Security Journal GAI Netconsult GmbH Juni 2011

Rechtsfragen des Cloud-Computing

von Dr. Jens Bücking und Ulrich Emmert, Partner der Kanzlei esb Rechtsanwälte

A.
Cloud-Computing

Cloud-Computing zeichnet sich dadurch aus, dass der Nutzer auf seine digitalen Daten von überall unkompliziert zugreifen kann, und zwar ohne die oft komplexe Installation von Software und ohne regelmäßig neue, leistungsfähigere Hardware anschaffen zu müssen. Dank der immer schneller werdenden Datenverbindungen werden Informationen, die der Nutzer zur Verfügung haben muss, nicht mehr lokal oder innerhalb eines Firmennetzes abgelegt, sondern auf Zentralservern im Internet. Auch ganze Programme können so über den Fernzugriff genutzt werden. Sie werden einfach im Browser ausgeführt und nehmen dem heimischen oder dem Arbeitsplatz-PC insbesondere die oft zum Hardwareaustausch führende, zeitaufwändige Rechenleistung ab.

Oft entfallen auch lästige Updates, da die dergestalt ferngenutzte Software stets in aktuellster Version vorhanden ist. Auch die Notwendigkeit für eine lokale IT, bestehend aus Servern, Netzwerk- und Datenbanksoftware etc., entfällt. Unternehmen können durch den Wegfall von Rechenzentren Fläche, Wartungsleistungen, Hardware- und Softwarekosten sowie natürlich auch Strom- und Kühlungskosten einsparen. Da die Server-Farmen von beispielsweise Amazon, Google oder auch künftig Microsoft mit dem Office-Programm Azure nur tatsächliche Zugriffe, also die wirklich in Anspruch genommene Serverleistung abrechnen, liegt hierin eine interessante Möglichkeit der Kostentransparenz und Kostensteuerung. Unnötige Kosten wegen ungenutzter Ressourcen gehören im Cloud-Computing der Vergangenheit an.

B.
Rechtsfragen des Cloud Computing

Die neue Technik hat jedoch auch juristische Implikationen, namentlich Fallstricke im Bereich des Vertragsrechts und insbesondere des internationalen Rechts (wegen der oft für den Nutzer intransparenten und

grundsätzlich auch technologisch nicht klar bestimmbaren Übermittlungen von Daten über Grenzen hinweg und deren Aufbewahrung an einem nicht definierten Ort irgendwo auf einem Server außerhalb der Rechtsordnung des Nutzers). Angesprochen sind insbesondere die Rechtsaspekte

- Bereitstellung von Speicherplatz
- Softwareanwendungen
- Rechnerkapazitäten
- E-Mail-Dienste
- Datenübermittlung.

Die Fehler früherer IT-Outsourcing- und Applikationsdienste-Provider-Verträge sollten im neuen Rechtsgebiet des Cloud Computing vermieden werden. Die Ausgangsfragen lauten daher:

- Wie sensibel sind meine Daten?
- Wie sicher sind diese Daten?
- Welche Leistungen muss der Provider bei Vertragsende erbringen?
- Kann der Vertragspartner unbeschränkt Subunternehmer einsetzen?

Das Cloud-Computing ist eigentlich keine bestimmte technische Lösung, sondern besteht aus einer Vielzahl von Komponenten, also virtualisierten IT-Dienstleistungen wie ASP, SAAS oder Managed Services und Hosting Services, die ausgelagert werden, um betriebliche und projektbezogene Services abzudecken. Die Vertragsgestaltung setzt daher an den bekannten Regelwerken aus Outsourcing- und ASP-Verträgen an, die in der Regel individuell ausgehandelt wurden und nur selten dem AGB-Recht unterfallen. Die vertragsrechtlichen Risiken liegen namentlich im Fehlen allgemeinverbindlicher oder gängiger, branchenüblicher Leistungsstandards. Daher ist es wichtig, dass der Vertrag eine besonders sorgfältige Leistungsbeschreibung enthält.

