

US-Behörden dürfen auf europäische Cloud-Daten zugreifen

30.06.2011 /

Cloud-Anbieter wie Microsoft (Amazon, Google, Apple, etc.) müssen US-Strafverfolgungsbehörden Zugriff auf von Kunden gespeicherte Daten gewähren, [berichtet](#) der US-Branchendienst *ZDNet*. **Das betrifft auch in der EU ansässige Firmen und in europäischen Rechenzentren liegende Daten**, wie Microsofts britischer Direktor Gordon Frazer anlässlich der Markteinführung von **Microsofts Office 365** in London erklärte. Er antwortete damit auf die Frage, ob Microsoft zusichern könne, dass in seinen EU-Rechenzentren gespeicherte Daten Europa niemals verlassen könnten.

Da das Unternehmen seinen Firmensitz in den USA habe, müsse es die dortigen Gesetze befolgen, sagte Frazer. Das gilt insbesondere für den [Patriot Act](#), der US-Strafverfolgern weitreichende Zugriffsrechte auf Daten gibt. Frazer zufolge würden Kunden über die Herausgabe von Daten "informiert, wann immer das möglich ist". Eine Garantie dafür könne er jedoch nicht geben. Denn in den USA kann das FBI mit einem [National Security Letter](#) (NSL) ein Redeverbot ([Gag order](#)) für den Betroffenen aussprechen. In diesem Fall darf er nicht einmal sagen, dass er einen NSL erhalten hat.

Ein [Online-Dokument](#) in Microsofts "[Trust Center](#)" bestätigt Frazers Aussagen und stellt klar, dass es keineswegs nur um Verfahren im Zusammenhang mit dem Patriot Act geht. Dort heißt es: "Unter bestimmten Umständen kann Microsoft Daten ohne Ihre vorherige Zustimmung weitergeben. Dazu gehört die Befolgung rechtlicher Anforderungen." Fordere eine Regierungsstelle Daten eines Kunden an, werde man sie zunächst an diesen verweisen. Sei das Unternehmen [gezwungen](#), selbst zu antworten, werde es nur das zwingend Erforderliche herausgeben. Es wolle zudem alles "geschäftlich Vernünftige" unternehmen, um seine Kunden von dem Vorgang zu unterrichten – es sei denn, das ist rechtlich nicht möglich.

Nach Einschätzung von Thilo Weichert, Chef des [Unabhängigen Landesentrums für Datenschutz Schleswig Holstein](#) (ULD), steht eine solche Datenweitergabe aus dem EU-Gebiet heraus im Widerspruch zu europäischem Datenschutzrecht. Das Risiko einer Datenweitergabe stelle die Vertraulichkeit der auf Microsoft-Rechenzentren gehosteten Daten und Anwendungen infrage und entziehe bestehenden Verträgen zur Datenverarbeitungsdienstleistung die Grundlage. Nach Auffassung Weicherts lasse sich daraus einerseits ein Sonderkündigungsrecht ableiten, und andererseits schließe es Service-Provider wie den Office-365- und Windows-Azure-Anbieter Microsoft als Kandidaten für personenbezogene IT-Dienstleistungen aus. Unternehmen sollten sich daher bei der Nutzung von Cloud-Diensten für personenbezogene Daten ausschließlich auf rein europäische Service-Provider beschränken.

Wie schwierig die Rechtslage zu beurteilen ist, erfuhren wir per Nachfrage bei Microsoft Deutschland: Dort war ad hoc nur die Antwort zu erhalten, man befolge selbstverständlich alle geltenden Gesetze. Was dies allerdings bedeutet, wenn US-amerikanische und europäische Gesetze zu widersprüchlichen Anforderungen führen, konnte man bei Microsoft so schnell nicht kommentieren. Besser könnten Großunternehmen fahren, die zum Beispiel Microsoft Office 365 als Angebot des deutschen Providers T-Systems nutzen und sich dann darauf verlassen können, dass ihre Daten ausschließlich auf Servern unter Kontrolle dieses Providers gespeichert werden. ([ck](#))