

Internetrecht und Digitale Gesellschaft

Band 5

**Die Nutzung von
Cloud-Diensten durch kleine und
mittelständische Unternehmen**

**Eine datenschutzrechtliche Betrachtung
der Auslagerung von Kunden-, Personal-
und Mandantendaten**

Von

Daniel Schmid



Duncker & Humblot · Berlin

DANIEL SCHMID

Die Nutzung von Cloud-Diensten durch
kleine und mittelständische Unternehmen

Internetrecht und Digitale Gesellschaft

Herausgegeben von
Dirk Heckmann

Band 5

Die Nutzung von Cloud-Diensten durch kleine und mittelständische Unternehmen

Eine datenschutzrechtliche Betrachtung
der Auslagerung von Kunden-, Personal-
und Mandantendaten

Von

Daniel Schmid



Duncker & Humblot · Berlin

Die Juristische Fakultät der Universität Augsburg
hat diese Arbeit im Sommersemester 2016
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
© 2017 Duncker & Humblot GmbH, Berlin
Satz: L101 Mediengestaltung, Fürstenwalde
Druck: buchbücher.de GmbH, Birkach
Printed in Germany

ISSN 2363-5479
ISBN 978-3-428-15092-2 (Print)
ISBN 978-3-428-55092-0 (E-Book)
ISBN 978-3-428-85092-1 (Print & E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

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

Meiner Familie

Vorwort

Cloud Computing, also die flexible und bedarfsabhängige Bereitstellung bzw. Nutzung von IT-Ressourcen, nimmt in Unternehmen eine immer größere Rolle ein. Die Nutzung von Cloud-Diensten stellt gerade kleine und mittelständische Unternehmen vor datenschutzrechtliche Herausforderungen. Die Rechtslage ist nicht leicht zu überblicken. Das gilt besonders derzeit, da es zu einigen weitreichenden Änderungen im europäischen Datenschutzrecht gekommen ist bzw. kommen wird. Im Oktober 2015 wurde beispielsweise das Safe Harbor-Abkommen, das jahrelang zur Rechtfertigung von Datentransfers an US-amerikanische Unternehmen diente, vom Europäischen Gerichtshof für ungültig erklärt. Im Juli 2016 verabschiedete die EU-Kommission das EU-US Privacy Shield, das die Nachfolge des Safe Harbor-Abkommens antritt. Im Mai 2016 ist außerdem die Europäische Datenschutzgrundverordnung in Kraft getreten, die ab 25. Mai 2018 in allen Mitgliedstaaten der EU gelten wird. Diese Untersuchung geht der Frage nach, ob kleine und mittelständische Unternehmen bzw. Rechtsanwaltskanzleien mit Sitz in Deutschland ihre Kunden-, Personal- bzw. Mandantendaten an einen deutschen, europäischen oder US-amerikanischen Cloud-Anbieter datenschutzkonform auslagern können und geht dabei auch auf die aktuellen Entwicklungen im europäischen Datenschutzrecht ein.

Die vorliegende Arbeit wurde von der Juristischen Fakultät der Universität Augsburg im Sommersemester 2016 als Dissertation angenommen. Rechtsprechung und Literatur wurden bis einschließlich Juli 2016 berücksichtigt.

Mein ganz besonderer Dank gilt meinem Doktorvater Herrn Professor Dr. Michael Kort für die Betreuung des Promotionsverfahrens und für die Erfahrungen, die ich als langjähriger Mitarbeiter an seinem Lehrstuhl für Bürgerliches Recht, Wirtschaftsrecht, Gewerblichen Rechtsschutz und Arbeitsrecht sammeln durfte. Außerdem danke ich Herrn Professor Dr. Ulrich Gassner für die rasche Erstellung des Zweitgutachtens und Herrn Prof. Dr. Dirk Heckmann für die Aufnahme in seine Schriftenreihe „Internetrecht und Digitale Gesellschaft“. Meiner Schwester Stefanie Schmid gilt mein Dank für das Korrekturlesen.

