

Internetrecht und Digitale Gesellschaft

Band 4

**Cloud Computing –
Herausforderungen an
den Rechtsrahmen für Datenschutz**

Von

Thorsten Hennrich



Duncker & Humblot · Berlin

THORSTEN HENNRICH

Cloud Computing –
Herausforderungen an
den Rechtsrahmen für Datenschutz

Internetrecht und Digitale Gesellschaft

Herausgegeben von
Dirk Heckmann

Band 4

Cloud Computing – Herausforderungen an den Rechtsrahmen für Datenschutz

Von

Thorsten Henrich



Duncker & Humblot · Berlin

Die Juristische Fakultät der Universität Passau
hat diese Arbeit im Jahre 2015 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische Daten
sind im Internet über <http://dnb.d-nb.de> abrufbar.

Alle Rechte vorbehalten
© 2016 Duncker & Humblot GmbH, Berlin
Fremddatenübernahme: L101 Mediengestaltung, Berlin
Druck: buchbücher.de gmbH, Birkach
Printed in Germany

ISSN 2363-5479
ISBN 978-3-428-14780-9 (Print)
ISBN 978-3-428-54780-7 (E-Book)
ISBN 978-3-428-84780-8 (Print & E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

Internet: <http://www.duncker-humblot.de>

Meiner Familie

Vorwort

Cloud Computing steht für das flexible, dynamische, skalierbare und bedarfsorientierte Anbieten, Nutzen und Abrechnen von Infrastruktur- und Anwendungskomponenten über das Internet „als Dienst“. Die vielfältigen Chancen und Vorteile von Cloud Computing treffen jedoch auf einen Rechtsrahmen, der die Besonderheiten (global) verteilter, multimandantenfähiger und virtualisierter IT-Infrastrukturen konzeptionell noch gar nicht zu berücksichtigen hatte.

Die zentralen Herausforderungen von Cloud Computing an den Rechtsrahmen für Datenschutz werden auf Grundlage des BDSG und der Entwicklungen im Zuge der EU-Datenschutzreform praxisnah und anhand typischer Spannungsfelder erörtert. Im Fokus stehen das anzuwendende Datenschutzrecht, der Personenbezug von Daten, die Daten- und Informationssicherheit sowie die Auftragsdatenverarbeitung. Da globale Datenströme und weltweite Netzwerke das technische Rückgrat einer globalisierten Wirtschaft und Gesellschaft bilden, liegt ein Schwerpunkt auch auf internationalen Datentransfers – aus Gründen der Praxisrelevanz vor allem in die USA auf Basis der „Safe-Harbor-Vereinbarung“.

Die vorliegende Arbeit wurde im ersten Halbjahr des Jahres 2015 von der Juristischen Fakultät der Universität Passau als Dissertation angenommen.

Sehr herzlich danke ich meinem Doktorvater, Herrn Prof. Dr. Dirk Heckmann, für die hervorragende Unterstützung und Betreuung des Promotionsvorhabens sowie für die Aufnahme in seine Schriftenreihe. Insbesondere die Gelegenheit zur Mitwirkung an einer Studie zum sicheren Einsatz von Cloud Computing für Kommunen ermöglichte Grundlagenforschung zum „status quo“ von IT-Outsourcing der öffentlichen Hand. Forschungsergebnisse dieser Studie sind auch in die vorliegende Arbeit eingeflossen.

Herrn Prof. Dr. Kai von Lewinski danke ich herzlich für die Erstellung des Zweitgutachtens und seine wertvollen Hinweise.

Ganz besonders danke ich meinen Eltern, Hiltrud und Lothar Hennrich, sowie meinen verstorbenen Großeltern, Hedwig und Franz Englmaier, die mit ihrer unschätzbaren und vielfältigen Unterstützung meine Ausbildung und diese Arbeit ermöglicht haben. Ihnen und meiner ganzen Familie – auch meinem kleinen Neffen und Patenkind Felix, der auf seine lustige Art oft zur Entspannung beitrug – ist diese Arbeit gewidmet.

