

Cloud Computing

Rechtshandbuch

Herausgegeben von

Prof. Dr. Georg Borges
Saarbrücken

Dr. Jan Geert Meents
München

Bearbeitet von
den Herausgebern und von

Dr. Thorsten B. Behling, Köln; Prof. Dr. Wolfgang Büchner, München; Dr. Guido Cahsor, Düsseldorf; Dr. Undine von Diemar, LL. M., München; Dr. Thomas Eckhold, LL. M., Düsseldorf; Prof. Dr. Marco Gercke, Köln; Prof. Dr. Florian Haase, Hamburg; Dr. Thomas Jansen, München; Prof. Dr. Helmut Krcmar, München; Birgit Kurtz, New York; Prof. Dr. Michael Lehmann, München; Prof. Dr. Ralf Müller-Terpitz, Mannheim; Prof. Dr. Norbert Nolte, Köln; Dr. Frank Roth, Köln; Dr. Dierk Schindler, Kirchheim; Prof. Dr. Christoph Sorge, Saarbrücken; Prof. Dr. Christoph Thole, Tübingen

2016

C.H.BECK

Inhaltsübersicht

	Seite
Vorwort	V
Bearbeiterverzeichnis	XXVII
Abkürzungsverzeichnis	XXIX
Kapitel 1. Grundlagen	
§ 1 Technische Grundlagen des Cloud Computing	1
§ 2 Business Modelle im Cloud Computing	18
Kapitel 2. Vertragsrecht	
§ 3 Anwendbares Recht	39
§ 4 Vertragliche Beziehungen zwischen Cloud-Nutzer und Cloud-Anbieter	50
§ 5 Vertragliche Beziehungen zwischen Cloud-Anbietern	168
Kapitel 3. Datenschutzrechtliche Aspekte des Cloud Computing	
§ 6 Einführung	209
§ 7 Cloud Computing als Auftragsdatenverarbeitung	225
§ 8 Weitere datenschutzrechtliche Grundlagen für Cloud Computing	277
§ 9 Cloud Computing mit Auslandsbezug	298
§ 10 Datensicherheit (technisch-organisatorische Maßnahmen)	356
§ 11 Kommunikationsrechtlicher Datenschutz	380
Kapitel 4. Haftung und Compliance	
§ 12 Haftungsaspekte beim Cloud Computing	397
§ 13 Compliance und Cloud Computing	416
Kapitel 5. Immaterialgüterrechtliche Aspekte	
§ 14 Immaterialgüterrechtliche Aspekte	441
Kapitel 6. Verfahren und Zugriff auf Daten	
§ 15 Die internationale Zuständigkeit bei grenzüberschreitenden Rechtsstreitigkeiten über Cloud Computing	473
§ 16 Internationaler Zugriff auf Daten (Reichweite von Discovery-Verfahren)	491
§ 17 Zugriff auf Daten durch hoheitliche Befugnisse	512
Kapitel 7. Wirtschaftsrechtliche Aspekte des Cloud Computing	
§ 18 Vergaberecht	533
§ 19 Exportkontrollrecht	559

	Seite
Kapitel 8. Strafrechtliche Fragen	
§ 20 Strafrechtliche und strafprozessuale Aspekte von Cloud Computing und Cloud Storage	581
Kapitel 9. Steuerrechtliche Aspekte	
§ 21 Steuerliche Aspekte	607
Kapitel 10. Bereichsspezifische Aspekte	
§ 22 Nutzung des Cloud Computing durch die öffentliche Hand	643
§ 23 Internationale Praxis der Cloud-Nutzung durch die öffentliche Hand	661
§ 24 Cloud Computing im Finanz-, Versicherungs- und Börsenwesen	677
Stichwortverzeichnis	721

Inhaltsverzeichnis

	Seite
Vorwort	V
Bearbeiterverzeichnis	XXVII
Abkürzungsverzeichnis	XXIX

Kapitel 1. Grundlagen

§ 1 Technische Grundlagen des Cloud Computing

I. Vom traditionellen Outsourcing zum Cloud Computing	3
II. Technische Grundlagen des Cloud Computing	7
1. Begriff und Abgrenzungen	9
2. Private Cloud und Public Cloud	12
3. Hybrid Cloud und Community Cloud	14
4. Datenübertragung/Schnittstellen	15

§ 2 Business Modelle im Cloud Computing

I. Theoretischer Hintergrund und Marktentwicklung	19
1. Dienstleistungen und Dienstleistungsorientierung	19
2. Marktentwicklung	22
II. Anwendungsformen von Cloud Services	22
1. Infrastructure as a Service (IaaS)	24
2. Platform as a Service (PaaS)	26
3. Software as a Service (SaaS)	27
III. Wertschöpfungsstrukturen	28
1. Akteure und Rollen	29
2. Das Cloud Service Ökosystem	32
3. Beispielhafte Illustration des Ökosystems	35
4. Aktuelle Herausforderungen im Wertschöpfungsnetzwerk	36

Kapitel 2. Vertragsrecht

§ 3 Anwendbares Recht

I. Einführung	40
1. Auslandsbezug und anwendbares Recht	40
2. Vertragsbeziehungen beim Cloud Computing	40
3. Anwendbares Recht und Gerichtsstand	40
4. Rechtsgrundlagen	41
II. Rechtswahl	41
1. Grundsatz	41
2. Einschränkungen der Rechtswahl	42
III. Objektive Anknüpfung	43
1. Grundsatz	43
2. Nähere Verbindung zu einem anderen Staat	44
IV. Verbraucherverträge	45
1. Anwendungsbereich des Art. 6 Rom I-VO	45
2. Das nach Art. 6 Rom I-VO anwendbare Recht	47
3. Praktische Bedeutung und Gestaltung	47
V. Umfang des Vertragsstatuts und Sonderanknüpfungen	48

