Datenschutz in der Wolke

Artikel für die Festschrift

„Von der Lochkarte zum Ultra Mobile Computing - 20 Jahre Datenschutz in der Schweiz"

Herausgeber „Datenschutzforum Schweiz"

Autorin: Cordula E. Niklaus, Fürsprecherin, ll.m., Rechstanwältin und Inhaberin der Anwaltskanzlei niclaw in Zürich, mit langjähriger Beratungspraxis im Bereich IT- Recht und Datenschutz – www.niclaw.ch

1. Viele Wege führen in die Cloud

1.1 Begriff und Definition von Cloud Computing

Mit dem Begriff „Cloud Computing" oder zu Deutsch „Rechnen in der Wolke" bezeichnet die Informationstechnologie den Ansatz, IT-Infrastrukturen oder IT-Dienstleistungen wie Rechnerleistungen, Software, Datenspeicher- oder Netzwerkkapazitäten, bedarfsorientiert und dynamisch über ein Netzwerk zur Verfügung zustellen bzw. diese aus dem Netz zu beziehen[1]. Die eigentliche IT-Infrastruktur wie das Rechenzentrum, Datenspeicher, Kommunikations- und Kollaborationssoftware oder Spezialsoftware wie Customer Relationship Management (CRM) werden vom Nutzer nicht mehr selber betrieben oder bereit gestellt, sondern ausgelagert und bedarfsorientiert bei einem oder mehreren Anbieter von Cloud-Services als eigentliche Dienstleistung (Service) gemietet. Cloud Computing ist somit eines von weiteren IT-Sourcing Modellen, welches von Unternehmungen genutzt wird, und diesen eine bedarfsgerechte und flexible Nutzung von IT-Dienstleistungen ermöglicht.

Die Daten und Anwendungen sind somit nicht mehr lokal beim Nutzer vor Ort im unternehmenseigenen Netzwerk oder im lokalen Rechner abgelegt, sondern befinden sich beim Anbieter, und der Zugang darauf erfolgt über ein Netzwerk wie beispielsweise das Internet mittels Fernzugriff.[2] Für den Benutzer verschwinden somit die Anwendungen sowie die Verarbeitung der Daten in der „Wolke" oder „Neudeutsch" in der „Cloud" des Dienstleistungsanbieters.

1.2 Die „offizielle" Definition von Cloud Computing

Im Jahr 2009 hat das NIST (National Institute for Standards and Technology, eine Agentur des U.S. Departement of Commerce) eine Definition von Cloud Computing veröffentlicht, welche verschiedene frühere Definitionsversuche zusammenfasste, und auf weitgehende Akzeptanz in der IT-Welt stiess. Gemäss dieser Definition werden drei verschiedene Servicemodelle:

- IaaS (Infrastructure as a Service)
- PaaS (Platform as a Service)
- SaaS (Software as a Service)

und vier verschiedende Liefermodelle:
- Private Cloud
- Public Cloud

[1] vgl. Wikipedia, Stichwort „Cloud Computing"<http://de.wikipedia.org/wiki/Cloud Computing>
[2] vgl. „Erläuterungen zu Cloud Computing" des EDÖB, Stand 10.2011, www.edoeb.admin.ch

- Hybrid Cloud
- Community Cloud

unterschieden.

1.3 Die drei verschiedenen Service-Modelle

Die Cloud Computing Architektur kann man sich pyramidenförmig in drei Ebenen vorstellen (sog. Cloud-Stack), wobei die unterste die Ebene der Infrastruktur bildet, darüber liegt die Plattform und zuoberst die Anwendungen.[3] Die oberen Schichten können dabei auf den unteren aufbauen, müssen das aber nicht.

Bei der Variante Infrastructure as a Service / **IaaS** greift der Nutzer auf das Fundament innerhalb des Cloud-Systems zu, auf dem er dann seine eigenen Daten und Anwendungen selber abspeichern und bearbeiten kann. Bei diesem Modell ist der Cloud-Anbieter verantwortlich für das Funktionieren des Netzes, den Zugang und der zur Verfügung gestellten Hardware. Der Benutzer hat hier aber vollen Zugriff auf die Recheninstanzen, die je nach Anforderungen beliebig um weitere Instanzen erweitert oder verkleinert werden können.