Gewidmet ist diese Arbeit meiner Frau Nadine Schmid und meinem Sohn Felix Schmid, die mein Leben außerordentlich bereichern, und meinen Eltern Waltraud und Georg Schmid, die mich auf meinem bisherigen Lebensweg in jeder Situation unterstützt haben.

Augsburg, im August 2016

Daniel Schmid

Inhaltsübersicht

A. Einführung	25
I. Problemstellung	25
II. Cloud Computing als Chance für kleine und mittelständische Unternehmen	28
III. Gang der Untersuchung	29
B. Grundlagen des Cloud Computing	31
I. Definition des Begriffs „Cloud Computing“	31
II. Historische Entwicklung	35
III. Grundlegende Techniken und Technologien als Basis des Cloud Computing	42
IV. Erscheinungsformen (Service-Modelle/Delivery Models)	47
V. Cloud-Modelle (Deployment-Modelle)	52
VI. Wirtschaftliche Bedeutung des Cloud Computing	56
VII. Vorteile von Cloud Computing	57
VIII. Cloud Computing und Datensicherheit	63
IX. Nachteile von Cloud Computing	65
X. Beteiligte Personen und deren datenschutzrechtliche Rollen	68
XI. Zusammenfassung	70
C. Auslagerung von Kunden- und Personaldaten in die Cloud	71
I. Anwendbares Datenschutzrecht	71
II. Datenschutzrechtliche Rechtmäßigkeit der Auslagerung von Kunden- und Personaldaten in die Cloud	111
D. Auslagerung von Mandantendaten in die Cloud durch Rechtsanwaltskanzleien	222
I. Anwendbares Datenschutzrecht	222
II. Datenschutzrechtliche Rechtmäßigkeit der Auslagerung von Mandantendaten	225
III. Eingeschränkte Möglichkeit der Auslagerung von Mandantendaten in die Cloud	246
E. Zusammenfassung und Ausblick	248
I. Zusammenfassung	248
II. Ausblick	254
Literaturverzeichnis	255
Glossar	280
Sachverzeichnis	286

Inhaltsverzeichnis

A. Einführung	25
I. Problemstellung	25
II. Cloud Computing als Chance für kleine und mittelständische Unternehmen	28
III. Gang der Untersuchung	29
B. Grundlagen des Cloud Computing	31
I. Definition des Begriffs „Cloud Computing“	31
1. National Institute of Standards and Technology (NIST)	31
2. EU-Kommission	33
3. Bundesamt für Sicherheit in der Informationstechnik (BSI)	33
4. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM)	33
5. Giedke	34
6. Baun/Kunze/Nimis/Tai	34
7. Youseff/Butrico/Da Silva	34
8. Buyya/Yeo/Venugopal	34
9. Gemeinsamkeiten der Definitionen von „Cloud Computing“	35
II. Historische Entwicklung	35
1. Verteilte Systeme und Skalierbarkeit	36
2. Cluster-Computing	36
3. Grid-Computing	37
4. Utility-Computing	38
5. IT-Outsourcing	38
6. Application Service Providing (ASP)	40
7. Cloud Computing	41
III. Grundlegende Techniken und Technologien als Basis des Cloud Computing	42
1. Virtualisierung	42
2. Service-orientierte Architektur (SOA)	46
3. Breitbandinternetverbindung	46
IV. Erscheinungsformen (Service-Modelle/Delivery Models)	47
1. Infrastructure-as-a-Service (IaaS)	48
2. Platform-as-a-Service (PaaS)	49
3. Software-as-a-Service (SaaS)	50
4. Passendes Service-Modell für das Kunden- und Personaldatenmanagement kleiner und mittelständischer Unternehmen	51