§ 4 Vertragliche Beziehungen zwischen Cloud-Nutzer und Cloud-Anbieter

I. Praxis des Vertragsabschlusses	55
1. Vertragsmodelle	55
2. Standardisierung und Customizing	59
3. Die Vertragsstruktur	60
a) Rahmenvertrag	60
b) Einzelverträge	64
II. Abgrenzung zu anderen Verträgen	65
III. Vertragstypologische Einordnung von Cloud Computing-Verträgen	67
1. Notwendigkeit und Funktion	67
2. Vertragsgegenstand	68
3. Typengemischter Vertrag	69
4. Einordnung entgeltlicher Cloud Computing-Verträge	70
a) Mietvertragliche Einordnung	70
b) Abweichende Einordnungsversuche in der Literatur	73
c) Einordnung der übrigen Vertragsleistungen	74
d) Fazit	76
5. Einordnung unentgeltlicher Cloud Computing-Verträge	77
IV. Die Pflichten der Vertragsparteien	77
1. Mietvertraglich einzuordnende Cloud Services	78
a) Pflichten des Cloud-Nutzers	78
aa) Hauptleistungspflichten	78
bb) Nebenpflichten	78
b) Pflichten des Cloud-Anbieters	79
aa) Hauptleistungspflichten	79
(1) Überlassungspflicht	79
(2) Erhaltungspflicht	81
bb) Nebenpflichten	84
2. Dienst- und werkvertraglich einzuordnende Cloud Services	84
V. Leistungsstörungen	85
1. Mietvertragsrecht	85
a) Vorliegen eines Mangels	86
b) Mängelanzeige des Cloud-Nutzers	87
c) Mängelrechte des Cloud-Nutzers	87
aa) Pflicht des Cloud-Anbieters zur Mängelbeseitigung	87
bb) Minderung	88
cc) Zurückbehaltungsrecht	89
dd) Schadensersatz	89
ee) Recht zur außerordentlichen Kündigung	91
ff) Mängelbeseitigungsrecht des Cloud-Nutzers	91
gg) Wegfall der Mängelrechte	92
2. Dienstvertragsrecht	92
3. Werkvertragsrecht	92
4. Vertragsgestaltung	94
a) Mietvertraglich einzuordnende Cloud Services	96
b) Dienstvertraglich einzuordnende Services	97
c) Werkvertraglich einzuordnende Services	97
VI. Typische Vertragsbestandteile des Cloud Computing-Vertrags	98
1. Notwendigkeit vertraglicher Regelungen	98
2. Die Leistungsbeschreibung	99
a) Bedeutung und Funktion der Leistungsbeschreibung	99
b) Inhalt der Leistungsbeschreibung	101
c) Festlegung der Verfügbarkeit	103
aa) Funktion	103
bb) Inhaltliche Regelung	104

	Seite
d) Festlegung der Performancekriterien	106
e) Change Request-Verfahren	107
3. Service Level Agreement	109
a) Abgrenzung der Leistungsbeschreibung vom Service Level Agreement	109
b) Bedeutung und Funktion	110
c) Grundstruktur eines Service Level Agreement	110
d) Typische Regelungsinhalte	111
aa) Festsetzung von Qualität und Quantität der Leistung	112
bb) Reaktions- und Fehlerbehebungszeiten	112
cc) Service Level Management: Messung, Monitoring und Reporting	113
e) Festlegung eines Sanktionensystems	115
aa) Pauschalierte Minderung	116
bb) Vertragsstrafenregelung und pauschalierter Schadensersatz	117
(1) Vereinbarung einer Vertragsstrafe	117
(2) Vereinbarung eines pauschalierten Schadensersatzes	118
cc) Bonus-Malus-Regelungen	119
dd) Außerordentliche Kündigung	119
f) Haftungsbegrenzungen und Freistellungsregelungen	121
4. Notfall-Management	121
5. Vergütung	122
a) Abrechnung von Cloud Services	123
b) Formen der Fälligkeit	125
c) Sanktionen bei Zahlungsverzug	126
d) Preisanpassungs- und Preiserhöhungsklauseln	127
6. Nutzungsrechte und Nutzungsbeschränkungen	128
7. Datenschutz und Compliance	130
8. Vertraulichkeitsvereinbarungen	130
9. Schutz vor Missbrauch anderer Cloud-Nutzer	132
10. Datensicherung	134
11. Identitätsmanagement	137
12. Dokumentation	138
13. Beendigung des Vertrags	138
a) Vertragsdauer	138
b) Ordentliche Kündigung des Vertrags	139
c) Außerordentliche Kündigung des Vertrags	141
d) Sonderkündigungsrechte	141
e) Sonderkonstellation: Höhere Gewalt	142
f) Form der Kündigungserklärung	142
g) Sonstige Beendigungsumstände	143
h) Exit Management	144
VII. Allgemeine Geschäftsbedingungen	147
1. Wirksame Einbeziehung	148
2. Inhaltskontrolle typischer Klauseln in Cloud Computing-Verträgen	149
a) Einschränkung der mietvertraglichen Erhaltungspflicht	149
b) Beschränkung und Veränderung des Leistungsgegenstands	150
c) Bestätigung der erhaltenen Leistung als vertragsgemäße Leistung	151
d) Pflicht zur Übernahme von Updates	152
e) Preisbeschreibende Klauseln, Preisanpassungs- und Preiserhöhungsklauseln	152
f) Untersagung der Nutzung von Geräten und Software Dritter	154
g) Beschränkung und Ausschluss der Gewährleistung	154
aa) Mietvertraglich einzuordnende Cloud Services	154
(1) Ausschluss des Minderungsrechts	154
(2) Ausschluss des Selbstvornahmerechts	155
(3) Schadensersatzansprüche	156
(4) Kündigungsrecht	159
bb) Dienstvertragliche und werkvertragliche Cloud Services	161

	Seite
h) Sicherung von Sanktionsmöglichkeiten	162
i) Service Level Agreements	162
aa) Kontrollfähigkeit von Verfügbarkeitsquoten	162
bb) Inhaltskontrolle	164
(1) Verfügbarkeitsquote	164
(2) Leistungsvorbehaltsklauseln	165
j) Datenverlust	165
k) Vertragsdauer	165
l) Erleichterung der Verjährung	166
3. Änderung von Allgemeinen Geschäftsbedingungen	166

