
(cc)	Beschränkung des Kopplungsverbots auf dringliche Angewiesenheit?	192
(d)	Grundrechtskonformität des Kopplungsverbots . .	193
(4)	Weitere Abwägungsgesichtspunkte	195
(a)	Täuschung, Drohung und Zwang	195
(b)	Einwilligung im Beschäftigtenverhältnis, §26 Abs. 2 BDSG	195
(5)	Anwendung auf die drei Leitfälle	196
(a)	Daten als Gegenleistung	196
(aa)	Vertragsinhalt bei „Daten als Gegenleistung“ mit datenbasiertem Grundmodell	196
α.	Legitimation durch Nutzerpflichten?	197
β.	Ablehnung aus teleologischer Perspektive	199
γ.	Rekurs auf Verarbeiterpflichten	200
(bb)	Rabattmodell	201
(cc)	Data on top-Modell	202
(b)	Datenerhebung durch Dritte (<i>tracking walls</i>)	202
(c)	Datenerhebung bei Dritten	202
(6)	Zusammenfassung zur Freiwilligkeit	203
ee)	Einwilligung und Genehmigungsmöglichkeit	204
b)	Besondere Voraussetzungen, Art. 7–9 DS-GVO	205
aa)	Separierungsgebot, Art. 7 Abs. 2 S. 1 DS-GVO	205
bb)	Widerruf, Art. 7 Abs. 3 DS-GVO	206
(1)	Datenschutzrechtliche Rechtsfolgen	206

(2) Vertraglicher Ausschluss oder Erschweris des Widerrufs?	208
(3) Vertragsrechtliche Folgen des Widerrufs	211
(a) Schadensersatz des Verantwortlichen	211
(aa) Anspruch auf Datenüberlassung	213
α. Nichtüberlassung von Daten	213
β. Überlassung von inkorrekten Daten	217
(bb) Anspruch auf Einwilligung	223
α. Bestehen des Anspruchs	223
β. Durchsetzbarkeit des Anspruchs	223
γ. Keine Pflichtverletzung durch Widerruf der Einwilligung	224
δ. Pflichtverletzung durch Nichtüberlassung von Daten oder Überlassung inkorrektur Daten	224
(cc) Zusammenfassung zum Schadensersatzanspruch bei Widerruf der Einwilligung	224
(b) Zurückbehaltungs- und Vertragslösungsrecht des Verantwortlichen	225
(aa) Synallagmatische Verknüpfung	225
α. Zurückbehaltungsrecht	225
β. Rücktritt, Kündigung und Wegfall der Geschäftsgrundlage	226
(bb) Konditionale Verknüpfung	228
(4) Zusammenfassung zum Widerruf	229
cc) Minderjährige, Art. 8 DS-GVO	230
(1) Mangelnder Gleichlauf mit dem BGB	231
(2) Partielle Auflösung durch Auslegung	233
dd) Sensitive Daten, Art. 9 DS-GVO	235
(1) Regelungsstruktur	235
(2) Unmittelbar und mittelbar sensitive Daten	236
c) Allgemeine Wirksamkeitsvoraussetzungen nach dem BGB ..	238
4. Cookies und andere Geräte-Identifizierer: Von der ePrivacy-Richtlinie über die DS-GVO zur ePrivacy-VO	238
a) Regelung nach der ePrivacy-Richtlinie	238
aa) Gesetzliche Grundlagen	239
(1) Art. 5 Abs. 3 ePrivacy-Richtlinie	239
(2) Deutsches Recht	240
bb) Voraussetzungen der Cookie-Einwilligung	241
(1) Das Erfordernis aktiver und gesonderter Einwilligung	241
(a) Rechtsprechung und Literatur bis 2019	241

(b) Die Rechtssache <i>Planet49</i>	242
(c) Folgen für das deutsche Recht	243
(2) Informiertheit der Einwilligung	244
(3) Freiwilligkeit der Einwilligung	244
b) Maßgeblichkeit der DS-GVO bis zum Inkrafttreten der ePrivacy-VO	245
aa) Die DS-GVO als Maßstab für Einwilligungen	246
(1) Anwendbarkeit der DS-GVO	246
(2) Konsequenzen (<i>tracking walls</i>)	248
