

Inhaltsverzeichnis

Abkürzungsverzeichnis	25
1. Kapitel Einführung	29
§ 1 Einleitung	29
I. Cloud Computing: Siegeszug einer innovativen Informationstechnologie	29
II. Praktische Relevanz von Haftungsfragen in der Cloud	30
III. Haftung für Datenverlust: Quo vadis?	31
§ 2 Gegenstand der Untersuchung: Maßgebliche Haftungsszenarien	33
I. Hackerangriff auf die Cloud durch externe Dritte	33
1. Haftungsszenario	33
2. Schadensursachen	34
3. Haftungsadressaten	34
II. Beeinflussung von Datenbeständen durch grundsätzlich berechtigte Cloud-Nutzer	35
1. Haftungsszenario	35
2. Schadensursache	36
3. Haftungsadressat	36
III. Datenverlust bei Betrieb des Cloud-Dienstes durch den Cloud-Anbieter	37
1. Haftungsszenario	37
2. Schadensursachen	37
3. Haftungsadressat	38
§ 3 Gang der Darstellung	38
2. Kapitel Technische und organisatorische Grundlagen des Cloud Computing	41
§ 4 Definition und technische Funktionsweise	41
I. Begriff und Abgrenzung	41
1. Definitionsansätze	41
2. Historische Entwicklung	42

3. Abgrenzung von vergleichbaren Technologien	43
a) IT-Outsourcing	43
b) Application Service Providing	43
c) Grid Computing	44
II. Technische Umsetzung	45
1. Ausgangspunkt: Ubiquitäre Erreichbarkeit für großen potentiellen Nutzerkreis	45
2. Umsetzungsansatz: Virtualisierung	45
3. Vereinheitlichung der Kommunikation	46
4. Flexible und ortsunabhängige Nutzbarkeit von IT-Ressourcen	47
5. Zwischenergebnis	48
III. Technische Ursachen für Datenverlust	48
1. Maßgebliches Haftungsszenario	48
2. Technisch bedingte Verlustursachen	49
§ 5 Leistungen und Nutzerkreis	50
I. Leistungsarten	50
1. Ausgangspunkt	50
2. Software as a Service (SaaS)	51
3. Platform as a Service (PaaS)	51
4. Infrastructure as a Service (IaaS)	52
5. Everything as a Service (XaaS)	53
II. Betroffener Nutzerkreis	53
1. Private und Public Clouds	54
2. Hybrid und Community Clouds	54
§ 6 Zwischenergebnis	55
3. Kapitel Anwendbares Recht	57
§ 7 Anwendbares Vertragsrecht	57
I. Anwendbarkeit der Rom I-VO	57
II. Rechtswahl	58
III. Objektive Anknüpfung	59
1. Grundsätzliche Anknüpfung	60
2. Keine offensichtlich engere Verbindung zu Drittstaat	61
IV. Besonderheiten bei Verbraucherverträgen	62
1. Verbraucherbegriff	62
2. Bezugspunkt zum Heimatstaat des Verbrauchers	63

3. Kein Ausschluss der Anwendbarkeit	65
4. Einschränkung der Rechtswahl	65
§ 8 Anwendbares Deliktsrecht	66
I. Anwendbarkeit der Rom II-VO	66
II. Rechtswahl	67
III. Objektive Anknüpfung	68
1. Ansprüche des Cloud-Nutzers gegen den Cloud-Anbieter	69
2. Ansprüche des Cloud-Nutzers gegen Dritte	69
a) Maßgebliche Haftungsszenarien	69
b) Ort des Schadenseintritts	70
aa) Erfolgsort bei Online-Delikten	70
bb) Problemstellung im Rahmen des Cloud Computing	71
cc) Ausweichklausel: Art. 4 Abs. 3 Rom II-VO	73
(1) Anknüpfung an das Vertragsstatut	73
(2) Kritische Würdigung	73
(3) Lösungsansatz: Differenzierte Anwendung der Ausweichklausel des Art. 4 Abs. 3 Rom II-VO	75
(a) Bedarf für eine kollisionsrechtliche Korrektur	75
(b) Haftung des externen Hackers	76
(c) Haftung des berechtigten Mitnutzers	76
§ 9 Ergebnis	77
4. Kapitel Vertragliche Haftung	79
§ 10 Vertragstypologische Einordnung	79
I. Ausgangspunkt: Vertragstypen	79
II. Die Typologie einzelner Leistungsarten	80
1. Software as a Service (SaaS)	80
a) Streitstand	80
b) Stellungnahme	81
2. Infrastructure as a Service (IaaS)	84
3. Platform as a Service (PaaS)	85
4. Everything as a Service (XaaS)	86
5. Unentgeltliche Erbringung von Cloud-Leistungen	86