§ 5 Vertragliche Beziehungen zwischen Cloud-Anbietern

I. Einführung	170
1. Die „Vision“ des Cloud Computing	170
2. Wirtschaftliche Überlegungen und zentrale Strategien der Beteiligten	171
3. Rechtliche Grenzen	172
II. Möglichkeiten der Arbeitsteilung in der Cloud, vertragstypologische Einordnung und Vertragsaufbau	173
1. Vielfältige Geschäftsmodelle	173
2. Vertragstypologische Einordnung	173
3. Modularer Vertragsaufbau	174
III. Typische Merkmale von Verträgen zwischen Cloud-Anbietern	175
1. Auf Langfristigkeit angelegte Vertragsbeziehung	175
2. Häufig grenzüberschreitend	176
3. Technologisch komplex	176
4. Häufig Kooperationen von Wettbewerbern	177
5. Existenzbedrohende Folgen von Systemausfällen und Daten-Lecks	177
6. Erhebliches Haftungsrisiko	177
7. Nutzungsabhängige Vergütungsstrukturen	177
8. Erhebliche Bedeutung von Schutzrechten und Geschäftsgeheimnissen	178
9. Eingeschränkte Austausch-/Ersetzbarkeit von Cloud-Services	178
IV. Cloud-Anbieter-Kooperationsvertrag, Allgemeiner Teil	178
1. Präambel	178
2. Autonomes Regelungswerk	178
3. Definitionenkatalog	179
4. Project Management, Governance	179
5. Anpassung an sich ändernde Rahmenbedingungen oder Anforderungen	179
a) Change-Management	179
b) Preisanpassungs-/Indexierungsklausel	179
c) Höhere Gewalt	180
d) Hardship Clause	180
6. Leistungsstörungen	181
7. Rechtswahl	182
8. Gerichtsstand, Schiedsabrede	183
9. Alternative Streitbeilegung	184
10. Kartellrechtlich verträgliche Exklusivbindungen	185
11. Daten- und Informationssicherheit	185
12. IT-Sicherheit	186
13. Faire und angemessene Haftungsverteilung	186
14. Zahlungsbedingungen, erfolgsabhängige Vergütungsstrukturen	187
15. Zuordnung von und Rechtseinräumung an Schutzrechten und Freistellungsverpflichtungen	187
16. Schutz von Know-How und Geschäftsgeheimnissen	188
17. Exit-Management, Migrationsunterstützung	188

V. Cloud-Anbieter-Kooperationsvertrag, Besonderer Teil: Unterschiedlichen Formen und Inhalte von Cloud-Anbieter-Kooperationen und deren systematische Einordnung	189
1. Implementierungsphase	189
2. Betriebsphase – die unterschiedlichen Cloud-Service-Varianten	189
VI. Unterschiedliche Cloud-Betriebsmodelle	189
1. Cloud-Anbieter-Kooperationen in der Public Cloud	189
2. Cloud-Anbieter-Kooperationen in der Private Cloud	190
3. Cloud-Anbieter-Kooperationen in der Community Cloud	190
4. Cloud-Anbieter-Kooperationen in der Hybrid Cloud	191
VII. Cloud-Kooperationsmodelle auf den verschiedenen Dienste-Ebenen	192
1. Cloud-Anbieter-Kooperation bei Infrastructure as a Service („IaaS“)	192
a) Cloud-Anbieter-Konsortium	192
b) Teilnahme an Angeboten, die über einen elektronischen Marktplatz platziert werden	192
c) Vereinbarungen mit Infrastruktur-Lieferanten	192
d) Beistellung von Hilfsdiensten	193
2. Platform as a Service („PaaS“)-Anbieter-Vertragsbeziehungen	193
a) Das PaaS-Geschäftsmodell	193
b) PaaS Cloud-App-Entwicklung	194
3. Cloud-Anbieter-Kooperation bei Software as a Service („SaaS“)	194
a) Beschaffung von Anwendersoftware	194
b) „Alles-aus-einer-Hand“-Lösungen	195
c) Generalunternehmer-Modell	195
d) Partnermodelle, insbesondere der VAR-Reseller	196
e) Diversifizierter Vertrieb durch Einschaltung „normaler“ Eigenhändler („Reseller“)	197
4. Communication as a Service („CaaS“)-Anbieter-Vertragsbeziehungen	197
VIII. Compliance-Verpflichtungen/regulatorische Vorgaben	198
1. Allgemeine Compliance-Vorgaben	198
a) Datenschutzrechtliche Verpflichtungen	198
b) Fernmeldegeheimnis, TK-Datenschutz	200
aa) „Ganz oder überwiegend“	200
bb) Cloud-Nutzer als TK-Anbieter	200
cc) Geltung des bereichsspezifischen TK-Datenschutzes und des Fernmeldegeheimnisses	201
dd) Unterauftragsvergabe an TK-Netzbetreiber	201
c) Handelsrecht, Steuerrecht	203
aa) Aufbewahrungspflichten	203
bb) Bücher im Inland	203
2. Branchenspezifische Vorgaben für regulierte Industrien	204
a) Banken, Finanzinstitute	204
b) Gesundheitswesen	205
c) Kranken-, Unfall- und Lebensversicherungen	206
d) Telekommunikations-Unternehmen	206
IX. Ergebnis und Ausblick	207

Kapitel 3. Datenschutzrechtliche Aspekte des Cloud Computing

§ 6 Einführung

I. Überblick	210
1. Gesetzliche Grundlagen des Datenschutzes	210
2. Die Reform des europäischen Datenschutzrechts	211
II. Der sachliche Anwendungsbereich des BDSG und der Landesdatenschutzgesetze ...	213
1. Die gesetzliche Regelung	213

	Seite
2. Der Begriff des personenbezogenen Datums	214
a) Die Legaldefinition des BDSG	214
b) Bestimmtheit und Bestimmbarkeit einer natürlichen Person	216
aa) Objektiver und relativer Begriff des Personenbezugs	217
bb) Die Berücksichtigung des Wissens Dritter	218
cc) Berücksichtigung rechtlicher Hindernisse	220
c) Der Personenbezug anonymer und pseudonymer Daten	220
d) Personenbezug und Verschlüsselung von Daten	221
e) Künftige Erkenntnismöglichkeiten	222
3. Anforderungen für die Praxis	223
§ 7 Cloud Computing als Auftragsdatenverarbeitung	
I. Grundlagen	228
1. Auftragsdatenverarbeitung als primäre datenschutzrechtliche Grundlage für Cloud Computing	228
2. Die gesetzliche Regelung der Auftragsdatenverarbeitung	229
a) Die Regelung der Auftragsdatenverarbeitung im BDSG	229
b) Europarechtliche Vorgaben	230
3. Der sachliche Anwendungsbereich der Auftragsdatenverarbeitung	231
4. Auftragsdatenverarbeitung und Drittstaaten	232
a) Anwendbares Recht und materielle rechtliche Zulässigkeit	232
b) Meinungsstand	232
c) Stellungnahme: Zulässigkeit der Auftragsverarbeitung in Drittstaaten	234
d) Praxis der Aufsichtsbehörden	234
e) Zuordnung der Auftragsdatenverarbeitung zum EWR	234
5. Fiktionswirkung und Mängel der Auftragsdatenverarbeitung	235
II. Die Voraussetzungen des § 11 BDSG	237
1. Schriftlicher Vertrag	237
2. Der Inhalt des Vertrags über die Auftragsdatenverarbeitung	239
a) Gegenstand und Dauer des Auftrags	239
b) Umfang, Art und Zweck der Datenverarbeitung	240
c) Technische und organisatorische Maßnahmen	240
d) Berichtigung, Löschung und Sperrung von Daten	242
e) Die Pflichten des Auftragnehmers nach § 11 Abs. 4 BDSG	242
f) Die Berechtigung zur Begründung von Unterauftragsverhältnissen	243
g) Kontrollrechte sowie Duldungs- und Mitwirkungspflichten	244
h) Mitteilung von Datenschutzverstößen	245
i) Umfang der Weisungsbefugnis	246
j) Rückgabe von Datenträgern und Datenlöschung	246
k) Rechtsfolgen unzureichender Angaben	247
3. Standardverträge und AGB-Kontrolle	248
4. Die Auswahl und Kontrolle des Cloud-Anbieters durch den Cloud-Nutzer	248
a) Die sorgfältige Auswahl des Auftragnehmers	248
b) Die Überwachung des Auftragnehmers	249
c) Gegenstand und Durchführung der Kontrolle	250
d) Anforderungen an die Intensität der Kontrolle	250
5. Erfüllung der Kontrollpflicht durch Zertifizierung	252
a) Aktuelle Entwicklungen	252
b) Erfüllung der Kontrollpflicht de lege lata	255
c) Rechtsfolge der Zertifizierung	256
d) Ausgestaltung und praktische Umsetzung der Zertifizierung	258
III. Das Weisungsrecht des Cloud-Nutzers	258
1. Grundlagen	258
2. Gegenstand und Inhalt des Weisungsrechts	258
3. Abweichungen des Auftragnehmers von Weisungen	260
4. Rechtswidrige Weisungen des Auftraggebers	261