bb) Rückgriff auf andere Erlaubnistatbestände der DS-GVO	248
c) Ausblick: Die Regelung der ePrivacy-VO	249
aa) Einwilligung durch Browsereinstellungen, Art. 9 Abs. 2 ePrivacy-VO-KommE	251
bb) Möglichkeit der Verhinderung von <i>third-party</i> <i>tracking</i> , Art. 10 ePrivacy-VO-KommE	251
cc) Regelung von <i>tracking walls</i> , Art. 8 Abs. 1a ePrivacy-VO-EP	253
5. Eine kurze Kritik der Einwilligung	255
a) Mangelnder direkter Nutzen für Betroffene	255
aa) Rationale Ignoranz	256
bb) Verhaltensökonomische Effekte	256
cc) Faktische Grenzen der Einwilligung im IoT-Kontext	257
b) Nutzen für Informationsintermediäre	257
6. Zusammenfassung zur Einwilligung	258
II. Vertragserforderliche Datenverarbeitung, Art. 6 Abs. 1 lit. b DS-GVO	260
1. Ermöglichungs- bzw. Permissivitätscharakter	260
2. Tatbestand	261
a) Zivilrechtliche Wirksamkeit des Vertrags	262
b) Erforderlichkeit	262
aa) Vertragserfüllung	262
bb) Erforderlichkeitsmaßstab	263
(1) Subjektiver Erforderlichkeitsmaßstab	263
(2) Relevanz von Nutzerpflichten?	264
3. Konsequenzen für das Verhältnis zu Art. 7 Abs. 4 DS-GVO und für die drei Leitfälle	264
4. Eine kurze Kritik der vertragserforderlichen Datenverarbeitung	265
III. Datenübertragung, Art. 20 DS-GVO	266
1. Ermöglichungscharakter	267
2. Tatbestand	267
3. Limitationen	268

IV. Zusammenfassung zu den Ermöglichungsstrukturen im Datenschutzrecht	269
C. Regulatorische Strukturen im Datenschutzrecht	270
I. Erlaubnistatbestand, Art. 6 Abs. 1 lit. f DS-GVO	271
1. Relevanz	271
a) Ökonomische Relevanz	272
b) Rechtliche Relevanz	272
2. Tatbestand	273
a) Berechtigte Interessen	273
aa) Interessen des/der Verantwortlichen	273
bb) Interessen Dritter	274
b) Erforderlichkeit der Datenverarbeitung zur Interessenwahrung	275
c) Abwägung	275
aa) Überwiegen	275
bb) Wertungskriterien	276
(1) Grundsätzliche Wertungskriterien	276
(2) Residualwirkung privatautonomer Gestaltung	278
3. Anwendung auf die drei Leitfälle	279
a) Datenweiterleitung an Dritte (<i>ad exchanges</i> und personalisierte Werbung)	279
aa) Grundsätzliche Abwägung	280
bb) Marktmacht	281
cc) Überraschungseffekt	282
b) Datenerhebung durch Dritte	283
c) Datenerhebung bei Dritten	283
4. Rechtssichere Operationalisierung für die beteiligten Akteure	284
5. Zusammenfassung zu Art. 6 Abs. 1 lit. f DS-GVO	286
II. Die Änderung der Verarbeitungszwecke, Art. 6 Abs. 4 DS-GVO	287
1. Relevanz	287
2. Kein eigener Erlaubnistatbestand	287
III. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Art. 25 DS-GVO	289
1. Relevanz	290
2. Rechtfertigung	291
4. Verpflichtungsgrad	293
4. Inhaltliche Ausformung	294
a) Art. 25 Abs. 1 DS-GVO	294
b) Art. 25 Abs. 2 DS-GVO	295
c) Operationalisierung	296
5. Anwendung auf die drei Leitfälle	297
a) Datenweiterleitung an Dritte	297
b) Datenerhebung durch Dritte	298

c) Datenerhebung bei Dritten	300
IV. Co-Regulierung	300
1. Allgemeine Funktionen und Relevanz der Co-Regulierung....	301