Bei meinem Bruder Matthias Hennrich bedanke ich mich für technischen Input zum Thema Cloud Computing, zahlreiche Anregungen sowie für die Möglichkeit, jederzeit auf sein großes Know-how in diesem Bereich zurückgreifen zu können. Durch die gemeinsame Führung eines Colocation-/Hosting-Anbieters seit dem Jahr 2001 konnte für diese Arbeit zugleich auf jahrelange Praxiserfahrung mit Cloud- und Virtualisierungstechnologien zurückgegriffen werden.

Meinem Bruder Dr. Stephan Hennrich danke ich für seine vielfältige Unterstützung, insbesondere für zahlreiche Diskussionen und wertvolle Tipps rund um diese Arbeit. Er hatte stets ein offenes Ohr für meine Anliegen und nahm sich auch bei komplexen juristischen Themen immer gerne die notwendige Zeit.

Für zahlreiche Gespräche, Feedback und gemeinsame Veröffentlichungen danke ich vor allem Herrn Dr. Fabian Niemann und Herrn Dr. Michael Marc Maisch.

Neben diversen Fachaufsätzen und Studien ist diese Arbeit das zentrale Ergebnis einer jahrelangen rechtlichen Befassung mit der Materie Cloud Computing, die auch künftig weitergehen wird.

Die Untersuchung wurde im September 2014 abgeschlossen. Die nachfolgende rechtliche Entwicklung wurde bis Juli 2015 berücksichtigt.

Frankfurt am Main, im Juli 2015

Thorsten Hennrich

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 Informationssicherheit	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 „Galaxia-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
a) 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

Abkürzungsverzeichnis

a. A.	andere Ansicht
a. a. O.	am angegebenen Ort
ABl.EG	Amtsblatt der Europäischen Gemeinschaften
ABl.EU	Amtsblatt der Europäischen Union
Abs.	Absatz
a. E.	am Ende
AEUV	Vertrag über die Arbeitsweise der Europäischen Union in der Fassung des Vertrags von Lissabon vom 13.12.2007
a. F.	alte Fassung
AG	Aktiengesellschaft, Arbeitsgruppe
AICPA	American Institute of Certified Public Accountants
AKDB	Anstalt für Kommunale Datenverarbeitung
AktG	Aktiengesetz
Alt.	Alternative
AMS-IX	Amsterdam Internet Exchange
Anm.	Anmerkung
AO	Abgabenordnung
App	Kurzform für Application (Anwendungssoftware)
ARPANET	Advanced Research Projects Agency Network
Art.	Artikel
ASP	Application Service Providing
AT	Allgemeiner Teil
Aufl.	Auflage
AWS	Amazon Web Services
B2B	Business-to-business
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BayDSG	Bayerisches Datenschutzgesetz
BayLfD	Der Bayerische Landesbeauftragte für den Datenschutz
BB	Betriebs-Berater
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
Begr.	Begründung

BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BlnBDI	Berliner Beauftragter für Datenschutz und Informationsfreiheit
BMI	Bundesministerium des Innern
BMWi	Bundesministerium für Wirtschaft und Energie
BPaaS	Business Process as a Service
BRD	Bundesrepublik Deutschland
BR-Drs.	Drucksache des Bundesrats
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Drucksache des Deutschen Bundestags
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichtes
BvR	Aktenzeichen einer Verfassungsbeschwerde zum BVerfG
bzw.	beziehungsweise
C3	Compliant Community Cloud
ca.	circa
CaaS	Communication as a Service
ccTLD	Country code top-level domain (länderspezifische Top-Level-Domain)
CCZ	Corporate Compliance Zeitschrift
CEN	Comité Européen de Normalisation/European Committee for Standardization/Europäisches Komitee für Normung
CERN	Conseil Européen pour la Recherche Nucléaire/European Organization for Nuclear Research
CICA	Canadian Institute of Chartered Accountants
CIIP	Critical Information Infrastructure Protection
COM	Dokument der Kommission
CPU	Central Processing Unit (Prozessor eines Computers)
CR	Computer und Recht – Zeitschrift für die Praxis des Rechts der Informationstechnologien