	Seite
IV. Cloud Computing und Unterauftragnehmer	262
1. Die Einschaltung von Unterauftragnehmern durch den Cloud-Anbieter	262
2. Das Leitbild der Unterauftragsdatenverarbeitung	264
3. Das Verhältnis zwischen Auftragnehmer und Unterauftragnehmer	266
a) Das Erfordernis eines Vertrags über Auftragsdatenverarbeitung	266
b) Auswahl und Kontrolle des Unterauftragnehmers	266
c) Das Weisungsrecht des Auftragnehmers	267
d) Die Verantwortlichkeit des Cloud-Anbieters für den Unterauftragnehmer ...	267
4. Das Verhältnis zwischen Cloud-Nutzer und Unterauftragnehmer	268
a) Der Stand der Diskussion	268
b) Auswahl und Kontrolle	269
aa) Stellungnahme: Aufsichtspflicht statt doppelter Kontrolle	269
bb) Durchgriffsmöglichkeit des Cloud-Nutzers	270
cc) Praktische Gestaltung der Organisationspflicht des Cloud-Nutzers	271
dd) Das Kontrollerfordernis bei mehrstufiger Auftragsdatenverarbeitung	271
ee) Die Organisationsverantwortung des Cloud-Anbieters	272
c) Weisungsrecht des Cloud-Nutzers?	272
5. Anforderungen an den Auftragsdatenverarbeitungsvertrag bei Einschaltung von Unterauftragnehmern	273
a) Anforderungen an den Vertrag zwischen Cloud-Nutzer und Cloud-Anbieter ..	273
b) Anforderungen an den Vertrag zwischen Cloud-Anbieter und seinen Unterauftragnehmern	275
§ 8 Weitere datenschutzrechtliche Grundlagen für Cloud Computing	
I. Cloud Computing und Einwilligung	278
1. Allgemeine Voraussetzungen der Einwilligung und Cloud Computing	278
2. Bezeichnung des Cloud-Anbieters als Empfänger der Daten	279
3. Freiwilligkeit der Einwilligung und AGB-Kontrolle	282
4. Die Form der Einwilligung	284
5. Widerruf und Erneuerung der Einwilligung	285
6. Fazit	286
II. Rechtfertigung von Cloud Computing nach § 28 BDSG	287
1. Einführung	287
a) Fallgruppen und praktische Bedeutung	287
b) Datenverarbeitung für eigene Zwecke des Cloud-Anbieters	288
2. Keine generelle Rechtfertigung von Cloud Computing nach § 28 BDSG	289
3. Rechtfertigung nach § 28 BDSG außerhalb des Anwendungsbereichs der Auftragsdatenverarbeitung	291
a) Maßgebliche Fallgruppen und Kriterien	291
b) Die Ausgestaltung des Diensts analog der Auftragsdatenverarbeitung	291
c) Technische Sicherungsmaßnahmen, insbesondere Verschlüsselung	292
d) Funktionsübertragung	293
e) Cloud-Dienste in Drittstaaten	293
III. Cloud-Dienste für Verbraucher	295
1. Fehlen einer gesetzlichen Regelung	295
2. Analoge Anwendung der Auftragsdatenverarbeitung	296
3. Die Anforderungen an die Auftragsdatenverarbeitung für Verbraucher	297
§ 9 Cloud Computing mit Auslandsbezug	
I. Aspekte des grenzüberschreitenden Cloud Computing	302
II. Das anwendbare Datenschutzrecht	303
1. Die maßgeblichen Kollisionsnormen	303
a) Überblick	303
b) Die gesetzliche Regelung des anwendbaren Datenschutzrechts	304
aa) Die kollisionsrechtliche Regelung der Datenschutzrichtlinie	304
bb) Die Kollisionsregeln des § 1 Abs. 5 BDSG	305

