www.bt-magazin.de 1.2013 Heft 12 Deutschland: € 14,90 Österreich: € 16,80 Schweiz: sFr 29,80 Luxemburg: € 16,90

Business Technology

Business Technology

Architektur, Innovation & Strategie

Nick Kratzer: „Burn-out – Problem oder Hype?“

VERNETZUNG

Start-up-Szene: Innovation für Enterprises

Emergente Software-Entwicklung 2020

Bring your own Device? Everything? Disaster?

4 191858 414906 01

Ist Datenschutz ein Hemmschuh für den technischen Fortschritt in Unternehmen?

Die Grenzen der Cloud

Die globale Vernetzung schreitet in technischer Hinsicht rasch voran. Große Datenpakete lassen sich ohne wesentliche Verzögerung nahezu in die gesamte Welt übermitteln. Gerade der Hype um Cloud Computing zeigt, dass längst auch die Unternehmen die Möglichkeit, Daten fernab eigener Kapazitäten zu verarbeiten, für sich entdeckt haben. Welche rechtlichen Haftungsrisiken sie dabei eingehen, ist ihnen indes oft nicht bewusst. Wir geben Ihnen einen Überblick über die wichtigsten datenschutzrechtlichen Aspekte.

AUTOR: CHRISTIAN HUFEN

Die wirtschaftlichen Vorteile von Cloud Computing sind offensichtlich: Es besteht nicht nur die Möglichkeit, per Fernzugriff von überall auf die in der Cloud abgelegten Daten zuzugreifen, was unter anderem die eigene Mobilität steigert; eine umfassende Datenauslagerung kann für Unternehmen auch einen Wegfall der lokalen kostenintensiven IT-Infrastruktur bedeuten. Immer mehr Unternehmen lagern daher ihre Datenverarbeitungsprozesse in die Cloud zu externen Dienstleistern aus. Gerade wegen der attraktiven wirtschaftlichen Möglichkeiten, die technische Entwicklungen mit sich bringen, begeben sich Unternehmen allerdings oft blauäugig in für sie schier unübersehbare rechtliche Haftungsrisiken. Denn so unbegrenzt die technischen Möglichkeiten für ihre Anwender auch sein mögen – sie werden durch die gesetzlichen Vorgaben eingeschränkt. Besonders durch datenschutzrechtliche Bestimmungen werden den scheinbar unbegrenzten technischen Möglichkeiten des Cloud Computing enge Grenzen gesetzt.

BEACHTUNG DATENSCHUTZRECHTLICHER VORGABEN

Datenschutzrechtliche Vorgaben sind immer dann zu beachten, wenn es um die Verarbeitung von personenbezogenen Daten geht, also Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, dem so genannten Betroffenen. Datenschutzrechtliche Relevanz besteht daher vor allem dann, wenn Kunden-, Lieferanten- oder Mitarbeiterdaten vom Cloud-Anwender in der Cloud des Anbieters gespeichert werden.

Aus rechtlicher Perspektive handelt es sich bei der Ablage solcher Daten in der nicht unternehmenseigenen Cloud um die Übermittlung personenbezogener Daten an den Cloud-Anbieter. Eine solche Übermittlung personenbezogener Daten an einen Dritten bedarf grundsätzlich der Einwilligung jeder einzelnen betroffenen Person. Im Falle des Cloud Computing muss sich die Einwilligung dabei konkret auf die Verlagerung der Daten in die Cloud beziehen. Liegt – wie in den meisten Fällen – eine entsprechende Einwilligung des Betroffenen nicht vor, kann die Übermittlung der Daten nur durch einen gesetzlichen Erlaubnistatbestand legitimiert werden. Aber nur in den seltensten Fällen gelingt es, die Voraussetzungen einer gesetzlichen Erlaubnis zur Speicherung personenbezogener Daten in der Cloud zu erfüllen – mit der Folge, dass die Auslagerung der Daten in die Cloud ohne weitere Maßnahmen als unzulässig zu qualifizieren ist. Beispielsweise muss ein Transfer von personenbezogenen Daten zur Erfüllung eines Vertrags mit der betroffenen Person oder zur Wahrung berechtigter Interessen des Cloud-Anbieters erforderlich sein – eine Konstellation, die kaum vorstellbar scheint.

