

Internet und Datenschutz

Cloud Computing: Rechtliches Ende vor dem Anfang?

„Arbeiten in der Internet-Wolke“ ist in aller Munde – auch in Forschungsabteilungen: Die nahezu unbegrenzten Ressourcen der Cloud sollen für rechenaufwändige Forschung aber auch für Entwicklungsplattformen genutzt werden. Gleichzeitig überschlagen sich die Medienberichte über Gefahren und rechtliche Grenzen. Können rechtliche Grenzen wirklich den nächsten logischen Schritt des Internet verhindern oder sollten Gesetze nicht immer nur „Nein“ sagen?!

Ein Beitrag von Max Mosing

Für Cloud Computing gibt es keine allgemein gültige Definition, dennoch wird bereits von einem Milliarden-Euro-Markt dafür gesprochen, der nach Studien im Jahr 2014 bereits 39,5 Mrd. Euro schwer sein soll. Die „Rechnerwolke“ steht für den Ansatz, abstrahierte IT-Infrastrukturen, insbesondere Rechenkapazität, Datenspeicher, aber auch fertige Software, dynamisch an den Bedarf angepasst über ein Netzwerk zur Verfügung zu stellen. Häufig lässt sich nicht mehr feststellen, wo genau sich die dabei verwendeten Daten physisch befinden. Wir kennen das wohl alle aus der Praxis: Speichern von Bildern auf Facebook®, Plattensammlung in der iCloud® oder Schreiben von e-Mails über hotmail®.

Potentielle Einsparung der eigenen IT

Die Business-Idee hinter betrieblichem Cloud Computing ist Einsparung einerseits und Ressourcenverfügbarkeit andererseits: Ein (Groß)Teil der IT-Landschaften, auf denen auch jeweils Software mit teuren „Lizenzen“ läuft, werden nicht mehr auf Nutzerseite betrieben und örtlich bereitgestellt, sondern bei einem oder mehreren Anbietern über das Internet als Dienst „gemietet“: Die Anwendungen und Daten befinden sich dann in der Cloud. Die Anbieter von Cloud-Lösungen nutzen den „on-demand-Effekt“, weil ja nicht immer alles von allen genutzt wird, wie auch den „Poolingeffekt“, weil die gemeinsame Nutzung von Ressourcen erhebliche Einsparungen bringen kann.



Bei Cloud Computing gibt es etliche juristische Unklarheiten.

Die technischen und politischen Ängste

Die Risiken am Milliardenmarkt des Cloud Computing sollen hoch sein: Von der gänzlichen Abhängigkeit des Kunden vom Anbieter und insbesondere Internet-Infrastruktur-Dienstleistern, über potentiellen Datenverlust, bis hin zur Industriespionage oder gar, dass die Geheimdienste der Vereinigten Staaten über die US-Clouds auf europäische Daten zugreifen können, wird in Medien berichtet – Fakten dazu gibt es bisher wenige.

US-Patriot Act als internationale Achillesferse?!

Der „US Patriot Act“, den die USA nur wenige Wochen nach den Terroranschlägen vom 11. September 2001 erlassen hat, gibt den US-Behörden tatsächlich umfassende rechtliche Handhabe, um ganz legal auch ohne richterli-

chen Beschluss an Daten zu kommen und die Betroffenen sind auch im Nachhinein darüber nicht zu informieren.

Festzuhalten ist daher zweifellos, dass die Cloud es faktisch erleichtern könnte, dass US-Behörden sich für „zuständig“ erklären und versuchen, auf Daten zu greifen – ob das allerdings nicht ohnedies auch ohne Cloud passiert?!

Rechtliche Fragestellungen zur Cloud

Praktisch ist es oft schwer, das Cloud Computing vom Grid Computing, Application Service Providing und auch vom klassischen Outsourcing abzugrenzen. Zweifel-

los wirft Cloud Computing neue Fragen auf, wie allein die rechtliche Qualifikation des Cloud Computing-Vertrages als Werk-, Miet-, Dienstleistungs- oder gar Verwahrungsvertrag; das auch noch im meist internationalen Umfeld. Es ist auch unklar, ob Sonderbestimmungen auf das Cloud Computing Anwendung finden, zB die Haftungsprivilegien des E-Commerce-Gesetzes, aber auch das Gewährleistungsrecht. Können bestehende Software-Lizenzen in der Cloud genutzt werden? Wie ist Daten- ohne Substanzverlust schadenersatzrechtlich zu beurteilen? Kann der Cloud Dienstleister Zurückbehaltungs- oder sonstige Rechte an Cloud Daten geltend machen?

