

Inhaltsübersicht

A. Einleitung	35
I. Cloud Computing – IT „as a Service“	35
II. Chancen und Risiken innovativer Technologielösungen als Herausforderungen an einen Rechtsrahmen	39
III. Gang der Darstellung	41
B. Die Grundlagen von Cloud Computing	42
I. Von Mainframes zu Datenwolken	42
II. Technische Rahmenbedingungen für Cloud Computing	46
III. Basistechnologien von Cloud Computing	49
IV. Begriff und Definition von Cloud Computing	56
V. Service Modelle	62
VI. Bereitstellungsmodelle	74
VII. Die geographischen Dimensionen von Cloud Computing	82
C. Zentrale Herausforderungen von Cloud Computing an den Rechtsrahmen für Datenschutz	84
I. Einleitung – Das Spannungsfeld zwischen Cloud Computing und Datenschutz	84
II. Das anzuwendende Datenschutzrecht bei einem „Rechnen in Datenwolken“	86
III. Der Personenbezug von Daten	126
IV. Internationale Datentransfers	147
V. Allgemeine Daten- und Informationssicherheit (§ 9 BDSG)	207
VI. Auftragsdatenverarbeitung (§ 11 BDSG)	235
VII. Datenübermittlung (nach § 28 Abs. 1 S. 1 Nr. 2 BDSG)	293
D. Zusammenfassung	298
I. Herausforderungen an das anzuwendende Datenschutzrecht	298
II. Herausforderungen an den Personenbezug von Daten	300
III. Herausforderungen im Kontext internationaler Datentransfers an EU-Standardvertragsklauseln und verbindliche Unternehmensregelungen	301
IV. Herausforderungen an transatlantische Datentransfers in die USA auf Basis von Safe Harbor	303

V. Herausforderungen an die Grundsätze der Daten- und Informationssi- cherheit.....	304
VI. Herausforderungen an eine Auftragsdatenverarbeitung	306
VII. Herausforderungen an eine Datenübermittlung	309
Literaturverzeichnis	311
Sachverzeichnis	338

Inhaltsverzeichnis

A. Einleitung	35
I. Cloud Computing – IT „as a Service“	35
II. Chancen und Risiken innovativer Technologielösungen als Herausforderungen an einen Rechtsrahmen	39
III. Gang der Darstellung	41
B. Die Grundlagen von Cloud Computing	42
I. Von Mainframes zu Datenwolken	42
1. Meilensteine des Informationszeitalters auf dem Weg zur Cloud	42
2. Cloud Computing – Evolution oder Revolution?	45
II. Technische Rahmenbedingungen für Cloud Computing	46
1. Breitbandige Internetzugänge und mobile Kommunikation	46
2. Vielfältige Zugangsgeräte	47
a) Von PC bis Smartphone – Zugangsgeräte in Zeiten wachsender mobiler Kommunikation	47
b) Zugangsgeräte in einem Smart Grid und Internet der Dinge	47
c) Thin Clients und Zero Clients	48
3. Einfache Zugriffsmöglichkeiten via Browser oder App	48
4. Leistungsstarke Hardware und breitbandige Standortvernetzung	49
III. Basistechnologien von Cloud Computing	49
1. Grid Computing	49
2. Computer Cluster	51
3. Service-orientierte Architekturen (SOA)	51
4. Virtualisierung	52
a) Systemvirtualisierung durch einen Hypervisor	53
b) Anwendungsvirtualisierung	54
c) Vorteile	54
5. Server-based Computing und Application Service Providing	55
IV. Begriff und Definition von Cloud Computing	56
1. Einleitung	56
2. The NIST Definition of Cloud Computing	57
3. Definition des BSI	59
4. Stellungnahme und zugrunde gelegte Begriffsdefinition	59
5. Abgrenzung zu „klassischem“ IT-Outsourcing	61
V. Service Modelle	62
1. Einleitung – Der Gedanke von „IT/Everything as a Service“ (XaaS)	62
2. Infrastructure as a Service (IaaS)	63