AUFTRAGSDATENVERARBEITUNG

Anders liegt der Fall, wenn zwischen dem Cloud-Anwender und dem Cloud-Anbieter eine vertragliche Vereinbarung über eine Datenverarbeitung im Auftrag abgeschlossen wurde. Eine solche Auftragsdatenverarbeitung liegt vor, wenn ein Dienstleister im Auftrag eines Unternehmens personenbezogene Daten erhebt, verarbeitet und nutzt. Das ist beim Cloud-Computing-Modell der Fall. Liegt eine entsprechende schriftliche Vereinbarung vor, ist der Cloud-Anbieter nicht als Dritter anzusehen. Die Ablage von personenbezogenen Daten in der Cloud stellt also keine rechtlich relevante Übermittlung personenbezogener Daten dar. Demnach wäre der Datentransfer in die Cloud zulässig.

Das Gesetz enthält einen Mindestkatalog an einzuhaltenden Anforderungen für eine rechtlich zulässige Auftragsdatenverarbeitungsvereinbarung, die schriftlich zu regeln sind. Neben einer konkreten Bezeichnung der betroffenen Daten soll der Auftragsdatenverarbeiter (hier: der Cloud-Anbieter) den Weisungen des Auftraggebers unterliegen. Zudem hat der Auftragsdatenverarbeiter die gesetzlich vorgesehenen technischen und organisatorischen Maßnahmen zu treffen und sieht sich entsprechenden regelmäßigen Kontrollen des Auftraggebers ausgesetzt. Man kann sich denken, dass die schriftliche Vereinbarung einer Auftragsdatenverarbeitungsvereinbarung unter Beachtung der gesetzlichen Anforderungen in der Praxis häufig scheitert. Denn viele Cloud-Anbieter sind nicht geneigt, sich durch die Cloud-Anwender überwachen zu lassen und deren Weisungen in Bezug auf die Datenverarbeitung Folge zu leisten.

GRENZÜBERSCHREITENDER DATENVERKEHR

Doch damit nicht genug: Die rechtlichen Beschränkungen der technischen Möglichkeiten, die eine globale Vernetzung mit sich bringen, werden gerade dann deutlich, wenn personenbezogene Daten grenzüberschreitend übermittelt werden. Aus Gründen einer optimalen Nutzung von Ressourcen verteilen Cloud-Anbieter die von ihnen angebotenen Systeme oftmals global auf verschiedene Cluster. Technisch gesehen macht es dabei zwar keinen Unterschied, in welchem Land der Server steht, auf dem sich die Daten gerade befinden. Aus rechtlichen Gründen sind diese geografischen Grenzen jedoch von äußerster Wichtigkeit.

Innereuropäischer Raum: Für Clouds, bei denen die Datenverarbeitung ausschließlich innerhalb des Europäischen Wirtschaftsraums (EWR) stattfindet, ergeben sich zunächst keine Besonderheiten gegenüber den genannten nationalen Anforderungen.

Außereuropäischer Raum: Erfolgen die Datenverarbeitungen außerhalb der EU und des EWR – indem die Cloud-Anbieter und/oder Unteranbieter eine Datenverarbeitung in Drittstaaten vornehmen –, gelten erhöhte Anforderungen an eine zulässige Datenverarbeitung. Andere Länder gelten als datenschutzrechtlich unsichere Drittstaaten, bei denen insbesondere die Privilegierung der Auftragsdatenverarbeitung nicht in Anspruch genommen werden kann. Es wird davon ausgegangen, dass bei derartigen Übermittlungen von personenbezogenen Daten besondere Risiken entstehen, weil keine hinreichende Kontrolle der Datenverarbeitung möglich ist. In diesen Fällen müssen für eine zulässige Datenübermittlung zusätzliche Hürden übersprungen werden. Die Zulässigkeit des Datentransfers hängt in diesen Fällen zunächst ebenfalls davon ab, ob eine Einwilligung der betroffenen Personen vorliegt oder eine gesetzliche Erlaubnis existiert. Darüber hinaus ist von entscheidender Bedeutung, ob in dem jeweiligen Drittstaat ein angemessenes Datenschutzniveau herrscht. Maßgeblicher Anhaltspunkt für die Beurteilung des Datenschutzniveaus in einem Empfängerland sind die dort geltenden Datenschutzgesetze.

Bisher hat die Europäische Kommission lediglich für einige wenige Länder wie z. B. Kanada, die Schweiz oder Argentinien entsprechende Feststellungen getroffen, nicht aber für andere wichtige Wirtschaftsnationen wie China oder Indien, und vor allem: nicht für die USA. Daher sollte im Einzelfall geprüft werden, ob ausnahmsweise ein angemessenes Schutzniveau angenommen werden kann.