Beim Modell Plattform as a Service / **PaaS** entwickelt der Service-Anbieter eine Anwendung und stellt diese in der Cloud zur Verfügung. Der Benutzer hat hier im Unterschied zum Modell IaaS keinen direkten Zugriff auf die Recheninstanzen und kann diese auch nicht verändern, er bringt lediglich seine Programmlogik ein, und kann damit seine Daten selber bearbeiten.

Auf der dritten Ebene, der Anwendungsebene, steht das Modell Software as a Service / **SaaS**. Hier muss sich der Benutzer weder um die Applikation noch um die Skalierbarkeit oder die Datenhaltung kümmern, sondern er ist lediglich noch Konsument und nutzt die ihm nach aussen zur Verfügung gestellte Funktionalität der Cloud. Dieses Modell basiert auf den beiden darunter liegenden Ebenen Plattfom und Infrastruktur.

1.4 Die vier verschiedenen Liefermodelle

Bei der sog. **Private Cloud** sind sowohl der Nutzer wie auch der Dienstleistungsanbieter in derselben Unternehmung, die angebotenen Anwendungen sind ausschliesslich auf das Unternehmen ausgerichtet und werden über ein firmeneigenes Netzwerk angeboten, und es handelt sich dabei in der Regel lediglich um eine unternehmensinterne Reorganisation der IT-Struktur. Sofern der Service-Anbieter ein externer Dritter ist, so handelt es sich um ein IT-Outsourcing im herkömmlichen Sinn.

Im Unterschied dazu wird bei der sog. **Public Cloud** die gesamte Intrastruktur sowie die Anwendungen vom externen Service- Anbieter angeboten und bewirtschaftet, und das einzelne Unternehmen oder der Nutzer hat keinen Einfluss auf deren Inhalt oder auch auf die Standorte der Server. Zudem können beliebige Personen und Unternehmen als Nutzer über ein Netzwerk, z.B. das Internet, Zugriff darauf nehmen und die Anwendungen ebenfalls nutzen[4].

Wenn eine Unternehmung sowohl eine unternehmensinterne Private Cloud sowie zusätzlich z.B. zum Absichern von Belastungsspitzen noch eine Public Cloud betreibt bzw. benützt, spricht man von einer **Hybrid Cloud**.

Bei der **Community Cloud** oder auch „Exclusive Cloud" schliesslich können mehrere Benutzer bzw. Organisationen, die sich untereinander kennen, dieselbe Infrastruktur gemeinsam nutzen.

---

[3] Wikipedia, Stichwort „Cloud Computing"<http://de.wikipedia.org/wiki/Cloud Computing>
[4] „Erläuterungen zu Cloud Computing" des EDÖB, Stand 10.2011, www.edoeb.admin.ch

2. Chancen und Risiken des Einsatzes von Cloud Computing Dienstleistungen

2.1 Chancen

Grundsätzlich bietet Cloud Computing gerade für Unternehmungen vielfältige Möglichkeiten und Chancen. Im Vordergrund stehen dabei sicher einmal die hohe Skalierbarkeit, die Flexibilität, die Standortunabhängigkeit sowie die Effizienz, indem die in Echtzeit zur Verfügung gestellten serverseitigen Ressourcen und Anwendungen besser, variabler und somit bedarfsgerechter genutzt werden können. Ein weiterer Vorteil sehen die Anwender von Cloud Computing in der Möglichkeit, von der spezifischen IT-Expertise des Anbieters profitieren zu können, indem die genutzten Anwendungen jeweils auf dem neuesten technischen Stand sind, diese allenfalls auch besser gewartet werden, und die Sicherheitsstandards beim Anbieter allenfalls höher sind.

