Seminararbeit aus

Seminar aus Informatik

Cloud Computing
Rechtliche Aspekte

Eingereicht von: Susanne Altendorfer, Bernhard Wagner

Eingereicht bei: Prof. Dr. Wolfgang Pree

Datum: Jänner 2009

Inhaltsverzeichnis

Abstract

Das 21. Jahrhundert bezeichnet eine Ära, in der die Geschäftsstrukturen die Veränderungen, die das Informationszeitalter mit sich bringt, in vollem Masse sichtbar machen. Obwohl Unternehmungen sich immer an den Stand der Technologie anpassen müssten, um im Wettbewerb bestehen zu können, waren sie bis jetzt meist nicht im Stande ihre Strukturen grundlegend zu ändern, bis heute.

Durch neue Modelle ist es nun möglich, die Geschäftsmodelle an die jeweiligen Bedürfnisse genau anzupassen. Für heutige Unternehmen ist es mehr denn je wichtig, dynamisch auf Marktveränderungen reagieren und Kosten so weit wie möglich reduzieren zu können. Dabei ist es wesentlich die IT-Ressourcen im eigenen Unternehmen so schlank wie möglich zu halten. Ein Weg in diese Richtung ist neben Utility Computing, die Möglichkeit Applikationen als Services „zuzukaufen“.

Diese Seminararbeit beschäftigt sich mit den rechtlichen Aspekten bei Cloud Computing, die Software wird dabei als Dienstleistung zur Verfügung gestellt und zielt darauf ab aufzuzeigen, welche Bedeutung das österreichische Recht in diesem Zusammenhang hat und welche Gesetze zur Anwendung kommen.

Der Beginn der Arbeit gibt dabei einen Überblick was Cloud Computing ist und welche technischen Konzepte dahinterliegen. Eine genauere Betrachtung kommt dann den rechtlichen Aspekten zu. Hier wird auf die Gesetzesebene eingegangen und auch Unterschiede zwischen Ländern werden aufgezeigt.

Um die Arbeit abzurunden gibt es am Schlussteil noch einige Beispiele zu Cloud Computing und den Nutzungsbestimmungen im Detail.

Executive Summary

The beginning of the twenty-first century marks the era in which the structure of business begins to reflect fully the changes brought about by the information age. Although businesses have certainly had to adapt the tools of the information age to stay competitive, they have not had to, nor been able to, fundamentally change their competitive and operational structures, until now.

With the help of newly emerging enablers changes in the nature of Business to adapt to new requirements are possible. For a company it is more important than ever to respond dynamically to market changes and to reduce costs through managing expenditures. Thus it is crucial to keep IT resources as lean as possible. One way in this direction is the possibility to “buy” applications as services.

This seminar paper deals with the legal aspects of Cloud Computing and aims to find out about the importance of the Austrian law and with specific laws are applicable. Beginning with basic facts about Cloud Computing and its realization in the first chapters we take then a closer look on the legal aspects.

To round off the paper there are some examples with their terms of use given, to see whether practical life proofs the theory.

1 Cloud Computing und seine Bedeutung

Um das Thema Cloud Computing überhaupt von der technischen Seite her betrachten zu können, ist es zuvor grundlegend zu definieren was Cloud Computing bedeutet und welche technischen Aspekte relevant sind.

1.1 Was ist Cloud Computing

Unter Cloud Computing versteht man Techniken und Geschäftsmodelle, die es einem Anbieter ermöglichen seinen Kunden IT-Leistungen in Form von Services, die dann nach Gebrauch verrechnet werden, anzubieten.

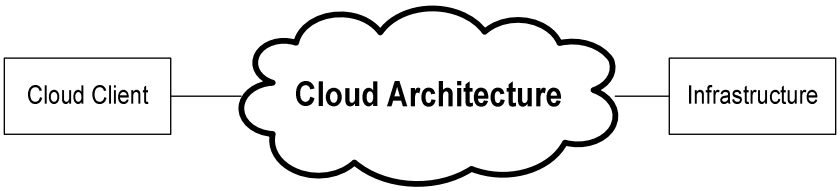


***Abb. 1** Schematische Cloud Darstellung*

Die „Cloud“, zu Deutsch „Wolke“ ist ein Begriff der Computer-Technologien und ist ein Synonym für das Internet.
Die Softwareanwender betreiben die Software und die dazugehörende Hardware nicht mehr selbst, sondern beziehen die Software als Service von einem Provider, der beides für sie betreibt. Da der Provider den Service für mehrere Anwender anbietet, kann er einen kompetitiven Preis anbieten.

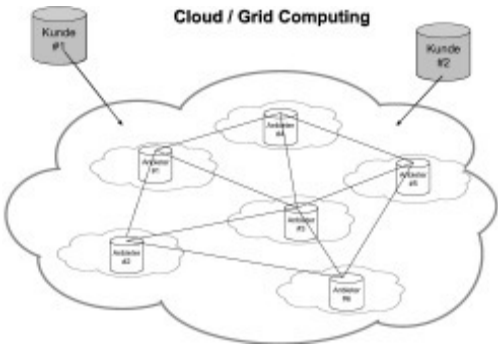


Abb. 2 *Cloud Netzwerk [Beck 2008]*

Die Anwendungen und die Daten befinden sich bei diesem Modell nicht mehr lokal beim Anwender, sondern werden vom Provider über eine Anzahl von Servern oder Serverfarmen verteilt abgelegt. Der Zugriff erfolgt dabei meist über einen Webbrowser.