CRI	Computer Law Review International – A Journal of Information Law and Technology
CRM	Customer Relationship Management
CRS	Congressional Research Service (Agentur innerhalb der Library of Congress in den USA)
CSA	Cloud Security Alliance
DBAN	Darik's Boot and Nuke (Software zur Löschung von Daten)
DDoS	Distributed Denial of Service
DE-CIX	Deutscher Commercial Internet Exchange
DIB	Datenschutz- und Informationsfreiheitsbericht
DIN	DIN-Norm, DIN Deutsches Institut für Normung e. V.
Diss.	Dissertation
DrittelbG	Gesetz über die Drittelbeteiligung der Arbeitnehmer im Aufsichtsrat
Drs.	Drucksache
DS-GVO	Datenschutz-Grundverordnung
DS-GVO-E	KOM(2012) 11, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)
DSK	Konferenz der Datenschutzbeauftragten des Bundes und der Länder
DSL	Digital Subscriber Line
DSRI	Deutsche Stiftung für Recht und Informatik
DuD	Datenschutz und Datensicherheit
DV	Datenverarbeitung
EC2	Elastic Compute Cloud (ein Dienst von Amazon Web Services)
EEG	Erneuerbare-Energien-Gesetz
EFTA	European Free Trade Association
EG	Europäische Gemeinschaft
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuch
EG-Datenschutz-Richtlinie	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
EGKS	Europäische Gemeinschaft für Kohle und Stahl
Einf	Einführung
EL	Ergänzungslieferung

EMEA	Europe, Middle East, Africa (Europa, Mittlerer Osten, Afrika)
EN	Europäische Norm
ENIAC	Electronic Numerical Integrator and Computer
ENISA	European Network and Information Security Agency (Europäische Agentur für Netz- und Informationssicherheit)
EN ISO 9001:2008 (D/E/F)	Europäische Norm ISO 9001:2008 – Dreisprachige Fassung (deutsch/englisch/französisch)
EP	Europäisches Parlament
EPIC	Electronic Privacy Information Center
et seq.	et sequens (und folgende)
ETSI	European Telecommunications Standards Institute (Europäisches Institut für Telekommunikationsnormen)
EU	Europäische Union
EuGH	Europäischer Gerichtshof, Gerichtshof der Europäischen Union
EUV	Vertrag über die Europäische Union in der Fassung des Vertrags von Lissabon vom 13.12.2007
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
e. V.	eingetragener Verein
EWR	Europäischer Wirtschaftsraum
f., ff.	folgend(e)
FA	Fachanwalt
FAQ	Frequently asked questions (Häufig gestellte Fragen)
FAZ	Frankfurter Allgemeine Zeitung
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
Fn.	Fußnote
Fraunhofer FOKUS	Fraunhofer-Institut für Offene Kommunikationssysteme
Fraunhofer SIT	Fraunhofer-Institut für Sichere Informationstechnologie
FS	Festschrift
FTC	Federal Trade Commission
GA	Generalanwalt
GB	Gigabyte
GCHQ	Government Communications Headquarters (britischer Nachrichtendienst)
GewO	Gewerbeordnung
GG	Grundgesetz

ggf.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
GRUR	Gewerblicher Rechtsschutz und Urheberrecht – Zeitschrift der Deutschen Vereinigung für gewerblichen Rechtsschutz und Urheberrecht
HessDSB	Der Hessische Datenschutzbeauftragte
HmbBfDI	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
HPCaaS	High Performance Computing as a Service
H.R.	House of Representatives
Hrsg., hrsg.	Herausgeber, herausgegeben
HTML	Hypertext Markup Language
IaaS	Infrastructure as a Service
IAASB	International Auditing and Assurance Standards Board
ICE	Intercity-Express, Zuggattung der Deutschen Bahn AG
IEC	International Electrotechnical Commission (Internationale Elektrotechnische Kommission)
IKT	Informations- und Kommunikationstechnologie
Inc.	Corporation (US-amerikanische Kapitalgesellschaft)
insb.	insbesondere
InvG	Investmentgesetz
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
i. R. v.	im Rahmen von
ISAE	International Standard on Assurance Engagements
i. S. d.	im Sinne des, im Sinne der
ISMS	Informationssicherheits-Managementsystem
ISO	International Organization for Standardization (Internationale Organisation für Normung)
ISO/IEC JTC 1/ SC 27	International Organization for Standardization/International Electrotechnical Commission – Joint Technical Committee 1 „Information Technology“/Subcommittee 27 „Security techniques“
i. S. v.	im Sinne von
IT	Informationstechnik, Informationstechnologie
ITA	International Trade Administration

