

# Rechtliche Anforderungen bei Cloud Computing

Risk in der Cloud

Was steckt wirklich hinter diesem Begriff?

SGRP-Frühlingsevent vom 05. Mai 2010

# Agenda

- Cloud Computing - eine Qualifikation aus rechtlicher Sicht
- Wichtige Vertragspunkte
- Outsourcing der Datenbearbeitung
- Datenschutz und Cloud Computing – ein Widerspruch?

# Eine Qualifikation aus rechtlicher Sicht

- Es handelt sich (aus rechtlicher Sicht) um einen **Outsourcingvertrag**, welcher die folgenden besonderen Merkmale aufweist:
  - Die Leistungen des Outsourcinggebers werden meist in Form von „Software as a Service (SaaS)“ oder „Infrastructure as a Service (IaaS)“, etc. erbracht.
  - Die Daten werden an verschiedenen geographischen Orten bearbeitet.
  - Daten werden in der Regel (auch) im Ausland bearbeitet.
  - Die Menge der geforderten Leistung kann variieren (Scalierbarkeit).
  - Es besteht eine grosse Abhängigkeit vom Netz.

## Wichtige Vertragspunkte

- Vertragsgegenstand – alles klar?
- Compliance – ist es erlaubt?
- Vertragsauflösung und die Folgen
- Haftung

## Vertragsgegenstand – alles klar?

- Die genaue Definition der durch den Vertragspartner geschuldeten Leistung ist eine wesentliche Massnahme zur Reduktion der eigenen Risiken.
- Aus der **Vereinbarung** muss klar hervorgehen, **welche Leistungen in welcher Menge und Qualität** bezogen werden!
- Zudem muss klar geregelt werden, **wer wofür verantwortlich** ist (Mitwirkungspflichten des Unternehmens, Systemgrenzen).

# Allgemeine Geschäftsbedingungen

- Es sind insbesondere die folgenden, in der Praxis häufig auftretenden Punkte zu beachten:
  - Die verwendeten AGB verweisen häufig wiederum auf AGB, die im Internet abrufbar sind und jederzeit geändert werden können.
  - Die Services sind allgemein beschrieben und stimmen nicht zu 100% mit dem überein, was das Unternehmen tatsächlich bezieht.
  - Es werden in den AGB sämtliche angebotenen Services beschrieben und nicht nur die, welche das Unternehmen bezieht.
- Es sollte schriftlich festgelegt werden, **welche AGB** in welcher Version Vertragsbestandteile bilden!

## Nutzungsrechte, Dienstleistungen, etc.

- Im Rahmen von SaaS, IaaS, etc. werden Nutzungsrechte an Software, Dienstleistungen wie Wartung und Support aber auch die Nutzung von Infrastruktur vereinbart.
- Es sollte klar geregelt werden, **welche Nutzungsrechte an welcher Software** das Unternehmen genau erwirbt.
- Die Qualität der Dienstleistungen sollte in **Service Level Agreements** nachvollziehbar und überprüfbar vereinbart werden.
- Es sollten **Konventionalstrafen** vereinbart werden, wenn die Dienstleistungen nicht die vereinbarte Qualität aufweisen (Malus-Regelung).

## Compliance – ist es erlaubt?

- Vor Vertragsabschluss ist zu überprüfen, ob die angebotenen Services in den Bereichen, in denen man sie nutzen möchte, alle gesetzlichen Vorgaben erfüllen.
- Dabei sollten beispielsweise die folgenden Fragen gestellt werden:
  - Bestehen Geheimhaltungspflichten, welche ein Outsourcing der Daten (ins Ausland) verbieten?
  - Erlauben die steuerrechtlichen Vorgaben (z.B. bei der Auslagerung aller Geschäftsdokumente in die Cloud) das Vorgehen?
  - Bei Archivierung in der Cloud – werden die Dokumente lange genug und integritätssicher archiviert?

## Vertragsauflösung und Folgen

- Um eine möglichst grosse **Unabhängigkeit** vom Anbieter zu bewahren, sollte vertraglich sichergestellt werden, dass ein Wechsel zu einem anderen Anbieter jederzeit möglich ist.
- Die **Kündigungsfristen** müssen den eigenen unternehmerischen Bedürfnissen entsprechen.
- Der Anbieter muss verpflichtet werden, bei Vertragsauflösung die erforderliche **Unterstützung** für die Migration der Daten und Dokumente auf die Systeme des neuen Vertragspartners zu leisten – die Kosten dieser Unterstützung sollten vertraglich vereinbart werden.

# Haftung

- Hände weg von Anbietern, die die Haftung für eigenes Verschulden ausschliessen oder massiv einschränken!
- Der Anbieter haftet immer **unbegrenzt** für Absicht und grobe Fahrlässigkeit sowie für Personenschäden.
- Es sollten Anbieter bevorzugt werden, welche die **Haftung für leicht fahrlässig zugefügte Schäden** nicht ausschliessen – üblich ist hier eine summenmässige Begrenzung in der Höhe der Projektkosten, der Jahresgebühren, etc.
- Die Haftungsbegrenzung sollte mit dem potenziellen Risiko des Unternehmens übereinstimmen!