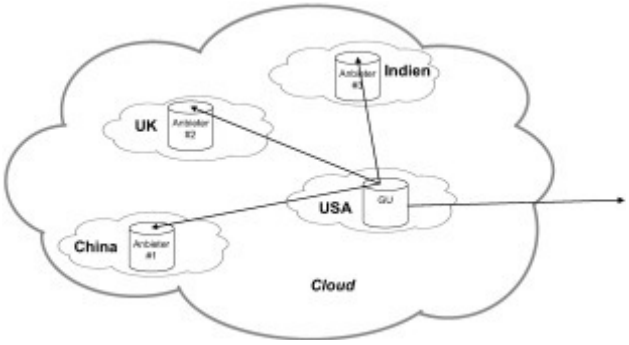


Abb. 3 *Verteilte Serverfarmen [Beck 2008]*

1.2 Entstehung von Cloud Computing

Vieles was heute unter Cloud Computing verstanden werden kann, ist eigentlich nichts Neues mehr. Ähnliche Ansätze gab es bereits mit dem klassischen Outsourcing von Infrastruktur, Modellen wie ASP – Application Service Providing sowie mit dem Grid oder Utility Computing.

Cloud Computing ist nach Meinung vieler Experten „*eine Fortführung von Konzepten wie „Software as a Service", nur das es weiter aufgestellt sei*". [vgl. PFM 2008]

2 Auswirkungen und Anforderungen

2.1 Vor- und Nachteile

Damit sich ein neues Geschäftsmodell durchsetzen kann, muss es sich von gängigen Modellen durch neue Eigenschaften abheben. Cloud Computing bietet in vielen Bereichen Vorteile gegenüber herkömmlichen Modellen.

2.1.1 Vorteile

Die Virtualisierung ermöglicht dramatische Kostenreduktionen, da die Software und Hardware, mit den anfallenden Lizenzen nicht mehr gekauft werden muss und auch höhe Wartungskosten wegfallen.
Ein weiterer Vorteil der Virtualisierung ist auch die Unabhängigkeit vom Arbeitsplatz. Eine Internetverbindung reicht aus um an seinen Daten zu arbeiten.
Die einfache Skalierbarkeit ist für das Unternehmen, das Cloud Computing verwendet ein weiterer entscheidender Faktor. Für Unternehmen entstehen keine hohen Kosten wenn die Serverkapazität erreicht wird. Kapazitätsauslastung, Performance und Skalierbarkeit liegen bei diesem Modell im Verantwortungsbereich des Anbieters.

2.1.2 Nachteile

Jedoch wo es Vorteile gibt, gibt es auch Schattenseiten, so ist es wesentlich sich im Vorfeld mit den Sicherheitsmaßnahmen der Anbieter genauer zu beschäftigen. Was passiert beispielsweise bei Datenverlust? Wie wird die Datensicherheit gewährleistet und welche Richtlinien kommen zur Anwendung?
Die Auswahl des Cloud Computing Providers spielt dabei eine wesentliche Rolle, und man sollte sich bei der Prüfung Zeit nehmen.

2.2 Anforderungen an Cloud Computing

Wenn man von Cloud Computing spricht, gibt es natürlich mehrere Seiten, aus deren Blickwinkel die Thematik betrachtet werden sollte.

Zum einen gibt es die Benutzer, die mit den zur Verfügung gestellten Anwendungen arbeiten müssen und zum anderen gibt es die Entwickler, die sicherzustellen haben, dass die Systeme in einer Art und Weise zur Verfügung gestellt werden, wie sie der Kunde benötigt und wie es technisch sinnvoll ist.

Anforderungen der Benutzer

- Klare Wertschöpfung
- Einfache Kontrolle und Feedback
- Dezentrale Kontrolle
- Spezielle Notfallszenarien
- Datenspeicherung, -sicherheit
- Einfaches Handling - mühelose Anpassung
- Accessability – besserer Zugriff
- Mandantenfähige Architektur

Anforderungen der Entwickler

- Tagging von Benutzerinformationen
- Zugangskontrollmechanismen
- Loggingmechanismen
- Sicherheitsmechanismen
- Datenschutz

[vgl. HON]

3 Technische Aspekte

Um ein Verständnis für die in weiterer Folge diskutierten rechtlichen Aspekte zu bekommen, wird an dieser Stelle noch ein technischer Überblick gegeben.

3.1 Realisierungsform

Generell kann man bei Cloud Computing von Client-Server-Service Plattformen sprechen. Dabei kommunizieren die einzelnen Komponenten über definierte Programmschnittstellen miteinander, oft über sogenannte Web-Services.

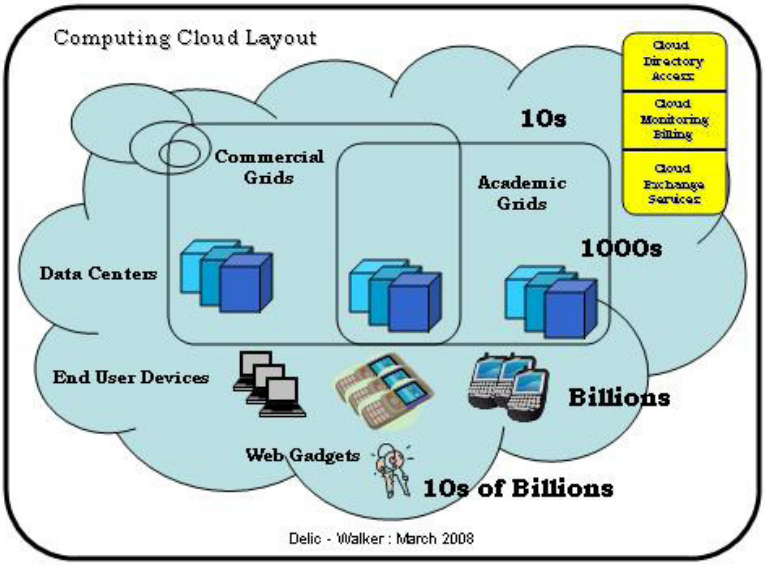


Abb. 4 *The Cloud [Delic,ACM]*

Client

Der Client kann dabei ein gewöhnlicher Thin-Client sein, der außer dem Zugang zum Internet keine wesentlichen Programme braucht. Auf ihm läuft ein Webbrowser, über den der Benutzer Zugriff auf die Applikationen bzw. Services hat, die typischerweise auf dem Server gespeichert sind.