Die Anwender und Nutzer umgekehrt müssen nicht selber in neue Technologien investieren, und können ihre Kosten von bisherigen Investitionen neu auf wiederkehrende Kosten verlagern. Die Unternehmungen finden somit einen effizienteren und schnelleren Marktzugang, können dadurch ihre Leistung erhöhen und so gegenüber konventionellen IT-Systemen Kostenvorteile erzielen, indem sich beispielsweise die Kosten lediglich nach der Dauer und dem Umfang der Nutzung richten und entsprechend abgerechnet werden, die Leistungen zudem nicht immer im selben Umfang in Anspruch genommen werden, und beispielsweise die Kosten für den Betrieb, die Wartung und die Erneuerung der lokalen IT-Systeme wegfallen. Der Cloud-Nutzer hat also die Möglichkeit, immer und von überall her auf die aktuellsten Technologien zugreifen zu können, ohne selber laufend in die Technologie-Entwicklung investieren zu müssen.

2.2 Risiken

Nebst den möglichen rechtlichen Risiken, welche nachtstehend noch genauer erörtert werden, ist hier sicher einmal die Abhängigkeit von der Technologie und vom Anbieter zu nennen. Dies ist jedoch kein grundsätzlich neues Phänomen, denn auch beim bisher unter dem Begriff „IT-Outsourcing" bekannten Auslagern von IT-Diensten und Unternehmensdaten an einen Dritten kann es zu einem Verlust an internem Know-How und vor allem von internen Know-How Trägern kommen, was die Abhängigkeit vom Anbieter stark erhöht. Wie beim Outsourcing bleibt auch beim Cloud Computing der Nutzer gegenüber seinen Kunden, Behörden und Ansprechpartnern verantwortlich, weshalb er sicherstellen muss, dass er auf seine ausgelagerten geschäftlichen Informationen und Daten jederzeit Zugriff hat, und er jederzeit seinen geschäftlichen Verpflichtungen nachkommen und seine rechtlichen Anforderungen erfüllen kann.

In seinen Erläuterungen zu Cloud Computing weist der Eidg. Datenschutzbeaufragte darauf hin, dass auch generell und unabhängig von Cloud Computing ein Datenverlust durch Diebstahl, Löschung, fehlerhafte Überschreibung usw. eintreten kann, dass durch System- und Netzwerkausfälle oder durch Nichtverfügbarkeit von Ressourcen und Dienstleistungen Daten verloren gehen oder unberechtigte Personen auf Daten Zugriff erhalten, oder dass letztlich durch böswillig agierende Mitarbeitende oder Insider auf Seiten des Outsourcing-Anbieters Daten missbräuchlich bearbeitet werden.[5]

Weitere mögliche Risiken sind sicher die Datenspeicherung, dabei insbesondere der Standort der Server, sowie die Sicherheitssysteme beim Cloud-Anbieter, insbesondere betreffend des Schutzes vor Hackern sowie vor Systemausfällen. Insbesondere beim Public Cloud Computing teilen sich unbekannte Nutzer eine gemeinsame Infrastruktur, was zu einem erhöhten Risiko von Missbrauch führen kann. Zudem erfolgt die Nutzung von Anwendungen und die Bearbeitung von Daten über das Internet, weshalb ein Netzausfall erhebliche Auswirkungen auf deren Verfügbarkeit hat.

3. Spezifische rechtliche Risiken

3.1 Vertragsrechtliche Risiken

[5] „Erläuterungen zu Cloud Computing" des EDÖB, Stand 10.2011, www.edoeb.admin.ch

Aus rechtlicher Sicht stellen sich insbesondere bei der „Private Cloud" wohl die kleinsten Probleme, da diese Service-Leistung in der Regel unternehmensintern angeboten wird, und keine vertragsrechtlichen Beziehungen mit aussenstehenden Dritten abgeschlossen werden müssen. Problematischer wird es jedoch im Zusammenhang mit der „Public Cloud", wo oft schon der eigentliche Vertragspartner „in den Wolken verschwindet", und es dem Nutzer nicht oder kaum bekannt ist, wer sein vertragliches Gegenüber und somit sein Vertragspartner ist, wie sein Vertragspartner intern organisiert ist, an wen er sich bei Problemen bei der Nutzung wenden kann, und wer letztlich bei auftretenden Fehlern oder Mängeln verantwortlich ist und die allfällige vertragliche Haftung übernimmt. Es gilt deshalb einerseits das Verhältnis des Nutzers mit dem Cloud-Anbieter vertraglich zu regeln, wie auch andererseits die möglichen Beziehungen innerhalb der „Cloud" zu klären. Vertraglich werden Cloud-Computing-Verhältnisse zwischen Nutzer und Anwendungs-Anbieter oft als sogenannte Outsourcing-Verträge qualifiziert