All diese Fragen sind oder werden früher oder später beantwortbar sein – jedenfalls sind sie aus der Sicht des Autors keine zwingenden „Show-Stopper“, auch wenn der Gesetzgeber kreativ beim „Fallstrickbinden“ ist, zB verbietet das Umsatzsteuergesetz, dass „die Buchhaltungsbücher“ im Ausland gespeichert werden.

Cloud Computing und Datenschutzrecht

Sind Software oder Speicherplatz Gegenstand des Cloud Computing, kommt es in der Regel zur Verarbeitung personenbezogener Daten und damit zu datenschutzrechtlichen Implikationen. Für Verletzungen des Datenschutzrechts haftet dann der Anwender und könnte sich höchstens beim Cloud-Anbieter regressieren, falls das internationale Umfeld bzw der Cloud-Vertrag dies überhaupt zulässt. Da aber diese Ansprüche bisher in der Praxis wenig Bedeutung haben, sollte man - zumindest aus heutiger Sicht - dem Cloud-Computing hier kein „haftungsrechtliches Ende“ bereiten.

ABER: Das Datenschutzrecht hält durchaus (angeblich) unüberkommene Hindernisse für das Cloud Computing parat: Es normiert zwar eine „Dienstleisterfreiheit“, dh, jeder darf sich eines Dienstleisters für die Datenverwendung bedienen, doch muss Letzterer ausreichend Gewähr für eine rechtmäßige und sichere Datenverwendung bieten, also „verlässlich“ sein. Zur Verlässlichkeit gehört auch, dass der Dienstleister, also in concreto der Cloud-Anbieter, umfassende gesetzliche Datensicherungsmaßnahmen ergreift – gerade bei medizinischer Forschung, also bei Gesundheitsdaten, sind die Anforderungen hoch. Meist werden Cloud-Anbieter, die ja meist selbst Leistungen auslagern,

solche Datensicherungsmaßnahmen nicht garantieren können – also ein möglicher Stolperstein. Weiters muss nach dem Datenschutzgesetz obgenannte Verlässlichkeit durch den Anwender überprüft werden – wie weit die Prüfpflicht geht, ist zwar unklar, doch kann beim Cloud Computing der Forscher wohl gar nichts faktisch überprüfen.

Datenschutzrechtliche Genehmigungspflicht als faktisches Aus?!

Ultimativer Stolperstein für das Cloud Computing für viele Forschungsprojekte ist aber wohl die österreichische Genehmigungspflicht für internationalen Datenverkehr und der damit verbundene Zeit- und Kostenaufwand: Wesen des Cloud Computing ist ja die physische Verteilung der Daten auf den gesamten Globus. Das Datenschutzgesetz schreibt für einen Datenexport nach außerhalb der EU eine Vorab-Genehmigungspflicht durch die Datenschutzkommission vor – ein meist mona-

telang dauernder Prozess, der überhaupt nur durch umfassende vertragliche Regelungen zwischen Anbieter und Cloud-Anbieter zu einem positiven Ende kommen kann; internationale Cloud-Anbieter sind über diese österreichische Besonderheit meist „not amused“.

Mittelweg als rechtspolitischer Wunsch

Durch das Cloud Computing stehen sich die „technische Idee“ der unendlichen globalen Ressourcen und die „rechtlichen Idee“ der Daten-Transparenz und -Kontrolle gegenüber und viele behaupten, dass dies derzeit nicht bzw schwer in Einklang zu bringen sei. Nach Ansicht des Autors sollten beide Seiten „die Kirche im Dorf lassen“: Die Techniker sollen angemessene Sicherheit und Rechtsdurchsetzung ermöglichen und die Juristen sollen Cloud Computing nicht schon vor dem Anfang ins „rechtliche Aus“ stellen.



Dr. Max W. Mosing, LL.M., LL.M., ist Rechtsanwalt und Partner der Gassauer-Fleissner Rechtsanwälte GmbH, Wallnerstraße 4, 1010 Wien, www.gassauer.at.

Kontakt: m.mosing@gassauer.at,
Tel.: +43 (0)1/20 52 06-150.