Thomas Hofer
(E-Mail: t.hofer@jura.uni-muenchen.de)
ist Akademischer Oberrat und leitet das Rechtsinformatikzentrum der Ludwig-Maximilians-Universität München. Seine Arbeitsschwerpunkte sind Rechtsfragen der IT-Compliance und Informationssicherheit, juristische Informationssysteme und E-Learning in den Rechtswissenschaften.

Ausgewählte Rechtsfragen des Cloud Computings: GU- und Multi-Vendor-Modell – ein Vergleich im Hinblick auf die Rechtswahl

Cloud Computing ist ein Beispiel für eine innovative Technologie, die sehr schnell von Verbrauchern und Unternehmen angenommen wurde. Unter Cloud Computing wird i. d. R. ein IT-Angebot verstanden, das es ermöglicht, eine oder mehrere IT-Dienstleistungen (z. B. Rechenleistung, Datenspeicher, Security, Anwendungssoftware) jederzeit, netzbasiert, standortunabhängig, schnell, dem tatsächlichen Bedarf entsprechend und nach tatsächlicher Nutzung abrechenbar zu beziehen. Die technische Entwicklung des Cloud Computings schreitet rasch voran. Cloud Computing ist folgerichtig als eine zentrale Komponente in der IKT-Strategie der Bundesregierung „Deutschland Digital 2015" definiert worden. Auch das Bundesministerium für Wirtschaft und Technologie fokussiert das Thema und hat den Technologiewettbewerb „Sichere Internet-Dienste – Sicheres Cloud Computing für Mittelstand und Öffentlichen Sektor (Trusted Cloud)" initiiert. Aber wie bei allen neuen technischen Entwicklungen gibt es auch hier Vorbehalte. Eine ganze Reihe anderer Indikatoren zeichnen ein ähnliches Bild. Höchste Zeit sich aktiv mit dem Thema auseinanderzusetzen. Was steckt denn nun hinter dieser Cloud?

Ob es sich um eine öffentliche Cloud im Internet oder eine private Cloud hinter der Firewall eines Unternehmens handelt, die Dienste müssen genauso gesichert werden wie alle anderen gemeinsam genutzten Ressourcen auch. Damit Unternehmen wie öffentliche Verwaltungen Risiken für ihre ausgelagerten Daten und Prozesse fundiert einschätzen und managen können, müssen die Fragen der Datensicherheit, der Einhaltung gesetzlicher Vorgaben und der Vertragsgestaltung vollständig beantwortet sein.

Dazu entwickelt z. B. der Forschungsbereich des Fraunhofer-Instituts für Sichere Informationstechnologie (SIT) Lösungen, mit denen sich das Sicherheitsniveau von Cloud-Angeboten in Form eines „Cloud-Cockpits" messen und Daten in der Cloud effektiv schützen lassen. Grundlage bildet ein feingranular verteiltes Verschlüsselungskonzept, das Informationen vor dem unbefugten Zugriff Dritter schützt und nur bei Bedarf diejenigen Informationen entschlüsselt, die wirklich benötigt werden (vgl. [sit]).

Das Bundesamt für Sicherheit in der Informationstechnik (BSI), das in Cloud Computing ebenfalls eine Zukunftstechnologie sieht, definiert in einem Eckpunktepapier Mindestsicherheitsanforderungen für Anbieter von Cloud-Lösungen (vgl. [bsi]).

Zu erwähnen ist auch das von der Europäischen Kommission geförderte Projekt „Trustworthy Clouds – Tclouds", dessen Ziel es ist, eine vertrauenswürdige Cloud-Infrastruktur zu entwickeln, die dem Anwender eine nachvollziehbare und revisionssichere Verarbeitung personenbezogener oder anderer sensibler Daten ohne den Aufbau einer physisch getrennten privaten Cloud ermöglicht (vgl. [tcl]). Der Verein „EuroCloud Deutschland" sieht eine Lösung in der Entwicklung eines SaaS-Gütesiegels, dessen Anforderungskatalog in Abstimmung mit dem BSI entwickelt wurde (vgl. [Wei11]).