	Seite
c) Die Aussagen des EuGH zum internationalen Anwendungsbereich	306
d) Gleichstellung von Tochtergesellschaft und Zweigniederlassung	308
e) Adressat des Datenschutzrechts	309
f) Betreiben der Datenverarbeitung als Grundlage der Zuordnung	310
g) Unterstützung durch Niederlassung als Anknüpfunggrundlage	311
h) Mehrheit von Anknüpfungspunkten	312
aa) Fragestellung bei mehreren Anknüpfungspunkten im EWR	312
bb) Mehrheit von Anknüpfungspunkten bei Tochtergesellschaften	312
cc) Mehrheit von Anknüpfungspunkten bei Zweigniederlassungen	313
dd) Reichweite der Anknüpfung an die Niederlassung	314
2. Die Anknüpfung an Sitz und Niederlassung der verantwortlichen Stelle	315
a) Die Reichweite der Anknüpfung nach § 1 Abs. 5 S. 1 BDSG	315
b) Die Belegenheit der verantwortlichen Stelle	316
c) Begriff und Belegenheit der Niederlassung	317
aa) Der Begriff der Niederlassung	317
bb) Die Bedeutung des Außenkontakts	318
cc) Belegenheit und Steuerung von Datenverarbeitungsanlagen	320
dd) Ergebnis: Der datenschutzrechtliche Niederlassungsbegriff	321
d) Subsidiarität der Anknüpfung an den wirtschaftlichen Zusammenhang	322
e) Kollisionsrechtliche Abspaltung der Anforderungen an die technische Sicherheit	323
f) Einzelfälle zur Niederlassung	324
g) Niederlassungen in Drittstaaten	326
3. Die Anknüpfung an den Ort der Datenverarbeitung	327
a) Ort der Datenverarbeitung und anwendbares Datenschutzrecht	327
b) Belegenheit von Rechnern im Inland	328
c) Datenverarbeitung über Websites	330
d) Nichtanwendung des BDSG auf Datentransit	330
4. Das anwendbare Datenschutzrecht bei der Auftragsdatenverarbeitung	331
a) Die akzessorische Anknüpfung der Auftragsdatenverarbeitung	331
b) Das für die technischen und organisatorischen Maßnahmen maßgebliche Recht	332
5. Umfang des Datenschutzstatuts und Statutenwechsel	333
6. Darstellung der Ergebnisse in Fallgruppen	334
a) Das auf den Cloud-Nutzer anwendbare Datenschutzrecht	334
aa) Cloud-Nutzer mit Sitz im EWR	334
bb) Cloud-Nutzer mit Sitz in Drittstaaten	335
b) Das auf den Cloud-Anbieter anwendbare Recht	336
aa) Die Vorfrage: Vorliegen einer Auftragsdatenverarbeitung	336
bb) Das anwendbare Recht im Fall der Auftragsdatenverarbeitung	337
cc) Anwendbares Datenschutzrecht außerhalb der Auftragsdatenverarbeitung	338
c) Das Betreiben der Datenverarbeitung	338
d) Umfang des Datenschutzstatuts und Statutenwechsel	338
III. Cloud Computing durch Anbieter im EWR	339
1. Die Zuordnung von Cloud-Diensten zum EWR	339
2. Besondere materiellrechtliche Anforderungen	340
IV. Cloud Computing durch Anbieter in Drittstaaten	341
1. Überblick	341
a) Auftragsdatenverarbeitung	341
b) Besondere materielle Anforderungen bei Übermittlung der Daten	341
2. Angemessenes Schutzniveau im Staat des Cloud-Anbieters	342
3. Safe Harbor	343
a) Die Bedeutung der Safe Harbor-Grundsätze	343
b) Die aktuelle Diskussion zu den Safe Harbor-Grundsätzen	344
4. Zulässigkeit der Übermittlung nach § 4c Abs. 1 BDSG (Einwilligung)	347

	Seite
5. Genehmigung und Binding Corporate Rules	348
a) Die Zulässigkeit der Datenübermittlung aufgrund Genehmigung	348
b) Verbindliche Unternehmensregeln (Binding Corporate Rules)	348
c) Binding Corporate Rules und Auftragsdatenverarbeitung	349
6. Standardvertragsklauseln und Cloud Computing	350
a) Standardvertragsklauseln	350
b) Die Voraussetzungen der Standardvertragsklauseln von 2010	352
c) Standardvertragsklauseln und Unterauftragnehmer	353
7. Die materiellen Anforderungen an Nutzung von Cloud-Diensten in Drittstaaten	354
§ 10 Datensicherheit (technische-organisatorische Maßnahmen)	
I. Schutzziele	357
II. Maßnahmen und Risiken	359
1. Allgemeines	359
2. Maßnahme Verschlüsselung	364
3. Cloud-spezifische Maßnahmen und Risiken	366
a) Einsatzmodeile	366
b) Dienste	368
aa) IaaS	368
bb) PaaS	371
cc) SaaS	373
III. Forschung	376
IV. Fazit	377
§ 11 Kommunikationsrechtlicher Datenschutz	
I. Einleitung	381
II. Anwendbarkeit der Datenschutzvorgaben im TKG und TMG	382
1. Fragestellung	382
2. Telekommunikations- und Telemediendienste	383
3. Cloud-Dienste als Telekommunikationsdienste	384
4. Cloud-Dienste als Telemediendienste	387
III. Einzelne telekommunikationsrechtliche Datenschutzvorschriften	388
1. Datenschutz nach §§ 91 ff. TKG	388
2. Fernmeldegeheimnis	389
a) Schutz nach § 88 TKG	389
b) Schutz nach § 206 StGB	389
3. IT-Sicherheit gemäß § 109 TKG	392
4. Herausgabepflicht nach § 113 TKG	392
5. Meldepflicht gemäß § 6 TKG	393
6. Kundenschutz gemäß §§ 43a ff. TKG	393
IV. Einzelne telemedienrechtliche Datenschutzvorschriften	393
Kapitel 4. Haftung und Compliance	
§ 12 Haftungsaspekte beim Cloud Computing	
I. Überblick	399
1. Schadensszenarien	399
2. Schäden und Anspruchsgrundlagen	399
II. Anwendbares Recht	400
1. Die maßgebliche Kollisionsnorm	400
2. Haftung des Cloud-Anbieters	400
a) Rechtswahl	401
b) Objektive Anknüpfung	401

	Seite
c) Die Bestimmung des Erfolgsorts im Cloud Computing	402
d) Umfang des Deliktsstatuts	402
3. Haftung des Cloud-Nutzers	403
III. Haftung für Datenverlust und Datenveränderung	403
1. Überblick	403
2. Haftungsprivilegierung nach TMG und Datenveränderung	403
3. Eingriff in Schutzgüter des Cloud-Nutzers oder Dritter	404
a) Verletzung von Urheberrechten	404
b) Eingriff in nach § 823 Abs. 1 BGB absolut geschützte Rechte	405
c) Sonstige deliktsrechtliche Anspruchsgrundlagen	406
d) Datenschutzrecht	407
4. Verkehrspflichten zur Datensicherung	408
5. Die Bedeutung des IT-Sicherheits-Gesetzes	409
a) Das IT-Sicherheits-Gesetz	409
b) Die Regelung zu Kritischen Infrastrukturen und Cloud Computing	410
c) Die Pflichten der Betreiber von Telemediendiensten	411
aa) Anwendungsbereich	412
bb) Schutzpflichten der Betreiber von Telemediendiensten	412
cc) Durchsetzungsmechanismen	414
d) Fazit	415
§ 13 Compliance und Cloud Computing	
I. Einleitung	417
II. Compliance-Anforderungen an das Cloud Computing im Allgemeinen	418
III. Spezielle Compliance-Anforderungen an das Cloud Computing – gesetzliche und regulatorische Vorgaben im Einzelnen	420
1. IT-Sicherheit	420
a) IT-Sicherheit als wesentliche Compliance-Pflicht	420
b) IT-Sicherheit und Compliance-Management	421
aa) Schutzbedarfsanalyse	421
bb) Verfügbarkeitsmanagement	421
cc) Zugriffsmanagement	422
dd) Trennungskontrolle und Security Breach-Management	423
ee) Datenlösch-, Sperr- und Archivierungs-Management	423
ff) Informationssicherheits-Managementsysteme (ISMS)	425
2. Datenschutzrechtliche Compliance-Anforderungen	426
a) Vorabkontrolle	426
b) Pflicht zur Durchführung von Audits	427
c) Compliance bei Drittstaatentransfers	428
aa) Safe Harbor-Zertifizierungen	429
bb) EU-Standardvertragsklauseln	430
cc) Binding Corporate Rules	430
dd) Sonderfall USA Patriot Act und NSA	431
3. Berufsrechtliche Compliance-Anforderungen	433
a) Berufsheimnisträger	434
b) Banken	436
4. Weitere gesetzliche Compliance-Anforderungen	436
a) Telekommunikationsrecht	436
b) Urheber- und Markenrecht	437
c) Sozialrecht	437
d) Exportkontrollrecht	438
IV Fazit	439

