

Inhaltsverzeichnis

Kapitel 1 – Einführung	17
A. Ziele der Arbeit und Gang der Untersuchung	18
B. Grundlagen der Untersuchung	22
I. Begriffliche Annäherung	23
1. Allgemeine Definition und Charakteristika des Cloud Computing	23
2. Abgrenzung zum Outsourcing und unterschiedliche Leistungsmodelle	25
II. Cloud Computing als neuer Standard und potenzieller Katalysator staatlicher Digitalisierung	28
1. Cloud Computing als neuer Standard für IT-Infrastrukturen	28
a) Historische Entwicklung und Funktionsweise des Cloud Computings	28
b) Cloud-Leistungen als neuer Standard für Software und IT-Sicherheit	34
2. Cloud Computing als potenzieller Katalysator der staatlichen Digitalisierung	37
a) Cloud-Anwendungen als Abhilfe für staatliche Fähigkeitslücken	38
b) Make or Buy-Entscheidung	40
3. Mögliche Nachteile einer staatlichen Nutzung von Cloud-Leistungen	43
C. Zwischenergebnis	44
Kapitel 2 – Problemaufriss zur Nutzung von Cloud-Anwendungen in staatlichen Stellen und bestehende Herausforderungen	47
A. Herausforderungen beim Aufbau eigener Cloud-Infrastrukturen (Make)	47

B. Herausforderungen bei der Beschaffung von Cloud-Leistungen (Buy)	48
I. Befürchteter Verlust an digitaler Souveränität	49
II. Weitere cloud-spezifische Herausforderungen	53
C. Eingrenzung des Untersuchungsgegenstandes	54
D. Zwischenergebnis	57
 Kapitel 3 – Statthaftigkeit der Nutzung von Cloud-Leistungen	59
A. Unionrechtliche Neutralität gegenüber der Nutzung von Cloud-Leistungen	59
B. Verfassungsrechtliche Grenzen einer Privatisierung von Datenverarbeitungen	60
I. Aussagen der Verfassung zur Datenverarbeitung als eigenständige Staatsaufgabe	61
II. Einordnung von Cloud-Leistungen in die verschiedenen Privatisierungsformen	64
III. Verpflichtungen staatlicher Stellen zu einer eigenhändigen Datenverarbeitung?	65
1. Pflicht zum staatlichen Betrieb der benötigten IT-Infrastruktur?	66
2. Notwendige staatliche Datenverarbeitung bei besonders wichtigen Daten?	67
3. Funktionsvorbehalt des Art. 33 Abs. 4 GG	68
4. Pflicht zur fortbestehenden Kontrolle über Verarbeitungsprozesse (Privatisierungsfolgenrecht)	70
C. Privatisierungsschranken aus dem nationalen einfachen Recht	72
I. Einschränkung der Nutzung von Cloud-Leistungen in Bundesgesetzen	72
II. Einschränkung der Nutzung von Cloud-Leistungen in Landesgesetzen	73
D. Zwischenergebnis	74
 Kapitel 4 – Steuerung der Nutzung und Beschaffung von Cloud-Leistungen durch das Vergaberecht	77
A. Rolle des Vergaberechts als Digitalisierungsgestaltungsrecht	77