V.	Cloud-Modelle (Deployment-Modelle)	52
1.	Private Cloud	52
2.	Public Cloud	53
3.	Community Cloud	54
4.	Hybrid Cloud	55
5.	Passendes Cloud-Modell für kleine und mittelständische Unternehmen	55
VI.	Wirtschaftliche Bedeutung des Cloud Computing	56
VII.	Vorteile von Cloud Computing	57
1.	Wirtschaftliche Vorteile	58
2.	Technische Vorteile	59
3.	Vorteile für den Cloud-Anbieter	61
VIII.	Cloud Computing und Datensicherheit	63
1.	„Klassische“ Risiken	64
2.	Cloudspezifische Risiken	64
IX.	Nachteile von Cloud Computing	65
X.	Beteiligte Personen und deren datenschutzrechtliche Rollen	68
1.	Der Cloud-Nutzer (Cloud-Anwender/Cloud-Kunde)	69
2.	Der Cloud-Anbieter	69
3.	Der Unterauftragnehmer (Subunternehmer/Ressourcen-Anbieter)	69
4.	Der Betroffene	70
XI.	Zusammenfassung	70
C.	Auslagerung von Kunden- und Personaldaten in die Cloud	71
I.	Anwendbares Datenschutzrecht	71
1.	Sachlicher Anwendungsbereich und Normadressat	73
a)	Vorrang spezialgesetzlicher Regelungen	74
aa)	Anwendbarkeit des TKG	74
bb)	Anwendbarkeit des TMG	76
cc)	Anwendbarkeit des BDSG	79
b)	BDSG	80
aa)	Das personenbezogene Datum	80
(1)	Einzelangaben über persönliche oder sachliche Verhältnisse	80
(2)	Bestimmte bzw. bestimmbare Person	81
(a)	Bestimmtheit	81
(b)	Bestimmbarkeit	82
(aa)	Theorie des absoluten (bzw. objektiven) Personenbezugs	83
(bb)	Theorie des relativen (bzw. subjektiven) Personenbezugs	84
(cc)	Subjektive Theorie unter Einbezug von ohne großem Aufwand beziehbarem Zusatzwissen	84

(dd) Stellungnahme	85
(ee) Anonymisieren und Pseudonymisieren	88
(ff) Auswirkungen durch Verschlüsselung	90
(gg) Verschlüsselung im Rahmen von SaaS-Diensten	92
(hh) Entfallen des Personenbezugs durch Einsatz der „Sealed Cloud“	93
(c) Kunden- und Personaldaten als bestimmte bzw. bestimmbare Daten	95
(3) Besondere Arten personenbezogener Daten	95
(4) Aufspaltung (Fragmentierung) der personenbezogenen Daten	96
(5) Natürliche Person	97
bb) Erhebung, Verarbeitung und Nutzung	97
(1) Erhebung	97
(2) Verarbeitung	98
(3) Nutzung	100
cc) Normadressat	100
c) Sachlicher Anwendungsbereich des BDSG	102
d) Sachlicher Anwendungsbereich der DS-GVO	102
2. Räumlicher Anwendungsbereich	104
a) Grundsatz: Territorialprinzip	104
b) Sitzlandprinzip (§ 1 Abs. 5 Satz 1 Halbsatz 1 BDSG)	105
c) Ausnahme vom Sitzlandprinzip: Niederlassungsprinzip bzw. abgeschwächtes Sitzlandprinzip (§ 1 Abs. 5 Satz 1 Halbsatz 2 BDSG)	106
d) Geltung des Territorialprinzips für verantwortliche Stellen außerhalb der EU bzw. des EWR (§ 1 Abs. 5 Satz 2 BDSG)	106
e) Problematik der Anwendbarkeit des Territorialprinzips und des Sitzlandprinzips auf das Cloud Computing	107
f) Anwendbarkeit des Territorialprinzips und des Sitzlandprinzips auf das Cloud Computing	108
g) Räumlicher Anwendungsbereich gem. BDSG	109
h) Räumlicher Anwendungsbereich gem. DS-GVO	110
II. Datenschutzrechtliche Rechtmäßigkeit der Auslagerung von Kunden- und Personaldaten in die Cloud	111
1. Prinzip des Verbots mit Erlaubnisvorbehalt	111
2. Vorliegen eines Erlaubnistatbestandes im nationalen Kontext	112
a) Abgrenzung von §§ 28, 29 und 32 BDSG	113
b) Prüfung der einschlägigen Rechtsgrundlage für die Auslagerung von Kunden- und Personaldaten	114
c) Kundendaten: Datenerhebung und -speicherung für eigene Geschäftszwecke (§ 28 BDSG)	115