Kapitel 5. Immaterialgüterrechtliche Aspekte

Seite

§ 14 Immaterialgüterrechtliche Aspekte

I. Internationale Aspekte	445
1. Das Prinzip der Territorialität	445
2. Gerichtsstand	448
a) Gerichtsstandsvereinbarungen (Prorogation)	448
b) Keine Gerichtsstandsvereinbarung für Klagen, welche die Eintragung und Gültigkeit von Immaterialgüterrechten betreffen	448
c) Keine Gerichtsstandsvereinbarung zu Lasten des europäischen Verbrauchers	449
3. Anwendbares Recht	450
a) Gesetzliche Ansprüche	450
b) Vertragliche Ansprüche, insbesondere aus Lizenzverträgen	452
II. Urheberrechtliche Aspekte des Cloud Computings	454
1. Begriff und Bedeutung der „Vervielfältigung“	455
2. Lizenzvertrag – Kaufvertrag – Dienstleistungsvertrag	459
3. Application Service Providing und Software as a Service	461
4. Kaufverträge und Lizenzverträge für digitale Inhalte	462
a) Kaufvertrag und Übertragung von digitalem „Eigentum“	462
b) Lizenzvertrag und zeitlich beschränkte Einräumung von Nutzungsrechten ..	463
III. Cloud Computing als patentrechtlich geschütztes Geschäftsmodell?	465
1. Schutz von Geschäftsmodellen	465
2. Computerimplementierte Erfindungen	465
IV. Die Störerhaftung von Cloud-Anbietern	467
1. Haftung der Service-Provider	467
2. Gerichtsstand	468
3. Anwendbares Recht	468
a) Unterlassungs- und Beseitigungsansprüche	469
b) Störerhaftung und Immaterialgüterrecht	470
c) Schadensersatz- und Auskunftsansprüche	470
d) Störerhaftung von Internet-Anschlussinhabern	472

Kapitel 6. Verfahren und Zugriff auf Daten**§ 15 Die internationale Zuständigkeit bei grenzüberschreitenden Rechtsstreitigkeiten über Cloud Computing**

I. Einführung	474
II. Anwendbare Regelungen für die internationale Zuständigkeit	475
1. Reichweite der EuGWO	475
a) Weichenstellung anhand des Sitzes des Beklagten	475
b) Kein qualifizierter Auslandsbezug erforderlich	476
2. Reichweite des Lugano-Übereinkommens	477
3. Reichweite des autonomen Zuständigkeitsrechts	477
III. Einzelne Gerichtsstände nach der EuGWO	477
1. Gerichtsstandsvereinbarung, Art. 25 (Art. 23 aF) EuGWO	478
2. Verbrauchergerichtsstand, Art. 17, 18 (Art. 15, 16 aF) EuGWO	479
3. Vertragsgerichtsstand, Art. 7 Nr. 1 (Art. 5 Nr. 1 aF) EuGWO	480
a) Grundlagen	480
b) Einordnung des Cloud Computings	481
c) Die Bestimmung des Erfüllungsorts unter Art. 7 Nr. 1 (Art. 5 Nr. 1 aF) lit. a und b EuGWO beim Cloud Computing	482
4. Deliktgerichtsstand, Art. 7 Nr. 2 (Art. 5 Nr. 3 aF) EuGWO	483
a) Grundlagen	483
b) Deliktssachen iSd Art. 7 Nr. 2 (Art. 5 Nr. 3 aF) EuGWO im Bereich des Cloud Computing	484

	Seite
5. Gerichtsstand der Niederlassung	486
6. Sonstige Gerichtsstände	486
IV. Einzelne Gerichtsstände nach deutschem autonomen Recht	486
V. Praktische Beispiele	487
Fall 1: Klage gegen einen Cloud-Anbieter mit Sitz in der EU	487
Fall 2: Klage gegen einen Cloud-Anbieter aus einem Drittstaat	488
Fall 3: Klage gegen einen Cloud-Anbieter im B2C-Bereich	488
Fall 4: Klage gegen einen Cloud-Anbieter im B2B-Bereich	489
Fall 5: Klage gegen Geschäftsleiter wegen mangelhafter IT-Compliance	489
Fall 6: Arbeits- und betriebsverfassungsrechtliche Streitigkeiten wegen Cloud Computing	489
§ 16 Internationaler Zugriff auf Daten (Reichweite von Discovery Verfahren)	
I. Einleitung	492
II. Zeitliche Einordnung	492
III. Zwecke der Discovery	493
IV. Reichweite der Discovery	493
1. Reichweite generell	494
2. Zuständigkeit des Gerichts	495
V. Herausgabe von Unterlagen	495
1. Wer muss Unterlagen herausgeben?	496
a) Konzerngesellschaften einer Partei	496
b) Dritte	497
2. Was muss herausgegeben werden?	497
3. „E-Discovery“	498
a) Daten in der Cloud	500
b) Datenschutz	501
c) Kostenabwälzung („Cost Shifting“)	501
d) Aufbewahrungspflicht („Duty to Preserve“)	502
e) Datenspeicher-Richtlinien („Document Retention Policy“)	503
VI. Zeugnisverweigerungsrechte	505
1. Attorney-Client Privilege	505
2. Work Product Doktrin	505
3. Verzicht auf den Schutz („Waiver“)	506
4. Vertrauliche Geschäftsinformationen	507
VII. Strafen für Nichtbeachtung („Sanctions“)	508
VIII. Das Haager Beweismittelübereinkommen	508
IX. Fazit	510
§ 17 Zugriff auf Daten durch hoheitliche Befugnisse	
I. Staatliche Zugriffsbefugnisse nach deutschem Recht	515
1. Zugriffsbefugnisse der Verfassungsschutzbehörden	515
a) Online-Durchsuchungen	515
b) Überwachung der Telekommunikation	516
c) Terrorismusbekämpfungsgesetz	517
2. Zugriffsbefugnisse der Polizeibehörden	518
a) Online-Durchsuchungen durch das Bundeskriminalamt	518
b) Online-Durchsuchungen durch Landespolizeibehörden	518
3. Zugriffsbefugnisse der Strafverfolgungsbehörden	519
a) Beschlagnahme von gespeicherten Daten	519
b) Durchsicht räumlich getrennter elektronischer Speichermedien	520
c) Überwachung der Telekommunikation	521
d) Verkehrsdaten und Bestandsdaten	521
4. Zugriffsbefugnisse unter dem Telekommunikationsgesetz	522