Rechtsfragen im Zusammenhang mit Cloud Computing

Gerade für mittelständische Unternehmen ist Cloud Computing höchst attraktiv, um ihre Wettbewerbsfähigkeit durch Einbinden externer Serviceangebote zu erhalten oder auszubauen. Jedoch verfügen diese Unternehmen häufig nicht über ausreichende Möglichkeiten, die rechtlichen Implikationen individuell zu prüfen. Die Frage der Ausgestaltung von Cloud Computing-Verträgen stellt Anbieter wie Anwender vor besondere Herausforderungen – erst recht, wenn der angebotene Cloud-Service grenzüberschreitend bereitgestellt oder genutzt werden soll.

1. Charakterisierung und Typologie

Wer sich dafür entscheidet, IT-Dienste aus der Cloud von Dritten außerhalb des eige-

nen Unternehmens (sogenannte „Public Clouds“) zu beziehen, sieht sich sofort einer Vielzahl von offenen Rechtsfragen gegenüber. Dabei ist Cloud Computing bei genauer Betrachtung häufig nur ein Sammelbegriff für bereits bekannte IT-Outsourcing-Dienstleistungen, wie z. B. Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Application-Service-Provider (ASP) oder Grid Computing.

Von einer *„Private Cloud“* spricht man, wenn sowohl die Services als auch die Infrastruktur einer Institution unterstehen und von ihr exklusiv genutzt werden. Dort sind die Risiken mit denen des traditionellen Eigenbetriebs vergleichbar. Jedoch müssen bei externen Private Clouds noch Risiken durch ungesicherte Handlungen des Betriebspersonals des Dienstleisters zugerechnet werden. Auch dieses Risiko besteht bereits bei reinem Outsourcing nach klassischer Vorstellung. Werden aus einer Private Cloud heraus Dienste einer *„Public Cloud“* genutzt, so spricht man von einer *„Hybrid Cloud“*.

Die folgenden Ausführungen beziehen sich ausschließlich auf die „Public Cloud“, da sich hier die rechtlichen Problemstellungen in besonderer Form manifestieren und rechtliche Vorgaben schwerer einzuhalten sind. In diesem Zusammenhang rücken regelmäßig folgende Themen in das Blickfeld der juristischen Betrachtung:

- Datenschutz in der Cloud
- Geheimhaltung
- Bestimmung der einzelnen Cloud-Leistungen und -Leistungsbeziehungen
- Auswahl der Art und Weise der zu erbringenden Cloud-Leistungen: Generalunternehmer (GU) vs. Multi-Vendor-Management-Modelle
- Bestimmung des anwendbaren Rechts
- Lizenzierungsmodelle in der Cloud
- Herausgabe der Daten nach Vertragsbeendigung
- Elektronische Archivierung.

2. Bedeutung von Datenschutz und Geheimhaltung bei der Vertragsgestaltung

Ein Wesensmerkmal vor allem der Public Cloud ist, dass externe Dritte in die Verarbeitung von (personenbezogenen) Daten „eingeschaltet“ werden. Die datenschutzrechtliche Zulässigkeit bestimmt sich nach den Regelungen zur Auftragsdatenverarbeitung, § 11 BDSG. Die Anforderungen wurden im Jahr 2009 um Kontrollen des Auftraggebers für Datenschutzmaßnahmen des Anbieters ergänzt.

Bevor man sich überhaupt mit der Frage beschäftigt, welchen Cloud-Anbieter man für welchen Dienst beauftragt, müssen sich sowohl Cloud-Anbieter als auch Kunden grundsätzlich darüber klar sein, ob und ggf. welche personenbezogenen Daten sie unter welchen Bedingungen wo speichern und verarbeiten dürfen. Die Konzeption des deutschen Datenschutzrechts sieht vor, dass zunächst alles verboten ist, was nicht durch gesetzliche Vorschrift oder Einwilligung des Betroffenen erlaubt ist (§ 4 Abs. 1 BDSG). Man spricht hier von einem Verbot mit Erlaubnisvorbehalt.