Mit Blick auf die USA, einen der wichtigsten Handelspartner, besteht eine Sonderkonstellation, wenn

sich der Cloud-Anbieter zur Einhaltung der so genannten *Safe-Harbor*-Grundsätze verpflichtet hat. Safe-Harbor ist eine Übereinkunft zwischen der Europäischen Union und den USA aus dem Jahr 2000, die sich nach US-Recht richtet und gewisse Grundsätze des Datenschutzes wie Informations- und Wahlrechte des Betroffenen sowie die Erfordernis von Transparenz enthält. Inhaltlich ist es also an die europäischen Datenschutzbestimmungen angelehnt. Cloud-Anbieter oder Unteranbieter mit Sitz in den USA können sich dabei auf freiwilliger Basis gegenüber dem US-Handelsministerium selbst zertifizieren, indem sie eine Beitrittserklärung unterzeichnen und eine entsprechende Datenschutzerklärung veröffentlichen. Bei Unterwerfung des jeweiligen US-Unternehmens unter die in dem Abkommen festgelegten Prinzipien ist somit grundsätzlich von einem angemessenen Schutzniveau auszugehen. Da es sich bei der Unterwerfung unter die Safe-Harbor-Prinzipien aber tatsächlich um eine reine Selbstverpflichtung der US-Unternehmen handelt und diese nicht oder nur unzureichend kontrolliert wird, wird seitens deutscher Datenschutzbehörden gefordert, dass sich der Cloud-Anwender im Einzelnen von der Einhaltung der Safe-Harbor-Regeln durch seinen Vertragspartner überzeugt, bevor er personenbezogene Daten an diesen übermittelt.

Es existieren zudem weitere Ausnahmen, unter denen die Übermittlung in ein Drittland auch dann zulässig sein kann, wenn – bezogen auf das Land – kein angemessenes Datenschutzniveau herrscht. Dazu zählt neben der Möglichkeit einer Ausnahmegenehmigung durch die zuständige Datenschutzaufsichtsbehörde auch die Verwendung der von der EU entwickelten Standardvertragsklauseln. Bei diesen handelt es sich um von der Europäischen Kommission freigegebene Standardverträge, bei deren unmodifizierter Unterzeichnung die europäischen Datenschutzbehörden davon ausgehen, dass ein angemessenes Datenschutzniveau gewährleistet ist. Allerdings wurden die spezifischen Regelungen der Auftragsdatenverarbeitung hier nicht vollständig abgebildet. Aus diesem Grund sind über die Vereinbarung von Standardvertragsklauseln hinaus die Anforderungen an eine zulässige Auftragsdatenverarbeitung zu beachten. Dies kann beispielsweise durch Regelungen in den Anlagen zum Standardvertrag oder durch separate vertragliche Regelungen erfolgen, vorausgesetzt, dass inhaltlich nicht von den Standardvertragsklauseln abgewichen wird.

Neben den in den Standardvertragsklauseln enthaltenen Garantien genügen auch entsprechende Selbstverpflichtungen in so genannten *Binding Corporate Rules*, d. h. verbindlichen Unternehmensrichtlinien.

Problemfall Patriot Act: Trotz entsprechender vertraglicher Ausgestaltung birgt die Verlagerung von personenbezogenen Daten in ein Drittland auch weiterhin nicht unerhebliche Risiken. Nach einheitlicher Auffassung der Datenschutzbeauftragten des Bundes und der Länder dürfen Cloud-Anwender Cloud-Services nur dann in Anspruch nehmen, wenn der Cloud-Anwender in der Lage ist, seine Pflichten als verantwortliche Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutzanforderungen geprüft hat. Diesen Anforderungen können Cloud-Anwender aber dann nicht in vollem Umfang gerecht werden, wenn sie Cloud-Anwendungen mit internationalen Verflechtungen in Anspruch nehmen. Zunächst wird sich nur schwer feststellen lassen, in welchem Land sich die Daten tatsächlich befinden. Zudem besteht die Gefahr einer nicht vermeidbaren Kollision mit ausländischen Rechtsordnungen. So kann etwa die Situation entstehen, dass der Cloud-Provider ausländischen Behörden Zugriffsrechte einräumen oder Daten in unsichere Drittstaaten übermitteln muss. Dies wurde insbesondere im Zusammenhang mit datenschutzrechtlich relevanten Datentransfers in die USA deutlich, als bekannt wurde, dass die bei US-Unternehmen gespeicherten Daten dem Zugriff staatlicher Stellen unterliegen. Das ergibt sich insbesondere aus dem so genannten *Patriot Act*, der nach den Terroranschlägen im September 2001 geschaffen wurde, um die Eingriffsbefugnisse der amerikanischen Sicherheitsbehörden zu erweitern. Danach sind europäische Daten selbst dann nicht vor dem Zugriff amerikanischer Behörden sicher, wenn sie gar nicht in den USA, sondern in europäischen Rechenzentren liegen und dort verarbeitet werden. Denn solange die Muttergesellschaft des Cloud-Anbieters ihren Sitz in den USA hat, sollen – so das US-Gesetz – auch die Tochterunternehmen die Verpflichtungen aus dem Patriot Act treffen.