ITIL	IT Infrastructure Library
i. V. m.	in Verbindung mit
iX	Magazin für professionelle Informationstechnik
JB	Jahresbericht
JTC	Joint Technical Committee (Technisches Gemeinschaftskomitee von ISO und IEC)
jurisAnwZert ITR	juris AnwaltZertifikatOnline IT-Recht
JZ	JuristenZeitung
K&R	Kommunikation & Recht
Kap.	Kapitel
KG	Kommanditgesellschaft
KMU	kleine und mittlere Unternehmen
KOM	Dokument der Kommission
Kommission	Europäische Kommission
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KWG	Gesetz über das Kreditwesen (Kreditwesengesetz)
LDA	Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht
LDI NRW	Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
LfD	Landesbeauftragter für Datenschutz
LfDI	Landesbeauftragter für Datenschutz und Informationsfreiheit
LG	Landgericht
LHC	Large Hadron Collider
LINX	London Internet Exchange
lit.	litera (Buchstabe)
LLC	Limited Liability Company (US-amerikanische Kapitalgesellschaft)
Ltd.	Limited Company (Kapitalgesellschaft in Großbritannien und Irland)
LT-Drs.	Landtagsdrucksache
LTE	Long Term Evolution (Mobilfunkstandard)
Mag.	Magistrate
MaRisk	Mindestanforderungen an das Risikomanagement (Rundschreiben der BaFin)
Mbit/s	Megabit pro Sekunde
MitbestG	Gesetz über die Mitbestimmung der Arbeitnehmer
MüKo	Münchener Kommentar
MVS	Multiple Virtual Storage

m. w. N.	mit weiteren Nachweisen
NASDAQ	National Association of Securities Dealers Automated Quotations
NDA	Non Disclosure Agreement
NIA	Normenausschuss Informationstechnik und Anwendungen im DIN
NIST	National Institute of Standards and Technology (USA)
NJW	Neue Juristische Wochenschrift
No.	Number (Nummer)
NQSZ	Normenausschuss Qualitätsmanagement, Statistik und Zertifizierungsgrundlagen im DIN
Nr.	Nummer
NRW	Nordrhein-Westfalen
NSA	National Security Agency
NSL	National Security Letter
NYSE	New York Stock Exchange
OECD	Organization for Economic Co-operation and Development (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung)
OHG	Offene Handelsgesellschaft
OS	Operating System (Betriebssystem)
OVG	Oberverwaltungsgericht
PaaS	Platform as a Service
PB	Petabyte
PBCR	Processor Binding Corporate Rules
PC	Personal Computer
PII	Personally Identifiable Information
PK	Praxiskommentar
PL	Public Law
PNR	Passenger Name Records (Fluggastdatensätze)
QM	Qualitätsmanagement
RAM	Random Access Memory
RDV	Recht der Datenverarbeitung
RFID	Radio Frequency Identification
RL	Richtlinie
Rn.	Randnummer

Rom I-VO	Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates v. 17.6.2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht
Rom II-VO	Verordnung (EG) Nr. 864/2007 des Europäischen Parlaments und des Rates vom 11.7.2007 über das auf außervertragliche Schuldverhältnisse anzuwendende Recht
Rs.	Rechtssache
S.	Satz, Seite
S3	Simple Storage Service (ein Dienst von Amazon Web Services)
SaaS	Software as a Service
SAN	Storage Area Network
SAS 70	Statement on Auditing Standards No. 70
SBC	Server-based Computing
S.D.N.Y.	Southern District of New York (Region eines United States District Courts)
SEC/SEK	Arbeitsdokument der Kommissionsdienststellen (Secretariat-General); beginnend Januar 2012 mit dem Identifikator SWD veröffentlicht
SETI	Search for Extraterrestrial Intelligence
SGB I	Sozialgesetzbuch, Erstes Buch (I) – Allgemeiner Teil
SGB X	Sozialgesetzbuch, Zehntes Buch (X) – Sozialverfahren und Sozialdatenschutz
S.L.	Sociedad de responsabilidad limitada (spanische Kapitalgesellschaft)
SLA	Service Level Agreement
SOA	Service-orientierte Architekturen
SOC	Service Organization Control
sog.	sogenannt
SOX	Sarbanes-Oxley Act
SSAE	Statement on Standards for Attestation Engagements
StaaS	Storage as a Service
StGB	Strafgesetzbuch
SWD	Staff Working Document (Arbeitsdokumente und gemeinsame Arbeitsdokumente der Kommissionsdienststellen)
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TB	Tätigkeitsbericht, Terabyte
TC	Technical Committee (Technisches Komitee der ISO)
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TLD	Top Level Domain