Server

Der Server an sich ist dem Benutzer verborgen. Was sich im Hintergrund abspielt ist für den Benutzer vollkommen uninteressant, solange seine Applikationen einwandfrei funktionieren. Anstelle eines einzigen Servers ist es zumeist so, dass es sich hier um ganze Serverfarmen handelt, die dezentral, über verschiedene Länder hinweg aufgestellt sein können. Die einzelnen Datenknoten sind dann untereinander verbunden und bilden das Datencenter.

Die Applikationen oder auch Services laufen auf den Servern des Providers. Der Betrieb, die Betreuung und Wartung fallen in die Pflichten des Providers. Die Speicherung der Daten erfolgt ebenfalls auf den Rechnern des Providers genauso wie die Datensicherung.

Abb. 5 *IBM Blue Cloud*[1]

3.2 Rollen innerhalb der Cloud

Bei Cloud Computing gibt es generell einige Rollenbilder, die es auch im Hinblick auf die rechtlichen Aspekte zu kennen gilt.

Provider

Dem Provider, auch oft als Service Provider bezeichnet, gehört die Hard- und Software, die dem Benutzer dann zur Verfügung gestellt wird. Den Provider trifft somit die meiste Verantwortung in der Bereitstellung der Applikationen und der korrekten Speicherung und Aufbewahrung der Daten. Auch das Sicherheitsmanagement gehört in sein Ressort.

[1] IBM Blue Cloud: IBM today introduced Blue Cloud, a series of cloud computing offerings that will link together computers to deliver Web 2.0 capabilities and allow corporate data centers to operate more like the Internet. Above is a photo of Europe's most powerful computer at Jülich. (Copyright: Forschungszentrum Jülich) [IBM 2007]

Benutzer (auch Endnutzer genannt)

Dieser mietet sich beim Provider ein und nutzt dann die Applikationen für seine Tätigkeiten gegen ein entsprechendes Entgelt. Ihm obliegt es, sich um der Integrität des Providers bei dessen Auswahl zu kümmern.

Verkäufer

Diese haben eher eine nebensächliche Bedeutung, als dass sie dem Provider die Hard- und Software verkaufen und dann nicht mehr involviert sind.

4 Rechtliche Aspekte

Der Datenschutz und die Privatsphäre sind wesentliche Aspekte für Unternehmen und deswegen auch immer ausschlaggebend, ob neue Technologien und Geschäftsmodelle nachhaltig erfolgreich sein können.

Um ein Verständnis dafür zu bekommen, was von rechtlicher Seite aus bei Cloud Computing machbar ist, soll dieser Abschnitt nun zeigen, welcher Sachverhalt der Thematik zugrunde liegt.

4.1 Gesetzliche Grundlagen

Grundsätzlich handelt es sich bei Cloud Computing, wenn man es von der reinen Nutzungsseite betrachtet um einen Mietvertrag über ein Service. [vgl. STA]
Jedoch geht Cloud Computing einen Schritt weiter, denn da die Daten nicht beim Benutzer direkt nach seinen Sicherheitsvorkehrungen gespeichert werden, wird die Sache problematisch, denn gerade die entfernt gespeicherten Daten verlangen nach einem besonderen Schutz.
Da es hier noch keine konkreten Vorschläge und Präzedenzfälle gibt, soll dieses Kapitel nun erarbeiten, welche Rechtsgrundlagen hier zur Anwendung kommen.

4.1.1 Das österreichisches Datenschutzgesetz - DSG 2000

Das österreichische Datenschutzgesetz in der aktuellen Fassung DSG 2000 als Bundesgesetz über den Schutz personenbezogener Daten findet als erste Anwendung, wenn es um die Verarbeitung von Daten und deren Speicherung geht.

4.1.1.1 Bestimmungen des DSG

Um in einem Beweisverfahren in Hinblick auf Cloud Computing die wesentlichen Bereiche trennen zu können, wie es auch schon durch die Rollen bei der Technischen Umsetzung erfolgt ist, siehe Kap. 3.2 *Rollen*

innerhalb der Cloud, gilt es auch von der rechtlichen Seite eine Begriffsklärung vorzunehmen:
Im § 4 DSG werden dazu folgende grundsätzliche Begriffe definiert: Die Person dessen Daten verwendet werden wird Betroffener genannt. Derjenige, der die personenbezogenen Daten in eigener Verantwortung verarbeitet wird als Auftraggeber bezeichnet. Ein Gehilfe des Auftraggebers ist der Dienstleister, welcher die Daten zur Herstellung eines ihm aufgetragenen Werkes verwendet. Auch bei der Übergabe der Daten zur Verarbeitung an einen Dienstleister bleibt der Auftraggeber der Verantwortliche (z.B. Rechtsanwalt).
Unter das Datenschutzgesetz fallen nur die personenbezogenen Daten über Betroffene, deren Identität bestimmt oder bestimmbar ist.
Weiters wird zwischen nichtsensiblen (§ 8 DSG) und sensiblen Daten (§ 9 DSG) unterschieden: Sensible Daten unterscheiden sich von nichtsensiblen Daten, dass sie besonders schutzwürdig sind (z.B. rassische und ethnische Herkunft, politische Meinung…).

Das Datenschutzgesetz schützt personenbezogene Daten, soweit ein schutzwürdiges Interesse daran besteht. Es besteht kein schutzwürdiges Interesse daran, wenn die Daten öffentlich verfügbar sind oder es keinen Rückschluss auf die Person zulässt.
Die schutzwürdigen Interessen werden bei nichtsensiblen Daten nicht verletzt, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht oder
2. der Betroffene der Verwendung seiner Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
3. lebenswichtige Interessen des Betroffenen die Verwendung erfordern oder
4. überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern. [vgl. § 8 Z1 DSG]

Die Daten dürfen nur verarbeitet werden, soweit der Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen. Jede Verwendung der Daten hat mit den gelindesten zur Verfügung stehenden Mitteln zu erfolgen.