	Seite
II. Staatliche Zugriffsbefugnisse nach US-Recht	523
1. Entstehungsgeschichte des Patriot Act	523
2. Foreign Intelligence Surveillance Act	523
3. National Security Letters	524
4. Geheimhaltung	525
5. Rechtshilfeabkommen	525
6. Extraterritoriale Erstreckung der US-Zugriffsbefugnisse	525
7. Zugriff auf Daten innerhalb nachrichtendienstlicher Programme (PRISM etc.)	526
III. Konsequenzen für die datenschutzrechtliche Zulässigkeit der Einschaltung von Cloud-Anbietern	527
1. Datenspeicherung in den USA	527
2. Datenspeicherung im Europäischen Wirtschaftsraum mit US-Bezug	529

Kapitel 7. Wirtschaftsrechtliche Aspekte des Cloud Computing

§ 18 Vergaberecht

I. Einführung	534
II. Stand der Bemühungen um Cloud Computing in der öffentlichen Verwaltung	535
III. Regelungsziele und Rechtsquellen des Vergaberechts	536
1. Gegenstand des Vergaberechts	536
2. Regelungsziele	537
3. Rechtsquellen	537
4. Vergabegrundsätze	540
5. Öffentliche Auftraggeber	541
6. Öffentlicher Auftrag und einschlägige Vergabeordnung	542
7. Vergabearten	543
8. Zuschlag und Vertragsabschluss	544
9. Rüge und Nachprüfungsverfahren	546
IV. Vorbereitung und Durchführung der Vergabe von Aufträgen für Cloud Computing	548
1. UfAB	548
2. Vorbereitung des Vergabeverfahrens	548
3. Schätzung des Auftragswerts	549
4. Wahl der Vergabeart	550
5. Losbildung	551
6. Vergabebekanntmachung und Teilnahmewettbewerb	551
7. Vergabeunterlagen und Vertragsbedingungen	554
8. Vertragsverhandlungen	555
9. Zuschlagskriterien und Angebotswertung	556
V. Angebot von Cloud Computing-Lösungen in konventionellen Vergabemaßnahmen	557

§ 19 Exportkontrollrecht

I. Exportkontrolle in Deutschland und Europa	561
1. Prinzipien	561
2. Rechtsgrundlagen	561
II. Cloud Computing als exportrechtlich relevanter Sachverhalt	562
1. Objekte der Exportkontrolle	562
2. Ausfuhrvorgang	563
a) Unterscheidung Ausfuhr/Verbringung	563
b) Cloud Computing als Exportvorgang	563
c) Ausführende bzw. verbringende Person	564
d) Verschlüsselung und Private Clouds	566
3. Technische Unterstützung	567
4. Ergebnis	567

	Seite
III. Durchführung der Exportkontrolle	567
1. Verfahren	567
a) Anwendbarkeit des allgemeinen Verwaltungsverfahrenrechts	567
b) Zu beantragende Genehmigungen	568
c) Allgemeine Genehmigungen	568
d) Meldepflichten	568
e) Nullbescheid	569
2. Unternehmensorganisation	569
a) Internal Compliance	569
b) Ausführverantwortlicher	570
c) Checkliste	571
3. Außenwirtschaftsprüfungen durch Hauptzollämter	571
4. Strafrechtliche Sanktionen	572
a) Objektive Tatbestände der §§ 17, 18 AWG (ex § 34 AWG)	572
b) Subjektiver Tatbestand	573
c) Rechtsfolgen	574
5. Ordnungswidrigkeiten	575
IV. US-Exportkontrollrecht	576
1. Internationale Anwendbarkeit	576
2. Anwendungsfälle und Rechtsgrundlagen	576
3. US-Exportkontrollrecht und Cloud Computing	577
V. Aktuelle rechtliche Entwicklungen	577
1. Deutschland	577
2. Europäische Union	578
3. USA	578
VI. Fazit und Handlungsempfehlungen	579

Kapitel 8. Strafrechtliche Fragen

§ 20 Strafrechtliche und strafprozessuale Aspekte von Cloud Computing und Cloud Storage

I. Einleitung	584
1. Begriffsbestimmung	584
2. Entwicklung der Diskussion um strafrechtliche Aspekte von Cloud Computing	584
II. Herausforderungen für die Strafverfolgungsbehörden	585
1. Transnationale Dimension	586
2. Geschwindigkeit der Datenübertragung	588
3. Beschränkte Zeit für Ermittlungen	588
4. Fehlender physischer Zugriff auf Daten im Ausland	590
5. Verschlüsselung von Daten als Herausforderung für die Ermittlungsbehörden	591
6. Bestimmung des physikalischen Speicherorts zur Zuständigkeitsbestimmung ...	592
III. Herausforderungen für die Cloud-Nutzer	593
IV. Problemfelder des materiellen Strafrechts und Fragen der Strafanwendung	594
1. Anwendung des Deutschen Strafrechts	594
2. Problembereiche des materiellen Strafrechts	595
a) Abfangen von Daten	595
b) Angriffe auf die Verfügbarkeit der Daten in der Cloud	596
c) Urheberstrafrechtliche Erfassung von Cloud-typischen Streaming-Diensten	597
d) Strafbarkeitslücken beim Einsatz von Streaming-Diensten im Zusammenhang mit kinderpornographischen Inhalten	598
V. Problemfelder des Strafprozessrechts	600
1. Überwachung der Kommunikation statt Durchsuchungsmaßnahmen	600
2. Offener Zugriff bei Cloud-Anbietern im Inland	601
3. Fernzugriff auf Daten bei Cloud-Anbietern im Inland	601
4. Fernzugriff auf Daten bei Cloud-Anbietern im Ausland	602