aa)	Verhältnis der drei Erlaubnistatbestände des § 28 Abs. 1 Satz 1 BDSG	115
bb)	Rechtsgeschäftliche oder rechtsgeschäftsähnliche Schuldverhältnisse (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG)	115
cc)	Wahrung berechtigter Interessen (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG)	116
	(1) Berechtigte Interessen des Unternehmens	119
	(2) Schutzwürdige Interessen des Kunden	119
	(3) Gegenüberstellung der betroffenen Interessen des Unternehmens und des Kunden	119
	(a) Verarbeitungszweck	120
	(b) Dauer der Speicherung	120
	(c) Art bzw. Sensibilität der ausgelagerten Daten	121
	(d) Größe des auslagernden Unternehmens	121
	(e) Transparenz der Datenverarbeitung	122
	(f) Größe und Vertrauenswürdigkeit des Cloud-Anbieters	122
	(g) Interessenabwägung zugunsten des Unternehmens	122
dd)	Allgemein zugängliche Daten (§ 28 Abs. 1 Satz 1 Nr. 3 BDSG)	123
d)	Personaldaten: § 32 Abs. 1 Satz 1 BDSG bzw. § 28 Abs. 1 Satz 1 Nr. 2 BDSG	123
e)	Besondere Arten personenbezogener Daten (§ 28 Abs. 6 bis 9 BDSG)	125
f)	Einschlägige Rechtsgrundlage für die Auslagerung von Kundendaten und Personaldaten im nationalen Kontext	126
g)	Erlaubnistatbestände der DS-GVO	127
3.	Einwilligung gem. § 4a BDSG	128
	a) Freiwillige Entscheidung des Betroffenen	129
	b) Bestimmtheit	131
	c) Schriftform	132
	d) Besondere Arten personenbezogener Daten	133
	e) Widerrufsmöglichkeit	134
	f) Konsequenzen bei Versagung der Einwilligung	134
	aa) Versagung der Einwilligung bei Vorliegen eines anderen Erlaubnistatbestandes	135
	bb) Versagung der Einwilligung bei Nicht-Vorliegen eines anderen Erlaubnistatbestandes	135
	g) Nachträgliches Einholen der Einwilligung	135
	h) Geringe Praktikabilität der Einwilligung bei der Auslagerung von Kunden- und Personaldaten	136
	i) Einwilligung gem. DS-GVO	136
4.	Betriebsvereinbarung	138
5.	Auftragsdatenverarbeitung	140

a) Dogmatische Einordnung und Rechtsnatur	141
b) Funktionsübertragungstheorie und Vertragstheorie	144
aa) Funktionsübertragungstheorie	144
bb) Vertragstheorie	146
cc) Bewertung	147
c) Voraussetzungen einer Auftragsdatenverarbeitung (§ 11 Abs. 2 BDSG)	149
aa) Auswahl des Auftragnehmers unter Berücksichtigung der Eignung der von ihm getroffenen technischen und organi- satorischen Maßnahmen (§ 11 Abs. 2 Satz 1 BDSG)	150
(1) Organisationskontrolle (Satz 1 der Anlage zu § 9 Satz 1 BDSG)	151
(2) Zutrittskontrolle (Satz 2 Nr. 1 der Anlage zu § 9 Satz 1 BDSG)	152
(3) Zugangskontrolle (Satz 2 Nr. 2 der Anlage zu § 9 Satz 1 BDSG)	152
(4) Zugriffskontrolle (Satz 2 Nr. 3 der Anlage zu § 9 Satz 1 BDSG)	154
(5) Weitergabekontrolle (Satz 2 Nr. 4 der Anlage zu § 9 Satz 1 BDSG)	155
(6) Eingabekontrolle (Satz 2 Nr. 5 der Anlage zu § 9 Satz 1 BDSG)	156
(7) Auftragskontrolle (Satz 2 Nr. 6 der Anlage zu § 9 Satz 1 BDSG)	156
(8) Verfügbarkeitskontrolle (Satz 2 Nr. 7 der Anlage zu § 9 Satz 1 BDSG)	156
(9) Trennungskontrolle (Satz 2 Nr. 8 der Anlage zu § 9 Satz 1 BDSG)	157
(10) Einhalten der Auswahlpflicht bei der Auswahl eines Cloud-Anbieters	158
(11) Kritik an der Anlage zu § 9 Satz 1 BDSG	158
bb) Vertragsgestaltung bei der Auftragsdatenverarbeitung (§ 11 Abs. 2 Satz 2 BDSG)	158
(1) Schriftformerfordernis	159
(2) Gegenstand und Dauer des Auftrags (§ 11 Abs. 2 Satz 2 Nr. 1 BDSG)	160
(3) Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, Art der Daten und Kreis der Betroffenen (§ 11 Abs. 2 Satz 2 Nr. 2 BDSG)	161
(4) Nach § 9 BDSG zu treffende technische und organi- satorische Maßnahmen (§ 11 Abs. 2 Satz 2 Nr. 3 BDSG).	161
(5) Berichtigung, Löschung und Sperrung von Daten (§ 11 Abs. 2 Satz 2 Nr. 4 BDSG)	162

