Risiko für Unternehmen

Warum Steuerdaten in der Cloud gefährlich sind

Ein Gastkommentar von Falk Borgmann und Michael Brünker

Seit der Europäische Gerichtshof den EU-Beschluss zum Datenaustausch mit den USA gekippt hat, bewegen sich deutsche Unternehmen, die US-Cloud-Anbieter nutzen, im rechtsfreien Raum. Das bringt nicht nur Probleme mit dem Datenschutz – sondern auch mit dem Finanzamt.

14.12.2020, 16.02 Uhr

Die Bürotürme des Europäischen Gerichtshofs in Luxemburg: Unternehmen in Deutschland benötigen dringend Rechtssicherheit beim Umgang mit internationalen Cloud-Anbietern Foto: Arne Immanuel Bänsch/ DPA

Die Digitalpolitik der Europäischen Union gleicht einem Scherbenhaufen: Im Jahr 2000 kassierte der Europäische Gerichtshof (EuGH) den umstrittenen "Safe-

Harbour"-Beschluss, der es erlaubte, personenbezogene Daten von EU-Bürgern in den USA zu speichern und zu verarbeiten. Im Juli 2020 erklärten die Luxemburger Richter auch dessen informellen Nachfolger "EU-US Privacy Shield" für ungültig – mit dem Ergebnis, dass seither kein verlässlicher gesetzlicher Rahmen mehr für die Speicherung sensibler Unternehmensdaten in der Cloud-Welt der großen US-Anbieter mehr besteht. Beispielsweise ist die Übertragung personenbezogener Daten aus EU-Mitgliedstaaten nur in Länder erlaubt, deren Datenschutz ein dem EU-Recht vergleichbares Schutzniveau aufweist. In den USA ist dies nicht der Fall.

Die Nichtbeachtung des Datenschutzes ist einige deutsche Unternehmen bereits teuer zu stehen gekommen: Im Mai 2019 erhielt die Deutsche Wohnen einen Bußgeldbescheid über 14,5 Millionen Euro, 1&1 Telecom sollte im November desselben Jahres 9,55 Millionen Euro zahlen. (Das Bußgeld wurde nach einem Widerspruch um 900.000 Euro reduziert.) Die Begründung in beiden Fällen: ein Verstoß gegen die europäische Datenschutzrichtlinie GDPR.

Falk Borgmann

Falk Borgmann ist Technischer Senior Consultant der Deepshore GmbH, die sich als Brainpool und Entwicklungszentrum für neue Konzepte und Lösungen im Bereich verteilte Netze und Applikationen versteht. Als Compliance-Spezialist beschäftigt er sich seit Jahren mit verteilten IT-Systemen, neuen Technologien und gesetzlichen Compliance-Anforderungen. Zudem koordiniert er die Forschungskooperationen von Deepshore unter anderem mit dem Konrad-Zuse-Zentrum für Informationstechnik.

Die aktuelle Rechtslage ist eine Katastrophe für Unternehmen, die lange vor der EuGH-Entscheidung damit begonnen hatten, sensible Unternehmens- und Finanzdaten sowie oft auch die dazugehörigen kaufmännischen Anwendungen in die Clouds von US-Unternehmen wie Google, Microsoft oder Amazon zu verlagern. Ein Schritt, der technisch sinnvoll, ja sogar überfällig ist und der Logik des digitalen Wandels entspricht.

Das Fehlen einer rechtlichen Regelung kann zur juristischen Falle für die verantwortlichen Unternehmensführer werden – und zwar nicht nur wegen des Datenschutzes. Denn wenn steuerlich relevante Daten in eine US-Cloud übertragen wurden, bekommen sie womöglich auch Stress mit einem ganz anderen Akteur: dem Finanzamt. Die steuerrechtlichen Regularien der Abgabenordnung (AO) und zur ordnungsmäßigen Führung und Aufbewahrung von Büchern und elektronischer Daten (GoBD) legen

Michael Brünker

Michael Brünker, CTO bei Deepshore, ist für Design und Implementierung unternehmens-kritischer IT-Anwendungen verantwortlich. Sein Schwerpunkt liegt auf hochverfügbaren und skalierbaren Cloud-Architekturen mit einem speziellen Fokus auf besonders schützenswerte Daten. Er hat verteilte Infrastrukturen in regulierten Anwendungsfeldern entwickelt und federführend an der DIN-Spezifikation im Bereich Blockchain und Compliance mitgewirkt.

fest, dass solche Daten (und sämtliche Kopien davon) an einem klar benannten Speicherort liegen müssen – und zwar im Inland. Damit soll unter anderem sichergestellt werden, dass die Behörden jederzeit auf die Daten zugreifen und diese nicht manipuliert oder vorzeitig gelöscht werden können

Wer solche Daten außerhalb Deutschlands, zum Beispiel in einer internationalen Cloud, speichern will, kann zwar einen "Antrag zur Aufbewahrung und Führung von elektronischen Büchern und Aufzeichnungen außerhalb des Geltungsbereichs der Abgabenordnung" stellen. Solche Anträge aber wurden und werden regelmäßig abgelehnt, da der konkrete Speicherort in der Regel nicht exakt benannt werden kann oder die Sicherheits-, Integritäts- und Löschbarkeitsbedingungen für die deutschen Ämter nicht nachvollziehbar sind. Es geht dabei wohlgemerkt nicht um Fragen der Verschlüsselung, sondern um den physikalischen Zugriff auf die Speicherorte selbst.