B. Einordnung von Cloud-Leistungen in den vergaberechtlichen Rahmen	80
I. Maßgebliche vergaberechtliche Rechtsquellen	80
II. Einordnung von Cloud-Leistungen in die vergaberechtlichen Leistungsarten	84
1. Schwierigkeiten bei Einordnung als Lieferauftrag oder Dienstleistungsauftrag	85
2. Cloud-Leistungen und der Warenbegriff des § 103 Abs. 2 GWB	86
3. Das Tatbestandsmerkmal der Beschaffung von Waren in § 103 Abs. 2 GWB	88
III. Cloud-Leistungen im Anwendungsbereich der Sektorenrichtlinie	90
IV. Cloud-Leistungen und verteidigungs- und sicherheitsspezifische Ausnahmetatbestände	92
1. Vergabe von Cloud-Leistungen nach der VSVgV	93
a) Voraussetzungen für eine Anwendung der VSVgV bei Cloud-Leistungen	94
b) Umfang der Anwendbarkeit der VSVgV	97
2. (Direkt-)Vergaben von Cloud-Leistungen nach § 107 Abs. 2 GWB i.V.m. Art. 346 AEUV	98
a) Cloud-Leistungen und die Güterliste des Art. 346 Abs. 1 lit. b), Abs. 2 AEUV	99
b) Voraussetzungen des § 107 Abs. 2 S. 1 Nr. 1 i.V.m. Art. 346 lit. a AEUV	100
c) Restriktive Auslegung des Art. 346 AEUV durch den EuGH	102
C. Kooperationsmöglichkeiten für staatliche Stellen	103
I. Gemeinsamer Aufbau und Nutzung von staatlichen (Cloud-)Rechenzentren	104
1. Rahmen der Kooperationsentscheidung	104
a) Verfassungsrechtliche Ermöglichung von Kooperationen im IT-Bereich	104
b) Notwendigkeit von Kooperationen für staatseigene Cloud-Infrastrukturen	106
2. Vergaberechtsfreie Umsetzungsmöglichkeiten	109
a) Teilnahme am Marktgeschehen und entgeltlicher öffentlicher Auftrag	109

b)	Nicht dem Vergaberecht unterfallende horizontale Kooperationen	111
aa)	Rechtsrahmen vergaberechtsfreier horizontaler Kooperationen nach dem EuGH	112
bb)	Nutzung der Cloud-Infrastrukturen eines anderen Rechtsträgers	113
c)	Nicht dem Vergaberecht unterfallende Inhouse-Vergaben	115
aa)	Primärrechtlicher Hintergrund und Rechtsprechung des EuGH	115
bb)	Besonderheiten bei Inhouse-Vergaben zur Beschaffung von Cloud-Leistungen	118
d)	Zusammenfassende Betrachtung zum gemeinsamen Rechenzentrumsaufbau	120
II.	Schaffung von Skaleneffekten bei der Leistungsbeschaffung am Markt	121
1.	Rahmen der Beschaffungsentscheidung	121
a)	Über Haushaltsrecht vorgeschriebene Nutzung von EVB-IT Cloud Verträgen	122
b)	Vereinheitlichung durch Datenschutz- und IT-Sicherheitsvorgaben	124
c)	Vereinheitlichung von Standards über Koordinierungen	124
d)	Vermehrte Nachfragebündelungen	126
2.	Vergaberechtliche Umsetzung	127
a)	Vorgabe von Standards über die Festlegung des Leistungsgegenstandes	127
b)	Vergabefreier Austausch von Cloud-Anwendung nach dem EfA-Prinzip	128
c)	Nachfragebündelungen verschiedener staatlicher Stellen	132
III.	Zwischenergebnis	133
D.	Erhalt digitaler Souveränität bei der Beschaffung von Cloud-Leistungen	135
I.	Umfang der im Grundgesetz vorgegebenen digitalen Souveränität	135
1.	Digitale Souveränität als Verfassungsvoraussetzung?	136
2.	Digitale Souveränität als verfassungsrechtliches Leitbild	137

3. Mindestmaß an digitaler Souveränität aus Pflicht zur fortbestehenden Kontrolle	139
a) Pflicht zu einer staatlichen Kontrolle aus dem Demokratieprinzip	139
b) Pflicht zu fortbestehender staatlicher Kontrolle aus dem Rechtsstaatsprinzip	141
c) Kontrollpflichten aus einer Gewährleistungsverantwortung für die Grundrechte	142
d) Pflicht zur fortbestehenden Kontrolle aus Art. 33 Abs. 4 GG	143
e) Etwaige Vorgaben zur Selbstorganisation und Eigenständigkeit der Verwaltung	143
4. Pflicht zu Datenverarbeitungen ausschließlich in Deutschland oder der EU?	144
5. Verfassungsrechtliche Pflicht zur Autarkie gegenüber anderen Staaten?	147
II. Digitale Souveränität als politische Zielstellung	149
III. Zielkonflikte von digitaler Souveränität und Vergaberechtsgrundsätzen?	151
IV. Gewährleistungsverantwortung für den Schutz personenbezogener Daten	153
1. Rahmen der Beschaffungsentscheidung	153
a) Recht auf informationelle Selbstbestimmung und Europäische Datenschutzgrundrechte	153
b) Vorgaben der DSGVO	157
aa) Regulierungsansatz der DSGVO	157
bb) Cloud Computing als Auftragsverarbeitung im Sinne der DSGVO	159
cc) Datenübermittlungen in Drittstaaten am Beispiel der USA	161
dd) Risiko behördlicher Herausgabeverlangen bei in der EU verarbeiteten Daten	166
(1) Risiken behördlicher Herausgabeverlangen nach dem US-CLOUD Act	166
(2) Rechtsfolgen entgegenstehender Verpflichtungen aus CLOUD Act und DSGVO	169