Der Auftraggeber hat folgende Pflichten:

- Verantwortung für die Zulässigkeit der Verwendung von Daten
- Vorkehrungen zur Datensicherheit
- Registrierungspflicht
- Informationspflicht, Auskunftspflicht, Pflicht zur Richtigstellung und Löschung
- Pflicht zur Offenlegung der Identität des Auftraggebers

Zur Wahrung des Datengeheimnisses sind Auftraggeber, Dienstleister und ihre Mitarbeiter verpflichtet.

4.1.1.2 Geltungsbereich

Generell sind die Bestimmungen dieses Bundesgesetzes auf die Verwendung der Daten im Inland anzuwenden, siehe dazu § 3 Z 1 und 2 DSG.

Eine Datenübermittlung ins Ausland bedarf einer Genehmigung durch die Datenschutzkomission (Bedingungen, Auflagen) wenn diese nicht genehmigungsfrei ist. Genehmigungsfrei ist die Datenübermittlung nur in folgenden Fällen:

1. die Übermittlung und Überlassung von Daten an Empfänger von Mitgliedstaaten der EU (dies ist wie ein Transfer im Inland zu betrachten).

2. Empfänger in Drittstaaten mit angemessenem Datenschutz (Welche dies sind wird durch Verordnung des Bundeskanzlers festgelegt – z.B. Schweiz).
3. „Safe Harbor“ Entscheidung sind Grundsätze des Datenschutzes denen sich US Unternehmen unterwerfen können, um einen angemessenem Datenschutz zu erhalten.
4. Standardvertragsklauseln ermöglichen eine Datenübermittlung an Auftraggeber in Drittländern ohne angemessenen Schutz, wenn entsprechende Vertragsklauseln zwischen Datenexporteur und Datenimporteur vereinbart werden. Statt der Genehmigungspflicht tritt die Anzeige bei der Datenschutzkommission.
5. Zahlreichte weitere Fälle z.B. wenn die Daten im Inland zulässigerweise veröffentlicht wurden.
6. Eine Zustimmung des Betroffenen vorliegt.
7. Die Übermittlung ins Ausland in einer Rechtsvorschrift vorgesehen ist oder die Daten aus Datenanwendungen für private Zwecke oder publizistische Tätigkeit übermittelt werden.
8. Übermittlung an Drittstaaten sind auch dann zulässig, wenn diese in der Standard- und Musterverordnung ausdrücklich vorgesehen ist.

4.1.1.3 Datensicherungmaßnahmen nach DSG

Die Maßnahmen zur Datensicherung nach dem DSG sind kaum noch zeitgemäß. Die Regelungen sind äußerst unbestimmt und stark auslegungsbedürftig, da sie vom „Stand der Technik“ und den „bei der Durchführung erwachsenden Kosten“ abhängen. Grundsätzlich kann jedoch gesagt werden, dass eine Aufgabenverteilung und Zugriffsbeschränkung meist vorzusehen sein wird.

DSG Datensicherheitsmaßnahmen

§ 14. *(1). Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, sind Maßnahmen zur*

Gewährleistung der Datensicherheit zu treffen. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, daß die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, daß ihre Verwendung ordnungsgemäß erfolgt und daß die Daten Unbefugten nicht zugänglich sind.

4.1.1.4 Datenschutzverletzungen

Bei Nichteinhaltung des Datenschutzes kennt das DSG folgende Strafbestimmungen: Man unterscheidet hier zwischen der „Datenverwendung in Gewinn – und Schädigungsabsicht“ und einer „Verwaltungsstrafbestimmung“.
Die „Datenverwendung in Gewinn – und Schädigungsabsicht“ wird mit Freiheitsstrafe bis zu einem Jahr geahndet. Wichtig ist allerdings hierbei, dass der Täter nur mit Ermächtigung des Verletzten verfolgt werden kann.

DSG Datenverwendung in Gewinn – und Schädigungsabsicht
§ 51. *(1) Wer in der Absicht, sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.*

Eine Verwaltungsübertretung liegt dann vor, wenn die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist. Die Höhe der Verwaltungsstrafe liegt je

nach Art der Datenverwendung entweder bei 18.890 Euro oder bei 9.445 Euro.

4.1.2 Datenschutz in den USA

Da sich das Thema Cloud Computing nicht ausschließlich auf den österreichischen Markt beschränkt, sei an der Stelle ein Exkurs zum Datenschutz in den USA gemacht, da dieser grundlegend anders ist als innerhalb der Europäischen Union.

Die USA verfügt im Gegensatz zu den EU – Mitgliedsstaaten sowie einer Reihe weiterer Länder wie der Schweiz, Ungarn, Norwegen und Kanada über kein nationales Datenschutzgesetz. Aus diesem Grund hat die EU mit den USA im Jahr 2000 ein Abkommen beschlossen, das unter dem Namen „Safe Harbour" bekannt ist: US – Unternehmen können sich selbst als „Safe Harbour" auszeichnen; Kontrolliert werden Verstöße nur wenn ein Missbrauch von Daten nachgewiesen werden kann. Dieses Abkommen soll eine Übereinstimmung mit der EU-Datenschutzrichtlinie[2] gewährleisten.

Nach dem Anschlag des 11.9.2001 wurde der Datenschutz zum Schutz der öffentlichen Sicherheit und der Abwehr von Terrormaßnahmen praktisch beseitigt. Mit der Veröffentlichung des Patriot Act[3] wurden die Bürgerrechte stark eingeschränkt. Die staatliche Überwachung aller Unternehmen sowie die Auskunft der Daten der Kunden wurde hier im Namen des Terrors legalisiert. Im Zuge dessen wurde auch dafür gesorgt, dass die Unternehmen, welche die Daten der Kunden herausgeben

2 Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist eine 1995 erlassene Richtlinie der Europäischen Gemeinschaft zum Schutz der Privatsphäre von natürlichen Personen bei der Verarbeitung von personenbezogenen Daten. Sie beschreibt Mindeststandards für den Datenschutz, die in allen Mitgliedstaaten der Europäischen Union durch nationale Gesetze sichergestellt werden müssen. [vgl. LEX]

3 Der USA PATRIOT Act (Apronym für Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, dt. etwa: „Gesetz zur Stärkung und Einigung Amerikas durch Bereitstellung geeigneter Werkzeuge, um Terrorismus aufzuhalten und zu blockieren", daher außer dem letzten Wort in Großbuchstaben) ist ein amerikanisches Bundesgesetz, das am 25. Oktober 2001 vom Kongress im Zuge des Krieges gegen den Terrorismus verabschiedet wurde. [vgl. WIKI]

müssen, die Kunden darüber nicht informieren dürfen. Stillschweigen wurde gesetzlich vorgeschrieben.
Auch das Recht die elektronische Kommunikation zu überwachen wurde im Zuge der Terrorgefahr zum Gesetz erklärt.

