

Cloud Computing – Chancen und Gefahren

Vortrag anlässlich der Konferenz des Verbandes Europäischer Rechtsanwaltskammern 2012 in Brüssel:

Was ist Cloud Computing?

Cloud Computing ist zwar vielen der hier Anwesenden als Begriff wahrscheinlich schon bekannt, jedoch möchte ich dies trotzdem kurz nochmals darlegen. Im Rahmen der Weiterentwicklung des Internets und der damit zusammenhängenden Technologien wurde der Begriff Cloud Computing entwickelt. Darunter versteht man grob zusammengefasst und vereinfacht ausgedrückt, die Auslagerung von IT-Services ins Web und gleichzeitig die Bereitstellung und Nutzung von IT-Infrastruktur über dieses System. Der extremste Ausbau des Cloud Computings resultiert darin, dass der einzelne Nutzer nur noch einen Internetzugang hat und seine gesamte IT-Infrastruktur, wie benötigte Programme, Daten, Speicherungen und Daten im Cloud oder der sogenannten Wolke enthalten sind. Dies bringt für den einzelnen Nutzer Nutzen und Vorteile, allerdings birgt dies auch zahlreiche Gefahren. Zwischenzeitlich haben sich drei Typen entwickelt und wurden auch mit Namen versehen, um die verschiedenen Möglichkeiten der Nutzung zu definieren:

IaaS oder Infrastructure as a Service

Hier wird die komplette Infrastruktur, wie Serverspeicher, Netzwerkdatenbanken zur Verfügung gestellt – quasi die komplette Auslagerung der Computerinfrastruktur.

PaaS oder Platform as a Service

Dies dient primär dazu, um über eine gemeinsame Plattform Software zu entwickeln, die in der Folge über das System des Clouds Dritten angeboten wird.

SaaS oder Software as a Service

Hier wird primär die Software, die erforderlich ist durch die Wolke zur Verfügung gestellt, was dazu führt, dass man keine eigene Software mehr über Lizenzen zu erwerben hat.

Der Vorteil all dieser Modelle ist, dass der einzelne Benutzer wesentlich weniger in den Aufbau und die Erhaltung einer einzelnen Infrastruktur investieren muss und nach Bedarf und Nutzung die beanspruchte Infrastruktur, Programme und usw. bezahlt. Gleichzeitig steht ihm auf diese Art und Weise immer die neueste Software zur Verfügung. Weiters hat der Nutzer die Möglichkeit, egal wo er sich befindet, sobald er einen Internetzugang hat, auf die entsprechenden Daten zu greifen.

Der Vorteil ist daher ein voraussichtlich wesentlich billigeres und flexibleres System als die klassische Computeranlage im Büro, die noch dazu unabhängig von der Örtlichkeit jederzeit benutzt werden kann.

Mit diesem Vorteil sind jedoch auch Risiken verbunden, die man nicht außer Acht lassen darf und die insbesondere in jenen Berufen, die auch gegenüber Dritten Geheimhaltungs- und Verschwiegenheitspflichten haben, erhöhte Risiken und Gefahren in sich bergen. Neben einigen anderen Berufen hat auch insbesondere die Rechtsanwaltschaft und der einzelne Rechtsanwalt umgehende und umfassende Geheimhaltungs- und Verschwiegenheitsverpflichtungen zugunsten seines Mandanten. Dies wurde ich ersucht hier näher zu erläutern, wobei ich primär auf das IssA – System Infrastructure as a Service – eingehe, da hier die extremsten Auswirkungen bestehen.

Vorausschicken darf ich noch, dass die sogenannte Wolke nicht bedeutet, dass die Daten irgendwo als Wolke oder in den Wolken herumschwebt, sondern dass die Daten auf diversesten Servern von jenen Firmen, die diese Service anbieten, gelagert sind, auf die man zurückgreifen kann. Um bei dieser Cloud mitmachen zu können, schließt man mit einem dieser Anbieter einen Vertrag in dem Umfang ab, in dem man die Dienste dieser sogenannten Wolke in Anspruch nehmen möchte, de facto seinem Anbieter. Die Wolke ist eine Art Auslagerung oder Out-Sourcing seines IT-Betriebes und ist man daher als Rechtsanwalt gezwungen, sich mit den Konsequenzen auseinander zu setzen, die die Auslagerung von Daten mit sich bringt. Gleichzeitig ist die sogenannte Wolke eine nicht an den Landesgrenzen endende Wolke, sondern teilweise weltweit verfügbar und daher mit zahlreichen grenzüberschreitenden Rechtsfragen konfrontiert, wobei ich hier auf die Probleme der Rechtsanwälte eingehen möchte und den normalen Datenschutz, diese Frage stellt sich nämlich auch, ausblende.