3.2 Prozessuale Risiken

Ein weiterer rechtlicher Aspekt, der allenfalls zu einem rechtlichen Risiko werden kann, ist die Frage nach dem Anwendbaren Recht und des Gerichtsstandes. Je nach Standort des Anbieters oder der im Vertrag getroffenen Rechtswahl, die sich in einem Land ausserhalb Europas befinden, kann man mit nicht unerheblichen Problemen konfrontiert sein, sollte man seine Rechte wegen Nicht- oder Schlechterfüllung des Vertrages auf dem Rechtsweg durchsetzen müssen.

3.3 Weitere rechtliche Aspekte

Nebst dem Einhalten von Datenschutzrechtlichen Bestimmungen, welche nachstehend noch eingehend erörtert werden, muss der Nutzer von IT-Leistungen aus der „Cloud" aber allenfalls auch Geheimhaltungsvorschriften beachten wie z. B. das Bankgeheimnis, das Arzt- oder das Anwaltsgeheimnis, oder ganz allgemein gegenüber Vertragspartnern vereinbarte Geschäftsgeheimnisse sicherstellen, deren Verletzung allenfalls auch strafrechtliche Konsequenzen gemäss Art. 162 StGB nach sich ziehen können, und auch deren Einhaltung muss im Zusammenhang mit Cloud Computing sichergestellt und deshalb entsprechend vertraglich geregelt werden.

Allenfalls können sich auch rechtliche Fragen im Zusammenhang mit der Nutzung von Urheberrechten in der „Cloud" stellen, einerseits weil es sich bei den in die „Cloud" ausgelagerten Daten um geschützte Werke im Sinne von Art. 2 des schweizerischen Urheberrechtsgesetzes wie Texte, Pläne, Bilder oder auch Software etc. handeln kann, andererseits weil auch die vom Cloud-Anbieter zur Nutzung zur Verfügung gestellten Anwendungen geschützte Werke im Sinne von Art. 2 URG sind, deren Nutzung durch den Anwender von Cloud-Computing ebenfalls nur in einem definierten Rahmen erfolgen soll. Auch hier kann die oftmals für den Nutzer „verschleierte Sicht in der Wolke" eine effektive und effiziente Kontrolle der allenfalls definierten Nutzungsrechte zumindest erschweren.

3. Insbesondere Datenschutzrechtliche Aspekte

Die vermehrte Nutzung von IT-Dienstleistungen über das Internet und die engere Verknüpfung von solchen Technologien und Dienstleistungen rücken auch die datenschutzrechtlichen Aspekte vermehrt in den Vordergrund. Werden geschäftsrelevante Daten oder Anwendungen vom Cloud-Nutzer an den Cloud-Anbieter in eine „Public Cloud" ausgelagert so hat das zur Konsequenz, dass diese der unmittelbaren eigenen Kontrolle durch den Dateninhaber entzogen werden. Werden in der „Cloud" Personendaten, d.h. Daten, die sich auf eine bestimmte oder bestimmbare Person gemäss Art. 3 Datenschutzgesetz[6] beziehen erhoben, bearbeitet oder genutzt, so müssen die Datenschutzrechtlichen Bestimmungen eingehalten und gewährleistet werden. Dabei gilt es zu berücksichtigen, dass wie beim Outsourcing auch beim Einsatz von Cloud Computing die Verantwortung für die Einhaltung und die Gewährleistung der Datenschutzrechtlichen Bestimmungen

[6] Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1

nicht outgesourct bzw. an den Cloud-Anbieter übertragen werden können, sondern dass diese Verantwortung beim Inhaber der Datensammlung verbleibt.