2. Datenschutz-Folgenabschätzung, Art. 35 DS-GVO	302
a) Relevanz	302
b) Norminhalt	304
c) Anwendung auf die drei Leitfälle	305
aa) Datenweiterleitung an Dritte	305
bb) Datenerhebung durch Dritte	306
cc) Datenerhebung bei Dritten	306
3. Verhaltensregeln und Zertifizierungsverfahren.....	306
a) Genehmigte Verhaltensregel, Art. 40f. DS-GVO.....	307
b) Genehmigtes Zertifizierungsverfahren, Art. 42f. DS-GVO..	309
D. Ergebnisse von §4	309
§5 <i>Vernetzte Datenerhebung und -analyse im allgemeinen Privatrecht</i> ...	313
A. Zum Verhältnis von unionalem Datenschutzrecht und mitgliedstaatlichem Privatrecht	314
I. Anwendungsvorrang des Unionsrechts.....	315
1. Direkte Kollision	318
a) Tatbestandliche Erfassung auf beiden Ebenen	318
b) Abschließende Regelung auf Unionsebene: Risikospezifizität zum Ersten	319
2. Indirekte Kollision	320
a) Allgemeine Grenzen des Effektivitätsgrundsatzes.....	322
b) Methodische Ausfüllung des Effektivitätsgrundsatzes	322
aa) Zweistufige Prüfung	323
(1) Risikospezifizität zum Zweiten	324
(2) Zielkompatibilität	324
bb) Folgerung: Sachgerechte Ergänzung des Unionsrechts durch nationales Recht.....	325
cc) Methodisches Ergebnis	325
c) Operationalisierung für das Datenprivatrecht	326
aa) Ziele des unionalen Datenschutzrechts	326
bb) Unionsrechtskompatible nationale Zielsetzungen	328
(1) Binnenmarktkompatibilität.....	329
(2) Datenschutzkompatibilität	330
(3) Sonstige Zielsetzungen.....	331
d) Ergebnis zur indirekten Kollision.....	332
3. Zusammenfassung zum Anwendungsvorrang	332
II. Sachintegration ebenengleichen Rechts	333
1. Rechtsbereichsübergreifende Auslegung	335
a) Die Fälle <i>Pereničová und Perenič</i> sowie <i>Bankia</i>	336

b)	Die Ausstrahlungswirkung im Unionsrecht	337
2.	Konkurrierende Rechtsfolgebestimmungen	339
a)	Kein grundsätzlicher Vorrang des Datenschutzrechts	339
b)	Grundrechtlich geprägte Normenkoordination	340
aa)	Explizite Regelung eines Wertungsvorrangs	341
bb)	Impliziter Wertungsvorrang: Risikospezifität zum Dritten	341
(1)	Abschließende Adressierung eines Risikos im Datenschutzrecht	341
(2)	Adressierung eines zusätzlichen Risikos in anderen Rechtsbereichen	342
III.	Zusammenfassung zum Verhältnis von Datenschutzrecht und Privatrecht	342
B.	Ermöglichende Strukturen im allgemeinen Privatrecht	343
I.	Einwilligung und Datenüberlassung als Gegenleistung	345
II.	Privatrechtliche Rechtsgeschäftslehre und datenschutzrechtlicher Einwilligungstatbestand	348
1.	Die Rechtsnatur der Einwilligung und der Rückgriff auf nationales Recht	348
a)	Die Einwilligung als geschäftsähnliche Handlung	349
b)	Punktuelle Rückgriffsmöglichkeit	350
aa)	Keine allgemeine Rechtsgeschäftslehre in der DS-GVO	351
bb)	Keine vollständige Präklusion nationaler Regelungen: Wahrung des Effektivitätsgrundsatzes	353
cc)	Die Bedeutung der Rechtssachen <i>Rabobank</i> und <i>Schyns</i>	354
dd)	Punktuelle Ergänzung der DS-GVO durch nationales Recht	355
2.	Einzelne Probleme der Rechtsgeschäftslehre	356