6. Zwischenergebnis	88
III. Vereinbarung von Zusatzleistungen	89
1. Grundsatz	89
2. Vertragstypologische Einordnung konkreter Zusatzleistungen	90
a) Schulung und Support	90
b) Softwarepflege und –anpassung	91
aa) Instandhaltungspflicht	91
bb) Softwareverbesserungen	92
c) Datensicherung	93
IV. Ergebnis	94
§ 11 Haftungsszenarien und Rechtsgrundlagen	94
§ 12 Haftung für den Verlust von Daten während des Betriebs des Cloud-Dienstes	96
I. Maßgebliches Haftungsszenario	96
II. Abgrenzung der anwendbaren Haftungsgrundlagen	96
III. Anspruch des Cloud-Nutzers gegen den Cloud-Anbieter aus § 536 a BGB	98
1. Maßgebliche Fallgruppe	98
2. Mangel der Mietsache	98
3. Vertretemüssen	99
a) Ausgangspunkt	99
b) Anfängliche Mängel der Mietsache	100
c) Nachträglich aufgetretene Mängel der Mietsache	101
aa) Grundsatz	101
bb) Aktiver Verursachungsbeitrag des Cloud-Anbieters zur Mangelbegründung	101
cc) Unterlassung von Instandhaltungsmaßnahmen	102
dd) Unterlassung von allgemeinen Schutzvorkehrungen	103
ee) Einschaltung von Subunternehmern	105
4. Kausalität	106
5. Zwischenergebnis	106
IV. Anspruch des Cloud-Nutzers gegen den Cloud-Anbieter aus § 280 Abs. 1 BGB	106
1. Maßgebliche Fallgruppe	106

2. Pflichtverletzung	107
a) Verletzung einer vertraglichen Hauptleistungspflicht	107
b) Verletzung der Verpflichtung zur Abwehr schädlicher natürlicher Einflüsse	108
aa) Maßgebliche Fallgruppe	108
bb) Mietrechtlicher Ausgangspunkt	108
cc) Konkretisierung durch Anforderungen an physische Datensicherheit	110
(1) Grundsatz: Verpflichtung zur Gewährleistung von IT-Sicherheit	110
(2) Physische Schutzmaßnahmen gegen natürliche Einflüsse als Teil der IT-Sicherheit	111
(3) Umfang der erforderlichen Schutzmaßnahmen	112
(a) Ausgangspunkt: Risikoanalyse	112
(b) Grenze: Zumutbarkeit der Sicherheitsvorkehrungen	113
(c) Erforderliche Maßnahmen zur Gewährleistung physischer Datensicherheit	114
(4) Verarbeitung personenbezogener Daten	116
(a) Gesetzliche Konkretisierung vertraglicher Schutzpflichten	116
(b) Grundlegende Anforderungen aus § 9 BDSG	116
(c) Auswirkungen auf erforderliche physische Datensicherheitsmaßnahmen	117
(5) Telemedienrechtliche Anforderungen	118
(a) Anwendungsbereich	119
(b) Auswirkungen im Hinblick auf Schutzvorkehrungen gegen äußere Einflüsse	119
c) Verletzung der Verpflichtung zur Datensicherung	122
aa) Maßgebliche Fallgruppe	122
bb) Meinungsstand	122
(1) Verpflichtung des Cloud-Nutzers	123
(2) Verpflichtung des Cloud-Anbieters	123