Die unternehmerischen Kunden sollten hier ihren Fokus auf kritische Geschäftsprozesse legen, wenn diese in die Cloud verlagert werden sollen, da dies einhergeht mit einer hohen Abhängigkeit betriebskritischer und besonders verwundbarer Geschäftsprozesse von einem externen Anbieter, der also durch strenge und mit jederzeitigen Audit- und sonstigen Kontrollmaßnahmen zugunsten des Auftraggebers flankierte und

sanktionierte Bestimmungen engmaschig vertraglich angebunden sein sollte, etwa indem geregelt ist

- welche Maßnahmen der Auftragnehmer beim DR-/BC- und Eskalationsmanagement zu treffen hat,
- welche Vergütungskriterien zugrunde zu legen sind, sowie
- welche Regelungen über Teilleistungen und deren Kündigung gelten.

Zu beachten ist, dass ähnlich wie beim Outsourcing die – insbesondere haftungsrechtliche – Verantwortlichkeit durch die Delegierung von bestimmten technisch- administrativen Leistungen an den externen Anbieter nicht auch gleichzeitig zu einer juristischen Verantwortungsverlagerung führt. Die gesetzliche Verantwortung, namentlich die kaufmännische Sorgfalts- und Organisationspflicht in Bezug auf ein Risiko- und Informationsmanagement und dessen Kontrolle, verbleibt als Maßnahme der Corporate Governance bei der Unternehmensführung. Die konventionellen Vereinbarungen zur Überprüfung des Dienstleisters, meist in Anlehnung an die Anlage zu § 9 BDSG formuliert, wie etwa Auditrechte zur Prüfung der Zutritts-, Zugangs- und Zugriffskontrolle, müssen bei einer Cloud-Struktur notwendig ins Leere laufen, weswegen eine Anpassung an die tatsächlichen virtuellen Verhältnisse erforderlich ist. Die Maßnahmen der IT-Compliance, die sonach vertraglich auf den Cloud-Anbieter übertragen werden müssen, sind daher insbesondere

- die Pflicht zur Geheimhaltung,
- die Implementierung verbindlicher Sicherheitskonzepte,
- die Einhaltung von IT-Notfallkonzepten und
- Pflichten im Reporting.

Es zeigt sich, dass der bestehende Rechtsrahmen wieder einmal der technischen Entwicklung hinterher hinkt. Vor allem im internationalen Leistungsumfeld entstehend durch die ungeregelten und durch die bestehenden Gesetzinstrumentarien nur mühsam – zumeist über die Rechtsprechung – auszufüllenden Lücken.

C.
Rechtliche Regelungsdetails

Angesprochen ist insbesondere – abermals – die Frage des anwendbaren Rechts für die Vertragsgestaltung, das Urheberrecht, der Datenschutz, die IT-Sicherheit und die Compliance.

Für Cloud-Dienste gilt grundsätzlich das Mietrecht, da hier eine Nutzung vieler, meist weltweit verteilter Dienstleister und deren Angebote zugrunde liegt. Es empfiehlt sich, das zugrunde liegende Vertragsverhältnis ausdrücklich einer bestimmten Rechtsordnung zuzuweisen durch entsprechende Rechtswahl- und Gerichtsstandsvereinbarung.

Des Weiteren sind klare Vorgaben in Gestalt von SLRs und – in deren Umsetzung – SLAs unabdingbar.

Gegebenenfalls erforderliche Rechte Dritter sollten zuvor recherchiert werden und sodann in den Vertag mit einfließen, ggf. über eine entsprechende Rechteinräumung seitens des Dritten/Rechteinhabers.

Wichtig ist auch eine flächendeckende Vereinbarung von verbindlichen Corporate Rules oder der EU-Vertragsklauseln zum Datenschutz, zur Datensicherheit und zur Datenübermittlung ins Ausland. Im Rechtsverkehr mit den USA besteht zudem die Option der Safe Harbor Rules.

Vertraglich sind die Betriebssicherheit, die Datensicherheit, der Datenschutz und die dazugehörigen Kontrollrechte in einer möglichst detaillierten Form aufzunehmen.

