

Rechtliche Rahmenbedingungen des Cloud Computing

Eine Untersuchung zur internationalen Zuständigkeit, zum anwendbaren Recht und zum Datenschutzrecht

von
RA Dr. Benno Barnitzke

1. Auflage

Nomos Baden-Baden 2014

Verlag C.H. Beck im Internet:
www.beck.de

ISBN 978 3 8487 1429 2

Benno Barnitzke

**Rechtliche
Rahmenbedingungen
des Cloud Computing**

Eine Untersuchung zur internationalen
Zuständigkeit, zum anwendbaren Recht
und zum Datenschutzrecht



Nomos

Nomos Universitätsschriften

Recht

Band 842

Dr. Benno Barnitzke, LL.M.

Rechtliche Rahmenbedingungen des Cloud Computing

Eine Untersuchung zur internationalen Zuständigkeit,
zum anwendbaren Recht und zum Datenschutzrecht



Nomos

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

Zugl.: Hannover, Univ., Diss., 2013

ISBN 978-3-8487-1429-2

1. Auflage 2014

© Nomos Verlagsgesellschaft, Baden-Baden 2014. Printed in Germany. Alle Rechte, auch die des Nachdrucks von Auszügen, der photomechanischen Wiedergabe und der Übersetzung, vorbehalten. Gedruckt auf alterungsbeständigem Papier.

Inhaltsverzeichnis

Abkürzungsverzeichnis	17
1. Kapitel – Einleitung und Einführung in Konzept und Technik des Cloud Computing	21
A. Einleitung	21
I. Allgemeine Einführung	21
II. Ziele dieser Arbeit	22
III. Aufbau dieser Arbeit	24
B. Begriff und Konzept des Cloud Computing	24
I. Begriff	25
II. Konzept	27
C. Attribute des Cloud Computing	29
I. Abgrenzung zum Grid Computing	29
II. Virtualisierung	30
III. Skalierbarkeit	33
1. Vertikale Skalierung	34
2. Horizontale Skalierung	35
3. Skalierungsbeispiel	36
IV. Multi-Mandantenfähigkeit	37
V. Verfügbarkeit	39
VI. Flexibilität	41
VII. Sofortige Abrufbarkeit (On-Demand)	41
VIII. Zugriff via Internettechnologie und Clients	42
IX. Verbrauchsabhängige Abrechnung (Utility Computing)	43
X. Zusammenfassung	43
D. Beteiligte Rechtssubjekte	44
I. Betroffene	44
II. Nutzer und End-Nutzer	44
III. Cloud Provider	45
1. Service Provider	45
2. Infrastrukturprovider	46
3. Cloud Broker	46

Inhaltsverzeichnis

E. Bestandteile des Cloud Computing – das Ebenenmodell	46
I. Infrastructure as a Service	47
II. Platform as a Service	49
III. Software as a Service	50
F. Organisationsformen von Clouds	52
I. Public Clouds	53
II. Private Clouds	53
III. Hybride Clouds	54
G. Praxisbeispiele für den Einsatz von Cloud Computing	55
H. Vorteile und Risiken des Cloud Computing	56
I. Vorteile	56
II. Risiken	58
1. Für Nutzer	58
2. Für Cloud Provider	59
I. Die Herausforderungen des Cloud Computing für die Rechtsanwendung	60
J. Cloud Computing in der Rechtsprechung	61
2. Kapitel – Internationale Zuständigkeit und anwendbares Recht	63
A. Internationale Zuständigkeit bei Cloud Computing-Sachverhalten	64
I. Anwendungsbereich, Art. 1 EuGVVO	65
II. Ausschließlicher Gerichtsstand, Art. 22 EuGVVO	66
III. Zuständigkeit für Verbrauchersachen, Art. 15 ff. EuGVVO	67
1. Vertragsschluss mit einem Cloud Provider	67
2. Datenschutzrechtliche Ansprüche auf Auskunft, Berichtigung und / oder Löschung	72
3. Rechtsfolge	73
IV. Gerichtsstandvereinbarung, Art. 23 EuGVVO	74
V. Besondere Zuständigkeit, Art. 5 EuGVVO	75
1. Gerichtsstand des Erfüllungsortes, Art. 5 Nr. 1 EuGVVO	75
2. Gerichtsstand am Ort der unerlaubten Handlung, Art. 5 Nr. 3 EuGVVO	81
a) Handlungsort als Anknüpfungspunkt unerlaubter Handlungen	85
b) Erfolgsort als Anknüpfungspunkt unerlaubter Handlungen	88