cc) Dogmatischer Anknüpfungspunkt	125
dd) Inhalt der Schutzpflicht	127
(1) Maßgebliche Kriterien	127
(2) Interessenverteilung im Cloud-Computing	129
(3) Einflussnahmemöglichkeit des Cloud-Anbieters	130
(4) Zumutbarkeit	131
(a) Schadenspotential	132
(b) Wahrscheinlichkeit der Schadensverwirklichung	133
(c) Korrespondierender Vermeidungsaufwand	134
(d) Abwägung	135
(5) Schutzwürdigkeit des Betroffenen	136
ee) Zwischenergebnis	138
ff) Umfang der Schutzpflicht	138
(1) Meinungsstand	139
(2) Umfang und Frequenz der Datensicherung durch den Cloud-Anbieter	139
(3) Ort der Datensicherung	141
gg) Zwischenergebnis: Pflicht des Cloud-Anbieters zur Datensicherung	141
3. Vertretenmüssen	142
a) Grundsatz	142
b) Vorsätzliche Verletzung von Sicherungspflichten	142
c) Vorliegen eines Organisationsverschuldens	143
4. Kausalität	144
5. Mitverschulden	144
V. Zwischenergebnis: Haftung des Cloud-Anbieters für Datenverlust während des Betriebs des Cloud-Dienstes	146
§ 13 Haftung für den Verlust von Daten aufgrund unbefugten Fremdzugriffs	146
I. Maßgebliches Haftungsszenario	146
II. Anspruch des Cloud-Nutzers gegen den Cloud-Anbieter aus § 280 Abs. 1 BGB	147
1. Pflichtverletzung	147
a) Verpflichtung zur Abwehr von externen Angriffen	147

b) Umfang der erforderlichen Schutzmaßnahmen	149
aa) Grundsatz	149
bb) Grundlegende Maßnahmen bei gewerblicher Datenverarbeitung	150
cc) Spezifische IT-Sicherheitsrisiken in der Cloud	151
dd) Auswirkungen auf das erforderliche IT-Sicherheitsniveau beim Cloud-Anbieter	153
(1) Erhöhte Anforderungen an technische Schutzvorkehrungen	153
(2) Regelmäßige Durchführung einer Datensicherung	154
(3) Implementierung angemessener Authentifizierungsverfahren	155
(4) Schulungs- und Informationspflichten	156
(5) Verarbeitung personenbezogener Daten	157
(6) Telemedienrechtliche Anforderungen	159
2. Vertretenmüssen	160
III. Zwischenergebnis: Haftung des Cloud-Anbieters bei externen Angriffen auf den Datenbestand	161
§ 14 Haftungsbeschränkung durch AGB	161
I. Grenzen der Haftungsbeschränkung in Cloud-AGB	162
1. Einfache Fahrlässigkeit	162
2. Haftungshöchstgrenzen	164
3. Klauselverbote ohne Wertungsmöglichkeit	164
II. Cloud-Lösungen für Privatanwender	165
1. Amazon Cloud Drive	165
2. Microsoft OneDrive	166
3. Google Cloud Drive	166
4. Haftungsrechtliche Analyse	167
a) Haftungsbeschränkung	167
b) Rezeption in der Rechtsprechung	168
5. Zwischenergebnis	168
III. Kommerzielle Cloud-Lösungen	169
1. Oracle Cloud Services	169
2. Dell Cloud Solutions	169
3. Telekom CRM Services Online	170
4. Analyse im Vergleich zu nicht kommerziellen Cloud-Angeboten	170

5. Zwischenergebnis	171
§ 15 Ergebnis: Vertragliche Haftung im Cloud Computing	171
5. Kapitel Deliktische Haftung	173
§ 16 Haftungsszenarien und Verhältnis zur vertraglichen Haftung	173
I. Maßgebliche Haftungsszenarien	173
II. Verhältnis zur vertraglichen Haftung	174
§ 17 Vorliegen einer Rechtsgutsverletzung im Rahmen des § 823 Abs. 1 BGB	175
I. Maßgebliche Haftungsszenarien	175
II. Verletzung des Eigentums	175
1. Anknüpfung an den Datenträger	176
2. Drittschadensliquidation	176
a) Ausgangspunkt	176
b) Anwendung auf Datenverlust in der Cloud	177
aa) Grundsatz	177
bb) Meinungsstand	177
cc) Stellungnahme	178
(1) Fehlen einer vergleichbaren Interessenlage	178
(2) Mangelnde Eignung zur sachgerechten Auflösung von Haftungsdefiziten	179
c) Zwischenergebnis	180
III. Verletzung des Besitzes	180
1. Qualifikation als sonstiges Recht	180
2. Bestehen eines Besitzrechts des Cloud-Nutzers	181
a) Voraussetzungen	181
b) Besitz an den eingesetzten Servern	182
aa) Meinungsstand	182
bb) Stellungnahme	183
IV. Verletzung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb	183
1. Maßgebliche Fallgruppen	184
2. Rechtsnatur und Qualifikation als sonstiges Recht	184
3. Schutzbereich	185
4. Potentielle Eingriffe	186
5. Rechtswidrigkeit	186
6. Beeinträchtigung von Datenbeständen in der Cloud	187