# Outsourcing

- Im Rahmen von Cloud Computing wird ein Teil der eigenen Geschäftstätigkeit auf ein externes Unternehmen ausgelagert.
- Zahlreiche gesetzliche Vorschriften halten fest, dass das Outsourcing zwar erlaubt ist, der Auftraggeber aber für das Funktionieren und die Gesetzeskonformität der ausgelagerten Tätigkeit verantwortlich bleibt (z.B. Art. 10a DSGVO).

# Informationspflichten und Kontrollrechte

- Der Vertragspartner sollte vertraglich verpflichtet werden, das Unternehmen **von sich aus** über Umstände zu **informieren**, welche die Vertragserfüllung beeinflussen könnten, beispielsweise
  - Sicherheits- und Datenschutzvorfälle
  - Wechsel in der Unternehmensleitung
  - Überschuldung
- **Kontrollrechte** können auch durch die Pflicht zur Ablieferung von Kopien von Auditberichten (z.B. im Rahmen von ISO 27002-Zertifizierungen, Datenschutzaudits, etc.) ausgeübt werden.

## Cloud Computing und Datenschutz- ein Widerspruch?

- Durch die Speicherung der Daten in der „Cloud“ ist die Kontrolle der Datenbearbeitung schwieriger als bei einem „normalen“ Outsourcingvertrag und die Risiken für die betroffenen Personen sind grösser!
- Der Anbieter muss ausdrücklich verpflichtet werden, die Daten nur für den **vereinbarten Zweck** zu bearbeiten, die Verwendung für eigene Zwecke und / oder die Weitergabe an Dritte sollte ausdrücklich untersagt werden!
- Es sollte zudem vertraglich geregelt werden, **in welchen Ländern** die Datenbearbeitung erfolgt.

## **Grenzüberschreitende Bekanntgabe (Art. 6 DSGVO)**

- Die Bekanntgabe ins Ausland ist verboten, wenn dadurch die Persönlichkeit der betroffenen Person schwerwiegend gefährdet wird – dies ist dann der Fall, wenn eine Gesetzgebung mit angemessenem Schutz fehlt
- EDÖB führt eine Liste der Staaten, in welchen ein angemessener Schutz besteht
- Länder mit ungenügender Gesetzgebung
  - Albanien, Andorra, Armenien, Aserbaidschan, Bosnien-Herzegowina, Vatikan, Mazedonien, Georgien, Kroatien, Moldawien, Monaco, Russland, San Marino, Serbien, Montenegro, Ukraine, Weissrussland

# Grenzüberschreitende Bekanntgabe (2)

Bei fehlender Gesetzgebung Bekanntgabe ins Ausland nur, wenn

- hinreichende Garantien, insbesondere durch Vertrag vorliegen
- Einwilligung der betroffenen Person im Einzelfall
- Zusammenhang mit Vertragsabwicklung
- überwiegendes öffentliches Interesse oder Durchsetzung von rechtlichen Ansprüchen vor Gericht
- Bekanntgabe schützt Leben und körperliche Integrität
- allgemeines Zugänglichmachen und kein Verbot
- innerhalb derselben juristischen Person oder Gesellschaft mit angemessenen Datenschutzregeln

## US Swiss Safe Harbor Agreement

- Betreibt der Anbieter auch Rechenzentren in den USA, dann werden Daten in einen Staat übermittelt, in welchem kein angemessenes Schutzniveau herrscht.
- Es muss daher entweder eine der Garantien gemäss Art. 6 Abs. 2 DSGVO vorliegen (z.B. Vertrag oder Einwilligung) oder es muss sichergestellt werden, dass der Empfänger der Daten sich zur Einhaltung der im U.S.-Swiss Safe Harbor Framework verpflichtet und zertifiziert hat.

# Sicherheit

- Bereits vor Vertragsabschluss sollte ein Sicherheitskonzept nachgewiesen werden und die Einhaltung sollte kontrollierbar sein!
- Sicherheitsvorfälle müssen rapportiert werden.
- Die Verletzung der Vereinbarung von Sicherheitsvorschriften sollte an Konventionalstrafen gebunden werden!

## Zusammenfassung

- Cloud Computing stellt aus rechtlicher Sicht nicht vollkommen neue Anforderungen.
- Die Kombination verschiedener Elemente erzeugt besondere Risiken, welche durch gut durchdachte und sorgfältig verhandelte Verträge soweit als möglich reduziert werden sollten.
- Die sorgfältige Auswahl des Anbieters und die Vereinbarung von Kontrollrechten und Informationspflichten sowie die Regelung der Folgen der Vertragsauflösung sind dabei zentrale Elemente der Risikoreduktion!

IT & LAW | CONSULTING GMBH

**Vielen Dank für die Aufmerksamkeit!**

mag. iur. Maria Winkler  
IT & Law Consulting GmbH  
Grafenastrasse 5  
6300 Zug  
041 711 74 08  
maria.winkler@itandlaw.ch  
www.itandlaw.ch