

Cloud Computing

Daniela Tschol

Cloud Computing ist zurzeit in aller Munde. Die Tendenz zum Outsourcing erreicht damit neue Dimensionen. Die technischen Möglichkeiten sind dabei die eine, die rechtlichen Anforderungen die andere Seite, welche es insbesondere auch im Hinblick auf die Risikominimierung unbedingt zu beachten gilt.

Die Cloud kann aus vielen verschiedenen IT-Dienstleistungen bestehen, sei es Datenspeicher, Rechenzentrum oder auch Spezialsoftware. Je nach Art der Cloud und Art der bezogenen Dienstleistungen stellen sich Fragen aus den verschiedensten Rechtsbereichen.

IT als bedeutender Stellenwert

Die IT nimmt im Unternehmen einen bedeutenden Stellenwert ein und dementsprechend weitreichende Folgen ergeben sich bei deren mangelhafter Funktion. Die Kenntnis über und das Bewusstsein der möglichen Rechtsrisiken und somit die möglichen Folgen ist deshalb unerlässlich. Die nachfolgenden Ausführungen zeigen nur einen Teil dieser vielfältigen rechtlichen Problemstellungen.

Unklarer Vertragspartner

Die Cloud umfasst verschiedenste Arten von IT-Dienstleistungen und damit auch eine Vielzahl von Lieferanten oder Dienstleistern.

Im vernebelten Umfeld der Cloud ist es für den outsourcenden Unternehmer oft schwer festzustellen, wer nun genau sein Vertragspartner ist. Dementsprechend lässt sich häufig auch nur schwer eruieren,

- wer bei Problemen der Ansprechpartner ist;
- wie der Anbieter organisiert ist;
- wer die Verantwortung trägt;
- usw.

Diese Informationen sind jedoch zentral, damit der outsourcende Unternehmer beispielsweise die Bonität und Seriosität seines Vertragspartners und somit auch seine eigenen Risiken einschätzen kann. Damit in Zusammenhang steht nämlich auch die wichtige Frage der Haftung.

Aus vertragsrechtlicher Sicht stellt sich dann auch insbesondere die Frage des anwendbaren Rechts und des Gerichtsstandes. Auch diesen Aspekt muss der outsour-

cende Unternehmer in seine Planung mit einbeziehen. Befindet sich der Vertragspartner nämlich ausserhalb von Europa, weichen die Rechtsordnungen doch erheblich vom EU-Standard ab und eine Vertragsdurchsetzung gestaltet sich dementsprechend schwierig.

Für den outsourcenden Unternehmer bedeutet dies, dass er seinen Dienstleistungsanbieter genauer unter die Lupe nehmen, Verträge überprüfen und entsprechend ausgestalten sollte. Dabei hat er insbesondere auch die Probleme aus den nachfolgend erläuterten Rechtsbereichen zu beachten.

Vernebelter Datenschutz

Je nach Art der bezogenen Dienstleistung werden personenbezogene Daten in die Cloud outsourct. Für die Bearbeitung von personenbezogenen Daten – also Da-

ten, welche sich auf eine bestimmte oder bestimmbare Person beziehen – ist das Datenschutzgesetz massgebend. Die Verantwortung für die Einhaltung dieser Vorschriften trägt der Inhaber der Datensammlung.

Die Verantwortung für die Datenbearbeitung kann durch das Outsourcing nicht einfach an den Outsourcing-Partner abgegeben werden. Das heisst, der outsourcende Unternehmer ist und bleibt für die Bearbeitung «seiner» personenbezogenen Daten in der Cloud verantwortlich. Er muss also dafür sorgen, dass auch sein Outsourcing-Partner die entsprechenden Datenbearbeitungsgrundsätze einhält. Dies muss er auch kontrollieren, was sich in der Praxis als schwieriges Unterfangen präsentieren dürfte.

Der Unternehmer muss also mit seinem Outsourcing-Partner in der Cloud entsprechende Vereinbarungen abschliessen und sicherstellen, dass der Vertragspartner die Daten nur gemäss seinen Weisungen bearbeitet und nur im Umfang, wie es der Dateninhaber selber auch dürfte. Darüber hinaus ist die grenzüberschreitende Bekanntgabe von Personendaten nur zulässig, wenn die Persönlichkeit der betroffenen Personen einen angemessenen Schutz geniesst. Dies kann durch entsprechende gesetzliche Regelungen im Ausland gegeben sein. Ist dies nicht der Fall, dürfen die Daten nur ins Ausland bekannt gegeben werden, wenn andere gesetzlich aufgeführte Gründe erfüllt sind (Art. 6 DSGVO; SR 235.1), beispielsweise wenn im mit dem Outsourcing-Partner abgeschlossenen Vertrag entsprechende Garantien enthalten sind oder die betroffene Person im Einzelfall eingewilligt hat.