a)	Einwilligungsfähigkeit	356
b)	Subjektiver Tatbestand, insbesondere Einwilligungsbewusstsein	357
c)	Abgabe und Zugang	359
aa)	Abgabe	359
bb)	Zugang	360
d)	Stellvertretung	362
e)	Die Behandlung von Willensmängeln	364
aa)	Widerrechtliche Drohung	364
(1)	Fortbestehendes Interesse der betroffenen Person	365
(2)	Doppelwirkung im Mehrebenenrecht?	366
bb)	Arglistige Täuschung	367
cc)	Erklärungs- und Inhaltsirrtum	367
(1)	Grundsätzliche Entbehrlichkeit neben dem Widerruf	368
(2)	Anfechtung im Fall von § 142 Abs. 2 BGB	369

dd) Beachtlicher Motivirrtum	369
3. Zusammenfassung zu Rechtsgeschäftslehre und Einwilligung	369
III. Vertragsschluss und DS-GVO	371
1. Ermöglichungsstrukturen zwischen Erstanbieter und Primärnutzer	371
2. Drittbezogene Ermöglichungsstrukturen	372
a) Einbeziehung von Drittanbietern	373
aa) Mehrseitiger Vertrag	374
(1) Grundsätzlich nur ausdrücklicher Vertragsschluss ...	375
(2) Ausnahmsweise konkludenter Vertragsschluss bei salientem Hinweis	376
bb) Bilateraler Vertrag mit Drittanbieter kraft Stellvertretung	377
cc) Vertrag zugunsten Dritter	378
dd) Bedingung zugunsten Dritter	379
(1) Datenschutzrechtliche Irrelevanz der drittbegünstigenden Bedingung	379
(2) Folgen für die Vertragsauslegung	380
ee) Zusammenfassung zur Einbeziehung von Drittanbietern	381
b) Einbeziehung von Drittnutzern und unbeteiligten Dritten ..	381
aa) Eigener Vertrag kraft Nutzung	381
(1) Bewusste Nutzung	382
(a) Angebot des Anbieters	382
(b) Annahme durch den Drittnutzer	384
(aa) Bestimmung der Identität des Anbieters	384
(bb) Erklärungsbewusstsein bei kurzzeitiger Nutzung	385
a. Mangelndes Erklärungsbewusstsein bei § 151 S. 1 BGB	385
β. Besonderheiten im Rahmen digitaler Austauschprozesse	387
(cc) Unmissverständlichkeit der Annahme bei nicht primär nutzungsorientierter Handlung	388
(c) Lösungsmöglichkeiten	390
(2) Erhebung bei Unbeteiligten	391
(3) Zusammenfassung zum eigenen Vertrag mit Drittnutzern	391
bb) Vertrag zugunsten Dritter	392
cc) Vertrag mit Schutzwirkung zugunsten Dritter	392
(1) Tatbestandliche Voraussetzungen	393
(2) Vereinbarkeit mit Unionsrecht	394
dd) Drittschadensliquidation	395

3. Zusammenfassung zu Vertragsschluss und DS-GVO	395
C. Regulatorische Strukturen im allgemeinen Privatrecht	397
I. § 134 BGB: Erstreckung der Datenschutzrechtswidrigkeit auf das Rechtsgeschäft?	397
1. Verträge mit Betroffenen: Entkopplung von Datenschutzrecht und Vertragsrecht	398
a) Vorrang der datenschutzrechtlichen Abwicklung	400
b) Umkehrung der Schutzrichtung der DS-GVO	402
c) Überlegenheit gegenüber anderen dogmatischen Figuren ...	404
aa) Halbseitige Teilnichtigkeit	404
bb) Rechtliche Unmöglichkeit, Geschäftsgrundlage und Nichtigkeit nach § 134 BGB	406
(1) Anspruch auf Überlassung von Daten	407
(2) Anspruch auf Einwilligung	408
(a) Partielle Verknüpfung von Einwilligung und Vertrag	409
(aa) Wirksame Einwilligung als Geschäftsgrundlage	409
(bb) Keine Verletzung des Effektivitätsgrundsatzes	411