Gleiches gilt für ein Berechtigungskonzept und, für den Fall der Offenbahrung geheimhaltungsbedürftiger Daten durch technische Fehler oder sonstiges Fehlverhalten auf Seiten des Providers, entsprechende Vertragsstrafenregelungen.

a) Mietrecht für Fragen der Softwareüberlassung

Da vom Blickwinkel des deutschen Rechts grundsätzlich Mietrecht gilt, würde der Cloud-Anbieter seinen Kunden grundsätzlich eine hundertprozentige Verfügbarkeit garantieren müssen. Dies lässt sich jedoch technisch nicht abbilden. Daher kann nur eine detaillierte

Leistungsbeschreibung die Gesetzeslage an die faktischen Gegebenheiten anpassen.

b) Urheberrecht

Ähnlich problematisch ist die Frage im Urheberrecht, insbesondere wenn die Inanspruchnahme Cloud-basierter Dienste als urheberrechtlich relevante Nutzungshandlung zu qualifizieren ist. Anbieter wie Anwender riskieren hier, die Urheberrechte Dritter, insbesondere von Softwareherstellern, zu verletzen. Dies betrifft wiederum den zuvor bereits angesprochenen Aspekt der vertraglichen Rechteeinräumung durch den Dritten.

c) Datenschutzrecht

aa) deutsches Datenschutzrecht

Des Weiteren sind Fragen des Datenschutzes angesprochen. Im internationalen Leistungsgeflecht bereitet schon die Bestimmung des jeweils anwendbaren nationalen Datenschutzrechts Probleme. Die Rechtmäßigkeit aus Sicht des deutschen Rechts bestimmt sich nach den Regelungen zur AUfrtagsdatenverarbeitung in § 11 Bundesdatenschutzgesetz. Hierbei gestaltet sich jedoch das weltweite Verteilen von Daten als immanenter Bestandteil Cloud-basierter Dienste schwierig. Ähnlich wie beim SAAS-Modell, wo die Anwendung und Datenbank beim Anbieter läuft, muss der Kunde seine Daten dem Anbieter anvertrauen, beispielsweise auch Mitarbeiterdaten oder Kundendaten sowie ggf. Betriebsgeheimnisse. Die Daten gehören weiterhin dem Kunden, der Anbieter hat jedoch die einschlägigen Datenschutzvorschriften zu beachten. Dies alles ist detailliert in einem Vertrag über die Auftragsdatenverarbeitung zu regeln. Dazu gehört auch, dass festgelegt wird, unter welchen Bedingungen der Anbieter und der Auftragnehmer beispielsweise externe Betreiber von Rechenzentren einschalten darf, sowie vertragliche Verpflichtungen für den Anbieter zu den von ihm konkret zu treffenden technischen und organisatorischen Maßnahmen zum Datenschutz. Das BDSG verlangt außerdem, dass sich der Auftraggeber von der Einhaltung der vereinbarten Maßnahmen überzeugt, was jedoch nur möglich ist, wenn entsprechende Audit-Rechte vertraglich vereinbart sind.

Der Auftraggeber von Cloud-Diensten ist zur Vorabkontrolle der Datenschutzkonformität und zur regelmäßigen Kontrolle während des Betriebs verpflichtet. Dabei sind bei Cloud-Diensten insbesondere folgende Punkte zu prüfen, zu überwachen und/oder zu kontrollieren:

1. Analyse der virtualisierten Dienste und Systeme
2. Lückenlose Kontrolle der Zugriffsberechtigungen auf virtualisierte Systeme
3. Kontrolle des sicheren Betrieb des Hostsystems und Absicherung der Gastsysteme untereinander, gegebenenfalls durch Vorlage von Zertifikaten oder anderen Prüfungsergebnissen durch den DIenstleister oder Vereinbarung von Inspektionsrechten
4. Changemanagement für virtualisierte Systeme
5. Verfügbarkeit von Backups, z.B. von Snapshots virtualisierter Systeme zur Wiederherstellung
6. Regelmäßige Kontrolle der Virtualisierten Dienste und Datenträger
7. Aufnahme der virtualisierten Systeme in die Sicherheitspolicy des Auftraggebers

Mit der Entwicklung, Prüfung und Freigabe von Cloud-Systemen ist die Überwachungspflicht aber noch nicht beendet. Konfigurationen und Einstellungen der meisten Komponenten eines Rechenzentrums oder Servernetzwerkes verändern sich innerhalb weniger Wochen. Daher ist auch während des Betriebs eine regelmäßige Kontrolle mit Dokumentation nach § 11 Abs. 2 BDSG vorgeschrieben.