TMG	Telemediengesetz
u. a.	unter anderem
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Anstalt des öffentlichen Rechts)
URL	Uniform Resource Locator
Urt.	Urteil
US/U.S.	United States
USA	United States of America (Vereinigte Staaten von Amerika)
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001
U.S.C.	United States Code (The Code of Laws of the United States of America)
U.S. SAFE WEB Act	Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act
USV	Unterbrechungsfreie Stromversorgung
v.	vom, von, vor
v. a.	vor allem
VAG	Gesetz über die Beaufsichtigung der Versicherungsunternehmen (Versicherungsaufsichtsgesetz)
Var.	Variante
VblBW	Verwaltungsblätter für Baden-Württemberg – Zeitschrift für öffentliches Recht und öffentliche Verwaltung
VG	Verwaltungsgericht
Vgl. (vgl.)	Vergleiche (vergleiche)
VO	Verordnung (Rechtsakt der EU)
WAN	Wide Area Network
WI	Wirtschaftsinformatik (Zeitschrift)
WLAN	Wireless Local Area Network
WP	Working Paper (Arbeitspapier der Art.-29-Datenschutzgruppe)
WpHG	Gesetz über den Wertpapierhandel (Wertpapierhandelsgesetz)
WTO	World Trade Organization (Welthandelsorganisation)
WWW	World Wide Web
XaaS	Everything as a Service
z. B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZUM	Zeitschrift für Urheber- und Medienrecht

A. Einleitung

I. Cloud Computing – IT „as a Service“

„Where the World Wide Web makes information available everywhere and to anyone, cloud computing makes computing power available everywhere and to anyone.“

Europäische Kommission¹

Der Einsatz von Informationstechnologie unterliegt seit einigen Jahren einem bedeutenden Wandel. Nahezu sämtliche Infrastruktur- und Anwendungskomponenten können – vergleichbar mit der Nutzung eines Web-Mail-Dienstes – flexibel, dynamisch, bedarfsgerecht und in beinahe unbegrenztem Umfang auch über das Internet „als Dienst“ aus Datenwolken bezogen werden.² Für die hiermit verbundene Abkehr von bisherigen Nutzungs- und Einsatzszenarien steht ein sowohl omnipräsentes wie auch nebulöses Schlagwort: Cloud Computing.

In rasanter Geschwindigkeit hat sich die Thematik der IT-Dienstleistungen aus der „Wolke des Internets“ in der weltweiten IT-Branche verbreitet. Bereits in den Jahren 2010 und 2011 wurde Cloud Computing nach einer Umfrage des Branchenverbands BITKOM³ zum IT-Trend des Jahres gewählt.⁴ Für die Folgejahre wurden hohe zweistellige Wachstumsraten allein in Deutschland prognostiziert.⁵ Sehr schnell rückten die Datenwolken daher auch in den Fokus von Initiativen großer Konzerne.⁶ Im Jahr 2013 wurde

¹ COM (2012) 529 EN, S. 2 (deutsche Übersetzung nach COM (2012) 529, S. 2: „Während das World Wide Web überall für jedermann Informationen zugänglich macht, stellt das Cloud-Computing überall für jedermann Rechenleistung zur Verfügung.“); Cloud Computing geht aber grundsätzlich (v.a. im Hinblick auf Software und Applikationen) über bloße „Rechenleistung“ hinaus, vgl. unten unter B.V.

² Vgl. COM (2012) 529, S. 3; BfDI, 23. TB, S. 63; LfD Rheinland-Pfalz, 22. TB, S. 94; LfDI Rheinland-Pfalz, 23. TB, S. 16; *Vossen/Haselmann/Hoeren*, Cloud Computing für Unternehmen, S. 1 f.

³ Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM).

⁴ BITKOM, Presseinformation v. 18.1.2011, S. 1 ff.; BSI, JB 2010, S. 26.

⁵ Vgl. BITKOM, Leitfaden Cloud Computing 2010, S. 14; BSI, JB 2010, S. 26.

⁶ Exemplarisch hierzu die Microsoft „Go Cloud“ Initiative für die deutsche IT-Industrie, in der ein Gesamtinvestitionsvolumen von 100 Millionen Euro bis 2013

Cloud Computing schon nicht mehr als Trend, sondern als fester Bestandteil der IT-Landschaft angesehen.⁷ Der Verband der deutschen Internetwirtschaft eco⁸ verwies auf die Bedeutung von Cloud Computing als Wirtschaftsmotor mit einem prognostizierten Umsatz-Gesamtwachstum von 150 Prozent bis in das Jahr 2016 (dies entspricht einem jährlichen Wachstum von 37 Prozent) bei Anbietern für Services und Anwendungen.⁹ Im Jahr 2014 war die Cloud-Nutzung weiterhin am Wachsen, auch wenn sich das Wachstum im Vergleich zum Vorjahr leicht abgeschwächt haben soll.¹⁰ Vor allem die NSA-Überwachungsaffäre soll das Bewusstsein für eine gefährdete IT-Sicherheit geschärft und die Einstellung von Unternehmen gegenüber Public Clouds und Private Clouds beeinflusst haben.¹¹ Auch gegenwärtig – im Jahr 2015 – sind es vor allem Sicherheitsbedenken, wie die Angst vor Datenverlust und unberechtigtem Datenzugriff, die als größtes Hemmnis der weiterhin wachsenden Cloud-Nutzung gegenüberstehen.¹²

Zahlreiche Technologieansätze, die sich hinter Cloud Computing verbergen, sind keineswegs neu.¹³ Mitunter gewinnt ein Betrachter daher den Eindruck, dass einige Unternehmen vor allem aus Werbe- und Marketinggesichtspunkten „in der Cloud“ sind und bestehende Services hierfür neu etikettiert haben.¹⁴ Für die künftige, alltägliche Nutzung von Informationstechnologien sind der unter dem Schlagwort Cloud Computing eingeleitete Paradigmenwechsel sowie das wirtschaftliche Potential jedoch von grundsätzlicher Bedeutung. In Bezug auf Hardware und Applikationen ist es der konsequente Schritt in der weiteren Entwicklung der Informationstechnologie. Computersysteme, wie sie noch heute in Unternehmen, öffentlichen Einrichtungen oder in Privathaushalten wiederzufinden sind, werden im Idealfall durch bloße „thin clients“¹⁵ ersetzt. Mittels Browser oder App wird über das Internet auf sämtliche Applikationen und Daten „in der Cloud“

angekündigt wurde, Pressemitteilung v. 29.9.2010, <http://www.microsoft.com/de-de/news/pressemitteilung.aspx?id=533235> (Stand: 1.7.2015).

⁷ eco/Arthur D. Little, Die deutsche Internetwirtschaft 2012–2016, S. 26.

⁸ eco – Verband der deutschen Internetwirtschaft e. V.

⁹ eco, Pressemeldung v. 20.8.2013, <http://www.eco.de/2013/pressemeldungen/wirtschaftsmotor-cloud-computing-37-prozent-wachstum-pro-jahr.html> (Stand: 1.7.2015); eco/Arthur D. Little, Die deutsche Internetwirtschaft 2012–2016, S. 16.

¹⁰ KPMG/Bitkom Research, Cloud-Monitor 2014, S. 10.

¹¹ KPMG/Bitkom Research, Cloud-Monitor 2014, S. 10, 30; ausführlich zu Public Clouds siehe unter B.VI.1, zu Private Clouds siehe unter B.VI.2.

¹² KPMG/Bitkom Research, Cloud-Monitor 2015, S. 29.

¹³ Hierzu ausführlich unter B.IV.