Der Schutz personenbezogener Daten umfasst ihren gesamten „Lebenszyklus“ – angefangen von der Erhebung über die Speicherung und Verarbeitung sowie eine mögliche Übermittlung bis zur unwiderruflichen Löschung. Die Zulässigkeit ist für jede einzelne Maßnahme mit den jeweiligen Daten zu klären. Die datenschutzkonforme Gestaltung der Cloud setzt also immer eine Analyse der in der Cloud zu verarbeitenden Daten und der dazu angebotenen Lösungen voraus.

Daten können darüber hinaus aus weiteren Gründen schutzbedürftig sein – auch wenn sie nicht personenbezogen sind: Informationen über Produktionsverfahren, Liefer- und Kundenbeziehungen, Konstruktionszeichnungen, Kalkulationsgrundlagen oder Preise enthalten häufig essenzielle Geschäfts- und Betriebsgeheimnisse und es muss sichergestellt sein, dass sie nicht von Unbefugten genutzt werden können.

Für bestimmte Daten gelten besondere Schutzvorschriften, etwa das Steuergeheimnis. Das Risiko der Verletzung steuerrechtlicher Vorgaben besteht zumindest aus deutscher Sicht, wenn Daten, die die Steuerbilanz des Unternehmens betreffen, über Ländergrenzen hinweg verlagert werden. Dies setzt eine Genehmigung der Finanzbehörden voraus.

3. Generalunternehmer- (GU) und Multi-Vendor-Management-Modelle in der Cloud – ein Vergleich

Die notwendigen Maßnahmen und Pflichten sind zwischen Kunde und Anbieter grundsätzlich schriftlich in einem „Cloud Computing-Vertrag“ zu vereinbaren und während der Vertragslaufzeit entsprechend umzusetzen. Im Folgenden geht es nun darum, die einzelnen Cloud-Leistungen und -Leistungsbeziehungen zu bestimmen sowie rechtlich relevante Kriterien für die Auswahl und den rechtlichen Rahmen der zu erbringenden Cloud-Leistungen zu definieren.

a. Bestimmung der einzelnen Leistungen

Wie bereits dargestellt, ist Cloud Computing i. d. R. mehr als Softwarevertrieb. Erscheinungsformen und Angebote sind vielfältig. Der Kunde hat also zunächst seinen Bedarf zu definieren. An dieser Stelle seien als Cloud-Dienste beispielhaft genannt:

- Datenbanken,
- CRM-Systeme mit Kunden- und Mitarbeiterdaten,
- Hardware-Infrastruktur,
- Backup-Lösungen,
- Storage-Lösung,
- File-Server/File-Space,
- Security-Appliances,
- Supportleistungen.

b. Das Generalunternehmer- (GU) Modell

Grundsätzlich hat der Kunde die Wahlmöglichkeit, die gewünschten Dienste und Leistungen bei einem einzigen oder bei verschiedenen Anbietern „einzukaufen“. Die weitere rechtliche Ausgestaltung und Einordnung ist immer von dieser Grundentscheidung abhängig. Häufig ist es bereits aufgrund der Spezialisierungen der Anbieterseite faktisch ausgeschlossen, verschiedenartige Leistungen von einem einzigen Anbieter zu beziehen (s. o.).

Probleme können dann entstehen, wenn der GU (einzelne) Vertragsleistungen nicht selbst erbringt, sondern sich Subunternehmern bedient. Dabei spricht in tatsächlicher Hinsicht vieles dafür: einen einzigen Ansprech- und Vertragspartner. Der Bezug nach dem Motto „alles aus einer Hand“ ermöglicht eine erleichterte Kontrolle (ein Vertrag, einheitliche Laufzeit und Kündigungsfrist) und Management (in organisatorischer und technischer Hinsicht).

Als Nachteil sind die mangelnde Flexibilität zu sehen, wenn andere Anbieter in technisch und/oder wirtschaftlicher Hinsicht ein besseres Angebot bereithalten sowie Leistungsstörungen, wie z. B. länger andauernde Betriebsunterbrechungen, ein Verkauf des Unternehmens des GU oder gar dessen Insolvenz. Für den Kunden notwendige Rechte müssen auch dann umgesetzt werden, wenn der Cloud-Anbieter seine Leistungen durch Subunternehmer erbringen lässt.