Vom Datenschutzrecht abgesehen ist angesichts der Komplexität heutiger Rechnernetze mit virtualisierten Umgebungen die regelmäßige Überwachung der Sicherheitsmaßnahmen, möglichst bei einem Verantwortlichen im Unternehmen, ohnehin Bestandteil der allgemeinen kaufmännischen aber auch behördlichen Sorgfalts-, Verkehrssicherungs- und Organisationspflicht.

Zu beachten ist auch, dass - durch die Datenschutznovelle vom September 2009 angestoßen - die Bundesregierung beabsichtigt, in Kürze einen weiteren Gesetzesentwurf vorzulegen, mit dem das BDSG um ein eigenständiges Kapitel zum Arbeitnehmerdatenschutz ergänzt werden soll, in dem sich Regelungen zum Datenschutz bei privater Internet- und E-Mail-Nutzung im Unternehmen und zur Datennutzung im Rahmen von Compliance-Prüfungen finden sollen. Unternehmen sollten daher in Abstimmung mit der

Personalabteilung Richtlinien erlassen, die die private Nutzung von Internet und E-Mail am Arbeitsplatz regeln.

§ 42 a BDSG, ebenfalls durch die Novelle vom September 2009 in das BDSG aufgenommen, normiert für Unternehmen die Pflicht, die Öffentlichkeit über die unrechtmäßige Kenntnis personenbezogener Daten zu informieren, zumindest dann, wenn schwerwiegende Beeinträchtigungen für die Reche oder schutzwürdige Interessen der Betroffenen drohen. Im Extremfall hat das betroffene Unternehmen durch halbseitige Anzeigen in mindestens zwei bundesweit erscheinenden Tageszeitungen über ein Datenleck zu informieren. Dies gilt es in jedem Fall schon aus Gründen des Verbrauchervertrauens und der Reputation zu vermeiden. Im Vorfeld muss es mithin verlässliche Prozesse geben und es müssen Verantwortliche benannt werden, die einen unternehmensweiten Datenschutz effektiv stützen. Dies kann nur gelingen durch entsprechende Risikoanalysen und eine umfassende, zusammen mit der hauseigenen IT-Abteilung, dem Datenschutzbeauftragten, dem Compliance-Beauftragten und ggf. externen Dritten aus dem juristischen und technischen Umfeld einzugehende Kooperation gelingen, in deren Zuge eine entsprechende IT-Sicherheitsrichtlinie erlassen wird, die fortan als Handlungsanweisung dient.

Nach § 4 BDSG müssen alle vertraglichen Vereinbarungen, bei denen personenbezügene Daten betroffen sind, schriftlich geschossen werden.

bb) europäisches Datenschutzrecht

Zusätzliche Anforderungen gelten, wenn der SAAS-Anbieter seinen Sitz außerhalb der EU hat oder die Daten dort in einem Rechenzentrum verarbeitet. Es muss dann sichergestellt sein, dass beim Anbieter ein ausreichendes Datenschutzniveau sichergestellt ist. Für bestimmte Länger wie die Schweiz oder Kanada hat die EU-Kommission entschieden, dass das Datenschutzniveau dort ausreicht. US-Anbieter können durch eine sogenannte Safe-Harbor-Zertifizierung ein angemessenes Datenschutzniveau sicherstellen. Zu achten ist auf jeden Fall darauf, dass der SAAS-Vertrag bestimmt, dass der Anbieter seine Zertifizierung, die jedes Jahr zu erneuern ist, aufrecht erhält und die Daten auch tatsächlich in jenem sicheren Hafen liegen. Die Zertifizierung kann nämlich auf bestimmte Arten von Daten beschränkt sein. Eine weitere Möglichkeit zur Sicherstellung eines angemessenen Datenschutzniveaus liegt in der Vereinbarung bestimmter

Standardklauseln, die die EU-Kommission veröffentlicht hat. Gerne weichen Anbieter von unliebsamen Regeln ab. Solche Abweichungen sollten jedoch in Zweifelsfällen mit der zuständigen Datenschutzbehörde, dem betrieblichen Datenschutzbeauftragen und einem Rechtsvertreter geklärt werden. Professionelle Anbieter von SAAS-Lösungen heben sich durch vorbildliche Regelungen zum Datenschutz hervor und gehen mit dem Datenschutzanliegen ihrer Kunden professionell um.