a) Wesentliche Charakteristika und Vorteile	63
b) Praxisbeispiele	64
aa) Amazon Web Services	65
(1) Amazon Elastic Compute Cloud (Amazon EC2).....	66
(2) Amazon Simple Storage Service (Amazon S3).....	66
(3) Availability Zones und Regionen	67
bb) Dropbox	67
3. Platform as a Service (PaaS)	68
a) Wesentliche Charakteristika und Vorteile	68
b) Praxisbeispiele	69
4. Software as a Service (SaaS)	69
a) Wesentliche Charakteristika und Vorteile	69
b) Praxisbeispiele	70
aa) Microsoft Office 365	71
bb) Google Apps for Business	72
cc) salesforce.com	72
dd) Apple iCloud	73
5. Weitere Ausprägungen und Spezifizierungen	74
VI. Bereitstellungsmodelle	74
1. Public Cloud	74
a) Charakteristika und wesentliche Elemente	74
b) Vor- und Nachteile von Public Clouds	75
2. Private Cloud	76
a) Charakteristika und wesentliche Elemente	76
b) Vor- und Nachteile von Private Clouds	77
c) „Echtes“ Cloud Computing in der Private Cloud? – Eine Frage des begrifflichen Verständnisses	78
3. Spezielle Ausprägungen	79
a) Hybrid Cloud	79
b) Virtual Private Cloud	80
c) Community Cloud	80
d) Regionale Clouds und weitere Unterteilungen	81
VII. Die geographischen Dimensionen von Cloud Computing	82
C. Zentrale Herausforderungen von Cloud Computing an den Rechtsrah- men für Datenschutz	84
I. Einleitung – Das Spannungsfeld zwischen Cloud Computing und Da- tenschutz	84
II. Das anzuwendende Datenschutzrecht bei einem „Rechnen in Daten- wolken“	86
1. Einleitung	86
2. Rechtsrahmen – § 1 BDSG	87
a) Territorialitätsprinzip	87

b) Kollisionsrechtliche Regelungen nach § 1 Abs. 5 BDSG	88
aa) Kollisionsregelung gegenüber EU/EWR-Staaten (§ 1 Abs. 5 S. 1 BDSG).....	88
(1) Sitzprinzip	88
(2) Niederlassungsprinzip	89
bb) Kollisionsregelung gegenüber Drittstaaten (§ 1 Abs. 5 S. 2–4 BDSG)	90
3. Herausforderungen von Cloud Computing an das anzuwendende Datenschutzrecht	91
a) Die Herausforderung der Bestimmung des Datenverarbeitungsstandorts und dessen territoriale Zuordnung zu einer Jurisdiktion bei grenzüberschreitenden Datenverarbeitungsszenarien	91
aa) Charakteristika dieser Herausforderung.....	91
(1) Verteiltes, IT-systemunabhängiges und standortübergreifendes Rechnen	91
(2) Datenreplikationen in hochverfügbaren Storage-Clustern	92
(3) Intransparente Anbieterinformationen und ungleiche Verhandlungskonstellationen	93
bb) Bewertung dieser Herausforderung	94
(1) Auswirkungen auf die Bestimmung des anzuwendenden Datenschutzrechts.	94
(a) Höhere Abstraktionsebene bei Standortbestimmung: Berücksichtigung sämtlicher der Datenwolke zugrunde liegenden Standorte	94
(b) Orientierung an allgemeinen Handlungsempfehlungen für Cloud Computing.....	95
(2) Auswirkungen auf die datenschutzrechtliche Verantwortlichkeit	96
(a) Keine oder nur unzureichende Kenntnis über Datenverarbeitungsstandorte	96
(b) Kenntnis über Datenverarbeitungsstandorte.....	97
(aa) Eingrenzbare Datenwolken.....	97
(bb) Jurisdiktionsübergreifende Datenwolken	97
(cc) Rechtliche Folgen einer jurisdiktionsübergreifenden Cloud-Infrastruktur.....	98
(3) Ergebnis	98
cc) Cloud Computing und die Anwendbarkeit des BDSG bei Kenntnis über die Datenverarbeitungsstandorte – Ein Blick auf praxisrelevante Datenverarbeitungsszenarien	99
(1) Sicht eines datenschutzrechtlich verantwortlichen Nutzers aus Deutschland.....	99
(a) Datenverarbeitung außerhalb von EU und EWR (Drittstaaten)	99