(cc) Rechtsfolgen für den Vertrag	412
(b) Modifikationen der Rückabwicklung	413
2. Verträge zwischen Dritten: Kopplung von Datenschutzrecht und Vertragsrecht	414
a) Nichtigkeit nach § 134 BGB	414
b) Einordnung der bisherigen Rechtsprechung	415
3. Zusammenfassung	417
II. Inhaltskontrolle im weiteren Sinne	417
1. AGB-Kontrolle	418
a) Anwendbarkeit neben der DS-GVO	419
b) Sachliche Anwendbarkeit: Vertragsbedingungen	422
c) Einbeziehungskontrolle	423
aa) Zumutbare Möglichkeit der Kenntnisnahme, § 305 Abs. 2 Nr. 2 BGB	423
bb) Überraschende Klauseln, § 305c Abs. 1 BGB	424
(1) Datenschutzrechtlicher Überraschungseffekt?	425
(2) Einbeziehung Dritter	426
d) Transparenzkontrolle	426
e) Inhaltskontrolle	430
aa) Kontrollfähigkeit, § 307 Abs. 3 S. 1 BGB	430
(1) Grundsatz: Mangelnde Kontrollfähigkeit des Hauptgegenstands des Vertrags und des Preis-/ Leistungsverhältnisses	430

(2) Zur Kontrollfähigkeit der Einwilligung	433
(3) Zur Kontrollfähigkeit von Vertragsklauseln	434
(a) Kontrollfähigkeit der Verpflichtung zur Datenüberlassung oder Einwilligung	434
(aa) Monetäres Grundmodell: Preisnebenabreden	435
(bb) Datenbasiertes Grundmodell: Preishauptabreden und teleologische Reduktion	435
a. Gründe für fehlende Kontrollfähigkeit nach Art. 4 Abs. 2 der Klauselrichtlinie ...	436
β. Marktversagen bei der Kontrolle des „Datenpreises“	437
(b) Kontrollfähigkeit des Preis-/ Leistungsverhältnisses	439
(c) Kontrollfähigkeit von Leistungsbeschreibungen ..	440
(4) Ergebnis	441
bb) Grundsätze der unangemessenen Benachteiligung	442
(1) § 307 Abs. 2 Nr. 1 BGB	442
(a) Datenschutzrecht allgemein als Maßstab	442
(b) Grundsätze der Datenverarbeitung als spezieller Maßstab	443
(2) § 307 Abs. 2 Nr. 2 BGB	445
(3) § 307 Abs. 1 S. 1 BGB	445
(a) Die Rechtsprechung von EuGH und BGH	445
(b) Unangemessenheitskriterien für Hauptleistungspflichten	447
(aa) Der <i>Aziz</i> -Test	448
(bb) Der relevante Referenzakteur	450
(c) Ergebnis	452
cc) Anwendung auf die drei Leitfälle	454
(1) Datenweiterleitung an und Datenerhebung durch Dritte	454
(a) Einwilligung	454
(b) Vertragsklauseln	455
(aa) Verpflichtung zur Einwilligung	456
(bb) Verpflichtung zur Datenüberlassung	456
(cc) Weite vertragliche Leistungspflichten	456
(2) Vertragliche Einbindung Dritter	459
dd) Erweiterung der §§ 308 f. BGB	459
f) Rechtsfolgen: Das Schicksal des Vertrags	459
aa) Deutsche Rechtsprechung und Literatur zu § 306 BGB ..	460
bb) Die Rechtsprechung des EuGH	461

(1) Geltungserhaltende Reduktion und selektive Streichung der Klausel	461
(2) Gesamtunwirksamkeit des Vertrags	462
(3) Vertragliche Lückenfüllung	463
cc) Lösungen für das Datenprivatrecht	464
(1) Unwirksame Einwilligung	465
(2) Unwirksame Hauptleistungspflicht	465
(3) Unwirksame weite Nebenleistungspflicht	468
g) Wechselwirkungen mit der DS-GVO	469
aa) Keine Grundlage der Datenverarbeitung nach Art. 6 Abs. 1 lit. a, b DS-GVO	469
bb) Auswirkungen auf Art. 6 Abs. 1 lit. f DS-GVO	469