4.2 Urheberrecht

Das Urheberrecht schützt persönliche geistige Schöpfungen wie auch Computerprogramme.
In Österreich wird zwischen so genannten Urheberpersönlichkeitsrechten und Verwertungsrechten unterschieden. Der Urheber kann vertraglich über seine Rechte verfügen, als er so genannte Werknutzungsrechte und Werknutzungsbewilligungen einräumen kann.

Urheberrechtsgesetz

ABGB Datenbanken und Datenbankwerke
§40f (1) Datenbanken im Sinn dieses Gesetzes sind Sammlungen von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit elektronischen Mitteln oder auf andere Weise zugänglich sind. Ein Computerprogramm, das für die Herstellung oder den Betrieb einer elektronisch zugänglichen Datenbank verwendet wird, ist nicht Bestandteil der Datenbank.
(2) Datenbanken werden als Sammelwerke (§ 6) urheberrechtlich geschützt, wenn sie infolge der Auswahl oder Anordnung des Stoffes eine eigentümliche geistige Schöpfung sind (Datenbankwerke).

Das heißt selbst entwickelte Datenbanken, die eine eigentümliche geistige Schöpfung darstellen, sind urheberrechtlich geschützt.

5 Rechtsgeschäft Cloud Computing

5.1 Verträge mit Cloud-IT Providern

Der Kunde hat in der Regel eine vertragliche Bindung zu einem oder mehreren Cloud IT Providern. Bedient sich der Kunde nur eines Generalunternehmers (GU), der sich verschiedener anderer Cloud IT Unternehmer als Subunternehmer bedient, so hat er eine Ansprechperson und nur einen Vertrag mit diesem Anbieter.

Wenn sich der Cloud IT Anbieter weiterer Anbieter (Subunternehmer) bedient greift in den meisten Fällen §1313a ABGB:

ABGB Haftung für den Erfüllungsgehilfen *§1313a. Wer einem andern zu einer Leistung verpflichtet ist, haftet ihm für das Verschulden seines gesetzlichen Vertreters sowie der Personen, deren er sich zur Erfüllung bedient, wie für sein eigenes*

Der Vertragspartner muss daher nicht den Subunternehmer klagen, sondern kann direkt auf den Cloud IT Anbieter zugreifen. Dieser kann dann Regress am Gehilfen nehmen.

Wie der Cloud Provider, dann intern aufgestellt ist, bleibt wiederum ihm überlassen. Benutzt ein Cloud Provider weltweit verstreute Serverfarmen, sind lediglich die entsprechenden Qualitäts- und Sicherheitsstandards wesentlich. Natürlich muss sich der Cloud IT-Anbieter auch das Recht einräumen lassen, dass er seine IT-Services aus dem Ausland oder von einem anderen Cloud IT-Anbieter beziehen darf.

Die zweite Möglichkeit wäre, dass der Kunde mehrere Verträge mit Cloud IT Anbietern abschließt, wobei diese harmonieren müssen und sich im Problemfall gegenseitig die Schuld zuweisen können. Auch die Frage der Haftung ist hier schwieriger zu klären, da erst der Verursacher

gefunden werden muss. Daher ist obwohl die zweite Variante vermutlich billiger sein wird, die erste wohl die Empfehlenswertere.

Bei jeglichen Vertragsabschlüssen ist es immer die Pflicht des Clients / Dienstenutzers vor Vertragsabschluss mit dem Provider, dessen Integrität und Seriosität zu prüfen. Wichtig sind hier vorrangig Themen wie Datenschutz, Datenintegrität und –wiederherstellung. Aber auch Themen wie Compliance und Auditing sind nicht zu vernachlässigen. [vgl. GAR1]

Dazu gibt es von Gartner eine eigene Studie, die auf die Sicherheitsrisiken aufmerksam macht und eine Reihe von Punkten aufzählt, mit der das Risiko vermindert werden soll:

1. Privilegierter Nutzerzugriff: Sensible Daten, die außerhalb des Unternehmens verarbeitet werden, bergen ein inhärentes Risiko. Der Grund: Ausgelagerte Services umgehen die physischen, logischen und von Mitarbeitern gesteuerten Kontrollmechanismen, die IT-Abteilungen auf interne Programme anwenden.
2. Compliance: Unternehmen sind letztendlich verantwortlich für den Schutz und die Integrität ihrer eigenen Daten - selbst dann, wenn sie von einem Service-Provider vorgehalten werden. Herkömmliche Dienstleister sind externen Audits und Sicherheitszertifizierungen unterworfen.
3. Ort der Daten: Wer die "Cloud" nutzt, wird nicht genau wissen, wo die eigenen Daten gehostet werden. Mit den Providern ist abzuklären, ob sie sich vertraglich verpflichten, Daten gemäß der jeweiligen Rechtsprechung zu speichern und zu verarbeiten, beziehungsweise die lokalen Datenschutzanforderungen im Namen ihrer Kunden zu erfüllen.
4. Trennung der Daten: Daten in der Cloud befinden sich in der Regel in einer von mehreren Parteien genutzten Umgebung. Deshalb ist es notwendig vorab über Sicherheitsmaßnahmen, wie Verschlüsselung, etc. Bescheid zu wissen.