7. Zwischenergebnis	188
V. Verletzung des Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme	188
1. Maßgebliche Fallgruppe	188
2. Grundrechtlicher Ausgangspunkt	189
3. Qualifikation als sonstiges Recht	189
4. Schutzbereich	190
a) Begriff des informationstechnischen Systems	190
b) Die Cloud als informationstechnisches System	191
aa) Die Entscheidung des BVerfG	191
bb) Stellungnahme	193
5. Potentielle Eingriffe	194
6. Rechtswidrigkeit	195
7. Zwischenergebnis	196
VI. Verletzung des Urheberrechts	196
1. Maßgebliche Fallgruppen	196
2. Qualifikation als sonstiges Recht	197
3. Anwendbarkeit der deliktischen Haftung	197
4. Schutzgut	197
5. Potentielle Verletzungshandlungen	198
6. Zwischenergebnis	199
VII Zwischenergebnis	199
§ 18 Verletzung von Verkehrspflichten	200
I. Maßgebliche Fallgruppe	200
II. Dogmatische Grundlage	201
III. Bestehen einer Verkehrspflicht	202
1. Ausgangspunkt	202
2. Verkehrspflicht des Cloud-Anbieters	203
IV. Ausgestaltung der Verkehrspflicht	203
V. Zwischenergebnis	205
§ 19 Verletzung eines Schutzgesetzes i.S.d. § 823 Abs. 2 BGB	205
I. Dogmatische Grundlage	206
II. Verstoß gegen § 202 a StGB	207
1. Maßgebliche Fallgruppe	207
2. Qualifizierung als Schutzgesetz	208
3. Tatbestand	208
a) Betroffene Datensätze	208

b) Personelle Zuweisung	209
c) Tathandlung	211
d) Subjektiver Tatbestand	211
e) Zugriff auf Daten in der Cloud	212
f) Verhältnis zu § 202 b StGB	212
4. Vorliegen eines Schadens	213
a) Ausgangspunkt	213
b) Rechtsverfolgungskosten	214
c) Schadensermittlungskosten	214
d) Imageschaden	215
5. Zwischenergebnis	216
III. Verstoß gegen § 303 a StGB	216
1. Maßgebliche Fallgruppen	216
2. Qualifizierung als Schutzgesetz	217
3. Tatbestand	217
a) Datenbegriff	217
b) Tathandlung	218
c) Subjektiver Tatbestand	219
d) Verhältnis zu § 303 b StGB	220
aa) Anwendungsbereich und Voraussetzungen	220
bb) Bedeutung im Cloud Computing	221
4. Verschulden	222
a) Grundsatz	222
b) Haftung des externen Hackers	222
c) Haftung des grundsätzlich berechtigten Cloud-Nutzers	223
5. Kausalität	223
6. Zwischenergebnis	225
IV. Verstoß gegen § 263 a StGB	225
1. Maßgebliche Fallgruppe	225
2. Qualifizierung als Schutzgesetz	226
3. Tatbestand	226
a) Tathandlung	226
aa) Bedrohungsszenario	226
bb) Unrichtige Gestaltung eines Programms	227
cc) Sonstige unbefugte Einflussnahme	228
b) Erfordernis eines Vermögensschadens	230
aa) Auseinanderfallen von Angriffsziel und Geschädigtem	230

