Verträge über Cloud-Anwendungen

Joachim Dorschel, Bartsch Rechtsanwälte

Rechtsprobleme im Zusammenhang mit Cloud Computing sind unter IT-Juristen beliebt. Es zeigt sich aber, dass sich die vielfach beschworenen rechtlichen Groß-Risiken in der Praxis nicht realisieren. Weder gab es spektakuläre Gerichtsverfahren noch hohe Bußgelder von Aufsichtsbehörden.

Ehrlicherweise muss man sagen, dass viele der im Zusammenhang mit Cloud Computing diskutierten Fragen aus dem Bereich des klassischen IT-Outsourcing hinreichend bekannt sind und von der Praxis pragmatisch gelöst wurden. Die juristischen Herausforderungen liegen auf einer anderen Ebene: Die etablierten CloudAnbieter sind Großunternehmen, häufig mit Sitz in den USA. Die Vertragsbedingungen werden vom Anbieter diktiert, Verhandlungsspielraum ist so gut wie nicht vorhanden. Die von Juristen vielfach gegebenen Hinweise erweisen sich in dem Massengeschäft „Cloud Computing" oft als nicht praxistauglich. Cloud-Kunden müssen wissen, welche Risiken sie hierdurch eingehen und in welchen Bereichen durch die Gestaltung von Anwendungen und Verträgen mit Endkunden Risiken reduziert werden können.

Anwendbares Recht

Zum Wesen des Cloud Computing gehören vernetzte Rechner-Strukturen, bei denen der Sitz des Kunden, der Sitz des Anbieters und der Ort der Datenverarbeitung häufig auseinanderfallen. Bei solchen internationalen Sachverhalten stellt sich immer die Frage des anwendbaren Rechts. Sie lässt sich nicht einheitlich beantworten. Je nach Art der zu beurteilenden Fragestellung gelten unterschiedliche Regeln:

- Für den Vertrag und die dort geregelten Leistungsbeziehungen gilt das Recht desjenigen Landes, dessen Rechtsordnung im Vertrag gewählt wurde. In der Regel ist dies das Recht am Sitz des Anbieters. Solche Rechtswahl-Klauseln sind auch in Formularverträgen zulässig. Fehlt eine Rechtswahl, so gilt das Recht desjenigen Landes, zu dem der Vertrag den nächsten Bezug hat. Häufig kommt man auch hier zu einer Anwendung des Rechts am Sitz des Anbieters.
- Im Datenschutz-Recht ist keine Rechtswahl möglich. Grundsätzlich gilt das Recht des Landes, in dem die Datenverarbeitung stattfindet. Dies kann dort sein, wo der Server steht, oder dort, wo dieser gesteuert wird. Innerhalb der Europäischen Union wurde das Datenschutzrecht in weiten Bereichen harmonisiert. Hier gilt das Recht des Landes, in dem die verantwortliche Stelle ihren Sitz hat.
- Im Urheberrecht gilt das Recht desjenigen Landes, in dem der Rechts-Inhaber Schutz begehrt. Will ein deutscher Software-Hersteller verhindern, dass seine Software in einem Cloud-Rechenzentrum in Großbritannien betrieben wird, gilt britisches Recht.

Es liegt auf der Hand, dass sich im Einzelfall schwierige Abgrenzungsfragen stellen, etwa bei der Auslegung von Lizenzverträgen oder Vereinbarungen über die Auftragsdatenverarbeitung.

Regelungsbereiche und Service Levels

Verträge zwischen Cloud-Anbietern und Cloud-Kunden unterscheiden sich in ihrer Struktur nicht von herkömmlichen IT-Outsourcing-Verträgen. Ein wesentliches Element sind die in Service-Level-Vereinbarungen niedergelegten Vorgaben zu Verfügbarkeit, Performance und Skalierbarkeit des Dienstes. Aufgrund der technischen Gegebenheiten wäre zu erwarten, dass Cloud-Anbieter hier bessere Konditionen bieten als herkömmliche Hosting-Provider. Die Vertragspraxis erfüllt diese Erwartung bislang nicht.

Besondere Risiken ergeben sich für Unternehmen, die Cloud-Dienste selbst als Plattform für eigene Dienste (zum Beispiel Internet-Dienste) nutzen. Die Verträge der großen Cloud-Anbieter richten sich häufig nach US-amerikanischem Recht. Dort sind umfassende Haftungsausschluss-Klauseln üblich und wirksam. Ein deutscher Cloud-Kunde, der Leistungen gegenüber deutschen Endkunden anbietet, muss diese Leistungsbeziehung dem deutschen Recht unterstellen. Das deutsche Recht der allgemeinen Geschäftsbedingungen verhindert hier wirtschaftlich effektive Haftungsbeschränkungen. Es gilt sowohl im B2B- als auch im B2C-Bereich. Es entsteht ein Haftungsdelta zu Lasten des Cloud-Kunden, der die ihm auferlegten Haftungsbeschränkungen nicht an seine Endkunden weitergeben kann. Bei Cloud-basierten Internetdiensten, die hohe Haftungsrisiken bergen, kann dies ein Motiv sein, auf Anbieter zurückzugreifen, die bereit sind, Verträge nach deutschem Recht zu schließen.