5. Datenwiederherstellung: Ein Cloud-Provider sollte mitteilen, was im Fall eines Desasters mit den Daten beziehungsweise dem Service geschieht und wie lange eine Datenrekonstruktion dauern kann.
6. Investigative Unterstützung: hier geht es um Logging Themen, damit keine illegalen Machenschaften mit den Daten und den Applikationen getan werden können.
7. Langfristige Lösung: Auch wenn nicht angedacht ist, dass man Cloud Provider ständig wechselt, ist es doch notwendig zu wissen, wie und ob man seine Daten im Ernstfall zurückbekommt und in welchem Format diese dann vorliegen. [vgl. GAR1]

5.2 Rechtsanwendung

Eine entscheidende Frage ist, ob das Recht des Staates in dem das Unternehmen niedergelassen ist oder das Recht des Staates des Verbrauchers zur Anwendung kommt. Wie oben beschrieben, kann dies den völligen Verlust des Datenschutzes bedeuten.
Innerhalb der EU gilt das Herkunftslandprinzip[4] das besagt, dass sich ein Dienstanbieter an die rechtlichen Anforderungen des Staates in dem er niedergelassen ist, richten muss.
Unter den Ausnahmen befinden sich die Verbraucherverträge, sodass in diesem Fall das Recht des Verbraucherstaates anwendbar ist.

In den USA hingegen gibt es meist keinen Verbraucherschutz und so ist hier meist das Recht des Staates in dem das Unternehmen niedergelassen ist anzuwenden. Da dies in den USA aber sehr unklar und auslegungsbedürftig ist, liegt die Entscheidung oft bei der entscheidenden Distanz.

4 Mit Herkunftsland- bzw. Ursprungslandprinzip werden Prinzipien, bezeichnet die die Rechtsstellung von Waren- und Dienstleistungsanbietern in einem Gemeinsamen Markt Union im grenzüberschreitenden Verkehr regeln. Dabei finden die Regeln des Herkunftslandes Anwendung. [vgl WIKI]

Das heißt innerhalb der EU sind der Datenschutz und auch der Rechtsschutz gegeben. Außerhalb, vor allem in der USA gilt dies jedoch nicht.

6 Schwierigkeiten mit international agierenden Unternehmen

6.1 Datenschutz bei Amazon

Wenn man sich die Datenschutzerklärung bei Amazon ansieht, entdeckt man auf den ersten Blick keine Gefahr für seine Daten. Amazon schützt persönliche Daten und gibt sie nur im folgenden Umfang mit entsprechender Einwilligung weiter:

- Verbundene Unternehmen die von Amazon.com, Inc. beherrscht werden und deren Tochtergesellschaften, wenn diese entweder dieser Datenschutzerklärung unterliegen oder Richtlinien befolgen, die mindestens ebenso viel Schutz bieten wie diese Datenschutzerklärung.
- Partnerunternehmen, die nicht von Amazon.com, Inc. beherrscht werden.
- Dienstleister welche die Datenschutzerklärung sowie das deutsche Datenschutzgesetz anerkennen.
- Promotionen: es werden weder der Name, die Adresse noch persönlich identifizierende Informationen weitergegeben.
- Übertragung von Geschäftsanteilen: Die Daten unterliegen den vor der Übertragung bestehenden Datenschutzerklärungen.
- Schutz von Amazon.de und Dritten: Kundenkonten und persönliche Daten über Kunden werden nur bekannt gegeben, wenn es hierzu eine gesetzliche Verpflichtung gibt oder wenn eine solche Weitergabe erforderlich ist, um die allgemeinen Geschäftsbedingungen oder andere Vereinbarungen durchzusetzen oder das Recht von Amazon sowie die Rechte unserer Kunden und diejenigen Dritter zu schützen.

Problematisch ist die Weitergabe der Daten innerhalb der Unternehmensgruppe. Die Zugangsdaten eines österreichischen Verbrauchers, der sich bei amazon.at angemeldet hat, werden sowohl auf amazon.de also auch auf amazon.com akzeptiert. Die Weitergabe der Daten in Drittländer ist rechtlich aufgrund des dort herrschenden abweichenden Datenschutzstandards jedoch sehr problematisch. Besonders riskant ist die Weitergabe der Daten an die USA, die wie oben beschrieben keinen nationalen Datenschutz bieten. Genau dies ist aber bei Amazon innerhalb der Unternehmensgruppe geschehen: Die Daten des Österreichers sind in den USA verfügbar.

Laut amazon.de sind die Daten der Kunden jedoch trotzdem „in höchstem Maße geschützt“. Das Unterbinden der Weitergabe der Daten an amazon.com kann jedoch nur mit dem gesamten Löschen des Accounts erreicht werden. Das heißt eine Anmeldung zu amazon.at allein ist nicht möglich. Die Weitergabe österreichischer Daten an amerikanische Behörden ist in der Datenschutzerklärung von Amazon nicht zu finden, allerdings die Weitergabe aufgrund einer gesetzlichen Verpflichtung, die in den USA schon bei einer Anschuldigung in terroristische Aktionen verwickelt zu sein, vorliegt.

Der Vergleich der Datenschutzerklärung zwischen amazon.{at,de,uk.com} kommt zu dem Ergebnis, dass es kaum Unterschiede gibt. Amazon gewährt also allen Nutzern denselben Datenschutz.

6.2 EBay

Wenig anders sieht es bei EBay aus. Auch dort stehen die Server in den USA und haben daher keinen Datenschutz. In den Nutzungbedingungen steht sogar explizit, dass EBay "*personenbezogenen Daten an Strafverfolgungs- und Aufsichtsbehörden zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten übermittelt."*
Datenschutz hat man hier also nur, wenn man die Dienste nicht nutzt.

