

Ursula Sury

Cloud Computing und Recht

AUSGANGSLAGE

Cloud Computing ist ein neues und im Moment viel diskutiertes Phänomen in der IT-Welt. Es geht dabei um ein neues Modell von IT-Outsourcing. Im Gegensatz zum klassischen Outsourcing oder Outsourcingformen wie „Software as a system“ (SaaS) oder „Application Service Providing“ (ASP) werden nicht für die aktuellen unternehmerischen Bedürfnisse mit einem bekannten konkreten IT-Partner Verträge abgeschlossen und darin Services ausgehandelt. Bei Cloud Computing stellt sich der Outsourcer aus einer Vielzahl bestehender Angeboten sein individuelles IT-Service Programm zusammen. Dabei kann jeglicher Service bezogen werden, sei dies Rechenleistung, Datenhaltung, Softwarefunktionalitäten etc. Die bestehenden Leistungen sind vorgefertigt, können schnell bezogen, ausgeweitet, eingeschränkt und miteinander verknüpft werden.

Es handelt sich also tatsächlich, wie der Name suggeriert, um bestehende Wassertropfen in einer Wolke, von denen man schnell profitieren kann oder auch nicht.

WER IST MEIN VERTRAGSPARTNER

Eine funktionierende IT-Unterstützung ist für jede Unternehmung existenziell. Auf diesem Hintergrund ist es ratsam, sich seine diesbezüglichen Lieferanten sorgfältig auszusuchen, sodass mindestens für die Zeitdauer des benötigten Service eine relativ grosse Abhängigkeit besteht. In der Computing Wolke tummeln sich global sehr viele verschiedene Anbieter, bei denen häufig schwierig eruiert ist, wer die unternehmerische Verantwortung trägt, wie seriös die Unternehmung arbeitet, wie es um deren Bonität steht etc.. Dies ist ein Risiko, mit welchem man bewusst umgehen muss. Ansonsten könnte man dann bald einmal feststellen, dass der vermeintlich seriöse Vertragspartner auf Wolke 7 ist.

DATENSCHUTZ UND GEHEIMHALTUNG

Wer personenbezogene Daten bearbeitet, ist dafür verantwortlich, dass dies gemäss den gesetzlichen Vorschriften geschieht. Diese Verantwortung trifft den Datenbearbeiter als Unternehmung aber auch individuell die dafür verantwortlichen natürlichen Personen. Ein Outsourcing der Datenbearbeitung ist deshalb schon vom Grundsatz her heikel, denn die entsprechende Verantwortung kann nicht einfach weitergegeben werden. Wer Datenbearbeitungen outsourct, bleibt dafür verantwortlich und hat deshalb dafür zu sorgen, dass sein Outsourcing-Partner sich an die entsprechenden Datenbearbeitungsgrundsätze hält. Das bedeutet, dass er ihn darüber instruieren, aber auch die Einhaltung der Instruktion regelmässig kontrollieren muss.

Werden personenbezogene Daten in einem Cloud outgesourct, so ist genau dieser Aspekt sehr schwierig umsetzbar. Im globalen Kontext kommt noch dazu, dass anderen Kulturen sich unser Datenschutz- und vor allem Persönlichkeitsschutzverständnis nicht oder weniger zugänglich ist und deshalb möglicherweise diesen Aspekten automatisch weniger Beachtung geschenkt wird.

Die gleichen Überlegungen gelten für verschiedene gesetzliche oder vertraglich Geheimhaltungspflichten, denen Unternehmungen unterliegen. Dazu zählen beispielsweise das Bankgeheimnis, die Geheimhaltungspflicht gemäss Versicherungsrecht, die Geheimhaltungspflicht von Ärzten, Anwälten etc. oder verschiedenste Geheimhaltungen, an welchen die Unternehmungen selber interessiert sind namentlich Geschäfts- oder Fabrikationsgeheimnisse.

