Cloud Computing – wie reduziert man die rechtlichen Risiken?

Aus rechtlicher Sicht handelt es sich beim Bezug von Dienstleistungen aus der Cloud um einen typischen Outsourcingvertrag mit allen bereits bekannten rechtlichen Risiken. Cloud Computing wirft daher grundsätzlich auch nicht vollkommen neue, noch nie da gewesene, rechtliche Fragen auf.

mag. iur. Maria Winkler

Die rechtliche Komplexität des Bezugs von Dienstleistungen aus der Cloud ergibt sich vielmehr aus der Kumulierung zahlreicher verschiedener Faktoren. Im Folgenden werden die wichtigsten Punkte in ihrer rechtlichen Bedeutung beleuchtet.

Vertragsinhalt und Vergütung

Dienstleistungen aus der Cloud werden meist im Rahmen von «Software as a Service (SaaS)» angeboten. Die Software wird dabei nicht mehr auf den eigenen Rechnern installiert und mittels Einmallizenz bezahlt, sondern über das Internet bezogen und bedarfsabhängig vergütet. Die vereinbarte Vergütung beinhaltet dabei neben den Nutzungsgebühren für die Software üblicherweise auch Dienstleistungen. Wartungs- und Updateverträge müssen nicht zusätzlich abgeschlossen werden. Den Standardverträgen der Anbieter ist aber häufig nicht klar zu entnehmen, welche Leistungen in welcher Qualität geschuldet und daher in der vereinbarten Vergütung beinhaltet sind. In der Praxis zeigt sich, dass es sehr teuer werden kann, wenn der Klärung des genauen Vertragsinhalts zu wenig Aufmerksamkeit geschenkt wird.

Compliance

Das outsourcende Unternehmen ist dafür verantwortlich, dass es im eigenen Geschäftsbereich die gesetzlichen Anforderungen erfüllt, auch wenn einzelne Aufgaben an externe Anbieter ausgelagert werden. Werden Software und Dienstleistungen wie beispielsweise Textverarbeitung, E-Mail oder Storage aus der Cloud bezogen, dann stellen sich insbesondere die Fragen, ob die gesetzlichen Anforderungen an den Umgang mit Geschäftsdokumenten, an den Datenschutz und die Datensicherheit oder an die Einhaltung von Geheimhaltungspflichten erfüllt werden.

Werden Geschäftsdokumente ausschliesslich elektronisch in der Cloud gespeichert und durch das Unternehmen nicht mehr zusätzlich in Papierform abgelegt und archiviert, dann ist zu überprüfen, ob dabei die Anforderungen von Art. 957 ff. OR und der Geschäftsbücherverordnung (GeBüV) erfüllt werden. Es sollte insbesondere nicht darauf vertraut werden, dass eine Dienstleistung, welche unter dem Namen «Archiv» angeboten wird, die gesetzlichen Anforderungen ohne Weiteres erfüllt. Kann beispielsweise nicht nachgewiesen werden, ob ein in der Cloud gespeichertes Dokument nachträglich verändert wurde, sind die Anforderungen an die Integrität nicht erfüllt. Es ist zu empfehlen, im Rahmen der Vertragsverhandlungen ausdrücklich die Einhaltung der genannten Vorschriften zu überprüfen, um unliebsamen Überraschungen vorzubeugen.

Viele Anbieter von Cloud Computing betreiben weltweit Rechenzentren und das outsourcende Unternehmen weiss oft nicht, in welchem Rechenzentrum die eigenen Daten lagern. Es muss somit in der Regel damit rechnen, dass die eigenen Daten und Dokumente im Ausland gespeichert werden. Aus Sicht des Schweizerischen Datenschutzgesetzes ist eine Bekanntgabe von Personendaten ins Ausland aber nur erlaubt, wenn im Empfängerstaat eine Gesetzgebung existiert, welche einen angemessenen Schutz gewährleistet. Ein solcher existiert beispielsweise in den Gesetzgebungen der EU-Staaten, nicht jedoch in denen der USA! Seit Februar 2009 ist das sogenannte US Swiss Safe Harbor Abkommen in Kraft, welches die Datenübermittlung an ein US-amerikanisches Unternehmen erleichtert, sofern dieses sich beim US-Handelsministerium verpflichtet, sich an die Grundsätze des Abkommens zu halten. In diesem Fall muss kein Vertrag ausgehandelt werden und die Meldepflicht an den EDÖB entfällt. Es ist somit dringend zu empfehlen abzuklären,

- in welchen Staaten der Anbieter Rechenzentren betreibt
- und falls ein Rechenzentrum in den USA betrieben wird, ob der Betreiber des Rechenzentrums (in der Regel eine Tochtergesellschaft des Anbieters) sich dem US Swiss Safe Harbor Abkommen unterworfen hat.