(b) Datenverarbeitung in „EU-Clouds“	100
(c) Datenverarbeitung in Deutschland (einschließlich EU-Stellen)	100
(d) Ergebnis	101
(2) Cloud Computing und die Anwendbarkeit des BDSG bei einer außereuropäischen Stelle	101
(a) § 1 Abs. 5 S. 2 BDSG	101
(b) Inländische Mittel	102
(aa) Technische Betrachtung	102
(bb) Normative Auslegung	103
(cc) Ergebnis	103
(c) Teleologische Reduktion des Anwendungsbereichs von § 1 Abs. 5 S. 2 BDSG (im Fall der Verarbeitung personenbezogener Daten ohne Verbindung zur EU)	104
(aa) Sicht der Art.-29-Datenschutzgruppe zu Art. 4 Abs. 1 lit. c) EG-Datenschutz-Richtlinie	104
(bb) Sicht des Düsseldorfer Kreises	106
(cc) Ergebnis	106
b) Die Herausforderung der intransparenten Struktur multinationaler Konzerne als Cloud-Anbieter	107
4. Das anzuwendende Datenschutzrecht nach der EU-Datenschutzreform	109
a) Hintergründe der Datenschutzreform und Cloud-Computing-Strategie der Kommission	109
aa) Die Entwicklung einer Strategie für Cloud Computing	110
bb) Cloud Computing „Public Consultation“ der Kommission ..	111
cc) Strategiepapier der Kommission zu Cloud Computing	112
b) Bewertung des geplanten Rechtsrahmens für das anzuwendende Datenschutzrecht	114
aa) Anwendung auf die für die Datenverarbeitung Verantwortlichen in der Union – Art. 3 Abs. 1 DS-GVO-E	114
bb) Anwendung der EU-Vorschriften auf für die Datenverarbeitung Verantwortliche in Drittländern – Art. 3 Abs. 2 DS-GVO-E	115
(1) EU-Bürger als Leistungsadressat bei Waren oder Dienstleistungen	116
(a) Allgemein in Betracht kommende Anknüpfungskriterien	117
(b) Übertragung i.R.v. Art. 4 Abs. 1 lit. c) EG-Datenschutz-Richtlinie anzulegender Kriterien	117
(c) Überlegungen zum Adressatengedanken bei Cloud Computing	118

(d) Zwischenfazit – Weitere Präzisierung der heranzuziehenden Kriterien.....	119
(e) Drei- oder Mehrpersonenverhältnisse.....	119
(2) Rückgriff auf inländische Mittel.....	120
(3) Aufsicht außereuropäischer Anbieter und Rechtsdurchsetzung.....	121
(4) Stellungnahme – Licht und Schatten bei der Anwendung der DS-GVO auf außereuropäische Stellen.....	122
5. Die rechtsordnungsübergreifende Herausforderung von uneinheitlichen nationalen Datenschutzvorschriften in den Mitgliedstaaten...	123
a) Die Rechtszersplitterung als Hindernis bei der Cloud-Service-Erbringung.....	123
b) Ein einheitlicher Rechtsrahmen durch die EU-Datenschutzreform.....	124
III. Der Personenbezug von Daten.....	126
1. Einleitung.....	126
2. Rechtsrahmen – Personenbezogene Daten (§ 3 Abs. 1 BDSG).....	127
a) Bestimmtheit.....	128
b) Bestimmbarkeit.....	128
aa) Absoluter Personenbezug.....	128
bb) Relativer Personenbezug.....	129
cc) Auswirkungen an dem Beispiel von dynamisch vergebenen IP-Adressen.....	129
dd) Neuere Entwicklungen und EU-Datenschutzreform.....	130
3. Die Herausforderung von datenschutzneutralen Verarbeitungsmöglichkeiten in einer Cloud durch Datenveränderung.....	132
4. Bewertung.....	132
a) Nutzerseitige Datenveränderung außerhalb der Cloud.....	133
aa) Anonymisierung – § 3 Abs. 6 BDSG.....	133
(1) Absolute, „echte“ Anonymisierung.....	133
(2) Faktische, „unechte“ Anonymisierung.....	134
(3) Einsatzbereich bei Cloud Computing.....	135
bb) Pseudonymisierung und Verschlüsselung.....	135
(1) Pseudonymisierung – § 3 Abs. 6a BDSG.....	135
(2) Verschlüsselung von Daten.....	136
(a) Rechtliche Einordnung reversibler Verschlüsselungstechniken.....	137
(b) Der Re-Identifizierungsaufwand bei Verschlüsselungstechniken.....	138
(aa) Allgemeines zu dem Re-Identifizierungsaufwand.....	138
(bb) Der Re-Identifizierungsaufwand im Lichte von „cloud power“, Datenreplikationen, Snapshots und verteilter Datenverarbeitungen.....	139