c) Datenschutzrechtliche Schadensersatzansprüche	92
VI. Allgemeine Zuständigkeit am Wohnsitz des Beklagten, Art. 2 EuGVVO	96
VII. Zusammenfassung	98
B. Cloud Computing und anwendbares Recht	99
I. Überblick	100
II. Cloud Computing-Verträge und anwendbares Vertragsrecht	101
1. Anwendungsbereich der Rom I-VO	101
2. Rechtswahlklauseln in Cloud Computing-Verträgen, Art. 3 Rom I-VO	102
a) Vertragsstatut	102
b) Rechtswahlklauseln im Datenschutzrecht?	102
3. Anwendbares Recht bei fehlender Rechtswahlklausel, Art. 4 Rom I-VO	106
4. Anwendbares Recht bei Cloud Computing-Verträgen unter Beteiligung von Verbrauchern, Art. 6 Rom I-VO	109
III. Cloud Computing und anwendbares Deliktsrecht	111
1. Anwendungsbereich der Rom II-VO	111
2. Das auf unerlaubte Handlungen anwendbare Recht beim Cloud Computing, Art. 4 Rom II-VO	112
a) Unerlaubte Handlungen des Cloud Providers gegenüber Nutzern	112
b) Unerlaubte Handlungen von Dritten gegenüber Nutzern	119
3. Rechtswahlklausel, Art. 14 Rom II-VO	119
IV. Anwendbares Recht im Bereich des Urheberrechts	120
a) Nutzungshandlungen des Cloud Providers	122
b) Nutzungshandlungen des Nutzers	124
c) Einschränkung des Schutzlandprinzips für das Cloud Computing	125
V. Anwendbares Datenschutzrecht	131
1. In einem anderen EU-Mitgliedsstaat oder dem EWR belegener Cloud Provider, § 1 Abs. 5 S. 1 Hs. 1 BDSG	133
2. Niederlassung eines Cloud Providers im Inland, § 1 Abs. 5 S. 1 Hs. 2 BDSG	134
a) Virtuelle Maschinen als Niederlassungen	134
b) Rechenzentren als Niederlassungen	135

Inhaltsverzeichnis

c) Anwendbares Recht bei Rechenzentren des Cloud Providers im Inland und gleichzeitig in verschiedenen Mitgliedsstaaten	141
d) Zusammenfassung	143
3. In einem Drittland belegener Cloud Provider, § 1 Abs. 5 S. 2 BDSG	143
a) „Mittel“ beim Cloud Computing	144
b) „Zurückgreifen“	145
aa) „Zurückgreifen“ auf Mittel bei IaaS	147
bb) „Zurückgreifen“ auf Mittel bei SaaS	156
c) De lege ferenda – alternative Lösungsansätze für die Bestimmung des anwendbaren Datenschutzrechts beim Cloud Computing	159
VI. Zusammenfassung	163
3. Kapitel – Datenschutz beim Cloud Computing	166
A. Einführung in die datenschutzrechtliche Problematik	166
B. Sachliche Anwendbarkeit des BDSG	167
I. Ausschluss des Personenbezuges durch Verschlüsselung der Daten	168
1. Die Erforderlichkeit zur Verschlüsselung personenbezogener Daten in Clouds	169
2. Grundlagen der Verschlüsselung	169
3. Der Personenbezug verschlüsselter Daten in Clouds	170
a) „Einzelangaben“ bzw. „Informationen“	171
b) „über“	171
c) Bestimmbarkeit	172
II. Ausschluss des Personenbezuges durch Fragmentierung der Daten	175
1. „Einzelangaben“ bzw. „Informationen“	176
2. „über“	176
3. Bestimmbarkeit	177
4. Zusammenfassung	177
C. Die verantwortliche Stelle beim Cloud Computing	177
I. Abgrenzungsprobleme	180
II. Bisherige Abgrenzung beim Cloud Computing	181
1. Cloud Computing als Auftragsdatenverarbeitung	181