cc) Rechtsgebietsübergreifende Fairness: Auswirkungen auf Art. 5 Abs. 1 lit. a Var. 2 DS-GVO	470
dd) Methodisches Ergebnis	473
h) Zusammenfassung zur AGB-Kontrolle	473
2. § 138 BGB	476
a) Anwendbarkeit neben der DS-GVO	476
aa) Verträge	476
bb) Einwilligung	477
(1) Preis-/Leistungs-Verhältnis: Datenbasierte <i>laesio</i> <i>enormis</i>	478
(a) Risikospezifizität gegenüber Art. 5 Abs. 1 lit. c DS-GVO	479
(b) Risikospezifizität gegenüber Art. 5 Abs. 1 lit. a Var. 2 DS-GVO	480
(2) Sonstige Sittenwidrigkeitstatbestände	480
b) Tatbestand der Sittenwidrigkeit: Wucherähnliches Geschäft 483	
aa) Einwilligung	486
(1) Der unsichere Marktwert von Leistung und Gegenleistung	486
(2) Qualitative Abwägung	487
(a) Bestimmbarer Marktwert der Anbieterleistung	487
(b) Kein bestimmbarer Marktwert der Anbieterleistung	488
(c) Die Rolle des Referenzakteurs – Maßvolle Personalisierung	489
bb) Vertrag	491
cc) Ergebnis zum wucherähnlichen Geschäft	491
c) Rechtsfolge	492
d) Wechselwirkungen mit der DS-GVO	493
e) Zusammenfassung zu § 138 BGB	493

3. § 242 BGB	494
a) Anwendbarkeit der erweiterten Inhaltskontrolle: Dogmatik des BGB	495
b) Anwendbarkeit bei Rechtsmissbrauch und als Ausübungskontrolle: Anwendungsvorrang der DS-GVO? ..	496
aa) Einwilligung	497
bb) Vertrag	499
c) Wechselwirkungen mit der DS-GVO	500
d) Zusammenfassung zu § 242 BGB	502
III. Haftung	502
1. Anwendbarkeit zivilrechtlicher Haftungsnormen neben der DS-GVO	503
2. Vertragliche Haftung	506
a) Wesentliche Pflichten der DS-GVO als vertragliche Nebenflichten nach § 241 Abs. 2 BGB	507
aa) Rechtslage im Bereich der Anlageberatung	507
bb) Übertragung auf datenschutzrechtliche Sachverhalte ...	508
b) Die Anwendbarkeit von § 278 BGB im Rahmen der Datenverarbeitung	509
aa) Tatbestandsvoraussetzungen	509
bb) Kein Anwendungsvorrang der DS-GVO	510
c) Zur Anwendbarkeit von § 280 Abs. 1 BGB	512
d) Zusammenfassung zu vertraglichen Nebenflichten	514
3. Haftung aus <i>culpa in contrahendo</i> und Bereicherungsrecht ...	514
4. Deliktische Haftung	515
a) § 823 Abs. 1 BGB i. V. m. sonstigen, datenschutzbezogenen Rechten	516
aa) Das unionale Datenschutzgrundrecht	516
bb) Das deutsche allgemeine Persönlichkeitsrecht im weiteren Sinne	519
(1) Recht auf informationelle Selbstbestimmung	520
(a) Art. 82 DS-GVO als <i>lex specialis</i> im Allgemeinen	520
(b) Der Bereich der Öffnungsklauseln	521
(2) Recht auf Gewährleistung der Integrität und Vertraulichkeit von informationstechnischen Systemen	523
(3) Allgemeines Persönlichkeitsrecht	525
(a) Vorrang von § 823 Abs. 1 BGB i. V. m. dem allgemeinen Persönlichkeitsrecht nach dem Bundesverfassungsgericht?	525
(b) Vorrang von Art. 82 DS-GVO nach dem Unionsrecht	526

(aa) Untrennbarkeit von Datenschutzrecht und Äußerungsrecht im datenverarbeitenden Bereich	526
(bb) Differenzen zwischen Grundrechten und Haftungsrecht	528
(cc) Mangelnde Risikospezifizität	529