(cc) Ergebnis zu dem Re-Identifizierungsaufwand bei Verschlüsselungstechniken	140
(c) Einsatzbereich reversibel verschlüsselter Daten bei Cloud Computing	142
(aa) Cloud-Storage	142
(bb) Weitergehende Datenverarbeitungszwecke (mit Rechenoperationen)	142
α) Unverschlüsselte Daten im Zeitpunkt der Verarbeitung	142
β) Homomorphe Verschlüsselung	143
(d) Ergebnis zu der Verschlüsselung von Daten	144
cc) Ergebnis zu nutzerseitig veränderten Daten außerhalb der Cloud.	144
b) Verschlüsselung in der Cloud	145
5. Lösungsmöglichkeiten – Überlegungen zu einem künftigen Rechtsrahmen	145
IV. Internationale Datentransfers	147
1. Einleitung – Globale Datenwolken und Datenströme in einem digitalen Zeitalter	147
2. Der allgemeine Rechtsrahmen für internationale Datentransfers (§§ 4b, 4c BDSG)	148
a) Freier Datenverkehr im Anwendungsbereich des EU-Rechts (§ 4b Abs. 1 BDSG)	149
b) Grundsätzliches Übermittlungsverbot bei Drittstaatentransfers (§ 4b Abs. 2 S. 2 BDSG)	150
c) Die Angemessenheit des Datenschutzniveaus (§ 4b Abs. 3 BDSG)	150
d) Angemessenheitsentscheidung der Kommission	151
e) Ausnahmetatbestände nach § 4c BDSG	153
3. Herausforderungen von Cloud Computing an den Rechtsrahmen für internationale Datentransfers	153
a) Die Herausforderung der Bestimmung einer Empfangsdestination und deren territoriale Zuordnung bei grenzüberschreitenden Datenverarbeitungsszenarien	154
b) Flexible und bedarfsgerechte Nutzungsszenarien als Herausforderung an Vertragsklauseln als ausreichende Garantien eines angemessenen Schutzniveaus	155
aa) Charakteristika dieser Herausforderung	155
bb) EU-Standardvertragsklauseln	155
(1) Rechtsrahmen – Kennzeichnende Elemente von Standardvertragsklauseln	155
(2) Cloud-spezifische Bewertung von Standardvertragsklauseln	157
(a) Zeitlicher und wirtschaftlicher Aufwand	158

(b) Anpassungsmöglichkeiten auf Seiten eines Cloud-Anbieters	159
(c) Aufsichtsbehördliche Ansicht der ergänzenden Berücksichtigung von § 11 Abs. 2 BDSG entsprechenden Anforderungen (am Beispiel der „Orientierungshilfe Cloud Computing“)	159
(d) Ergebnis – Notwendigkeit eines differenzierten Umgangs	160
cc) Verbindliche Unternehmensregelungen („Binding Corporate Rules“)	161
(1) Rechtsrahmen	161
(a) Kennzeichnende Elemente	161
(b) Genehmigungspflicht	162
(c) Kooperationsverfahren und „mutual recognition“ ..	164
(2) Cloud-spezifische Bewertung von verbindlichen Unternehmensregelungen	165
(a) Anwendungsbereich bei Cloud Computing: Private Clouds	165
(b) Vereinfachungen und Standardisierungen	166
(c) Processor Binding Corporate Rules	167
dd) Vertragsklauseln nach der geplanten EU-Datenschutzreform	168
(1) Datenübermittlung auf Grundlage eines Angemessenheitsbeschlusses der Kommission (Art. 41 DS-GVO-E)	168
(2) Datenübermittlung auf Grundlage geeigneter Garantien (Art. 42 DS-GVO-E)	169
(3) Stellungnahme und Überlegungen zu einem künftigen Rechtsrahmen	170
c) Die Herausforderung globaler Unterauftragsverhältnisse	171
d) Transatlantische Datentransfers in die USA – Die Marktdominanz und hohe Beliebtheit von US-Cloud-Anbietern als Herausforderung an einen praxistauglichen Rechtsrahmen	172
aa) Die „Safe-Harbor-Vereinbarung“ als Sonderregelung für Datentransfers in die USA	172
(1) Einleitung – Freiwillige Selbstregulierung des US-Datenempfängers	172
(2) Rechtsrahmen – Gegenstand und Inhalt der Safe-Harbor-Kommissionsentscheidung	174
(a) Die Angemessenheit des von den Safe-Harbor-Grundsätzen gewährleisteten Schutzes	174
(b) Die sieben Grundsätze des „sicheren Hafens“ zum Datenschutz	174
(aa) Informationspflicht („Notice“)	175
(bb) Wahlmöglichkeit („Choice“)	175