(3) DSGVO-Verstöße einzelner Cloud-Angebote am Beispiel von Microsoft 365	171
ee) Mögliche Erleichterungen für staatliche Stellen	173
(1) Neuer Angemessenheitsbeschluss der Europäischen Kommission	173
(2) Technische Lösungen	174
(3) Datentreuhandmodelle	175
2. Vergaberechtliche Umsetzung	178
a) Zweckmäßigkeit eines Verhandlungsverfahrens mit Teilnahmewettbewerb	178
b) Sicherstellung von Datenschutz über Eingrenzungen des Teilnehmerfeldes?	180
c) Sicherstellung von Datenschutz über die Festlegung des Leistungsgegenstandes	183
aa) Einhaltung der DSGVO und weitergehende Vorgaben	183
bb) Vorgabe technischer Schutzmaßnahmen im Rahmen der Leistungsbeschreibung	185
cc) Vorgaben zu Datentreuhandmodellen	186
d) Sicherstellung von Datenschutz über die Ausführungsbedingungen	187
e) Prüfung der Einhaltung des Datenschutzrechts innerhalb des Vergabeverfahrens	189
aa) Allgemeiner Prüfungsmaßstab einer Änderung der Vergabeunterlagen	190
bb) Übertragung auf den Cloud-Bereich	192
cc) Auswirkungen des neuen Angemessenheitsbeschlusses auf die Angebotsprüfung	194
f) Zwischenergebnis zur Umsetzung der Gewährleistungsverantwortung für den Datenschutz	195
V. Sicherstellung von Informationssicherheit/IT-Sicherheit	197
1. Rahmen der Beschaffungsentscheidung	197
a) Rechtliche Rahmenbedingungen	198
aa) Verhältnis des Informationssicherheitsrechts zum Datenschutzrecht	198
bb) Verfassungsrechtliche Pflicht zur Informationssicherheit	199

cc) Zu beachtendes Informationssicherheitsrecht	202
(1) Vorgaben im BSIG	203
(2) Mindeststandards für die Nutzung von Cloud-Leistungen nach dem BSI	205
(3) Weitere relevante Standards im IT- Sicherheitsrecht	206
b) Politischer Rahmen	208
aa) Cloud-Leistungen als Reaktion auf aktuelle Bedrohungslagen	208
bb) Bestreben zum Schutz vor staatlicher Spionage am Beispiel der VR China	209
2. Vergaberechtliche Umsetzung	212
a) Vorgaben zur IT-Sicherheit in den Vergabeunterlagen	212
aa) IT-Sicherheit als Teil der Festlegung des Leistungsgegenstandes	212
bb) Schaffung von IT-Sicherheit über die Eignungsanforderungen	215
(1) IT-Sicherheit als Teil der technischen und beruflichen Leistungsfähigkeit	215
(2) Forderung von IT-Sicherheitszertifizierungen als Eignungsnachweis	217
cc) Zusätzliche Möglichkeiten zur Informationssicherheit bei Verschlussachen	219
b) Situation bei fehlendem Vertrauen gegenüber konkreten Bietern	220
aa) Ausschlussmöglichkeiten bei Fehlverhalten eines Bieters in der Vergangenheit	221
bb) Präventive Adressierung von Spionagerisiken	223
(1) Nutzung von „No Spy“-Erklärungen	224
(2) Ausschlussentscheidungen bei konkreten Verdachtsmomenten für Spionage	224
(a.) Fehlen eines Ausschlussgrundes für Sicherheitsbedenken in der VgV	224
(b.) Eignungskriterium des Fehlens von Interessenskonflikten	225
(aa.) Systematische Einordnung	226
(bb.) Von § 46 Abs. 2 VgV erfasste Interessenskonflikte	226