3.1 Spezifische Bestimmungen im Datenschutzgesetz

Im Zusammenhang mit der Auslagerung von Personendaten an den Cloud-Anbieter und deren Bearbeitung im Rahmen der Nutzung von Cloud Computing-Dienstleistungen, kann es sich um eine Datenbearbeitung durch Dritte gemäss Art. 10a DSG handeln. Darin wird vorgesehen, dass die Bearbeitung von Personendaten *durch Vereinbarung oder Gesetz Dritten übertragen werden kann, sofern die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte, und sofern keine gesetzlichen oder vertraglichen Geheimhaltungsvorschriften dies verbieten.* Der Auftraggeber ist in diesem Fall der Nutzer von Cloud Computing-Dienstleistungen, der vertraglich sicherstellen muss, dass sich der Anbieter von Cloud Computing Dienstleistungen an die gesetzlichen Vorgaben hält, und dass zudem keine weiteren Geheimhaltungsverpflichtungen verletzt werden. Der Cloud-Nutzer und Dateninhaber muss dabei ebenfalls sicherstellen, dass die Bearbeitungsgrundsätze gemäss Art. 4 und 5 DSG[7] wie Rechtmässigkeit, Treu und Glauben, Zweckmässigkeit und Richtigkeit vom Cloud-Anbieter eingehalten werden.

Im übrigen muss der Cloud-Nutzer gemäss Art. 10a Abs. 2 DSG sicherstellen, dass der Cloud-Anbieter die Datensicherheit im Sinne von Art. 7 DSG bzw. Art. 8 ff. und Art. 20 ff. VDSG[8] gewährleistet. So müssen Personendaten *durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt* werden, und die *Vertraulichkeit, die Verfügbarkeit sowie die Integrität der Daten* muss sichergestellt sein. Diese Verpflichtungen gelten im übrigen nicht nur für den Cloud-Anbieter als Dritten, sondern auch für allfällige von diesem beauftragte Subunternehmer. Dieses Erfordernis bietet im Umfeld von Cloud Computing unter Umständen gewisse Schwierigkeiten bei der Umsetzung, ist doch wie bereits erwähnt dem Cloud-Nutzer nicht immer eindeutig klar und für ihn auch nicht einfach nachvollziehbar, wer genau sein Vertragspartner ist, geschweige denn, wer als allfälliger Subunternehmer noch von diesem beigezogen worden ist.[9]

Weitere im Zusammenhang mit Cloud Computing zu beachtende Bestimmungen des Datenschutzgesetzes sind das Auskunftsrecht gemäss Art. 8 DSG sowie das Recht auf Berichtigung und auf Vernichtung von falschen und unvollständigen Daten gemäss Art.5 DSG. Der Cloud-Nutzer bleibt gesetzlich verpflichtet, dass auch diese Verpflichtungen gegenüber den betroffenen Personen jederzeit gewährleistet und eingehalten werden. Der Cloud-Nutzer muss also vertraglich sicherstellen, dass der Cloud-Anbieter und allfällige von diesem beauftragte Subunternehmer die Daten nur gemäss seinen Weisungen und nur in dem Umfang, wie er das selber auch dürfte, bearbeiten.

3.2 Insbesondere Datenübertragung ins Ausland gemäss Art. 6 DSG

Viele Cloud-Anbieter sind multinational tätig und betreiben ihre Rechenzentren an verschiedenen Standorten auf der Welt. Der Nutzer, der seine Daten in die „Cloud" ausgelagert hat, weiss deshalb oft nicht, wo genau seine Daten gelagert sind, bzw. woher er diese aus der „Cloud" bezieht, weshalb es bei der Nutzung von Cloud Computing aus Datenschutzrechtlicher Sicht oft zu einer grenzüberschreitenden Bekanntgabe von Daten gemäss Art. 6 DSG[10] kommt. Eine grenzüberschreitende Datenbekanntgabe darf demnach nur erfolgen, wenn dadurch die Persönlichkeit der betroffenen Personen nicht schwerwiegend gefährdet würde, *namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.* Falls jedoch im entsprechenden Land eine solche Gesetzgebung fehlt, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn *hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten* (vgl. Art. 6 Abs. 2 lit. a. DSG).