(6)	Nach § 11 Abs. 4 BDSG bestehende Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen (§ 11 Abs. 2 Satz 2 Nr. 5 BDSG)	162
(7)	Berechtigung zur Begründung von Unterauftragsverhältnissen (§ 11 Abs. 2 Satz 2 Nr. 6 BDSG)	163
(8)	Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers (§ 11 Abs. 2 Satz 2 Nr. 7 BDSG)	163
(9)	Mitteilungen über Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen die im Auftrag getroffenen Festlegungen (§ 11 Abs. 2 Satz 2 Nr. 8 BDSG)	164
(10)	Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält (§ 11 Abs. 2 Satz 2 Nr. 9 BDSG)	164
(11)	Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags (§ 11 Abs. 2 Satz 2 Nr. 10 BDSG)	165
(12)	Kontrolle des Cloud-Anbieters und Dokumentation der Kontrollen	165
(a)	Kontrolle vor Beginn der Datenverarbeitung	166
(b)	Regelmäßige Kontrolle während der Datenverarbeitung	167
(c)	Vorgehensweise bei Kontrollen	167
(d)	Problematik der Durchführung von Kontrollen beim Cloud Computing	168
(e)	Zertifizierung	169
d)	Weisungsgebundenheit (§ 11 Abs. 3 BDSG)	172
e)	Einsatz von Unterauftragnehmern	173
f)	Privilegierungswirkung der Auftragsdatenverarbeitung	174
aa)	Nicht-Vorliegen einer Nutzung i. S. v. § 3 Abs. 5 BDSG bei der Auslagerung von Daten im Rahmen einer Auftragsdatenverarbeitung	175
bb)	Vorliegen einer Nutzung i. S. v. § 3 Abs. 5 BDSG bei der Auslagerung von Daten im Rahmen einer Auftragsdatenverarbeitung	176
cc)	Bewertung	176
g)	Erlaubnistatbestand für die Nutzung der personenbezogenen Daten	177
h)	Auftragsdatenverarbeitung gem. DS-GVO	178
6.	Datenübermittlung und Auftragsdatenverarbeitung im internationalen Kontext	179
a)	Datenübermittlung und Auftragsdatenverarbeitung innerhalb der EU bzw. des EWR	179