2. Cloud Computing als „Funktionsübertragung“	182
III. Abgrenzung gemäß Art. 2 lit. d) DSRL	183
1. Entscheidungsbefugnis	185
2. Zwecke und Mittel der Verarbeitung	187
3. Beteiligung mehrerer an den Datenverarbeitungsaktivitäten	189
4. Ausübung von Kontrolle als gemeinsames normatives Merkmal	189
5. Zusammenfassung	191
IV. Verantwortliche Stellen bei Nutzung eines selbständigen Cloud Providers	192
1. Nutzer	192
2. Cloud Provider	193
a) Entscheidungsbefugnis des Cloud Providers	193
b) Zwecke und Mittel der Verarbeitung	194
c) Der Grad der Kontrolle des Cloud Providers	195
V. Verantwortliche Stellen in Federated Cloud Architekturen („Single Point of Contact“)	196
1. Nutzer	197
2. Service Provider	198
a) Beteiligung mehrerer an der Datenverarbeitung	198
b) Der Grad der Kontrolle des Service Providers über die Datenverarbeitungsvorgänge	198
3. Infrastrukturprovider	199
a) Entscheidungsbefugnis des Infrastruktur Providers	199
b) Zwecke und Mittel der Verarbeitung	200
c) Der Grad der Kontrolle des Infrastruktur Providers über die Datenverarbeitungsvorgänge	201
VI. Verantwortliche Stellen in Multi-Cloud Architekturen („Multivendor“-Strategie)	202
1. Nutzer	203
2. Service Provider	203
a) Entscheidungsbefugnis des Service Providers	204
b) Zwecke und Mittel der Datenverarbeitung	204
c) Der Grad der Kontrolle des Service Providers über die Datenverarbeitungsvorgänge	206
3. Infrastrukturprovider	208
VII. Verantwortliche Stellen in Hybrid Cloud Architekturen	209
1. Private Cloud Provider	209

Inhaltsverzeichnis

2. Public Cloud Provider	210
a) Entscheidungsbefugnis des Public Cloud Infrastruktur Providers	210
b) Zwecke und Mittel der Datenverarbeitung	211
c) Der Grad der Kontrolle des Public Cloud Providers über die Datenverarbeitungsvorgänge	211
VIII. Weitere mögliche Cloud-Konstellationen	211
IX. Rolle der eigenen Rechenzentren eines Cloud Providers	212
X. Rechtsfolge	213
D. Zulässigkeit und Anforderungen für die Auftragsdatenverarbeitung in europäischen Clouds, § 11 BDSG	214
I. Zulässigkeit der Auftragsdatenverarbeitung in Clouds	215
1. Technische Einflussmöglichkeiten des Nutzers	216
2. Unkenntnis vom Ort der Datenverarbeitung	216
3. Weisungsgebundenheit	221
4. Zusammenfassung	224
II. Anforderungen an die Rechte und Pflichten bei als Auftragsdatenverarbeitung ausgestaltetem Cloud Computing	225
1. Schriftliche Fixierung	225
2. Umfang, Art und Zweck der Datenverwendung, Art der Daten und Kreis der Betroffenen	227
3. Technische und organisatorische Schutzmaßnahmen	229
4. Berechtigung zur Begründung von Unterauftragsverhältnissen	231
5. Kontrollrechte des Auftraggebers und Mitwirkungspflichten des Auftragnehmers	234
6. Umfang der Weisungsbefugnisse	238
7. Löschen beim Auftragnehmer gespeicherter Daten nach Vertragsbeendigung	241
a) Verpflichtung des Cloud Providers zur Löschung von Daten	241
b) Rechtliche Anforderungen an den Löschvorgang	243
8. Benachrichtigungspflichten beauftragter Cloud Provider	244
9. Zusammenfassung	245