bb) Vorliegen eines Vermögensschadens	232
(1) Grundsatz	232
(2) Unbefugte Inanspruchnahme von (IT-)Leistungen	232
(3) Datenbeschädigung und Datenverlust	233
(4) Vermögensgefährdung als Schaden	234
c) Subjektiver Tatbestand	236
4. Zwischenergebnis	236
V. Zwischenergebnis	237
§ 20 Eigenständige deliktische Haftungsgrundlagen	238
I. Sittenwidrige Schädigung i.S.d. § 826 BGB	238
1. Maßgebliche Fallgruppe	238
2. Haftungsvoraussetzungen	238
3. Vernichtung von Datenbeständen in der Cloud	239
4. Zwischenergebnis	240
II. Wettbewerbsrechtliche Haftung aus § 9 S. 1 UWG	240
1. Maßgebliche Fallgruppen	241
2. Sachlicher und personeller Anwendungsbereich	242
3. Vorliegen einer gezielten Behinderung	243
a) Grundsatz	243
b) Beeinträchtigung von Datenbeständen in der Cloud	244
4. Zwischenergebnis	244
III. Haftung aus § 1 Abs. 1 S. 1 ProdHaftG	245
1. Maßgebliche Fallgruppe	245
2. Haftungssadressat	246
3. Taugliches Haftungsobjekt	247
a) Streitstand	247
b) Stellungnahme	248
aa) Gänzliche Verneinung der Produkteigenschaft	248
bb) Begrenzung auf Individualsoftware	249
cc) Differenzierung anhand der Übermittlungsart	250
dd) Differenzierung anhand eines Übermittlungserfordernisses	251
(1) Meinungsstand	251
(2) Stellungnahme	252
(a) Wortlaut der Norm	252
(b) Rechtsprechung des EuGH	252
(3) Risikoentscheidung des Herstellers	253

c) Zwischenergebnis	254
4. Fehlerhaftigkeit des Produkts	254
5. Haftungsausschluss aufgrund mangelnder Vorhersehbarkeit	256
6. Subjektives Element	258
7. Erfasste Schadenspositionen	258
8. Zwischenergebnis	259
IV. Zwischenergebnis	259
§ 21 Zwischenergebnis: Rechtschutzlücken im deliktischen Schutz von Datenbeständen	259
§ 22 Lösungsansätze: Absolute Rechtspositionen am Datenbestand	261
I. Bedürfnis nach einer Haftungserweiterung	261
1. Lückenhafter deliktischer Schutz von Datenbeständen	261
2. Gesteigerte Bedeutung digitaler Inhalte in der Cloud	262
3. Erweiterungstendenzen in Rechtsprechung und Literatur	263
4. Zwischenergebnis	264
II. Eigentum am Datenbestand	265
1. Problemstellung	265
2. Meinungsstand	266
3. Rechtsprechung des BGH	267
4. Stellungnahme	268
III. Besitz am Datenbestand	272
1. Meinungsstand	272
2. Stellungnahme	273
IV. Zwischenergebnis	274
V. Recht am generierten Datenbestand	275
1. Bisherige Lösungsansätze in der Literatur	275
a) Meinungsstand	275
b) Stellungnahme	277
c) Vorzüge gegenüber der Anerkennung von sonstigen absoluten Rechten am Datenbestand	278
2. Dogmatische Herleitung	279
a) Anknüpfungspunkt	279
b) Grundlegende Voraussetzungen	280
aa) Zuweisungsfunktion	281
bb) Ausschlussfunktion	281
c) Schutzwürdigkeit	284

3. Personelle Zuordnung	285
a) Problemstellung bei der Zuweisung von Rechtspositionen an Daten	285
b) Potentielle Anknüpfungspunkte	286
aa) Anknüpfung an die inhaltliche Betroffenheit	286
bb) Anknüpfung an faktische Ausschlussmöglichkeiten	287
cc) Anknüpfung an den Datenträger	287
dd) Anknüpfung an die Urheberschaft	289
(1) Ausgangspunkt	289
(2) Kritik	289
(3) Stellungnahme	290
ee) Anknüpfung an den Skripturakt	291
(1) Ausgangspunkt	291
(2) Eignung als Zuordnungskriterium	292
(3) Datenskriptur in Weisungsverhältnissen	293
(a) Meinungsstand	293
(b) Stellungnahme	293
c) Zwischenergebnis	294
4. Terminologische Abgrenzung	295
5. Schutzmfang und Grenzen	297
a) Geschütztes Rechtsgut	297
aa) Betriebsrelevante Daten	297
bb) Ausschließlich personenbezogene Daten	298
cc) Lokal gespeicherte Daten	298
b) Verletzungshandlungen	299
aa) Ausgangspunkt	299
bb) Ausspähung von Daten	299
cc) Datenmanipulation	301
dd) Datenvernichtung	302
c) Anwendung einschränkender Kriterien	302
6. Verschulden	303
7. Zwischenergebnis	304
§ 23 Ergebnis: Deliktische Haftung im Cloud Computing	305
6. Kapitel Ersatzfähiger Schaden	306
§ 24 Grundlagen der Schadensquantifizierung	306
I. Maßgebliche Haftungsszenarien	306