(c) Zusammenfassung zum Verhältnis von allgemeinem Persönlichkeitsrecht und Art. 82 DS-GVO	533
b) § 823 Abs. 2 BGB i. V. m. Normen der DS-GVO	533
c) § 824 BGB	534
d) § 826 BGB	535
e) § 831 BGB	537
f) Zusammenfassung zu deliktischen Ansprüchen	537
D. Ergebnisse von § 5	538
Teil 3: Reformperspektiven	545
§ 6 <i>Präferenzverwirklichung durch Technikgestaltung</i>	547
A. Autonomie, Informiertheit und Datenschutzpräferenzen	548
B. Minimierung von Datenschutzrisiken durch Technik	553
I. <i>Privacy-enhancing technologies</i>	555
1. Relevante nutzerbasierte Techniken (Selbstdatenschutz)	556
a) Verschlüsselung	556
b) Identity-Management-Systeme	558
c) Anti-Tracking-Tools	559
2. Rechtlicher Rahmen	561
a) Allgemeine Kriterien	562
b) Unterstützungspflicht	562
c) Tolerierungspflicht	563
3. Anreize und Beschränkungen	564
II. Rechtmäßigkeitskontrolle durch maschinelles Lernen	566
1. Relevante Techniken	567
a) Automatisierte Kontrolle der Datenschutzerklärung	567
aa) Modelle zur Unterstützung von Nutzern	568
bb) Modelle zur Unterstützung von Aufsichtsbehörden	570
b) Automatisierte Kontrolle der Nutzungsbedingungen	571
2. Rechtlicher Rahmen	572
3. Anreize und Beschränkungen	573
III. Zusammenfassung zur Minimierung von Datenschutzrisiken durch Technik	576

C. Entscheidungsunterstützung durch Recht	577
I. Verbesserung der Einwilligung und der Präferenzkommunikation	578
1. Transparenzbasierte Ansätze	578
a) Verbesserungsmöglichkeiten	579
aa) Kognitive Optimierung des Inhalts	579
(1) Verständlichkeit der Sprache	579
(2) Staffelung der Information auf mehreren Ebenen (<i>multi-layered notices</i>)	580
(a) Empirischer Nutzen	581
(b) Pflicht nach der DS-GVO?	583
(3) Icons	585
bb) Timing: Kontextualisierung und Zeitabhängigkeit	587
b) Bewertung	588
2. Verhaltensbasierte Ansätze: <i>privacy nudges</i>	590
a) Interventionsmöglichkeiten	590
b) Bewertung	591
3. Technologiebasierte Ansätze: Wege zu einer automatisierten Kommunikation von Datenschutzpräferenzen	593
a) Technische Möglichkeiten	594
aa) Manuelles Datenschutz-Dashboard	594
bb) Automatisierte Kontrollinstrumente	597
b) Bewertung	599
aa) Potenzial	599
bb) Limitationen	600
(1) Technische Ebene: Technikreife	601
(2) Ökonomische Ebene: Anreize und Präferenzen	601
(a) Kontrolle und Veröffentlichungsbereitschaft	602
(b) Formung und Modellierung von Präferenzen	603
(3) Regulatorische Ebene	604
c) Eingeschränkter rechtlicher Reformbedarf	605
aa) Rechtssichere automatisierte und autonome Kommunikation von Präferenzen	605
(1) Einwilligungsregime nach der DS-GVO	605
(a) Automatisierte Einwilligung	606
(aa) Schwach autonome Datenschutzassistenten	606
(bb) Browser-Spezifikationen	608
(b) Autonome Einwilligung	608
(aa) Grundsätze der Zurechnung der Erklärung zum Nutzer	609
(bb) Dogmatische Umsetzung: §§ 164 ff. BGB analog	610

(2) Automatisierter und autonomer Widerspruch gegen bestimmte Formen der Datenverarbeitung, Art. 21 f. DS-GVO	613
(a) Art. 21 f. Abs. 2 DS-GVO	613