Besonders wichtig ist auch die Dauer der Vertragsbindung. Bei längeren Laufzeiten sollte eine nutzungsabhängige Vergütung ohne die Möglichkeit zur flexiblen Reduzierung des Nutzungsumfangs vorgesehen sein. Wichtig ist auch vertraglich festzulegen, in welchem Zeitrahmen und unter welchen Bedingungen, insbesondere zu welchen Kosten, am Ende der Laufzeit die Daten zurück übertragen werden und in welchem Format.

d) Schutz von Betriebsgeheimnissen

Zu guter Letzt ist das Kernproblem von SAAS- und Cloud-basierten Verträgen der Geheimnisschutz. Werden solche Dienste in Anspruch genommen, lagert der Auftraggeber häufig unternehmenskritische Daten, beispielweise solche mit Personenbezug oder Betriebsgeheimnisse aus, oft ohne zu wissen, auf welchen Servern, an welchen Orten und zu welcher Zeit welche Informationen von wem verarbeitet werden. Es gehört jedoch zu den Kardinalspflichten der Unternehmensführung, für einen angemessenen Schutz dieser Daten zu sorgen durch ein Risikovorsorgekonzept, ein Risikocontrolling und dessen interne Kontrolle und Dokumentation. Zum einen ist hier § 9 BDSG mit seiner Anlage 1 angesprochen, zum anderen aber auch die jederzeitige oder zumindest hinreichend gesicherte und vertragsstrafen- abgesicherte Verfügbarkeit der Systeme durch geeignete SLAs. (siehe auch unten zu Sicherheitsaspekten unter D)

e) Steuerrecht

Ferner hat das jeweilige Angebot Cloud-basierter Dienste die steuerrechtlichen Vorgaben zur Führung von Büchern und Aufzeichnungen zu erfüllen. Auch hier tritt der zwangsläufige Konflikt der gesetzlichen Vorgaben mit dem Grundprinzip des Cloud-Computing, der internationalen Flexibilität der Leistungserbringung auf. Entsprechendes gilt für die handelsrechtlichen Grundsätze ordnungemäßer Buchführung. Spezifische

vertragliche Vorkehrungen versprechen Abhilfe. Im Einzelfall ist das konkrete Leistungsangebot auch mit den regulatorischen Vorgaben für den Finanzbereich bzw. für Berufsgeheimnisträger aus den Bereichen Rechtsberatung, Gesundheitswesen oder Versicherungen abzugleichen. Ähnlich wie die steuerrechtlichen Vorgaben können diese der Nutzung Cloud-basierter Dienste entgegenstehen. So ist beispielsweise die Datenhaltung von kaufmännischen oder buchhalterischen Daten im Ausland nur unter engen Grenzen möglich und kann in jedem einzelnen Verletzungsfall Bußgelder von bis zu 250.000,00 EUR auslösen. § 146a der Abgabenordnung erlaubt erst seit Anfang 2009 die Speicherung von Buchhaltungsdaten in der Europäischen Union (EU) oder den Mitgliedsländern des Europäischen Wirtschaftsraums (EWR). Seit 1.1.2011 ist auch die Speicherung außerhalb des EWR erlaubt, sofern die Voraussetzungen des jederzeitigen Zugriffs der Finanzverwaltung gegeben sind. Dazu ist eine Bewilligung des Finanzamtes auf schriftlichen Antrag bei der Finanzverwaltung erforderlich. Weiter müssen die Buchführungsvorschriften insbesondere der §§ 140-147 AO peinlich genau eingehalten werden. Sind diese Voraussetzungen nicht mehr gegeben, kann die Finanzverwaltung die Rückführung der Daten nach Deutschland verlangen und dies bereits bei Verzögerung der Rückführung mit Bußgeldern bis zu 250.000 Euro belegen. Die neueste Fassungen des § 146 Abs. 2a und 2b AO lauten:

> *„(2a) Abweichend von Absatz 2 Satz 1 kann die zuständige Finanzbehörde auf schriftlichen Antrag des Steuerpflichtigen bewilligen, dass elektronische Bücher und sonstige erforderliche elektronische Aufzeichnungen oder Teile davon außerhalb des Geltungsbereichs dieses Gesetzes geführt und aufbewahrt werden können. Voraussetzung ist, dass*
>
> *1. der Steuerpflichtige der zuständigen Finanzbehörde den Standort des Datenverarbeitungssystems und bei Beauftragung eines Dritten dessen Namen und Anschrift mitteilt,*
>
> *2. der Steuerpflichtige seinen sich aus den §§ 90, 93, 97, 140 bis 147 und 200 Absatz 1 und 2 ergebenden Pflichten ordnungsgemäß nachgekommen ist,*
>
> *3. der Datenzugriff nach § 147 Absatz 6 in vollem Umfang möglich ist und*
>
> *4. die Besteuerung hierdurch nicht beeinträchtigt wird.*

Werden der Finanzbehörde Umstände bekannt, die zu einer Beeinträchtigung der Besteuerung führen, hat sie die Bewilligung zu widerrufen und die unverzügliche Rückverlagerung der elektronischen Bücher und sonstigen erforderlichen elektronischen Aufzeichnungen in den Geltungsbereich dieses Gesetzes zu verlangen. Eine Änderung der unter Satz 2 Nummer 1 benannten Umstände ist der zuständigen Finanzbehörde unverzüglich mitzuteilen.

(2b) Kommt der Steuerpflichtige der Aufforderung zur Rückverlagerung seiner elektronischen Buchführung oder seinen Pflichten nach Absatz 2a Satz 4, zur Einräumung des Datenzugriffs nach § 147 Abs. 6, zur Erteilung von Auskünften oder zur Vorlage angeforderter Unterlagen im Sinne des § 200 Abs. 1 im Rahmen einer Außenprüfung innerhalb einer ihm bestimmten angemessenen Frist nach Bekanntgabe durch die zuständige Finanzbehörde nicht nach oder hat er seine elektronische Buchführung ohne Bewilligung der zuständigen Finanzbehörde ins Ausland verlagert, kann ein Verzögerungsgeld von 2 500 Euro bis 250 000 Euro festgesetzt werden.“

e) Aufbewahrungs- und Löschungspflichten im In- und Ausland

Auch und gerade in Sachen Dokumentenmanagement bewegen sich die Unternehmen in einem Spannungsfeld. Zum einen besteht die gesetzliche Verpflichtung zur Aufbewahrung von Unterlagen aufgrund von handels- und steuerrechtlicher Bestimmungen über sechs respektive zehn Jahre, zum anderen müssen bestimmte Daten aufgrund datenschutzrechtlicher Vorgaben, insbesondere den Grundsätzen der Datenvermeidung und Datensparsamkeit, jedenfalls spätestens nach Ablauf der gesetzlichen Vorhaltefristen gelöscht und vernichtet oder zumindest gesperrt werden. Dies steht häufig im diametralen Gegensatz zu den Anforderungen des US-Rechts, das nicht selten Ausstrahlungswirkung auf inländische Unternehmen hat, beispielsweise im Rahmen von engen Geschäftspartnerschaften, oder wenn es sich um inländische Tochtergesellschaften US-börsennotierter Unternehmen handelt. Diese unternehmens- oder gesetzgeberischen Vorgaben aus den USA sind unabhängig von den hiesigen gesetzlichen Vorgaben zu sehen und sehen häufig unternehmensspezifische Löschungslücken und -tücken für elektronische Daten vor, mit der Folge, dass in diesem diametralen Gegensatz der Bruch von Gesetzesrecht

gleichsam vorprogrammiert ist. Daher sollten neben Richtlinien zur Archivierung auch solche zu systematischen Löschungen von Dokumenten verabschiedet werden.