In den einzelnen Jurisdiktionen gibt es äußerst unterschiedliche Regelungen über die anwaltschaftliche Verschwiegenheitspflicht und das Recht auf Geheimhaltung von Informationen. Bereits jetzt, ohne Cloud, muss man sich als Rechtsanwalt, sobald man grenzüberschreitend tätig ist, mit dieser Problematik auseinandersetzen. Einheitliche Regelungen oder – mit Ausnahme von Empfehlungen – grenzüberschreitende Bestimmungen gibt es derzeit nicht und ist auch nicht absehbar, dass sich solche Regelungen in naher Zukunft entwickeln werden. Ich muss daher bei der Beurteilung, ob ich als Rechtsanwalt an solchen neuen Technologien teilnehmen kann, von der Rechtssituation des eigenen Landes ausgehen und mache ich dies am Beispiel Österreichs.

Die österreichische Verschwiegenheitspflicht ist in einigen Fällen sehr stark und für den Anwalt und den Klienten günstig geregelt, in anderen Bereichen gibt es in anderen europäischen Ländern striktere Vorschriften. So gibt es beispielsweise in Frankreich das Privileg der Anwälte einen sogenannten und als solchen deklarierten Anwaltsbrief keinesfalls in Prozessen oder ähnlichen vorlegen zu müssen. Als österreichischer Anwalt habe ich mich jedoch nur nach der österreichischen Regelung zu orientieren. Es muss daher auch bei der Wolke gewährleistet sein, dass ausschließlich österreichisches Recht in Bezug auf das Anwaltsrecht anwendbar ist. Im Rahmen des Datenschutzes gibt es beispielsweise in der Datenschutzrichtlinie eine Sitzstadtregelung, im Anwaltsrecht ist dies noch nicht gegeben, insbesondere auch dann, wenn es nicht um reine Verschwiegenheitsfragen geht, sondern beispielsweise um strafrechtliche relevante Tatbestände bei einem Klienten.

Im Rahmen des Cloud Computing IaaS schließt man mit einer Servicefirma einen Vertrag ab, mit dem diese Speicher zur Verfügung stellt. Wo diese Speicher platziert sind, ist verschieden. Es gibt Anbieter, die ausschließlich national ihre Server aufgestellt haben, beispielsweise für österreichische Anwälte nur in Österreich. In wie weit dies von diesen Firmen auch beibehalten wird und beibehalten werden kann, ist noch fraglich, da die Wolke ja geografisch nicht beschränkt ist. Größere Firmen haben ihre Server jedoch in zahlreichen Ländern aufgestellt und sind auch nicht in der Lage oder nicht Willens, Daten eines Kunden ausschließlich auf nationalen Servern abzulegen. Dies kann zu dem Problem führen, dass Behörden von Drittländern – nicht nur außerhalb sondern auch innerhalb der EU – die Möglichkeit haben im Zuge von primär Strafverfahren, Kartellverfahren auf Daten zu greifen, die auf Servern außerhalb der eigenen Jurisdiktion gespeichert sind und nach den Vorschriften dieser Länder die Daten auch auswerten können.

Als Beispiel: In England sind Anwälte sehr weitgehend verpflichtet, Steuervergehen auch eigener Mandanten bei den Behörden anzuzeigen, widrigenfalls sie sich selbst strafbar machen. In Österreich gibt es noch das Recht, dass auch jemand, der strafbare Handlungen getätigt hat, die für mich selbstverständliche Möglichkeit gegeben ist, Beratung einzuholen und beraten zu werden, ohne Gefahr zu laufen, dass er durch Einholung dieser Beratung, den Behörden ausgeliefert wird. sicher. Sollte daher im Zusammenhang mit einem Verfahren in England solche Taten ans Licht kommen, wäre möglicherweise der österreichische Anwalt in England strafbar bzw. würde dies jedenfalls zu einer Strafverfolgung des Mandanten führen, auch wenn diese Daten im Zuge eines komplett anderen Verfahrens ans Licht kämen.