(cc) Weitergabe („Onward Transfer“)	175
(dd) Sicherheit („Security“)	176
(ee) Datenintegrität („Data Integrity“)	176
(ff) Auskunftsrecht („Access“)	176
(gg) Durchsetzung („Enforcement“)	176
(c) Safe-Harbor-Beitritt einer US-Organisation	177
(aa) Selbstzertifizierung durch öffentliche Verpflichtung zu den Safe-Harbor-Grundsätzen	177
(bb) US-Organisation unterliegt den gesetzlichen Befugnissen einer staatlichen Einrichtung	178
(3) US-Cloud-Anbieter und Safe Harbor	179
(4) Safe or Unsafe Harbor? – Datenwolken-taugliche Vereinbarung oder Schönwetterabkommen?	180
(a) Praxiserfahrungen in dem ersten Jahrzehnt des Abkommens	181
(aa) Umsetzungsberichte der Kommissionsdienststellen aus den Jahren 2002 und 2004	181
(bb) Safe Harbor: Fact or Fiction? – Die „Galectia-Studie“ aus dem Jahr 2008	182
(cc) Zwischenergebnis	184
(b) Auswirkungen und Folgen der Kritiken an Safe Harbor	185
(aa) Safe Harbor aus der Sicht der Aufsichtsbehörden für den Datenschutz	185
α) Der Beschluss des Düsseldorfer Kreises vom 28./29. April 2010	185
β) Orientierungshilfe Cloud Computing	186
γ) Art.-29-Datenschutzgruppe – Stellungnahme zum Cloud Computing (WP 196)	187
δ) Weitere Ansichten (exemplarisch)	188
ε) Stellungnahme – Dokumentations- und Nachweispflichten in flexiblen Nutzungsszenarien	189
(bb) Safe Harbor aus Sicht der juristischen Literatur	191
(cc) Safe Harbor aus Sicht der Kommission – Mitteilung aus dem November 2013	192
(dd) Safe Harbor aus Sicht des Europäischen Parlaments – Entschließung vom 12. März 2014	193
(c) Ein vergleichender Blick über den Atlantik – Ansichten und Entwicklungen in den USA	193
(aa) Safe Harbor und Cloud Computing aus Sicht des US-Handelsministeriums	193