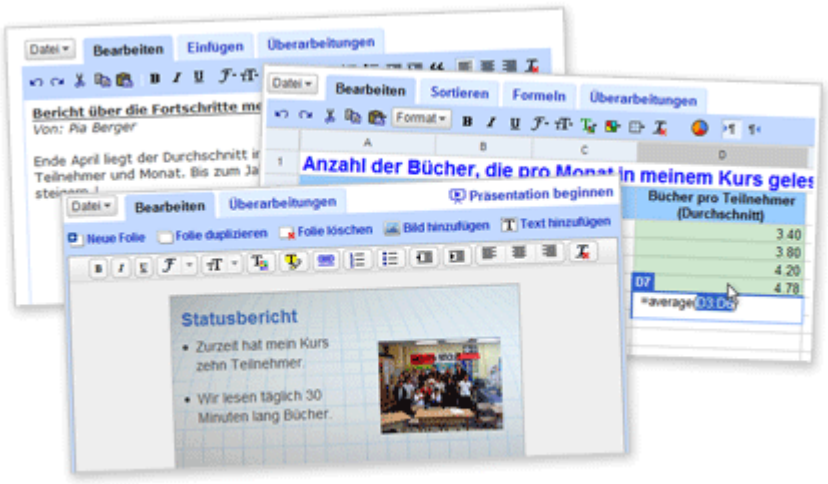
7 Fallbeispiele

Hier sollen einige Beispiele die Anwendungsmöglichkeiten von Cloud Computing aufzeigen und auch die rechtlichen Nutzungsbedingungen aufzeigen.

7.1 Google Text & Tabellen

7.1.1 Anwendungsbereiche

"Google Text & Tabellen" ist ein Webservice von Google mit welchem Dokumente, Tabellen und Präsentationen online erstellt werden können. Hier handelt es sich um eine klassische Umsetzung des Cloud Computing Modells. Dabei können unterschiedliche Dateien (Text, Tabellen, Präsentationen) sehr einfach erstellt werden und online gespeichert werden, sodass ein Zugriff jederzeit von jedem Ort aus möglich ist. Außerdem können mehrere Personen gleichzeitig an einen Dokument arbeiten, wenn diese Einstellung durch den Besitzer der Dokumente aktiviert wurde.



7.1.2 Datenschutz & Nutzungsbedingungen

Um die Google Applikationen nutzen zu können ist die erste Voraussetzung, dass man bei Google ein Konto hat und angemeldet ist. Über dieses Benutzerkonto werden dann nämlich alle Einstellungen und auch Dokumente gespeichert.

Google selbst erfüllt laut Datenschutzerklärung die Datenschutzbestimmungen und beachtet auch das „US-Safe-Harbor"

Abkommen. Das Problem ist auch hier folgende Stelle: Google verarbeitet persönliche Daten auf seinen Servern in den USA und in anderen Ländern.
Wie bei Amazon und EBay liegt also auch bei Google das Problem des fehlenden Datenschutzes in den USA vor.

Es hängt natürlich immer vom jeweiligen Ort des Cloud-Providers ab welcher Gerichtsstand Anwendung findet. Da Google ein amerikanisches Unternehmen ist, richtet es sich auch nach den amerikanischen Datenschutzrichtlinien.

Generell muss der Provider seine Datenschutzbestimmungen ersichtliche auf der Website publizieren.

7.2 Salesforce.com

7.2.1 Anwendungsbereiche

Salesforce ist der Marktführer im Bereich Customer Relationship Management und Cloud Computing. Salesforce bietet dabei einfach zu verwendende webbasierte CRM-Lösung für Vertrieb, Service, Marketing und Call Center, ERP bis hin zu SCM.
Als erste Plattform als Service der Welt (PaaS, Platform as a Service) können mit Force.com Webanwendungen für Unternehmen On-Demand bereit gestellt werden, ohne die Kosten für die Infastruktur aufbringen zu müssen. Schließlich dreht sich alles um "Cloud Computing" und Force.com ist die Plattform mit dem neuen Software-als-Service-Vorbild. [vgl SF]

7.2.2 Datenschutz & Nutzungsbestimmungen

Salesforce.com, inc., sowie salesforce.com sàrl und andere Tochtergesellschaften (insgesamt: salesforce.com) sind Lizenznehmer des TRUSTe Privacy Program[5].

Kunden von Salesforce nutzen die Zentralserver für Daten und Informationen („Daten“). Diese Daten werden von salesforce.com nicht geprüft, mit anderen gemeinsam benutzt, verteilt, ausgedruckt oder veröffentlich, außer soweit in dem salesforce.com Rahmen-Abonnementvertrag vorgesehen oder gesetzlich vorgeschrieben. Individuelle Daten dürfen jeweils nur für den Zweck der Lösung eines Problems, zu Supportzwecken oder bei Verdacht auf eine Verletzung des Rahmen-Abonnementvertrags oder im Rahmen gesetzlicher Vorschriften eingesehen bzw. darf darauf zugegriffen werden. Selbstverständlich sind die Kunden für die Wahrung der Vertraulichkeit und Sicherheit ihres Benutzernamens und Kennworts verantwortlich.

Die Daten werden durch die Secure Socket Layer (SSL) Technologie geschützt, die sowohl Server-Authentifizierung als auch Datenverschlüsselung benutzt.. Salesforce.com hat außerdem eine erweiterte Sicherheitsmethode auf Basis von dynamischen Daten und kodierten Session-IDs implementiert und führt die Site in einer sicheren Serverumgebung, die eine Firewall und andere moderne Technologien zur Verhinderung von Störungen oder Eindringversuchen benutzt. [vgl. SF]

Salesforce ist als kommerzielles Tool sehr seriös und scheint für Unternehmen hervorragend geeignet zu sein. Ob es dann natürlich wirklich alle Anforderungen erfüllt, muss jedes Unternehmen individuell entscheiden.

[5] TRUSTe ist eine unabhängige, gemeinnützige amerikanische Organisation, die es sich zur Aufgabe gemacht hat, das Vertrauen der Nutzer ins Internet zu stärken, indem sie für die Anwendung transparenter Praktiken bei der Nutzung von personenbezogenen Daten eintritt.