---

[7] Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1
[8] Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG) SR235.11
[9] „Erläuterungen zu Cloud Computing" des EDÖB, Stand 10.2011, www.edoeb.admin.ch
[10] Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1

In der Datenschutz-Gesetzgebung der EU-Länder beispielsweise existiert ein solcher angemessener Schutz, nicht jedoch in derjenigen der USA. Seit 2009 gibt es diesbezüglich das US Swiss Safe Harbour-Abkommen, welches die Datenübermittlung an ein Nordamerikanisches Unternehmen regeln soll. Sofern sich ein US-Unternehmen diesen Safe Harbour Rules unterstellt, indem es sich gegenüber dem US Departement of Commerce (Handelsministerium) verpflichtet, sich an dieses Abkommen zu halten, muss kein entsprechender Vertrag betreffend Übertragung der Daten mit diesem Unternehmen abgeschlossen werden. Grundsätzlich muss derjenige, welcher Personendaten grenzüberschreitend übermittelt nachweisen, dass er alle erforderlichen Massnahmen getroffen hat, um ein angemessenes Schutzniveau zu gewährleisten. Der Nutzer von Cloud-Dienstleistungen muss demzufolge je nach Zielort der auszulagernden Daten mit dem Cloud-Anbieter und allfälligen von diesem beauftragten Subunternehmern auf vertraglicher Basis Datenschutzgarantien abschliessen, was er jedoch nur verbindlich tun kann, wenn ihm diese Vertragspartner und involvierte Parteien bekannt sind.

4. Cloud Computing als Chance für den Datenschutz?

Global bewegen sich die Umsätze mit Cloud Computing bereits im zweitstelligen Milliardenbereich, und es wird mit Wachstumsraten von über 30% gerechnet.[11] Umgekehrt gibt es wie dargelegt in der Anwendung und Umsetzung dieser neuen IT-Dienstleistung noch zahlreiche Unsicherheiten und Risikofaktoren, die es konkret zu definieren und wirksam beheben gilt. Insbesondere empfiehlt sich für Unternehmungen, die eine Nutzung von Cloud Computing planen, die rechtlichen Risiken genau abzuschätzen, den künftigen Vertragspartner seriös zu evaluieren und die notwendigen vertraglichen Vorkehrungen zu treffen, damit das geplante Projekt erfolgreich auf- und umgesetzt werden kann. Insbesondere im Zusammenhang mit den Datenschutzrechtlichen Bestimmungen gilt es zudem unternehmensintern eine genaue Evaluation zu machen, welche Daten sich für diese Form der externen Nutzung von IT-Ressourcen und Anwendungen eignen und welche nicht.

Wie einer Studie des *Netzwerk und IT-Dienstleisters BT Germany* entnommen werden kann, sind die Aspekte Datenschutz und Datensicherheit offenbar für deutsche Unternehmen die wichtigsten Kriterien beim Entscheid, ob Cloud Computing zum Einsatz kommen soll oder nicht. Demnach wäre mehr als jedes vierte deutsche Unternehmen bereit, Teile seiner Infrastruktur an einen Dienstleister auszulagern, sofern dieser versichern würde, die Daten in Deutschland zu speichern. 90% der Teilnehmenden dieser BT-Studie sagten weiter, dass die Festlegung von Datenschutzrechtlichen Bestimmungen in einem Vertrag zwischen Nutzer und Anbieter wichtig oder sogar ausschlaggebend für eine Zusammenarbeit mit einem Anbieter von Cloud Computing – Dienstleistungen sei.[12]
Somit könnte im Zusammenhang mit Cloud Computing das gerade im Umfeld der IT-Industrie nicht immer und überall sehr aktiv gelebte Thema Datenschutz, und die damit verbundenen gesetzlichen Bestimmungen durchaus neuen Auftrieb und nachhaltig mehr Relevanz erhalten.

[11] BITKOM: Leitfaden zu Cloud Computing, Oktober 2009, S. 10
[12] "Business & IT", 9/11, Special Cloud Computing, S. 27