

Die rechtlichen Grundlagen für Cloud Computing sind in vielen Ländern ungeklärt

Weltweit Daten schützen

Der globale Datenverbund bereitet technisch schon lange keine Probleme mehr. Aber was sagen die Gesetzgeber zu Ihren Daten im Ausland? **Oliver Huq**

Auf einen Blick

Inhalt

Die technischen Möglichkeiten des Cloud Computing erlauben es problemlos, über weite geografische Entfernungen IT-Dienstleistungen aller Art anzubieten. Problematisch wird es allerdings, wenn datenschutzrechtlich relevante Inhalte auf ausländischen Servern gespeichert und verwaltet werden. Der Artikel zeigt die Risiken der Verletzung von Datenschutzanforderungen auf und gibt Hinweise, wie Sie möglichen Problemen vorbeugen können.

Inhalt

Oliver Huq ist Volljurist und arbeitet als Redakteur bei der Zeitschrift MACup. Er ist unter anderem auf Internet-, Multimedia- und Wirtschaftsrecht spezialisiert und verfolgt seit mehr als zehn Jahren die rechtlichen Entwicklungen in diesen Bereichen.

Die IT-Landschaft wandelt sich immer mehr in Richtung des Cloud Computing. Darunter versteht man beispielsweise den Betrieb von Rechenzentren und Speicherkapazitäten sowie die Bereitstellung von Entwicklungs-umgebungen, Mail- oder Gruppen-Software und/oder Customer-Relationship-Management-(CRM-)Systemen durch einen oder mehrere Dritte und nicht durch den Anwender selbst. Der Zugriff auf die bereitgestellten Systeme erfolgt dabei in der Regel über das Internet.

Damit werden personenbezogene Daten meist nicht mehr vom Anwender selbst gespeichert und verwaltet, sondern vom Anbieter. Sitzt dieser im Ausland, kann das zu rechtlichen Komplikationen führen, da dies eine erhöhte Gefährdung von datenschutzrechtlich geschützten Daten darstellt und unter Umständen sogar unzulässig ist. Doch wie lässt sich das Ganze rechtlich in den Griff bekommen?

Personenbezogene Daten

Zunächst ist es wichtig zu wissen, was personenbezogene Daten sind. In Deutschland definiert § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) personenbezogene Daten als „Einzelfangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person“. Darunter fallen neben Namen und Anschriften auch Daten wie Telefonnummern, E-Mail- oder IP-Adressen. Besonders geschützt sind in Deutschland nach § 3 Abs. 9 BDSG Informationen über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder das Sexualleben. Anders als in Österreich und der Schweiz, aber ebenso wie in der übrigen EU werden vom BDSG Daten juristischer Personen (GmbH, AG et cetera) nicht geschützt.

Grundsätze

Werden erhobene Daten nicht ausschließlich für familiäre oder persönliche Tätigkeiten genutzt, so gilt auch für Private das BDSG (§ 1 Abs. 2 Nr. 3 BDSG). Beim Datenschutz geht es in Deutschland darum, den Einzelnen vor Beeinträchtigungen in seinem Grundrecht auf informationelle Selbstbestimmung zu bewahren. Grundsätzlich

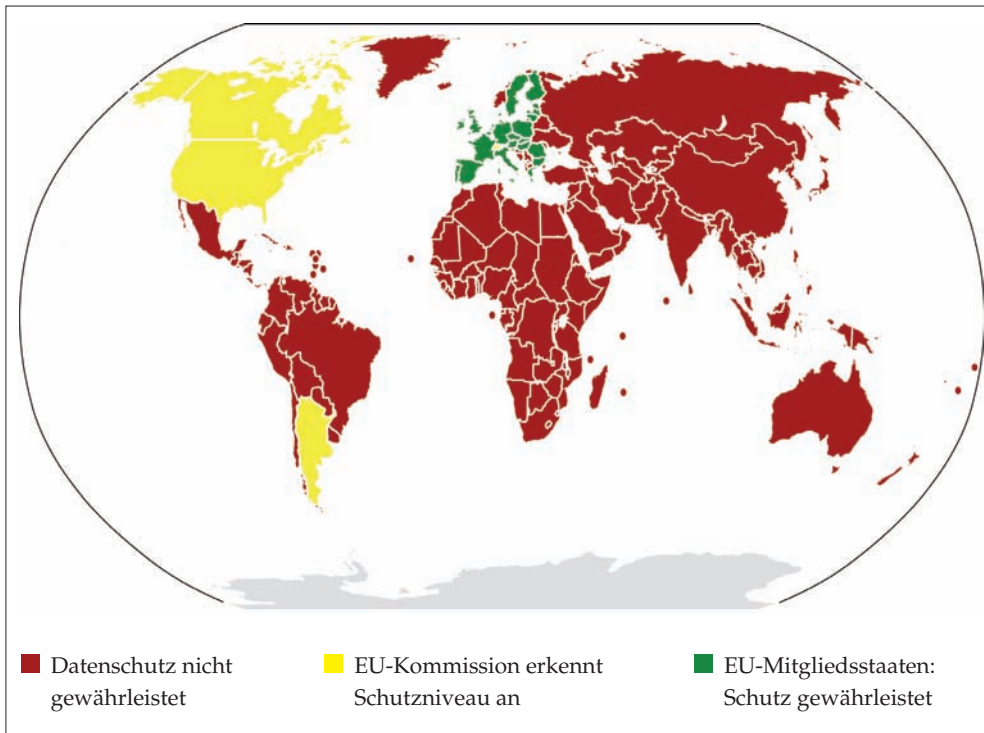
soll jeder selbst entscheiden, wann und für wen welche persönlichen Daten zugänglich sind.