aa)	Datenübermittlung innerhalb der EU bzw. des EWR	179
bb)	Auftragsdatenverarbeitung innerhalb der EU bzw. des EWR	180
b)	Datenübermittlung und Auftragsvergabe in einen Drittstaat . . .	180
aa)	Datenübermittlung in einen Drittstaat	180
bb)	Auftragsvergabe in einen Drittstaat	181
	(1) Bestimmen der Grenzüberschreitung	181
	(2) Privilegierungswirkung bei Auftragsdatenverarbeitern aus Drittstaaten	182
	(a) Fehlende Privilegierungswirkung des § 3 Abs. 8 Satz 3 BDSG für Auftragsdatenverarbeiter aus Drittstaaten	183
	(b) Privilegierung des Auftragsdatenverarbeiters aus einem Drittstaat bei der Verwendung von EU- Standardvertragsklauseln	184
	(aa) Analogie zu § 3 Abs. 8 BDSG	185
	(bb) Modifizierte Interessenabwägung im Rah- men von § 28 Abs. 1 Satz 1 Nr. 2 BDSG . .	186
	(c) Vollharmonisierende Wirkung der DS-RL: Mög- lichkeit der unmittelbaren Anwendung	187
	(d) Konsequenzen der Rechtsprechung des EuGH: Unionsrechtswidrigkeit von § 3 Abs. 8 Satz 3 BDSG	189
cc)	Prüfung der ersten Stufe: Zulässigkeit der Datenübermitt- lung bzw. der Auftragsdatenverarbeitung nach dem BDSG	189
	(1) Zulässigkeit der Datenübermittlung	189
	(a) § 28 Abs. 1 Satz 1 Nr. 1 BDSG	190
	(b) § 28 Abs. 1 Satz 1 Nr. 2 BDSG	190
	(c) § 28 Abs. 6 bis 9 BDSG	191
	(2) Zulässigkeit der Auftragsdatenverarbeitung	191
	(3) Möglichkeit einer Datenübermittlung bzw. Auftrags- datenverarbeitung nach dem BDSG	191
dd)	Prüfung der zweiten Stufe: Einhalten der besonderen Anfor- derungen im Rahmen von Datentransfers an Cloud-Anbieter aus Drittstaaten	192
	(1) Angemessenes Datenschutzniveau	193
	(a) Unionsrechtswidrigkeit von § 4b Abs. 2 Satz 2 Halbsatz 2 BDSG	193
	(b) Kriterien für die Angemessenheit des Daten- schutzniveaus	193
	(c) Feststellung der Angemessenheit durch die EU- Kommission	194
	(2) Sonderfall USA: Safe Harbor-Prinzipien	195
	(a) „Safe Harbor 1.0“	195
	(aa) Grundlagen der Safe Harbor-Zertifizierung	195

(bb) Kritik an der Safe Harbor-Zertifizierung . . .	198
(b) Urteil des EuGH: Ungültigkeit von „Safe Harbor“	199
(aa) Ursachen	199
(bb) Sachverhalt	201
(cc) Aussagen und Folgen des Urteils	202
(c) „Safe Harbor 2.0“	207
(3) Erlaubnistatbestände trotz unangemessenem Datenschutzniveau	210
(4) Angemessene Garantien	212
(a) Genehmigung durch die zuständige Aufsichtsbehörde	212
(b) EU-Standardvertragsklauseln	213
(c) Binding Corporate Rules (BCR)	216
ee) Eingeschränkte Möglichkeit des datenschutzkonformen Auslagerns der Kunden- und Personaldaten in die USA . . .	217
ff) Datentransfers auf europäische Server von US-amerikanischen Cloud-Anbietern	217
c) Eingeschränkte Möglichkeit der datenschutzkonformen Auslagerung von Kunden- bzw. Personaldaten auf internationale Cloud-Anbieter	219
d) Datenübermittlung und Auftragsdatenverarbeitung im internationalen Kontext gem. DS-GVO	220
7. Rechtskonformität der Auslagerung von Kunden- bzw. Personaldaten in die Cloud nach dem BDSG	221
D. Auslagerung von Mandantendaten in die Cloud durch Rechtsanwaltskanzleien	222
I. Anwendbares Datenschutzrecht	222
1. Vorrang der Bundesrechtsanwaltsordnung (BRAO) bzw. der Berufsordnung für Rechtsanwälte (BORA)	222
2. Normadressat	225
3. Räumlicher Anwendungsbereich	225
II. Datenschutzrechtliche Rechtmäßigkeit der Auslagerung von Mandantendaten	225
1. Datenschutzrechtliche Prüfung: Einwilligung, Erlaubnistatbestand oder Auftragsdatenverarbeitung	226
2. Prüfung von § 203 StGB	227
a) Geschütztes Rechtsgut	227
b) Fremdes Geheimnis	228
c) Täterkreis, Tathandlung und Taterfolg	229
d) Befugnis zur Offenbarung	230
e) Subjektiver Tatbestand	231
f) Drittgeheimnis	231