α)	Stellungnahme der International Trade Administration zu WP 196 der Art.-29-Datenschutzgruppe – „Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing“	193
β)	Anmerkung	194
(bb)	Die (fehlende) Durchsetzung durch die FTC – Entwicklungen in den letzten Jahren	195
α)	Erste Verfahren der FTC zu dem Vorliegen der Selbstzertifizierung an sich	195
β)	Der Google-Buzz-Vergleich	196
γ)	Vergleiche der FTC mit Facebook und MySpace	197
δ)	Vergleiche der FTC mit US-Unternehmen in der ersten Hälfte des Jahres 2014	198
ε)	„Privacy Enforcement and Safe Harbor“ – Stellungnahme von Mitarbeitern der FTC an die Kommission aus dem November 2013	199
ζ)	Stellungnahme	200
(d)	Ergebnis – Safe Harbor als geltender Rechtsrahmen auch für Cloud Computing	201
bb)	Vorschläge für eine Verbesserung des Safe-Harbor-Rechtsrahmens zur Wiederherstellung von Vertrauen im Zuge der NSA-Überwachungsaffäre	202
(1)	Vorschläge der Kommission aus dem November 2013 ..	202
(2)	Verbesserungsvorschläge der Art.-29-Datenschutzgruppe zu Safe Harbor	203
cc)	Vorlage an den EuGH zur Verbindlichkeit der Safe-Harbor-Kommissionsentscheidung durch den irischen High Court in Dublin	204
dd)	Gedanken zu einem künftigen Rechtsrahmen für transatlantische Datentransfers; „EU-Safe-Harbour“	204
e)	Weitere Auswirkungen der Überwachungsaktivitäten der NSA auf internationale Datentransfers in die USA	205
aa)	Reaktion der Datenschutzkonferenz – Pressemitteilung vom 24. Juli 2013	205
bb)	Stellungnahme	206
V.	Allgemeine Daten- und Informationssicherheit (§ 9 BDSG)	207
1.	Einleitung	207
2.	Rechtsrahmen	207
a)	Schutzziele der Daten- und Informationssicherheit	207
b)	Technische und organisatorische Daten- und Informationssicherheit nach § 9 BDSG und dessen konkretisierender Anlage	208
c)	Die Daten- und Informationssicherheit außerhalb des BDSG ..	211

3. Herausforderungen von Cloud Computing an die Daten- und Informationssicherheit	212
a) Technische und organisatorische Risiken auf den Ebenen einer IT-Sicherheitsarchitektur	213
aa) Infrastruktur-/Rechenzentrumsebene (Sicherheit von Gelände und Gebäude)	213
(1) Gefährdungslage und typische technische und organisatorische Maßnahmen	213
(2) Colocation und Serverhousing als klassisches Praxisbeispiel auf Rechenzentrumsebene	214
(3) Bewertung	215
bb) IT-System-Ebene und Systemvirtualisierung (Sicherheit der Server, Router, Switches und anderer IT-Systeme; Sicherheit virtueller IT-System-Umgebungen)	216
(1) Gefährdungslage und typische technische und organisatorische Maßnahmen	216
(2) Bewertung	218
cc) Netzwerkebene	219
(1) Gefährdungslage und typische technische und organisatorische Maßnahmen	219
(2) Bewertung	219
dd) Anwendungs-/Software-Ebene	220
(1) Gefährdungslage und typische technische und organisatorische Maßnahmen	220
(2) Bewertung	220
ee) Ebenenübergreifende, allgemeine Gefahren	221
(1) Administrative Schnittstellen	222
(2) Anbieterabhängigkeit („vendor lock-in“), Portabilität und Insolvenz eines Anbieters	222
(3) Verfügbarkeit eines Cloud-Services und der Leitungswege	222
(4) Vervielfältigung und Verteilung von Daten aufgrund von breitbandigen Datenleitungen und schnellen Glasfaserverbindungen	223
(5) Die Löschung von Daten bei einem verteilten Rechnen	223
ff) Ergebnis – Neue Konzepte zur Gewährleistung der Daten- und Informationssicherheit bei Cloud Computing und modernen Formen der Datenverarbeitung	224
gg) Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)	225
hh) EU-Datenschutzreform	226