	(cc.) Prüfungsmaßstab	227
	(c.) Ausschlussgrund des § 147 GWB im Bereich Verteidigung und Sicherheit	229
c)	Zwischenergebnis zur Gewährleistung von Informationssicherheit	233
VI.	Sicherstellung staatlicher Kontrolle und politischer Unabhängigkeit	234
1.	Rahmen der Beschaffungsentscheidung	234
a)	Rechtliche und politische Zielstellung	234
b)	Deutsche Verwaltungscloud-Strategie	235
2.	Vergaberechtliche Umsetzung	237
a)	Sicherstellung von Autonomie über die Festlegung des Leistungsgenstandes	237
b)	Sicherung von Autonomie über eine Eingrenzung des Teilnehmerfeldes	240
c)	Sicherung von Handlungshoheit durch Standortvorgaben für Rechenzentren	241
aa)	Standortvorgaben als Teil des Leistungsgegenstandes	241
bb)	Anforderungen an Standortvorgaben in der Rechtsprechung des EuGH	243
(1)	Standortvorgabe Deutschland	244
(2)	Standortvorgabe Europäische Union	245
(3)	Absicherung der Versorgungssicherheit im Anwendungsbereich der VSvG	247
VII.	Gesamtschau der Möglichkeiten zum Erhalt digitaler Souveränität	248
E.	Cloud-spezifische Herausforderungen und vergaberechtliche Steuerungsinstrumente	250
I.	Steuerung der Einbindung von Dritten in die Leistungserbringung	250
1.	Rahmen der Beschaffungsentscheidung	250
2.	Vergaberechtliche Umsetzung	252
a)	Vorgabe einer Selbsterbringung durch den Auftragnehmer	252
b)	Abgrenzung zwischen Nachunternehmern und Zulieferern	254

c) Rechtsfolgen einer Einordnung Dritter als Unterauftragnehmer oder Zulieferer	256
aa) Aufforderung zur Benennung von Nachunternehmern und Zulieferern im Angebot	256
bb) Unterschiede in der Eignungsprüfung	258
(1) Erstreckung der Eignungsprüfung auf Nachunternehmer	258
(2) Erstreckung der Eignungsprüfung auf Zulieferer	259
d) Zwischenergebnis zur Steuerung der Einbindung Dritter	260
II. Standardisierte Verträge der Cloud-Anbieter	261
1. Rahmen der Beschaffungsentscheidung	261
2. Vergaberechtliche Umsetzung	262
a) Problematik abweichender Allgemeiner Geschäftsbedingungen	262
b) Lösungsansatz der EVB-IT Cloud	263
c) Adäquate Berücksichtigung von bieterseitigen AGBs im Rahmen der Zuschlagskriterien	264
III. Nachhaltige Beschaffungen	267
1. Rahmen der Beschaffungsentscheidung	267
2. Vergaberechtliche Umsetzung	269
a) Besondere gesetzliche Vorgaben für energieverbrauchsrelevante Leistungen	270
b) Umweltbezogene Vorgaben innerhalb der Leistungsbeschreibung	272
c) Umweltbezogene Ausführungsbedingungen	272
d) Voraussetzung einer Vorgabe als Zuschlagskriterium	273
IV. Interessenausgleich im Rahmen des vergaberechtlichen Rechtsschutzes	275
1. Rechtsrahmen für Cloud-Leistungen und Bieterrechte gemäß § 97 Abs. 6 GWB	275
2. Berücksichtigung von nicht offengelegtem Vortrag („In- Camera“-Verfahren)	277
F. Handlungsimpulse für Beschaffungs- und Vergabestellen sowie Nachprüfungsinstanzen	281
Literaturverzeichnis	291