Daraus ergibt sich das generelle Verbot, personenbezogene Daten zu erheben, außer es ist gesetzlich ausdrücklich erlaubt oder der Betroffene hat seine Einwilligung (am besten schriftlich) dazu erteilt (§ 4 Abs. 1 BDSG). Ferner gilt der Grundsatz der Datenvermeidung und Datensparsamkeit. Das bedeutet, so wenig wie möglich an personenbezogenen Daten überhaupt erst zu erheben und möglichst von Anonymisierung und Pseudonymisierung erhobener Daten Gebrauch zu machen (§ 3a BDSG).

Datenverarbeitung im Ausland

Benutzt man einen „Cloud“-Dienst, der eine Datenspeicherung im Ausland vornimmt, so verkompliziert sich die Sachlage. Grundsätzlich gilt, dass in dem Land, in das übertragen wird, ein angemessenes Datenschutzniveau bestehen muss. Ansonsten ist eine Übertragung unzulässig. Für die Mitgliedsstaaten der EU gelten dieselben Bestimmungen wie für die Übermittlung im Inland. Problematisch wird es also nur bei der Übermittlung in andere Länder. Um festzustellen, ob ein angemessenes Datenschutzniveau vorliegt, hilft die Europäische Kommission weiter, die solch eine Feststellung treffen kann und das bisher auch für die Schweiz, Kanada, Argentinien, Guernsey, die Isle of Man und für die Anwendung der vom US-Handelsministerium vorgelegten Grundsätze des „Sicheren Hafens“ (Safe Harbor) sowie die Übermittlung von Fluggastdatensätzen an die US-Zoll- und Grenzschutzbehörde (CBP) festgestellt hat. Die Website der Kommission gibt immer aktuell Auskunft über solche Länder [1]. Besonders relevant in diesem Zusammenhang sind die Safe-Harbor-Vereinbarungen, die unter anderem auch von Amazon, Google, Microsoft und IBM unterzeichnet worden sind.

Inwieweit das Sicherheit gewährt, ist fraglich, da nationale Gesetzgebungen doch zu einer unterschiedlichen Handhabung führen könnten. Eine gerichtliche Entscheidung liegt zumindest noch nicht vor. Sollte solch ein „Test-Fall“ eintreten, dann ist das Kind wohl ohnehin schon in den Brunnen gefallen und die Daten sind kompromittiert. Gerade auch der jüngst im April in den USA verabschiedete „Cybersecurity Act“,



Orientierung für den weltweiten Schutz Ihrer Daten – „grünes Licht“ gilt nur in wenigen Ländern (Bild 1)

der unter bestimmten Voraussetzungen die oben genannten Datenschutzbestimmungen in den USA komplett aushebeln kann, lässt es ratsam erscheinen, sich nicht auf die einfache Feststellung der Kommission zu verlassen, sondern sich die „Clouds“, in denen man Daten unterbringt, genauer anzusehen.

Verantwortlichkeit

Zu verantworten hat derjenige die Einhaltung des Datenschutzes, der die Datenverarbeitung personenbezogener Daten auch betriebswirtschaftlich verwaltet. Das ist beispielsweise der Arbeitgeber, der die Verdienstabrechnung über die „Cloud“ auslagert. Dem eigentlichen Dienst-erbringer sind umso unmissverständlicher die Voraussetzungen und Anforderungen an den Datenschutz (siehe Anlage zu § 9 Satz 1 BDSG) zu kommunizieren und die Einhaltung bei diesem ist regelmäßig zu überprüfen. Bei Verstößen gegen Datenschutzbestimmungen drohen empfindliche Geldbußen in Höhe von bis zu 250.000 Euro, Geldstrafen oder sogar Freiheitsentzug von bis zu zwei Jahren. Nach § 4f Abs. 1

BDSG sind nichtöffentliche Stellen, bei denen mindestens zehn Personen ständig mit der Bearbeitung personenbezogener Daten mittels elektronischer Datenverarbeitung beschäftigt sind, dazu verpflichtet, einen Datenschutzbeauftragten schriftlich zu benennen.

Datenschutz im eigenen Rechenzentrum ist schon eine Herausforderung. In der „Cloud“ den Überblick zu behalten und alle rechtlichen Bestimmungen zu erfüllen macht die Aufgabe nicht leichter. Es ist also ratsam, in Vertragsvereinbarungen mit dem Service Provider – gerade bei US-Firmen – die Anforderungen an den Datenschutz mit aufzunehmen und Verstöße mit Geldbußen zu sanktionieren. Auch die Kontrolle der Einhaltung der vereinbarten Datenschutzvorkehrungen sollte geregelt werden, und man sollte die Einwilligung zur Weitergabe von Daten gleich prophylaktisch einfordern (sofern möglich). Nur so ist man gut absichert. [ef]

[1] http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_de.htm

[2] http://www.brak.de/seiten/01_03.php

[3] http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm

Erste Hilfe: Wohin im Notfall wenden?

■ Ist das Kind bereits in den Brunnen gefallen, dann hilft nur die Flucht nach vorne. Verträge müssen überarbeitet werden und mögliche Problembereiche eliminiert. Das sollten Sie in jedem Fall einem Profi überlassen. Besitzt noch kein Anwalt Ihr Vertrauen, so können Sie über die regionalen Anwaltskammern das Anwaltsverzeichnis einsehen. Auf der Seite der Bun-

desrechtsanwaltskammer finden Sie eine Linkliste zu den regionalen Kammern [2].

■ Wer noch vor der Entscheidung steht, der findet im Bereich Datenschutz auf der Website der Europäischen Kommission umfassendes Informationsmaterial und auch Standardvertragsklauseln, die den Bestimmungen zum Datenschutz gerecht werden [3].