b) Die Herausforderung der potentiellen Zugriffsmöglichkeiten durch Sicherheitsbehörden in Drittstaaten am Beispiel des USA PATRIOT Act.	226
aa) USA PATRIOT Act – Ausweitung sicherheitsbehördlicher Befugnisse zur Terrorismusbekämpfung	227
(1) Foreign Intelligence Surveillance Act (FISA)	227
(2) National Security Letter (NSL)	228
(3) Statistiken zur „FISA Implementation“	229
bb) Auswirkungen auf die Daten- und Informationssicherheit bei Cloud Computing	229
(1) Extraterritoriale Auswirkungen des USA PATRIOT Act – Kreis der von US-Anordnungen potentiell betroffenen Unternehmen	230
(2) Folgen für den Cloud-Anbieter – Rechtsunsicherheiten aufgrund konträrer Verpflichtungen zweier Rechtsordnungen	231
(3) Folgen für den Cloud-Nutzer – Eingeschränkte Wahrnehmung der datenschutzrechtlichen Verantwortlichkeit (etwa aufgrund einer fehlenden Kenntnis durch eine „gag order“)	231
cc) Entscheidung des „United States District Court for the Southern District of New York“ vom 25. April 2014	232
dd) Handlungsbedarf zur Beseitigung bestehender Rechtsunsicherheiten	233
ee) EU-Datenschutzreform	234
VI. Auftragsdatenverarbeitung (§ 11 BDSG)	235
1. Einleitung – Modernes IT-Outsourcing	235
2. Das „Privileg“ der Auftragsdatenverarbeitung	236
3. Abgrenzung zur Funktionsübertragung – Cloud Computing als klassische Konstellation einer Auftragsdatenverarbeitung	237
4. Internationale Auftragsdatenverarbeitung	239
a) Rechtsrahmen – § 3 Abs. 8 S. 3 BDSG	239
b) Herausforderungen von Cloud Computing	240
aa) Die Sicherstellung einer Datenverarbeitung auf EU/EWR-Gebiet	240
bb) Die rechtliche Privilegierung einer internationalen Auftragsdatenverarbeitung in „sicheren Drittstaaten“ als Herausforderung der globalen Dimension von Cloud Computing	241
(1) Ausgangslage und Problematik	241
(2) Privilegierung bei festgestelltem angemessenen Schutzniveau („sicherer Drittstaat“)	243
(a) Fehlende Grundlage im BDSG und Gleichstellungsgebot	243
(b) Gesetzesänderungsvorschlag des Bundesrates	243

(c) Stellungnahme.....	244
(3) Privilegierung bei Einsatz von Standardvertragsklauseln für Auftragsdatenverarbeiter („Set III“).....	245
(a) Modifizierte Erforderlichkeitsprüfung i. R. v. § 28 Abs. 1 S. 1 Nr. 2 BDSG.....	245
(b) Richtlinienkonforme Auslegung.....	246
(aa) Vollharmonisierungswirkung der EG-Datenschutz-Richtlinie.....	246
(bb) Begriffsverständnis i. S. d. EG-Datenschutz-Richtlinie.....	247
(c) Analogie zu § 3 Abs. 8 BDSG.....	247
(d) Stellungnahme.....	247
cc) Unterauftragsdatenverarbeitung in Drittstaaten.....	248
c) Ergebnis und Blick auf die Datenschutzreform.....	249
5. Anforderungen nach § 11 BDSG.....	249
a) Vertragliche Festlegungen bei Auftragserteilung – Verhandlungskonstellationen im Anbieter-Nutzer-Verhältnis und die Verhandlungsbereitschaft von Cloud-Anbietern.....	249
aa) Rechtsrahmen – § 11 Abs. 2 S. 2 BDSG.....	249
bb) Anbieterseitige Mitwirkungshandlungen als Herausforderung von Cloud Computing.....	250
cc) Bewertung.....	251
dd) Lösungsmöglichkeiten und Anforderungen an einen künftigen Rechtsrahmen.....	252
b) Form der Auftragserteilung.....	253
aa) Rechtsrahmen – § 11 Abs. 2 S. 2 BDSG.....	253
bb) Herausforderungen von Cloud Computing: Flexible Nutzungsmodelle und vielfältige Zugangsgeräte.....	254
cc) Bewertung.....	254
dd) Lösungsmöglichkeiten und Anforderungen an einen künftigen Rechtsrahmen.....	255
ee) EU-Datenschutzreform.....	256
c) Technische und organisatorische Maßnahmen – Auswahlentscheidung, vertragliche Festlegung und Auftragskontrolle.....	257
aa) Rechtsrahmen.....	258
(1) Sorgfältige Auswahlentscheidung – § 11 Abs. 2 S. 1 BDSG.....	258
(2) Vertragliche Festlegung – § 11 Abs. 2 S. 1, S. 2 Nr. 3 BDSG, § 9 BDSG i. V. m. Anlage zu § 9 BDSG.....	258
(3) Auftragskontrolle – § 11 Abs. 2 S. 2 Nr. 7, S. 4 BDSG.....	259
bb) Herausforderungen von Cloud Computing.....	260
(1) Intransparente Anbieterinformationen und eine hohe technische Komplexität.....	260
(a) Charakteristika dieser Herausforderungen.....	260

