

Cloud Computing

Recht problematisch

[01.03.2012] Vor der Verlagerung von Anwendungen und Daten in die Wolke hat die öffentliche Verwaltung zunächst eine Reihe rechtlicher Herausforderungen zu klären. Neben dem Datenschutz sind beispielsweise auch vergaberechtliche Bestimmungen zu beachten.

Während viele Unternehmen es bereits selbstverständlich nutzen, steht die öffentliche Verwaltung in Deutschland dem Cloud Computing trotz erheblichen Kostendrucks noch verhalten gegenüber. Dies liegt wohl daran, dass sich Behörden bei der Nutzung von Cloud Computing mit zahlreichen rechtlichen Problemen konfrontiert sehen.

Cloud Computing bietet die klassischen Vorteile des Outsourcing, nämlich die Senkung von Ausgaben für Hard- und Software oder eigenes IT-Personal sowie die Nutzung des Know-hows Dritter, um ein höheres Qualitätsniveau zu erreichen. IT-Leistungen werden dabei in Echtzeit von einem Dienstleister als Service über das Inter- oder Intranet bereitgestellt und nach Nutzung abgerechnet. Um die weltweit vorhandenen Speicherressourcen bestmöglich zu nutzen, werden Daten seitens des Anbieters je nach Auslastung stets dort gespeichert, wo entsprechende Kapazität vorhanden ist. Ein Problem dieser Vorgehensweise ist, dass eine physische Lokalisierung der gespeicherten Daten seitens des Nutzers nicht möglich ist.

#titel+Sondervorschriften beachten#titel-

Die öffentliche Hand ist bei der Nutzung von Cloud-Angeboten neben dem normalen Datenschutz mit der Beachtung des Schutzes spezieller Daten konfrontiert. Während der neue Beschäftigtendatenschutz viel diskutiert wird, hat die öffentliche Hand zusätzlich etwa den Personalaktenschutz nach dem Bundesbeamtengesetz (§§ 106, 111, 114 BBG) zu beachten. Demnach dürfen Personalaktendaten an Dritte nur mit Einwilligung des betroffenen Beamten erteilt werden, es sei denn, „dass die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz berechtigter, höherrangiger Interessen der oder des Dritten die Auskunftserteilung zwingend erfordert.“ Sollen Daten aus Personalakten von Beamten in die Cloud ausgelagert werden, ist daher eingehend zu prüfen, ob und gegebenenfalls wie diesen Anforderungen entsprochen werden kann.

Eine weitere Sondervorschrift betrifft steuerpflichtige öffentliche Unternehmen. Für Finanzdaten von Steuersubjekten trifft die Abgabenordnung (AO) besondere Regelungen. Eine Verlagerung der elektronischen Buchführung in eine Cloud, die sich nicht in Deutschland befindet, ist gemäß § 146 Abs. 2a AO bewilligungspflichtig und an gewisse Voraussetzungen geknüpft.

#titel+Speicherung bedarf der Erlaubnis#titel-

Neben solchen datenspezifischen Sondervorschriften sind die Vorschriften des allgemeinen Datenschutzes zu beachten, wenn die öffentliche Verwaltung beabsichtigt, personenbezogene Daten an einen Cloud-Anbieter zum Zwecke der Speicherung zu übermitteln. Die Speicherung von Daten in der Cloud ist regelmäßig nur dann zulässig, wenn das Bundesdatenschutzgesetz (BDSG) oder eine andere Rechtsvorschrift es erlaubt (Erlaubnistatbestand) oder der Betroffene eingewilligt hat. Da eine Einwilligung jedoch stets widerruflich ist, ist es kaum ratsam, eine Datenverlagerung in die Cloud auf die Einwilligung der Betroffenen zu stützen. Eine genaue Prüfung der Erlaubnistatbestände ist daher meist unerlässlich. Verzichtbar ist ein Erlaubnistatbestand allerdings, wenn zwischen Cloud-Nutzer und -Anbieter eine

wirksame Vereinbarung zur privilegierten Auftragsdatenverarbeitung geschlossen wird (§ 3 Abs. 8 BDSG). Die Idee der Auftragsdatenverarbeitung ist, dass der Auftragnehmer unter bestimmten Voraussetzungen nicht Dritter im Sinne des Bundesdatenschutzgesetzes ist, sondern als verlängerter Arm der verantwortlichen Stelle beziehungsweise des Auftraggebers gesehen wird und mit ihr eine rechtliche Einheit bildet. Dies hat zur Folge, dass zwischen Auftragnehmer und Auftraggeber keine Übermittlung von Daten im Sinne des Bundesdatenschutzgesetzes stattfindet. Befindet sich die Cloud teilweise auch auf außereuropäischen Servern, dürfte diese Lösung jedoch ausscheiden: Vereinbarungen zur privilegierten Auftragsdatenvereinbarung sind nur innerhalb der EU und des Europäischen Wirtschaftsraumes möglich.

#titel+Verschlüsselung als technische Lösung#titel-

Die Zulässigkeit des Cloud Computing kann eventuell auch durch technische Lösungen erreicht werden. So wäre die Verschlüsselung von Daten denkbar, um Cloud Computing für die öffentliche Verwaltung unter datenschutzrechtlichen Aspekten handhabbar zu machen. Verschlüsselte Daten stellen aufgrund ihrer Unlesbarkeit für den Cloud-Anbieter und für Dritte keine personenbezogenen Daten mehr dar. Dies bedeutet allerdings, dass alle zu übermittelnden Daten bereits vor ihrer Übermittlung an den Cloud-Anbieter verschlüsselt werden müssten. Der damit verbundene technische Aufwand könnte sich jedoch eventuell rechnen, wenn eine solche Lösung die rechtmäßige Nutzung weltweiter Public Clouds ermöglichen könnte.

#titel+Vergaberechtliche Herausforderungen#titel-

Bei der Verlagerung von Daten in die Wolke sind darüber hinaus Bestimmungen des Vergaberechts zu beachten. Denn die Beauftragung eines externen Cloud-Providers stellt eine Beschaffung von Dienstleistungen dar und ist somit europaweit ausschreibungspflichtig, wenn der Schwellenwert von 200.000 Euro überschritten wird. Eine vergaberechtliche Privilegierung käme jedoch vor allem bei der Kooperation von Rechenzentren der öffentlichen Hand zur Erfüllung ihrer Aufgaben in Betracht. Eine Herausforderung bei der Ausschreibung von Cloud-Computing-Leistungen stellt die Tatsache dar, dass die Angebote der Provider am Markt nicht standardisiert sind und es vor allem für die öffentliche Hand wenig spezialisierte Angebote gibt. Darüber hinaus fehlen passende EVB-IT-Musterverträge, derer sich die öffentliche Hand bei einer Ausschreibung bedienen könnte. Dies hat zur Folge, dass die öffentliche Hand selbst die Verträge für die Ausschreibung vorgeben muss.

Cloud Computing stellt Behörden also vor eine Vielzahl rechtlicher Herausforderungen. Ob die öffentliche Verwaltung sich zulässigerweise des Cloud Computing bedienen darf, wird letztlich von der Wahl des Cloud-Computing-Modells, der Sensibilität der Anwendungen und Daten, die in die Wolke verlagert werden sollen, sowie den vertraglichen Beziehungen zum Cloud-Anbieter abhängen.

()

Stichwörter: IT-Infrastruktur, Recht