g) Strafblose Auslagerung von Mandantendaten in die Cloud	232
aa) Hilfe i. S. v. § 203 Abs. 3 Satz 2 StGB	232
bb) Ausdrückliche Einwilligung in Form einer Schweigepflicht- entbindung	238
cc) Befugnis in Form einer konkludenten oder mutmaßlichen Einwilligung	239
dd) Gesetzliche Befugnisnorm	240
ee) Verschlüsselung	240
ff) Arbeitnehmerüberlassung oder Doppelarbeitsverhältnis . . .	241
gg) Verschwiegenheitserklärung des Cloud-Anbieters und des- sen Mitarbeiter	241
hh) Genossenschaft von Berufsheimnisträgern am Beispiel der DATEV e.G.	242
ii) Community Cloud und Sealed Cloud für Rechtsanwälte . .	242
h) Auswirkung der Neufassung von § 2 BORA auf die Strafbar- keit im Rahmen von § 203 StGB	243
III. Eingeschränkte Möglichkeit der Auslagerung von Mandantendaten in die Cloud	246
E. Zusammenfassung und Ausblick	248
I. Zusammenfassung	248
II. Ausblick	254
Literaturverzeichnis	255
Glossar	280
Sachverzeichnis	286

Abkürzungsverzeichnis

a. A.	andere Ansicht
ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
a. E.	am Ende
AEUV	Vertrag über die Arbeitsweise der europäischen Union
AG	Amtsgericht
Anwbl.	Anwaltsblatt (Zeitschrift)
API	Application Programming Interface
ArbR Aktuell	Arbeitsrecht Aktuell (Zeitschrift)
ASP	Application Service Providing
Aufl.	Auflage
BAG	Bundesarbeitsgericht
BB	Betriebs-Berater (Zeitschrift)
BCR	Bindung Corporate Rules
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BORA	Berufsordnung der Rechtsanwälte
BRAK-Mitt.	Bundesrechtsanwaltskammer-Mitteilungen (Zeitschrift)
BRAO	Bundesrechtsanwaltsordnung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BYOD	Bring Your Own Device
bzw.	beziehungsweise
ca.	circa
CaaS	Communication-as-a-Service
CCZ	Corporate Compliance Zeitschrift (Zeitschrift)

CR	Computer und Recht (Zeitschrift)
CuA	Computer und Arbeit (Zeitschrift)
DB	Der Betrieb (Zeitschrift)
DDoS	Distributed Denial of Service
d. h.	das heißt
Dok.	Dokument
DS-GVO	EU-Datenschutzgrundverordnung
DS-GVO-E	EU-Datenschutzgrundverordnung-Entwurf
DSK	Datenschutzkonferenz der Datenschutzbeauftragten des Bundes und der Länder
DStR	Deutsches Steuerrecht (Zeitschrift)
DuD	Datenschutz und Datensicherheit (Zeitschrift)
EDV	Elektronische Datenverarbeitung
e. g.	exempli gratia
e.G.	eingetragene Genossenschaft
EG	Europäische Gemeinschaft
engl.	englisch
ENISA	European Network and Information Security Agency
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum
f.	folgend
FBI	Federal Bureau of Investigation
ff.	fortfolgend
FISA	Foreign Intelligence Surveillance Act
FS	Festschrift
FTC	Federal Trade Commission
gem.	gemäß
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GRCh	Grundrechtecharta
h. M.	herrschende Meinung
HMD	Praxis der Wirtschaftsinformatik (Zeitschrift)
Hrsg.	Herausgeber
IaaS	Infrastructure-as-a-Service
IDE	Integrated Development Environment