II. Grundlegende Berechnung der Schadenshöhe	306
§ 25 Konkrete Schadenspositionen im Zusammenhang mit dem Verlust von Daten	307
I. Datenwiederherstellung	307
1. Haftung des externen Hackers	308
2. Haftung des berechtigten Mitnutzers	309
3. Haftung des Cloud-Anbieters	310
II. Datenneuerfassung	310
1. Haftung des externen Hackers	311
2. Haftung des berechtigten Mitnutzers	311
3. Haftungs des Cloud-Anbieters	312
III. Entgangener Gewinn	312
1. Maßgebliche Haftungsszenarien	312
2. Beweismaßstab	313
3. Praxisrelevanz	313
§ 26 Der Verlust von Daten als selbstständige Schädigungsfolge	313
I. Ausgangspunkt	314
II. Am Markt handelbare Daten	314
III. Sonstige private Daten	316
IV. Unternehmensdaten mit betrieblicher Relevanz	319
V. Zwischenergebnis: Der materielle Wert von Daten	321
§ 27 Ergebnis	322
7. Kapitel Rechtfertigungsgründe für die Löschung von Daten	323
§ 28 Rechtfertigung einer Datenlöschung durch den Cloud-Anbieter	323
I. Rechtfertigung der Datenlöschung im Rahmen einer Vertragsbeziehung	323
1. Maßgebliches Haftungsszenario	323
2. Rechtfertigende Wirkung der Löschungsverpflichtung	324
a) Dogmatische Einordnung	324
b) Bestehen einer vertraglichen Löschungsbefugnis	325
aa) Grundsatz	325
bb) Ausgestaltung der Klausel	326
c) Fehlen einer vertraglichen Regelung: Ergänzende Vertragsauslegung	326
aa) Vorliegen einer vertraglichen Regelungslücke	327
bb) Ausfüllung der vertraglichen Regelungslücke	328

II. Rechtfertigung der Datenlöschung bei Fehlen einer Vertragsbeziehung	329
1. Maßgebliches Haftungsszenario	329
2. Rechtfertigender Notstand gemäß § 34 StGB	330
a) Systematik	330
b) Notstandslage	331
aa) Maßstab der Gefahrenermittlung	331
bb) Take-down bei vollständiger und zutreffender Sachverhaltskenntnis	332
cc) Take-down bei unvollständiger Sachverhaltskenntnis	332
c) Notstandshandlung	333
3. Geschäftsführung ohne Auftrag	334
a) Anwendbarkeit	335
b) Fremdheit des Geschäfts	335
c) Berechtigung der Geschäftsführung	336
4. Virtuelles Hausrecht	336
a) Meinungsstand	337
b) Stellungnahme	338
5. Rechtfertigende Pflichtenkollision	339
a) Dogmatische Einordnung	340
b) Voraussetzungen	341
III. Zwischenergebnis	342
§ 29 Rechtfertigung einer Datenlöschung durch den Cloud-Nutzer	343
I. Maßgebliches Haftungsszenario	343
II. Ausgangspunkt: § 859 BGB	344
III. Geschäftsführung ohne Auftrag	345
§ 30 Ergebnis	346
8. Kapitel Beweisrechtliche Aspekte	347
§ 31 Grundlegende Nachweisschwierigkeiten im Cloud Computing	347
§ 32 Der Nachweis haftungsbegründender Merkmale durch den Cloud-Nutzer	348
I. Grundlegende Verteilung der Beweislast	348
II. Anspruch gegen den Cloud-Anbieter aus § 536 a BGB	349
1. Maßgebliches Haftungsszenario	349