Über solche Regelungen in den Subunternehmerverträgen sollte sich der Kunde

unbedingt informieren. Die Bindung an einen einzigen Anbieter wird auch unter dem Schlagwort „Vendor Lockin“ erfasst. Im Hinblick auf die Rechtswahl gilt für das GU-Modell: Ohne eine gesonderte Vereinbarung findet grundsätzlich das Recht des Leistungsschuldners, also des Cloud-Anbieters, der abweichenden Rechtswahlvereinbarungen nicht immer zugänglich sein dürfte, Anwendung.

c. Das Multi-Vendor-Modell

Dem gegenüber steht das Multi-Vendor-Management-Modell, nach dem der Kunde die Leistungen von verschiedenen Anbietern bezieht, die unter Kosten-/Leistungsaspekten seine Bedürfnisse jeweils am besten abdecken. Hier sind vielfältige Leistungsmatrizen und gültige Rechtsordnungen denkbar, denn ohne Rechtswahl gilt, wie beim GU-Modell auch, für jeden Cloud- bzw. Sub-Cloud-Provider zunächst das jeweilige Heimatrecht. Dies kann dazu führen, dass die Anzahl der anzuwendenden Rechtsordnungen sogar noch die Anzahl der genutzten Cloud-Dienstleistungen übersteigt – eine Situation, die selbst für Rechtsabteilungen mutlinationaler Unternehmen eine Herausforderung darstellt.

d. Ort der Datenverarbeitung und Rechtswahl

Sowohl beim GU- als auch beim Multi-Vendor-Modell gilt: Findet die Auftragsdatenverarbeitung in der Cloud statt, muss dem Auftraggeber bekannt sein, in welchen Staaten die Datenverarbeitung und –speicherung ablaufen. Dies ist gerade bei Public Clouds nicht immer gewährleistet, da sich die für eine Vereinbarung zur Auftragsdatenverarbeitung notwendigen Inhalte nicht mit jedem Cloud-Anbieter in der Welt rechtlich einwandfrei umsetzen lassen.

(1) Nutzt die Cloud-Lösung der Wahl nur Standorte innerhalb der EU oder den anerkannt „sicheren“ Staaten, die ein von der EU als angemessen bewertetes Datenschutzniveau aufweisen, so gelten dafür dieselben Anforderungen wie innerhalb Deutschlands. Eine Übermittlung personenbezogener Daten außerhalb dieser Staaten unterliegt hingegen zusätzlichen Bestimmungen. „Drittstaaten“, dazu zählen auch die USA, sehen teilweise ein deutlich niedriges Datenschutzniveau vor. Manche verzichten ganz auf Datenschutz. Nicht wenige Cloud-Anbieter nutzen Standorte weltweit. Die zusätzlichen Voraussetzungen für eine Datenübermittlung in „Drittstaaten“ liegen bei diesen Anbietern selten vor und sind de facto nicht kontrollierbar.

(2) Eine Möglichkeit, personenbezogene Daten trotzdem in Drittstaaten zu übermitteln, sind Vertragsregelungen für ein angemessenes Schutzniveau. Die EU hat Standard-Vertragsklauseln für unterschiedliche Konstellationen beschlossen und verbindliche Unternehmensregelungen („Binding Corporate Rules“) können innerhalb eines Konzerns ein angemessenes Datenschutzniveau auch für Unternehmen in Drittstaaten bewirken. Daneben erteilt die zuständige deutsche Aufsichtsbehörde für bestimmte Datenverarbeitungen unter Umstände eine Genehmigung.

Dieser Weg erscheint im Zusammenhang mit dem ubiquitären Charakter von Cloud Compting aber kaum praktikabel. Cloud-Anbieter in den USA können sich den Regelungen des „Safe Harbor“ für ein angemessenes Datenschutzniveau unterwerfen. Allerdings hat ein deutscher Kunde zu prüfen, ob dies vertraglich durchsetzbar ist und ob ein US-Anbieter diese Regeln auch praktisch anwendet. Selbst die Zertifizierung von US-Unternehmen durch Safe Harbor ist unzulänglich (vgl. [ldi].)