Öffentliche Geheimnisse

Beim Outsourcing von Daten in die Cloud stellt sich nebst dem Datenschutz auch die Frage der Einhaltung von gesetzlichen oder vertraglichen Geheimhaltungspflichten. Die Verletzung solcher Pflichten

kann zu einer Haftung führen und gegebenenfalls zu entsprechenden strafrechtlichen Konsequenzen (vgl. Art. 162 StGB; SR 311.0).

Viele Unternehmer verfügen über Daten, welche Geschäftsgeheimnisse beinhalten. Neben vertraglich vereinbarten Geheimhaltungspflichten gibt es auch sehr weit verbreitete, sich direkt aus dem Gesetz ergebende Schweigepflichten, wie beispielsweise das Arztgeheimnis, das Anwaltsgeheimnis oder auch das Bankgeheimnis.

Der outsourcende Unternehmer muss sich also vorab die Frage stellen, ob und in welcher Art er Daten in die Cloud stellt. Zudem kann er durch entsprechende vertragliche Regelungen diese Geheimhaltungspflichten an den Outsourcing-Partner weitergeben. Hierbei muss er sich aber über seine Vertragspartner im Klaren sein, wobei wir wieder am Anfang der Ausführungen sind.

Verteilte Nutzungsrechte

Je nach Art der in die Cloud outzusourcenden Daten stellt sich weiter die Frage der Nutzung und Verwendung von Urheberrechten. Diese outgesourceten Daten stellen in vielen Fällen Werke dar, welche urheberrechtlich geschützt sind. Solche geschützten Werke sind beispielsweise Texte, Bilder, Konzepte oder auch Software. Dabei fragt sich einerseits, wie weit das Nutzungsrecht der outsourcenden Unternehmung an vom Outsourcing-Partner zur Verfügung gestellten Werken geht. Dieselbe Frage stellt sich andererseits auch in der umgekehrten Variante, nämlich ob und wie weit die Nutzungsrechte des Outsourcing-Partners an den Werken in der Cloud gehen.

Ist die Art und der Umfang des Nutzungsrechtes geklärt, stellt sich die Kontrolle als eine grosse Hürde dar. In den Tiefen der Cloud ist nämlich eine Nachverfolgung der geschützten Werke und die Kontrolle der Einhaltung von Nutzungsrechten äusserst schwierig.

Unklare Security-Standards

Im Zusammenhang mit den sämtlichen obig ausgeführten Problemfeldern stellt sich die zentrale Frage der notwendigen Sicherheitsmassnahmen. Mittels entsprechenden Vereinbarungen kann nämlich der Vertragspartner zur Einhaltung der relevanten gesetzlichen Vorschriften und die vom outsourcenden Unternehmer geforderten Sicherheitsstandards verpflichtet werden.

Der Vertragspartner sollte unbedingt über entsprechende Security-Standards verfügen, damit beispielsweise Zugriffe von unberechtigten Personen vermieden werden können. Entsprechend reduzieren sich auch die oben bereits ausgeführten Risiken für den outsourcenden Unternehmer.

Zusammenfassung

Der Unternehmer, welcher Dienstleistungen aus der Cloud beziehen will, sollte sich den rechtlichen Risiken bewusst sein. Es stellen sich dabei Fragen wie:

- Wer ist mein Ansprech- bzw. Vertragspartner?
- Wie ist mein Vertragspartner organisiert bzw. wer haftet?
- Welches Recht ist anwendbar und wo muss ich meine Rechte durchsetzen?
- Wie stelle ich die Einhaltung des Datenschutzes sicher?
- Wie gut sind meine Daten geschützt?
- Sind meine Geschäftsgeheimnisse entsprechend geschützt?
- Wie weit gehen die Nutzungsrechte an urheberrechtlich geschützten Werken?

Ist sich der outsourcende Unternehmer diesen Problembereichen bewusst, kann er seine Risiken einschätzen und entsprechende Vorkehrungen treffen. Viele dieser Problembereiche können mit entsprechenden Vorsichtsmassnahmen umgangen bzw. deren Eintrittsrisiko minimiert werden. ■