8 Fazit

„*Das sog. Cloud Computing werde künftig eine zentrale Rolle in der Informationstechnologie spielen*“, verkündete Mr. Ballmer, CEO von Microsoft, in einem Interview im Februar 2008. Cloud Computing und das damit verbundene Grid Computing sind die IT-Themen der Zukunft. [FTD]

Laut Gartner befinden sich viele Unternehmen gerade in einer Software-Upgradephase, die in etws alle 5-7 Jahre stattfindet, und hier kann nun ein entscheidender Schritt in Richtung Cloud Computing getan werden. Es gilt hier allerdings auch zu beachten, dass Cloud Computing keineswegs nur ein Technologiethema ist. Erst wenn das Thema auch bei der Managementebene Anklang findet, kann es ein dauerhaftes Geschäftsmodell werden.

Auf Seiten der Gesetzeslage ist zu beachten, dass das DSG und die jeweiligen Nutzungsbedingungen und ABGs Anwendung finden. Außerdem orientiert man sich sehr stark an den Regelungen für ASP und Outsourcing-Verträgen.
Wie sooft hinkt auch hier die Gesetzgebung dem technischen Fortschritt hinterher. Das Datenschutzgesetz schützt ausschließlich personenbezogene Daten, nicht aber die Daten, die andere Inhalte haben. Das heißt ein Datenschutz beim Cloud Computing von nicht personenbezogenen Daten, mit Ausnahme von Datenbankwerken, ist nicht gegeben.
Der weltweit uneinheitliche Datenschutz (Beispiel USA) ist die größte Gefahr des Cloud Computing.

Experten sind sich einig, dass eines der schwierigsten Probleme des Cloud Computing die Kontrolle der Einhaltung der Qualitäts- und Sicherheitsstandards sein dürfte.

Da die Server der Provider allerdings auf der ganzen Welt sein können, stellen sich auf Grund der Datensicherheit nach dem DSG noch einige Fragen, wenn nämlich andere Datenschutzgesetze zur Anwendung kommen, als in dem Land wo das Unternehmen seinen Sitz hat.

Es hängt natürlich immer vom Anwender ab, ob diese lokalen Regelungen für seine Daten ausreichend sind. Oft kann es auch vorkommen, und es gibt in der EU beispielsweise Gesetze, die es verbieten Kundendaten außerhalb des eigenen Landes zu speichern. Dann kann Cloud Computing natürlich nicht verwendet werden.
Bei dieser Thematik befinden wir uns momentan aber in einer Grauzone und sie ist zurzeit von der Judikatur noch unbeantwortet.

Abschließend kann gesagt werden, dass Cloud Computing ein hohes Zukunftspotential hat, jedoch die rechtliche Situation wird auch in Zukunft ein brisantes, wenn auch zum Teil von den Unternehmen ein noch unterschätztes Thema sein.
Schlussendlich muss aber jeder selbst entscheiden, inwieweit er Cloud Computing nutzen will und kann.

9 Literaturverzeichnis

9.1 Bücher & Zeitschriften

[ACM] Heyes, Brian: Cloud Computing. Communications of the ACM.07/08 Volume 51. No. 7. p.9-10.

[COM]Communications of the ACM: Cloud Computing. 07/08 Vol.51 No.7 S.9

[HON] Hong, Jason I./ Landay, James A.: An Architecture for Privacy-Sensitive Ubiquitous Computing. University of California at Berkeley.

[HP] Delic, Kemal/ Walker, Martin: Emergence of the Academic Computing Clouds. ACM Ubiquity, Volume 9, Issue 31.Hewlett-Packard Co. 2008.

[LEX]Lex:itec:Fachzeitschrift für Recht und Informationstechnologien. Ausgaben 2006-2007

[STA] Jahnel D./Schramm A./Staudegger E. (Hrsg.): Informatikrecht. Zweite aktualisierte und erweiterte Auflage. Springer Verlag. Wien. Wien. S.79-118.

[WEI]Weiss A.: Computing in the Clouds. ACM netWorker.December 2007.

9.2 Online Quellen

[BEC] Rechtsanwälte Beck: Cloud Computing:IT Strategien der Zukunft rechtlich betrachtet. Online im Internet: http://rsw.beck.de/rsw/shop/default.asp?docid=259482&highlight=cloud+computing (Stand: Jänner 2009)

[FTD] Financial Times Deutschland, Richard Walters:Ballmer kämpft um Dominanz. 25.02.2008. Online im Internet: http://www.ftd.de/technik/medien_internet/:Ballmer%20Dominanz/322228.html (Stand: Jänner 2009)

[GAR] Gartner Analysis: Gartner Says Worldwide IT Spending On Pace to Surpass $3.4 Trillion in 2008. Online im Internet:

[GAR1] Computerwoche (Hrsg.): Gartner: Wo Gefahren lauern. Online im Internet: http://www.computerwoche.de/knowledge_center/security/1867951/index.html (Stand: Jänner 2009)

[GOO]Google: Allgemeine Informationen zu Google und seinen Bestimmungen. Online im Internet: http://www.google.com/intl/de/privacypolicy.html#information (Stand: Jänner 2009)

[HEI] Heise (Hrsg.): Datenschutz. Online im Internet: http://www.heise.de/ix/artikel/2003/05/096/ (Stand: Jänner 2009)

[IBM] IBM: Blue Cloud: Online im Internet: http://www-03.ibm.com/press/us/en/photo/22615.wss (Stand: Jänner 2009) http://www.gartner.com/it/page.jsp?id=742913 (Stand: Jänner 2009)

[LEX] Amtsblatt der Europäischen Gemeinschaft. RL 2002/58/EG. Online im Internet: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:DE:PDF (Stand: Jänner 2009)

http://www.internet4jurists.at/formalrecht/zustaendigkeit1a.htm

[NW] Netzwelt (Hrsg.): Mangelnder Datenschutz beim Online Auktionshaus. Online im Internet: http://www.netzwelt.de/news/67935-ebay-mangelnder-datenschutz-beim-online-auktionshaus.html (Stand: Jänner 2009)

[Ris] Rechtsinformationssystem Österreich. Online im Internet: http://ris.bka.gv.at/bundesrecht/ (Stand: Jänner 2009)

[SF]Salesforce: Online im Internet: http://www.salesforce.com (Stand: Jänner 2009)

[Wik] Wikipedia. Online im Internet: http://de.wikipedia.org/wiki/Hauptseite