	Seite
a) Keine Ermächtigung durch § 110 Abs. 3 StPO	602
b) Umstrittene und territorial nur eingeschränkte Befugnis des Art. 32b) der Cybercrime Konvention	603
c) Rechtshilfeersuchen	604

Kapitel 9. Steuerrechtliche Aspekte

§ 21 Steuerrechtliche Aspekte

I. Einleitung	609
II. Ertragsteuern	612
1. Nationale Sachverhalte	612
2. Betriebsstättenbegründung durch Cloud Computing	612
a) Relevanz	612
b) Definition der Betriebsstätte	613
aa) Nationales Steuerrecht	614
bb) Abkommensrecht	617
c) Schlussfolgerungen für das Cloud Computing	618
3. Quellensteuern	620
a) Grundlagen	620
b) Relevanter Abzugstatbestand	621
c) Steuersatz	623
d) Stufenverhältnisse	624
e) Abgeltungswirkung	625
f) Entstehung der Steuer	627
g) Missbrauchsvermeidung	629
aa) Steuerabzug als Grundregel	629
bb) Erstattungsverfahren	630
cc) Freistellungs- und Kontrollmeldeverfahren	631
dd) § 50d Abs. 3 EStG	631
4. Buchführungsfragen	632
a) Grundlagen	632
aa) Verpflichtung zur Buchführung und Aufzeichnungspflichten	632
bb) Führen von Büchern	632
cc) Elektronische Buchführung	632
dd) Digitalisierung von Unterlagen	634
b) Vagabundierende Buchführung und Cloud Computing	634
aa) IaaS	634
bb) PaaS	634
cc) SaaS	634
III. Umsatzsteuer	635
1. Grundlagen	635
a) Steuerbarer Umsatz als sonstige Leistung	635
b) Unterscheidung nach dem Leistungsempfänger	636
c) Elektronische Leistungen	637
d) Grenzfälle	639
2. Schlussfolgerungen für das Cloud Computing	639
a) IaaS	639
b) PaaS	640
c) SaaS	640

Kapitel 10. Bereichsspezifische Aspekte

§ 22 Nutzung des Cloud Computing durch die öffentliche Hand	Seite
I. Thematische Eingrenzung	644
1. Begriff und Bedeutung des Cloud Computing	644
2. „Public“ und „Private Clouds“	645
a) „Echtes“ Cloud Computing in der „Public Cloud“	645
b) „Unechtes“ Cloud Computing in der „Private Cloud“	646
II. Cloud Computing in der öffentlichen Verwaltung	646
1. „Ist-Zustand“	646
2. Zukunftsperspektiven	647
a) Perspektiven für die „Private Cloud“	647
b) Perspektiven für die „Public“ und „Hybrid Cloud“	648
c) Cloud Computing in Europa	650
III. Verfassungsrechtliche Vorgaben für die Nutzung von Cloud Computing	650
1. Grundrechtliche Vorgaben	650
a) Recht auf informationelle Selbstbestimmung	650
b) Recht auf Datensicherheit	651
2. Legitimations- und Kompetenzprobleme	652
a) Cloud Computing und Privatisierung	652
b) Cloud Computing und vertikale Verwaltungskooperationen	653
aa) Verbot der Mischverwaltung	654
bb) Schlussfolgerungen für das Cloud Computing	654
c) Cloud Computing und horizontale Verwaltungskooperationen	655
IV. Einfachrechtliche Vorgaben für die Nutzung von Cloud Computing	655
1. Vergaberechtliche Vorgaben	655
a) „Private Cloud“ und Vergaberecht	655
b) „Public Cloud“ und Vergaberecht	657
2. Sonstige spezialgesetzliche Vorgaben	658
a) Landesdatenschutzrecht	658
b) Sozialrecht	658
c) Steuerrecht	659
V. Fazit	659
 § 23 Internationale Praxis der Cloud-Nutzung durch die öffentliche Hand	
I. Übersicht	662
II. Länderberichte	663
1. USA	663
a) Hintergrund	663
b) Der Lösungsansatz zur G-Cloud in den USA	664
c) Fazit	666
2. Singapur	666
a) Hintergrund	666
b) Der Lösungsansatz zur G-Cloud in Singapur	667
c) Fazit	670
3. UK	670
a) Hintergrund	670
b) Der Lösungsansatz zur G-Cloud in UK	670
c) Fazit	672
4. Frankreich	673
a) Hintergrund	673
b) Der Lösungsansatz zur G-Cloud in Frankreich	674
c) Fazit	675
III. Zusammenfassender Vergleich	675

§ 24 Cloud Computing im Finanz-, Versicherungs- und Börsenwesen	Seite
I. Aufsichtsrechtliche Bedeutung der Technik des Cloud Computings	683
II. Aufsichtsrechtliche Anforderungen	685
1. Ordnungsgemäße IT-Infrastrukturen	686
a) Gesetzlich normierte Grundsätze	686
aa) Ordnungsgemäßheit der Geschäftsorganisation	686
bb) Ordnungsgemäßheit der IT-Infrastruktur	688
cc) Auslagerung (Outsourcing) von IT-Infrastruktur	691
dd) Unternehmensgruppen	695
b) Konkretisierung der Grundsätze durch Mindestanforderungen der Aufsicht	695
aa) Rechtliche Einordnung	696
bb) Inhaltliche Konkretisierungen zur IT-Sicherheit und IT-Zuverlässigkeit	697
cc) Inhaltliche Konkretisierungen des Notfallkonzepts	700
dd) Inhaltliche Konkretisierung der IT-Auslagerung (Outsourcing)	701
2. Bedeutung für das Cloud Computing	704
a) Aufsichtsrelevante Funktionsweise	705
b) Auslagerung (Outsourcing)	706
c) Typisierende aufsichtsrechtliche Einordnung	707
aa) Private Cloud	707
bb) Public Cloud	708
cc) Typübergreifende aufsichtsrechtliche Problemstellungen	709
d) Aufsichtsrechtliche Gesamteinordnung	711
III. Aufsichtsrechtliche Eingriffsbefugnisse und Sanktionen	712
IV. Geheimnisschutz	713
1. Bankgeheimnis	714
2. Strafrechtlich verbürgter Geheimnisschutz	716
a) Kreditinstitute	716
b) Versicherungsunternehmen	717
c) Rechtsdogmatische Lösungsansätze	717
3. Geheimnisschutz trotz Auslagerung	719
Stichwortverzeichnis	721