Zudem muss unter anderem vertraglich sichergestellt werden, dass der Vertragspartner die Daten nicht für eigene Zwecke verwendet oder an unberechtigte Dritte weitergibt. Im Rahmen der Prüfung des Sicherheitskonzepts des Anbieters sollte unter anderem ausdrücklich geklärt werden, wer für Back-ups zuständig ist und wer genau Zugriff auf die Daten erhält.

Verbieten Verträge mit Lieferanten, Kunden oder Geschäftspartnern die Weiterleitung von Geschäfts- und Betriebsgeheimnissen ins Ausland, dann sollten Dokumente, welche solche Informationen beinhalten entweder nicht in der Cloud gespeichert werden, oder es sollte die ausdrückliche Zustimmung der jeweiligen Vertragspartner zu diesem Vorgehen ein-

geholt werden. Eine Verletzung von Geschäfts- und Betriebsgeheimnissen ist gemäss Art. 162 StGB mit Strafe bedroht.

Abhängigkeit vom Anbieter

Das Outsourcing von Unternehmensaufgaben an externe Dienstleister ist heute nicht mehr aus der wirtschaftlichen Realität wegzudenken. Aus juristischer Sicht gilt es grundsätzlich zu beachten, dass der Outsourcinggeber gegenüber Behörden, Vertragspartnern oder Privatpersonen für das Handeln des Outsourcingnehmers verantwortlich bleibt – dessen Fehler werden also dem outsourcenden Unternehmen zugerechnet.

Daher ist dringend anzuraten, sich über den zukünftigen Vertragspartner vor Vertragsabschluss ausreichend zu informieren und insbesondere das Vertragswerk, welches die Basis der zukünftigen Zusammenarbeit bilden wird, insbesondere im Hinblick auf die folgenden Punkte genau zu überprüfen.

Zugriff auf eigene Daten

Die Sicherstellung des jederzeitigen Zugriffs auf geschäftliche Informationen sollte im Vertrag geregelt werden. Damit dieses Vertragsziel dauernd erreicht werden kann, sollten Anbieter bevorzugt werden, welche garantieren, dass die Rückführung der Daten und Dokumente, bzw. der Migration auf die Systeme eines anderen Anbieters bei Vertragsauflösung gewährleistet ist.

Informationspflichten und Kontrollrechte

Vertrauen ist gut – Kontrolle ist besser. Das outsourcende Unternehmen sollte das Recht haben, die Einhaltung des Vertrages vor Ort selbst oder durch externe Unternehmen zu kontrollieren. Ist der Anbieter z. B. ISO 27001 zertifiziert, dann kann der Nachweis der Beachtung der vereinbarten Sicherheitsmassnahmen auch durch die Bestätigung der erfolgreichen Zertifizierung bzw. der erfolgreichen Aufrecht- oder Wiederholaudits erfolgen.

Haftungsbestimmungen

Schliesst der Anbieter die Haftung für eigene Fehler weitgehend aus, dann ist Vorsicht geboten! Grundsätzlich gilt zu beachten, dass die Haftung für Absicht und grobe Fahrlässigkeit nicht zum vornherein ausgeschlossen werden kann. Auch eine Beschränkung der Haftung auf eine bestimmte Höchstsumme oder der Ausschluss der Haftung für bestimmte Schadensarten ist in diesem Bereich gemäss der herrschenden Lehre nicht zulässig. Zulässig ist hingegen der Ausschluss oder die Beschränkung der Haftung für leichte Fahrlässigkeit. Da der Nachweis, dass ein Schaden grob fahrlässig verursacht wurde, im Einzelfall sehr schwierig zu erbringen ist, ist dringend zu empfehlen, darauf zu achten, dass die Haftung für leichte Fahrlässigkeit nicht ausgeschlossen wird. In der Praxis üblich ist eine summenmässige Beschränkung der Haftung für leichte Fahrlässigkeit.

Fazit

Cloud Computing bringt keine wesentlichen neuen juristischen Probleme oder bisher vollkommen unbekannte rechtliche Risiken. Durch die Abhängigkeit vom Anbieter, den Bezug von Dienstleistungen aus dem Internet und der damit verbundenen Übermittlung von Daten ins Ausland sind aber rechtliche Risiken vorhanden, welche bei nicht genügender Beachtung die wirtschaftlichen Vorteile des Cloud Computings zunichtemachen können. Der Auswahl des Vertragspartners und der sorgfältigen Ausarbeitung des Vertrages insbesondere im Hinblick auf die genaue Definition der geschuldeten Leistungen, der Vereinbarung von Kontrollrechten und der Regelung der Rahmenbedingungen der Vertragsauflösung sind daher genügend Aufmerksamkeit zu schenken. Damit können die rechtlichen Risiken auf ein vertretbares Mass reduziert werden. ■