Ein weiterer Aspekt ist die Datensicherheit. Wenn ich als Nutzer von überall Zugang zu meinen Daten habe, ist die Gefahr, dass ein Dritter dies auch hat, wesentlich größer. Erst letzte Woche ist eine Studie des deutschen Fraunhofer-Institutes veröffentlicht worden, dass die wesentlichen Cloud-Anbieter überprüft und festgestellt hat, dass bei keinem einzigen Anbieter, auch nicht bei den großen sogenannten renommierten Anbietern, die Datensicherheit gewährleistet ist und die eigentlich geforderten Standards eingehalten werden. Es besteht sohin eine erhöhte Gefahr des Zugriffes Dritter auf die Daten.

Ein weiterer Aspekt ist, in wie weit ich über meine Daten noch frei verfügen kann oder ob auch Dritte diese auch nutzen können. Gerade erst ist Facebook an die Börse gegangen und hat auch ihr Geschäftsmodell vorgestellt. Wesentlicher Teil des Geschäftsmodelles ist nicht Zurverfügungstellung einer kostenlosen Plattform, wo einzelne miteinander kommunizieren können, sondern die Auswertung und Verwertung der dabei gesammelten Informationen. Probieren Sie dies auch einmal selbst aus, zB sollten Sie Kunde bei Amazon sein, schauen Sie welche Werbungen und Buchvorschläge aufscheinen, wenn sie auf die Einstiegsseite von Amazon gehen und wenn dies Bekannt mit anderen Interessen tun. Die Angebote richten sich sehr oft nach dem zuletzt gefragten Büchern und weiteren Interessen, die durch diese Computerfirmen herausgefiltert wurden. Hier besteht natürlich sehr stark die Gefahr, dass auch die Daten der Rechtsanwaltskanzlei für solche Zwecke herangezogen werden.

Auch im Zuge der Hoheit über die Daten ist sicher zu stellen, dass diese Daten verfügbar sind und zwar solange dies rechtlich in der einzelnen Jurisdiktion erforderlich ist. Österreichische Anwälte haben eine Nachhaftung bis zu 30 Jahren, steuerliche Unterlagen müssen bis zu 20

Jahre aufgehoben werden. Die Aufzeichnung und Zurverfügungstellung dieser Daten für diesen Zeitraum muss jedenfalls gewährleistet sein. Hier werden einige der Anbieter wahrscheinlich nicht mithalten können. Ein weiteres Kriterium ist die Transferierbarkeit der Daten zu einem anderen Betreiber. Der Wechsel der Anbieter muss auch unter Mitnahme sämtlicher Daten gewährleistet sein. Dies muss einerseits bei einer Kündigung durch den Rechtsanwalt möglich sein, als auch, was möglicherweise gravierender ist, bei Übernahme der Firma durch eine andere oder aufgrund eines Konkurses der Gesellschaft.

Obwohl die Wiener Rechtsanwaltskammer neuen technischen Errungenschaften sehr offen gegenübersteht und sich auch bemüht, diese zu fördern, auch im Zusammenhang mit der öffentlichen Hand, ich darf hier auf unsere in vielen Bereichen schon elektronisch abgewickelten juristischen Grundbereiche verweisen, elektronisches Grundbuch, Firmenbuch, elektronischer Rechtsverkehr, elektronische Urkundensammlung etc., ist es aufgrund der derzeitigen gegebenen Rechts- und Sachlage aus Ansicht unserer Kammer nicht empfehlenswert und rechtlich wahrscheinlich gar nicht möglich, sich voll der Wolke anzuliefern. Eine teilweise Nutzung der Wolke als technischer Support bzw. Zurverfügungstellung von Programmen wird unter gewissen Voraussetzungen möglich sein. Die Möglichkeit der Einführung einer privaten Wolke wird noch zu überprüfen sein, wobei hier auch der technische Aufwand und die Kosten-Nutzen-Rechnung erst zu erfolgen hat. Erstrebenswert wäre es im ersten Schritte einmal europaweite, im nächsten Schritt möglicherweise weltweite Regelungen herbeizuführen, die es nicht nur Anwälten, sondern auch vielen anderen Berufsgruppen ermöglicht, dieses Instrument der Wolke zu nutzen, ohne dabei auf ihre nationalen Rechte und Pflichten vergessen zu müssen und diese nicht einhalten zu können. Hier ist die Europäische Gemeinschaft, wie auch die Internationale Gemeinschaft gefordert.

Guidelines oder Weisungen hat die Rechtsanwaltskammer Wien bisher nicht in diesem Sinne herausgebracht, jedoch auf die Risiken hingewiesen, ebenso dass die Auslagerung von Daten und darum geht es im Prinzip im Wesentlichen, jedenfalls nur im Einklang mit der Einhaltung der österreichischen Vorschriften erfolgen kann.