E. Clouds innerhalb der EU	247
I. Datenschutzrechtlich relevante Vorgänge zwischen Nutzer und Cloud Provider	248
1. Cloud Provider als Auftragsdatenverarbeiter des Nutzers	248
2. Datenübermittlung vom Nutzer an den Cloud Provider als verantwortliche Stelle	248
a) Hilfsmittleigenschaft des Cloud Computing	249
b) Erforderlichkeit für den Vertrag	249
c) Berechtigtes Interesse an der Nutzung von Cloud Computing	250
d) Widerstreitende Interessen von Cloud Nutzern und Betroffenen	252
e) Intensität der Beeinträchtigung der Interessen von Cloud Nutzer und Betroffenen	254
f) Abwägung der Interessen des Nutzers mit denen des Betroffenen	255
3. Ausnahme: Besondere Arten personenbezogener Daten	257
II. Datenschutzrechtlich relevante Vorgänge zwischen Cloud Providern	257
1. Ermittlung der einschlägigen Rechtsgrundlage	257
2. Voraussetzungen von § 28 BDSG	258
III. Datenschutzrechtlich relevante Vorgänge innerhalb einer Private Cloud	259
F. Die Übermittlung personenbezogener Daten in EU-grenzüberschreitenden Clouds	262
I. Voraussetzungen für die Übermittlung personenbezogener Daten in Drittländer	263
1. Angemessenes Datenschutzniveau beim Empfänger	263
2. Fehlendes angemessenes Datenschutzniveau beim Empfänger	265
II. Standardvertragsklauseln bei der Nutzung von Clouds	265
1. Cloud Provider und Unterauftragnehmer in Drittland	266
2. Ungeregelter Fall: Cloud Provider in EU/EWR, Unterauftragnehmer in Drittland	267
a) Direkter Vertrag zwischen Nutzer und unterbeauftragtem Cloud Provider in einem Drittland	270

Inhaltsverzeichnis

b) Beauftragung des Cloud Providers zum Abschluss der Standardvertragsklauseln im Namen des verantwortlichen Nutzers	271
c) Problem der praktischen Umsetzung	272
III. Binding Corporate Rules	272
IV. Safe Harbor und die Problematik des legalen Drittzugriffs auf Daten in der Cloud	274
1. Legale Zugriffsmöglichkeiten Dritter auf in der Cloud gespeicherte Daten	275
2. Vereinbarkeit mit europäischem Datenschutzrecht	276
a) Safe Harbor als Rechtsgrundlage für Übermittlungen von Cloud Providern an US-amerikanische Sicherheitsbehörden	280
b) Problem konkurrierender Rechtsordnungen durch länderübergreifende Clouds	282
V. Zusammenfassung	285
4. Kapitel – Schlussbemerkungen	287
A. Ort der Datenverarbeitung als ungeeigneter Anknüpfungspunkt	287
B. Datenschutzrechtliche Zulässigkeit des Cloud Computing	288
I. Einzelfallbezogene Prüfung der datenschutzrechtlichen Verantwortlichkeit	288
II. Keine überspannten datenschutzrechtlichen Anforderungen an Cloud Computing	288
Literaturverzeichnis	293
Verzeichnis der Internetquellen	305