2. Nachweis der Mangelhaftigkeit der Mietsache	349
a) Ausgangspunkt der Rechtsprechung	349
b) Kritik und Stellungnahme	350
c) Abgrenzung nach Risikosphären	352
d) Beweisantritt im Prozess	353
3. Nachweis des Vertretenmüssens	354
4. Nachweis des Schadenseintritts	355
a) Problemstellung	355
b) Beweiserleichterung aus § 287 ZPO	356
aa) Grundsatz	356
bb) Quantifizierung des Verlustschadens	357
cc) Eintritt eines Schadens	358
c) Beweisantritt im Prozess	359
5. Nachweis der Kausalität	360
6. Zwischenergebnis	360
III. Anspruch gegen den Cloud-Anbieter aus § 280	
Abs. 1 BGB	360
1. Maßgebliches Haftungsszenario	360
2. Nachweis der Pflichtverletzung	361
3. Nachweis des Vertretenmüssens	361
4. Nachweis der Kausalität	362
a) Grundsatz	362
b) Verletzung der Verpflichtung zur Abwehr schädlicher natürlicher Einflüsse und externer Angriffe	363
aa) Sachverständigenbeweis	363
(1) Grundsätzliche Relevanz im IT-Prozess	363
(2) Besonderheiten im Cloud-Bereich	364
(a) Zugriffsverweigerung durch den Cloud-Anbieter	365
(aa) Zumutbarkeit	365
(bb) Ermessensentscheidung	365
(b) Beweissicherung	367
(aa) Ausgangspunkt	367
(bb) Besorgnis der Beweiserschwerung	368
(cc) Beweissicherungsbeschluss für Cloud-Daten	369
(c) Auslandsbezug	369

(aa) Einbeziehung des Zielstaats	370
(bb) Fehlende Durchsetzbarkeit vor nationalen Gerichten	370
bb) Zeugenbeweis	371
cc) Inaugenscheinnahme	371
dd) Anordnung der Vorlegung durch die Gegenpartei	372
ee) Zwischenergebnis	373
c) Verletzung der Verpflichtung zur Datensicherung	373
aa) Beweislastumkehr durch die Rechtsprechung	373
bb) Datensicherung durch den Cloud-Anbieter	374
IV. Schadensersatzanspruch gegen den externen Hacker	375
1. Maßgebliches Haftungsszenario	375
2. Nachweis einer Verletzungshandlung	375
3. Nachweis des Verschuldens	376
4. Nachweis der Kausalität	376
5. Nachweis der Belegenheit der Daten im Schädigungszeitpunkt	376
a) Problemstellung	376
b) Dem Cloud-Anbieter bekannter Belegenheitsort	377
c) Unaufklärbarkeit des Belegenheitsorts	377
V. Schadensersatzanspruch gegen den berechtigten Mitnutzer	378
1. Maßgebliches Haftungsszenario	378
2. Nachweis einer Verletzungshandlung	379
3. Nachweis des Verschuldens	379
4. Zwischenergebnis	379
§ 33 Zwischenergebnis: Unbefriedigende Beweissituation	380
§ 34 Lösungsansätze: Modifizierung der Darlegungs- und Beweislast	381
I. Grundlagen	381
1. Beweislastumkehr	381
a) Dogmatische Einordnung	381
b) Voraussetzungen und Fallgruppen	383
c) Rechtsfolge	384
2. Sonstige Beweiserleichterungen	385
a) Anscheinsbeweis	385
b) Reduzierung des Beweismaßes	386
c) Sekundäre Darlegungslast	387

II. Anspruch gegen den Cloud-Anbieter aus § 536 a BGB	388
1. Nachweis der Mangelhaftigkeit der Mietsache	388
2. Nachweis des Vertretenmüssens	389
3. Nachweis des Schadenseintritts	389
4. Nachweis der Kausalität	390
5. Zwischenergebnis	390
III. Anspruch gegen den Cloud-Anbieter aus § 280	
Abs. 1 BGB	390
1. Nachweis der Pflichtverletzung	390
2. Nachweis des Verschuldens	391
3. Nachweis der Kausalität	392
a) Verletzung der Verpflichtung zur Abwehr schädlicher natürlicher Einflüsse und externer Angriffe	392
b) Verletzung der Verpflichtung zur Datensicherung	393
4. Zwischenergebnis	394
IV. Schadensersatzanspruch gegen den externen Hacker	394
1. Nachweis der Verletzungshandlung	394
2. Nachweis des Verschuldens	395
3. Nachweis der Kausalität	395
V. Schadensersatzanspruch gegen den berechtigten Mitnutzer	395
§ 35 Ergebnis: Beweisführung im Cloud Computing	396
9. Kapitel Zusammenfassung der Ergebnisse	398
§ 36 Anwendbares Recht	398
§ 37 Vertragliche Haftung	399
§ 38 Deliktische Haftung	401
§ 39 Ersatzfähiger Schaden	402
§ 40 Beweisrechtliche Aspekte	403
§ 41 Gesamtergebnis	404
Literaturverzeichnis	407