(aa) Intransparente Anbieterinformationen zu den Datenverarbeitungsstandorten und den dort implementierten technischen und organisatorischen Maßnahmen	260
(bb) Die technische und organisatorische Komplexität von Cloud-Umgebungen	261
(b) Bewertung und Lösungsmöglichkeiten	261
(2) Standortkontrollen in Zeiten eines verteilten Rechnens	262
(a) Charakteristika dieser Herausforderung	262
(aa) Fehlende Kontrollmöglichkeiten	262
(bb) Praktische Handhabung eines „Vor-Ort-Kontroll-Tourismus“	262
(cc) Kontrolle geographisch verteilter Standorte ..	262
(b) Bewertung und Lösungsmöglichkeiten	263
(3) Zwischenfazit zu den Herausforderungen von Cloud Computing	264
(a) Zielkonflikt zwischen dem Rechtsrahmen und modernen Datenverarbeitungsformen	264
(b) Zeitgemäße Auslegung des geltenden Rechts (Technische und organisatorische Maßnahmen im Lichte der technologischen Realität)	265
(aa) Enge, wortlautgetreue Auslegung	265
(bb) Cloud-spezifische Auslegung	266
(4) Die Vielfalt der gegenwärtig in Bezug genommenen Zertifizierungen	267
(a) ISO/IEC 27001 (einschließlich ISO/IEC 27002, ISO/IEC 27017, ISO/IEC 27018)	267
(aa) Darstellung des Standards	267
(bb) Bewertung	270
(cc) Ausblick auf Weiterentwicklungen: ISO/IEC 27017 (Cloud Computing auf Basis von ISO/IEC 27002) und ISO/IEC 27018 (Datenschutz in Public Clouds)	271
(b) ISO 9001	271
(c) SAS 70, SSAE 16 und ISAE 3402	273
(aa) Darstellung der Standards	273
(bb) Bewertung	274
(d) TRUSTe Privacy Program	275
(e) Cloud Security Alliance STAR Certification	276
(f) EuroCloud Star Audit	276
(aa) Gegenstand der Zertifizierung	276
(bb) Bewertung	278
(g) Ergebnis – Die Entwicklung geeigneter Zertifizierungen für das Cloud-Zeitalter	279

cc) Lösungsmöglichkeiten, Anforderungen an einen künftigen Rechtsrahmen und EU-Datenschutzreform	280
d) Unterauftragsverhältnisse (§ 11 Abs. 2 S. 2 Nr. 6 BDSG).....	283
aa) Rechtsrahmen	283
bb) Herausforderungen von Cloud Computing	283
cc) Bewertung	284
dd) Lösungsmöglichkeiten und Blick auf die EU-Datenschutzreform.	285
e) Weisungen (§ 11 Abs. 2 S. 2 Nr. 9, Abs. 3 BDSG)	287
aa) Rechtsrahmen	287
bb) Herausforderungen von Cloud Computing	288
cc) Bewertung	288
dd) Lösungsmöglichkeiten und Blick auf die EU-Datenschutzreform.	289
f) Rückgabe überlassener Datenträger und Löschung von Daten (§ 11 Abs. 2 S. 2 Nr. 10 BDSG).....	290
aa) Rechtsrahmen	290
bb) Herausforderungen von Cloud Computing	291
cc) Bewertung	291
dd) Lösungsmöglichkeiten und Blick auf die EU-Datenschutzreform.	292
VII. Datenübermittlung (nach § 28 Abs. 1 S. 1 Nr. 2 BDSG).....	293
1. Wahrung berechtigter Interessen der verantwortlichen Stelle.....	293
2. Erforderlichkeit	294
3. Interessenabwägung	295
4. Ergebnis	296
D. Zusammenfassung	298
I. Herausforderungen an das anzuwendende Datenschutzrecht.....	298
II. Herausforderungen an den Personenbezug von Daten.....	300
III. Herausforderungen im Kontext internationaler Datentransfers an EU-Standardvertragsklauseln und verbindliche Unternehmensregelungen ..	301
IV. Herausforderungen an transatlantische Datentransfers in die USA auf Basis von Safe Harbor	303
V. Herausforderungen an die Grundsätze der Daten- und Informationssicherheit.....	304
VI. Herausforderungen an eine Auftragsdatenverarbeitung	306
VII. Herausforderungen an eine Datenübermittlung	309
Literaturverzeichnis	311
Sachverzeichnis	338