¹⁴ Vgl. *Giebichenstein*, BB 2011, 2218; *Heckmann*, in: Hill/Schliesky, Innovationen im und durch Recht, S. 97; *Höllwarth*, Cloud Migration, S. 145.

¹⁵ Zu „thin clients“ siehe unter B.II.2.c).

zugegriffen. Lokale Software-Installationen macht dies entbehrlich.¹⁶ Flexible Nutzungs- und Abrechnungsmodelle tragen zugleich dazu bei, dass sich die Nutzung von Informationstechnologie langfristig zu einer „Utility“ wandeln wird und einem Versorgungsgut gleichkommen kann.¹⁷ In dem Cloud Computing zugrunde liegenden Technologieansatz wird daher häufig eine Parallele zu der Versorgung mit elektrischem Strom gesehen: während Industriebetriebe gerade in den Anfängen der Stromnutzung noch eigene, kleine Energieerzeuger unterhielten (Parallele zu lokal vorgehaltenen IT-Systemen), wurden diese im Laufe der Zeit entbehrlich, da nach dem Aufbau von Versorgungsnetzen die Belieferung mit elektrischem Strom schließlich zentral über Elektrizitätsversorgungsunternehmen erfolgte (Parallele zu Cloud-Anbietern).¹⁸ IT-Leistungen sollen demnach quasi wie Strom „aus der Steckdose“ direkt ins Haus gelangen.¹⁹

Das Potential der Datenwolken wurde auch auf staatlicher Seite erkannt. Mit Blick auf die zur öffentlichen Aufgabenerfüllung in den Grenzen des Haushalts- und Vergaberechts verfügbaren Mittel ist Cloud Computing gerade auch für Kommunen und andere öffentliche Stellen wirtschaftlich attraktiv.²⁰ International für Aufmerksamkeit sorgte im Jahr 2010 eine Entscheidung der kalifornischen Stadt Los Angeles, den gesamten E-Mail-Verkehr der Stadtverwaltung auf Server von Google auszulagern.²¹ Aufgrund von Sicherheitsfragen wurde dies im Folgejahr zwar wieder revidiert.²² Mittlerweile bieten aber alle großen US-Dienstleister spezielle Lösungen

¹⁶ Vgl. *Vossen/Haselmann/Hoeren*, Cloud Computing für Unternehmen, S. 2 f.

¹⁷ *Carr*, The Big Switch, S. 20; *Kroes*, SPEECH/11/199, S. 2; siehe auch *Vossen/Haselmann/Hoeren*, Cloud Computing für Unternehmen, S. 19 und die dort enthaltene Darstellung der bereits im Jahr 1961 von *John McCarthy* geprägten Vision „computing may someday be organized as a public utility“, die mit dem Aufkommen von Cloud Computing wieder aufgegriffen wurde.

¹⁸ *Carr*, The Big Switch, S. 19 f.

¹⁹ Vgl. *Carr*, The Big Switch, S. 20 ff.; *Heckmann*, jurisPK-Internetrecht, Kap. 9 Rn. 600; *Pohle/Ammann*, CR 2010, 273; Arbeitskreise Technik und Medien der DSK, Orientierungshilfe Cloud Computing, S. 4; LfD Thüringen, 8. TB, S. 125; LfDI Rheinland-Pfalz, 23. TB, S. 16; *Vossen/Haselmann/Hoeren*, Cloud Computing für Unternehmen, S. 2; *Eiermann*, DuD 2013, 92 (93); *Schulz*, in: Krallmann/Zapp, Bausteine einer vernetzten Verwaltung, S. 53.

²⁰ *Heckmann/von Lucke/Hennrich/Maisch*, C3-Studie, S. 24, 47 f.

²¹ FAZ v. 4.10.2010, <http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/datenspeicherung-jetzt-kommt-die-cloud-1230186.html> (Stand: 1.7.2015).

²² <http://www.heise.de/ix/meldung/Los-Angeles-beklagt-Sicherheitsprobleme-bei-Goo-gles-Cloud-1364534.html> v. 21.10.2011 (Stand: 1.7.2015); <http://www.heise.de/ix/meldung/Polizei-von-Los-Angeles-verzichtet-auf-Goo-gles-Cloud-1405726.html> v. 9.1.2012 (Stand: 1.7.2015).