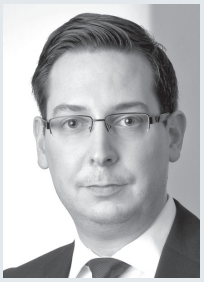
Das zeigt: Anwendern von Cloud-Lösungen mit US-Bezug kann nicht garantiert werden, dass die strengen deutschen beziehungsweise europäischen Datenschutzgrundsätze von den Cloud-Dienstleistern eingehalten werden. Cloud-Anbieter mit gesellschaftsrechtlichen Verbindungen in die USA befinden sich dem gegenüber in einer Zwickmühle. Entweder verstoßen sie gegen US-Recht oder gegen das Datenschutzrecht ihrer Cloud-Kunden und damit gegen vertragliche Obliegenheiten. Aber auch bei der Auswahl von Cloud-Dienstleistern, die ihren Sitz in anderen unsicheren Drittländern haben, besteht die Gefahr, dass Behörden der inneren Sicherheit, wie Polizei, Geheimdienste und Finanzbehörden, Zugriff auf die Daten nehmen. Je niedriger das Datenschutzniveau innerhalb

dieser Länder ist, desto größer ist die Gefahr behördlicher Zugriffe und damit auch der etwaigen Gefährdung oder Verletzung der Betroffeneninteressen.

ZUSAMMENFASSUNG

Die vorstehenden Ausführungen zeigen, dass der technologische Fortschritt, hier dargestellt am Beispiel des Cloud Computing, von seinen Nutzern nicht ungeprüft in Anspruch genommen werden sollte. So birgt die Auslagerung von personenbezogenen Daten in die Cloud nicht unerhebliche rechtliche Risiken. Insbesondere die Implementierung internationaler Cloud Services ist mit Vorsicht zu genießen. Hier bestehen komplexe Voraussetzungen, um die stattfindenden Datenübermittlungen zu legitimieren. Bei Nichteinhaltung der Datenschutzbestimmungen drohen dem Cloud-Anwender als datenschutzrechtlich verantwortlicher Stelle haftungsrechtliche Konsequenzen. Denn er ist gegenüber den Betroffenen zum Schadensersatz verpflichtet, und es können Bußgelder verhängt oder Anordnungen verfügt werden.

Trotz alledem ist von der Nutzung von Cloud-Services aus rechtlicher Sicht nicht abzuraten. Anwender und Anbieter sollten jedoch sorgfältig prüfen, welche rechtlichen Anforderungen im konkreten Fall bestehen. Wenn die datenschutzrechtliche Zulässigkeit nicht gewährleistet ist, sollten sowohl der Cloud-Anwender als auch der Cloud-Anbieter von der jeweiligen Cloud-Lösung Abstand nehmen.



Christian Hufen

ist Rechtsanwalt und seit 2012 bei der Rechtsanwaltsgesellschaft Luther beschäftigt. Er berät nationale und internationale Mandanten in allen Bereichen des IT- und Medienrechts, insbesondere im Softwarerecht, E-Commerce und E-Business. Ein Schwerpunkt seiner Tätigkeit liegt im Bereich des Datenschutzrechts. Daneben berät er Mandanten bei der Gestaltung und Strukturierung von Marketingkampagnen im On- und Offline-Bereich. Seine Tätigkeit umfasst außerdem die Vertragsgestaltung und -verhandlung sowie die allgemeine urheber- und wettbewerbsrechtliche Beratung.