(b) Art. 21 Abs. 1 S. 1 und Abs. 6 DS-GVO	614
(c) Art. 22 Abs. 1 DS-GVO	615
(3) Entwicklungsperspektiven	615
bb) Interoperabilität durch Datenschutz-Schnittstelle	616
4. Zusammenfassung zur Verbesserung der Einwilligung und der Präferenzkommunikation	618
a) Bewertung der verschiedenen Ansätze	618
b) Rechtlicher Reformbedarf	619
II. Verbesserung reeller Wahlmöglichkeiten: Das Recht auf eine datenschonende Option	620
1. Grundidee: Datenschonende Option und <i>privacy score</i>	621
a) Datenschonende Option <i>de lege lata</i> und <i>de lege ferenda</i>	621
b) Grundlegender Inhalt des Vorschlags: Drei Weichenstellungen	622
aa) Pflichtangebot der datenschonenden Option	623
bb) Verbindung mit <i>privacy scores</i>	623
cc) Sektorspezifität	624
c) Argumente	624
aa) Marktergänzende Alternativen zur Durchsetzung von Datenschutzpräferenzen	624
bb) Rechtssicherheit für Anbieter und Nutzer mit niedrigen Datenschutzpräferenzen	626
cc) Aktive Wahl statt rationaler Ignoranz	626
dd) Förderung von rationalen Entscheidungen und Reduzierung von Preisunschärfe durch <i>privacy scores</i>	627
2. Tatsächliche Voraussetzungen	628
a) Hinreichende Zahlungsbereitschaft	628
aa) Zahlungsbereitschaft und Salienz	629
bb) Datenschonende Option als Minderheitenschutz	632
b) Berechnung des <i>privacy score</i>	632
3. Implementierung der Wahlmöglichkeit	634
a) Wahlmöglichkeiten	635
aa) Vertraglich erforderliche vs. nicht erforderliche Daten	635
bb) Wahl der Cookies	636
(1) Typen von Cookies	636
(2) Datenschonende Cookies	637
b) Ausübung der Wahl (<i>agreement technologies</i>)	638
4. Sektorspezifität	639
a) Soziale Netzwerke	640

b) Suchmaschinen	641
c) IoT-Geräte, besonders autonome Fahrzeuge	642
5. Einwände	643
a) Wirkungslosigkeit	643
aa) Wirksamkeit für Altnutzer	644
bb) Wirksamkeit trotz Datenerhebung an anderer Stelle	644
cc) Strategische Nutzung bei sensiblen Daten	645
b) Zwei-Klassen-Datengesellschaft	645
aa) Pareto-Verbesserung	646
bb) Preiskontrolle	646
cc) Kein Recht auf völlig kostenlose Leistung	649
c) Mangelnde Stabilität von Präferenzen	649
d) Mangelnde Rationalität	650
6. Grundrechtskonformität	650
a) Betroffene unionale Grundrechtspositionen	650
b) Rechtfertigung	651
7. Zusammenfassung zum Recht auf eine datenschonende Option	654
D. Ergebnisse von § 6	655
Teil 4: Schluss	657
§ 7 <i>Lösungsansätze für die drei rechtlichen Herausforderungen, de lege lata und de lege ferenda</i>	659
A. Erste rechtliche Herausforderung: Multirelationalität von Daten	659
I. Regulatorische Dimension	660
II. Ermöglichende Dimension	662
B. Zweite rechtliche Herausforderung: Ambivalenz von Nutzen und Risiken	662
I. Marktversagen	663
II. Soziale Risiken	664
C. Dritte rechtliche Herausforderung: Heterogenität von Datenschutzpräferenzen	666
I. Das Dilemma individueller Kontrolle	666
II. Ein Lösungsvorschlag in drei Schritten	666
§ 8 <i>Wesentliche Ergebnisse der Arbeit in zehn Thesen</i>	669
Literaturverzeichnis	673
Sachregister	741