Die Einhaltung dieser Pflichten kann mit einer Preisgabe von Informationen in am Cloud beteiligten Systemen weniger oder fast gar nicht mehr kontrolliert werden. Es ist also sehr gut möglich, dass im Rahmen eines Outsourcings die sehr schützenswerten personenbezogenen Daten im Nebel der Wolke verschwinden.

SECURITY

Jede Unternehmung ist im Rahmen der elektronischen Datenbearbeitung verpflichtet, die dafür notwendigen Sicherheitsmassnahmen einzuhalten. Eine gesetzliche Pflicht zur Einhaltung von Informatiksicherheit ergibt sich aus der Datenschutzgesetzgebung, leitet sich ab aus den Pflichten für eine sorgfältige Unternehmungsführung, aus der Gesetzgebung betreffend Intellectual Property etc..

Die Einhaltung dieser Sicherheitsstandards wird an viele verschiedene Teilnehmer im Cloud verteilt. Wie seriös und ob diese überhaupt eingehalten werden, kann, genau gleich wie die Frage des Datenschutzes, kaum oder nicht kontrolliert werden.

Um bei der Metapher der Wolke zu bleiben, müssen Cloud-Kunden Acht geben, dass sie nicht nass werden.

INTELLECTUAL PROPERTY

Im Rahmen eines Outsourcings werden dem Outsourcing Partner verschiedenste urheberrechtliche Werke übergeben, resp. diese gelangen in seinen Zugriffsbereich. Dazu zählen Software, Bilder, Konzepte, Texte etc. Zudem kann es sein, dass der Outsourcing-Partner seinerseits der outsourcenden Unternehmung Software zum Gebrauch überlässt. Sowohl in der einen wie auch in der anderen Variante ist es sehr wichtig, dass sich der Outsourcing-Partner an die Regeln des Urheberrechtes hält. Wenn er die ihm überlassenen Werke unbefugt Dritten übergibt, so kann das für das outsourcende Unternehmen mit grossen Schäden verbunden sein, welche im globalen und vielleicht etwas undurchsichtigen Kontext dann kaum einforderbar sind. Überlässt der Outsourcing-Partner dem outsourcenden Unternehmen Software zur Benutzung, an welcher er vielleicht selber nicht die notwendigen Rechte besitzt, kann dies hingegen das Risiko mit sich bringen, dass die Unternehmung wegen Urheberrechtsverletzung eingeklagt und schadenersatzpflichtig wird und sich ein möglicher Regress aus den obgenannten Gründen sehr schwierig gestaltet.

Bildlich gesprochen können in der Wolke unwahre Spiegelungen auftreten, welche beim Kunden zu irreparablen Blendungen und Schäden führen.

TAKE A RISK

Trotz den oben ausgeführten nicht unbedeutenden Rechtsrisiken, kann ein Bezug von Cloud Computing Dienstleistungen durchaus attraktiv sein. Dies wird insbesondere dann der Fall sein, wenn sehr schnell und auch relativ kostengünstig leicht skalierbare Dienstleistungen notwendig sind und man dabei darauf achtet, möglichst wenig personenbezogene Daten oder urheberrechtlich geschützte Werke damit zu bearbeiten. Es kann durchaus auch sinnvoll sein, gewisse Teilbereiche über Cloud Computing zu organisieren, bis ein traditionelleres und somit auch risikoärmeres Outsourcingsystem aufgebaut ist.

ZUSAMMENFASSUNG

Cloud Computing birgt verschiedene Rechtsrisiken, insbesondere im Bereich

- Datenschutz
- Urheberrecht
- Geheimhaltung
- Security

Aufgrund der spezifischen Konstellation sind diese Rechtsrisiken (anders als beim traditionellen Outsourcing wie SaaS/ASP etc. schlechter steuer- und kontrollierbar, weshalb bei einem längerfristigen Outsourcingverhältnis traditionellere Formen vorzuziehen sind.

5909 ohne Leerschlag

6733 mit Leerschlag

Februar 2009