4. Vertragsgestaltung

Unabhängig vom Ursprungsland des Anbieters und der Entscheidung für ein bestimmtes Vertragsmodell werden die Details des Cloud-Leistungsportfolios regelmäßig in Dienstevereinbarungen niedergelegt, sogenannte Service Level Agreements (SLA). Darin sollte auch festgelegt werden, was im Falle von Leistungsstörungen geschieht. Zu stark standardisierte SLA, wie sie gerade von Anbietern mir Marktmacht favorisiert werden, sind regelmäßig ein großes Risiko: Unternehmen müssen oft das gerade am besten passende SLA des Anbieters nutzen und haben wenig Spielraum für Anpassungen an das eigene Geschäftsmodell oder eine Rechtswahl.

Damit gehen Kontrollverluste und mögliche Haftungsrisiken gerade bei Datenschutzverstößen einher, auch wenn der Cloud-Anbieter vertraglich dazu verpflichtet wird, alle notwendigen technischen und organisatorischen Maßnahmen für den Datenschutz zu treffen, die sonst dem Kunden oblägen.

5. Vertragsdurchführung

Der Auftraggeber muss die Einhaltung der Vertragspflichten kontrollieren – schon vor einer Nutzung der Cloud-Lösung und später regelmäßig. Allerdings muss er das nicht vor Ort beim Cloud-Anbieter. Vielmehr kann die Prüfung anhand der Konzepte des Cloud-Anbieters und der dokumentierten Maßnahmen, Zertifizierungen etc. erfolgen. Das Prüfungsergebnis stellt ein gesetzliches Kriterium für die Auswahl des Cloud-Anbieters dar und ist vom Auftraggeber zu dokumentieren.

Eine weitere Möglichkeit sind sogenannte Service Control Boards (SCB), bei denen sich die Vertragsparteien regelmäßig absprechen. Auch bei einer Auftragsdatenverarbeitung bleibt der Kunde immer für die inhaltliche Verarbeitung personenbezogener Daten selbst verantwortlich. Er bleibt Ansprechpartner des Betroffenen für dessen Rechte – von der Auskunft über Datensperrung und -löschung bis zu Schadensersatzansprüchen.

Fazit

So kompliziert die genannten Vorgaben klingen mögen, der praktische Ansatz des Kunden für den Datenschutz in der Cloud beginnt mit einfachen Schritten. Die Kernfragen sind, welche personenbezogenen Daten in welcher Cloud-Variante verarbeitet werden sollen und in welchem Umfang der Kunde sie intern nutzen darf. Eine weitergehende Verarbeitung ist auch in einer Cloud immer unzulässig.

Es gelten beim Umzug in die Cloud die gleichen Vorteile und Risikoabwägung, wie sie auch im Zusammenhang mit einem unternehmenseigenen Rechenzentrum anzutreffen sind – jedoch in viel größerem Umfang.

Realistisch betrachtet, kann ein typisches mittelständisches Unternehmen die zahlreichen unterschiedlichen Verträge mit unterschiedlichen Cloud-Anbietern, wie beim Multi-Vendor-Modell unumgänglich, kaum mehr im Detail durchdringen. Diese Gruppe ist daher aus rechtlicher Sicht gut beraten, ihre Cloud-Aktivitäten von einem zentralen, möglichst innerhalb der EU beheimateten IT-Dienstleister (=GU) betreuen zu lassen, der wiederum unterschiedliche Cloud-Lösungen im Portfolio hat. Für sämtliche Hard- und Softwarelösungen gelten so die in dem Vertrag mit dem einen Anbieter vereinbarten Service- und Sicherheitsrichtlinien, ein einheitlicher Rechtsrahmen und die Rechtsdurchsetzung im Krisenfall stellt den Nutzer vor keine unüberwindbaren Hürden. ■

Literatur & Links

[sit] http://www.sit.fraunhofer.de/presse/20110128_CloudCockpit.jsp

[bsi] https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2010/Cloud_Computing_28092010.html

[tcl] http://www.tclouds-project.eu

[Wei11] Andreas Weiss, Gütesiegel für die Coud, kes Beilage März 2011, S. 16f; http://www.eurocloud.de

[ldi] Beschluss des Düsseldorfer Kreises „Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe-Harbor-Abkommen durch das Daten exportierende Unternehmen“, 2010,
http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.html?nn=409242