Nachdem alle Versuche, den Datenverkehr zwischen der EU und den USA, rechtssicher zu regeln, gescheitert sind, ist fraglich, ob irgendeine Cloud, die von einem in den Vereinigten Staaten angesiedelten Unternehmen betrieben wird, diese Anforderungen erfüllen kann, sofern sie auf den Diensten von Microsoft Azure, Amazon AWS oder Google Cloud basiert. Das betrifft nicht nur die Angebote dieser Big Player selbst, sondern auch sämtliche als SaaS oder Managed Services verfügbaren Angebote anderer Provider, die im Hintergrund (und auf den ersten Blick nicht immer ersichtlich) die Cloud-Dienste der großen Drei nutzen. Daraus folgt: Der größte Teil des derzeitigen Cloudmarkts müsste vom deutschen Gesetzgeber in den Bereichen Steuerrecht und DSGVO eigentlich beanstandet werden.

Unternehmen im juristischen Niemandsland

Besonders bitter ist die Lage für Unternehmen, die bereits Tatsachen geschaffen haben, ohne dass sie jemals einen entsprechenden Antrag bei den deutschen Behörden gestellt zu haben. Sie bewegen sich im juristischen Niemandsland – und erfahrungsgemäß ist es nur eine Frage der Zeit, bis die zuständigen Finanzbehörden Prüfungslücken dieser Dimension für sich entdecken und nutzen.

Dabei hat die Unerbittlichkeit der Finanzbehörden in diesem Punkt einen durchaus nachvollziehbaren Hintergrund, der jedem betroffenen Unternehmen zu denken geben sollte: Die fraglichen Anbieter unterliegen nicht nur dem US-Cloud-Act, der amerikanischen Behörden den Zugriff auf aus dem Ausland stammende Daten gewährt. Sie haben zudem große Schwierigkeiten, Transparenz in der Datenspeicherung herzustellen – eine vollständig transparente Datenverwaltung ist für deutsche Behörden aber unabdingbar. Auch fehlen technische Garantien, zum Beispiel dafür, dass gelöschte Daten auch wirklich rückstandslos aus den weltweit verteilten Infrastrukturen verschwinden.

Was können Entscheider in deutschen Unternehmen in dieser Situation tun?

Zunächst müssen sie sich Klarheit verschaffen, welcher Cloud-Dienst tatsächlich hinter den von ihnen genutzten Anwendungen und Speichern steckt, wo er residiert und wie viel Transparenz er für seine Kunden und die deutschen Behörden bietet. Die meisten aktuellen Cloud-Lösungen der Hyperscaler werden diesen Stresstest vermutlich nicht bestehen.

Bleibt die Frage nach möglichen Alternativen – und die sind dünn gesät. Der vierte Mega-Player im Cloud-Business, Alibabas Aliyun-Plattform, entzieht sich als chinesischer Anbieter jedem europäischen Rechtsverständnis. Und die europäische Cloud-Alternative Gaia-X lässt weiter auf sich warten. Aktuell gibt es daher nur zwei sinnvolle Optionen: Entweder werden sensible Daten im Herrschaftsbereich des eigenen Unternehmens gehalten (wo übrigens dennoch der Architekturwandel auf Cloud-basierte Infrastrukturen möglich ist), oder man nutzt die Angebote nationaler oder europäischer Rechenzentrumsbetreiber – zum Beispiel dedizierte Server und Storages. Solche Partner können in aller Regel eine eindeutige Lokalisierung der Daten bieten und offerieren einen über jeden Zweifel erhabenen verteilten Zugriff mit Cloud-Technologien.

Es bleibt daher eine zentrale Aufgabe für die EU und die nationalen Gesetzgeber, im Datenaustausch mit den USA sichere rechtliche Grundlagen zu schaffen. Wann Gaia-X-basierte Standards und Services einsatzbereit sein werden, ist ungewiss. Aber sofern europäische Unternehmen im internationalen Wettbewerb nicht langfristig massiv benachteiligt sein sollten, wäre es wichtig, dass die europäische Cloud-Initiative ein Erfolg wird und der Gesetzgeber nicht nur den Datenschutz seiner Bürger regelt, sondern endlich auch Planungssicherheit bei der Datenverarbeitung in der Cloud für deutsche Unternehmen herstellt. Die aktuelle Situation entspricht – leider – dem technischen Stand von vor zehn bis 15 Jahren. **m**