Ort der Datenverarbeitung

Für den Cloud-Kunden ist es aus mehreren Gründen wichtig, den Standort der Cloud-Server festzulegen:

- Die Verlagerung personenbezogener Daten im Sinne des Bundesdatenschutzgesetzes (BDSG) in die Cloud setzt in der Regel eine Auftragsdatenverarbeitung nach § 11 BDSG voraus. Eine Auftragsdatenverarbeitung ist aber nur möglich, wenn die Datenverarbeitung innerhalb der EU oder des Europäischen Wirtschaftsraums stattfindet.
- Wenn steuerlich relevante Daten in die Cloud ausgelagert werden sollen, schreibt die Abgabenordnung eine Aufbewahrung im Inland vor. Eine Verlagerung in einen EU-Staat bedarf der Zu-

stimmung der Finanzverwaltung. Die Verlagerung in einen anderen EWR-Staat ist an weitere Voraussetzungen geknüpft. Unter anderem ist dann dem Finanzamt der Standort des Datenverarbeitungs-Systems zu nennen.

Viele Cloud-Anbieter haben diese Rechtslage bei ihren Angeboten berücksichtigt und ermöglichen eine vertragliche Fixierung des Rechners-Standorts. Für einen europäischen Cloud-Kunden ist eine Beschränkung der Datenverarbeitung auf das Gebiet der Europäischen Union immer vorzugswürdig.

Es ist umstritten, unter welchen Voraussetzungen eine Einbeziehung von Clouds in den USA zulässig ist. Die Probleme liegen auch hier im Bereich des Datenschutzrechts. In der Praxis finden sich hier Gestaltungen, bei denen das Europäische Regime über die Auftragsdatenverarbeitung durch Verträge nachgebildet wird. Auch ist ein Rückgriff auf die von der Europäischen Kommission veröffentlichten Standard-Vertragsklauseln möglich. Häufig schließen sich amerikanische Cloud-Anbieter dem SafeHarborAbkommen an. All diese Konstruktionen bergen jedoch ein Moment der Rechtsunsicherheit in sich, da die Zulässigkeit der Datenverarbeitung außerhalb der eigentlichen Auftragsdatenverarbeitung nach § 11 BDSG stets unter dem Vorbehalt einer Interessenabwägung zwischen dem Interesse der Betroffenen und dem verantwortlichen Unternehmen steht.

Abb. Fotolia

Kontrollrechte

Ein ungelöstes Problem ist die richtige Implementierung von Kontrollrechten in CloudVerträgen. Nach dem BDSG sind Kontrollrechte des Auftraggebers zwingender Bestandteil einer Vereinbarung über die Auftragsdatenverarbeitung. Die von Datenschützern verlangte Möglichkeit, dass der Auftraggeber die Datenverarbeitungs-Anlagen mit eigenen Augen beim Auftragnehmer inspiziert, geht an der Realität des Cloud Computing vorbei. Der Auftraggeber wird sich hier auf Zertifikate und die Ergebnisse von Audits verlassen müssen, die der Auftragnehmer selbst durchführt. Bei der Vertragsprüfung sollte der Cloud-Kunde darauf achten, dass sich der Cloud-Anbieter dazu verpflichtet, regelmäßige Kontrollen unabhängiger und anerkannter Stellen durchzuführen, dass diese Kontrollen auf Standards fußen, die auch in Deutschland etabliert sind, und dass dem Cloud-Kunden die Ergebnisse dieser Überprüfungen regelmäßig vorgelegt werden.

Zugriffsrechte auf Daten

Bei jeder Auslagerung von IT-Prozessen auf einen Dienstleister muss der Auftraggeber Herr seiner Daten bleiben. Dies gebietet das Datenschutz-Recht genauso wie eine sorgfältige Unternehmens-Organisation. Der Cloud-Kunde benötigt ein jederzeitiges und einredefreies Recht auf Herausgabe seiner Daten. Streitigkeiten über die Vergütung, die bei komplexen Vergütungsmodellen nicht auszuschließen sind, dürfen nicht zu einem Zurückberatungs-Recht des Cloud-Anbieters führen.

Software in der Cloud

Will ein Cloud-Kunde Software Dritter in der Cloud betreiben, so bedarf es einer genauen Prüfung der Lizenz-Bedingungen für diese Software. Häufig schreiben die Regeln der Software-Hersteller vor, dass die Server, auf denen die Software läuft, im Eigentum und unmittelbaren Besitz des Lizenz-Nehmers stehen müssen. Dies würde eine Verlagerung in die Cloud ausschließen. Allerdings sind solche Beschränkungen nach deutschem AGB-Recht nicht immer wirksam.

Fazit

Die rechtlichen Schwierigkeiten beim Bezug von Cloud-Diensten liegen vor allem in den unterschiedlichen Vorgaben und Gestaltungsmöglichkeiten in den verschiedenen Rechtsordnungen. Das Datenschutz-Recht und das Recht der allgemeinen Geschäftsbedingungen sind hier die wichtigsten Beispiele. Hiermit verbundene Risiken werden vor allem durch die Wahl eines renommierten und verlässlichen Cloud-Anbieters begrenzt. Auf rechtlicher Seite sollten die Vertragsbedingungen des Cloud-Anbieters kritisch dahingehend überprüft werden, inwieweit zwingende Vorgaben des deutschen Rechts berücksichtigt sind. Hier gibt es unter den etablierten Cloud-Anbietern erhebliche Unterschiede. Auswahlkriterien sind auch die Einhaltung in Deutschland anerkannter Standards und eine regelmäßige, unabhängige Überprüfung des Anbieters.

Joachim Dorschel
jd@bartsch-rechtsanwaelte.de