von Rechtsanwalt **Dr. Daniel S. Huber**

Wolkenfreier Himmel beim Cloud Computing?– strenge Anforderungen an Datenschutz

Das Bundesdatenschutzgesetz stellt strenge Anforderungen an die Verarbeitung und Übermittlung personenbezogener Daten. In vielen Fällen findet das BDSG auf den Trend Cloud Computing Anwendung. Lesen Sie heute, welchen Anforderungen das Cloud Computing in rechtlicher Hinsicht daher nach den Vorschriften des BDSG genügen muss.

Das deutsche Datenschutzrecht gilt

Wie die IT-Recht Kanzlei im vorhergehenden Beitrag zum Thema Cloud Computing und Datenschutzrecht festgestellt hat, kommt in vielen Fällen des Cloud Computing das deutsche Bundesdatenschutzgesetz (kurz: BDSG) zur Anwendung.

Dies führt zu zahlreichen rechtlichen Problemen, die im Folgenden kurz einführend vorgestellt werden sollen.

Lesen Sie für eine weiter gehende Einführung in die Thematik „Cloud Computing“ zudem den Artikel zum Start der Serie „Wolkenfreier Himmel beim Cloud Computing“.

Technische und organisatorische Maßnahmen nach § 9 BDSG

Nach § 9 Satz 1 BDSG haben Unternehmen, die Daten erheben, verarbeiten und/oder speichern diejenigen technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um den Anforderungen, die das BDSG an die Datenverarbeitung und Datenspeicherung stellt, genüge zu leisten. Dies gilt somit auch für Cloud Computing-Anbieter, die an Datenverarbeitungsprozessen beteiligt sind. Relevant sind hierbei vor allem die in der Anlage zum BDSG genannten Anforderungen.

Die Anforderungen nach der Anlage zu § 9 Satz 1 BDSG

Demnach ist die Organisation der innerbetrieblichen Abläufe bei der datenverarbeitenden Stelle so zu wählen, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

Insbesondere sind dabei Maßnahmen zu treffen, wie etwa die Einrichtung von Zutritts-, Zugangs- und Zugriffskontrollen, so dass Unbefugte keinen Zugang zu personenbezogenen Daten erhalten. Das gilt sowohl für den Zugang zu Räumen, in denen entsprechenden Daten gespeichert bzw. aufbewahrt werden, als auch für die EDV.

Angriffen von außen, insbesondere von Hackern etc. müssen demnach möglichst wirksam vorgebeugt oder begegnet werden.

Daneben müssen die nach dem BDSG geschützten Daten auch gegen Verlust oder Zerstörung hinreichend gesichert werden, u.a. bedeutet dies eine Pflicht zur Vornahme von Backups.

Anforderungsmaßstab

Die Anforderungen nach § 9 Satz 1 BDSG bzw der Anlage zu § 9 Satz BDSG gelten aber nicht maßlos.

Ein Unternehmen muss somit nicht unendlich großen Aufwand betreiben, um die Daten entsprechend zu schützen. Übermäßige finanzielle Anstrengungen muss ein Unternehmen nicht auf sich nehmen. Denn laut § 9 Satz 2 BDSG sind Schutzmaßnahmen nach § 9 Satz 1 BDSG nur erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen.

Hieraus ergibt sich somit keine klare Abgrenzungslinie, sondern lediglich Abwägungskriterien, die von Einzelfall zu Einzelfall betrachtet und bewertet werden müssen.

Verschiebungen in der Wolke als relevanter Datenvorgang

Wann ist Datenverarbeitung überhaupt erlaubt?

Eine Erhebung, Speicherung und Verarbeitung von nach dem BDSG geschützten Daten ist nach § 4 Absatz 1 BDSG ganz allgemein dann erlaubt, soweit das BDSG selbst oder eine anderes Gesetz dies erlaubt oder der Betroffene einwilligt.

Da die Anforderungen an eine wirksame Einwilligung des Betroffenen recht hoch sind – die Einwilligung muss nach § 4a BDSG u.a. schriftlich erfolgen – sind Cloud Computing-Anbieter in der Praxis darauf angewiesen, dass ihre Tätigkeit unter einen gesetzlichen Erlaubnistatbestand fällt.

Denn es wäre extrem unwirtschaftlich, wenn jedes Unternehmen, dass Cloud Computing betreibt, alle seine Kunden in formgerechter Weise fragen müsste, ob sie mit der Datenverarbeitung bzw. Datenübermittlung in die „Cloud“ einverstanden sind und dies sich schriftlich bestätigen zu lassen.

Die Lösung – Auftragsdatenverarbeitung nach § 11 BDSG?

Auf den ersten Blick könnte die Auftragsdatenverarbeitung nach § 11 BDSG die rechtliche Lösung für das Cloud Computing sein.

Wenn ein Auftragsdatenverhältnis nach § 11 BDSG zwischen dem Kunden (etwa einem Unternehmen) und dem Cloud Computing-Anbieter vorliegt, so hat das den Vorteil, dass die Übermittlung der Daten von dem Kunden an den Cloud Computing-Anbieter bzw. dessen Server nicht als Datenverarbeitung bzw. -übermittlung in dem Sinne angesehen würde. Vielmehr würde der Cloud Computing-Anbieter vom Gesetz dann so gesehen, als sehr er Teil des Unternehmens des Kunden.

Man kann sich das so vorstellen, dass bei einer Auftragsdatenverarbeitung die Zusammenarbeit zwischen dem Auftraggeber und dem Auftragnehmer so eng ist, dass das Gesetz der Ansicht ist, dass der Auftragnehmer praktisch wie ein Teil des Auftraggebers, z.B. eine Abteilung im Unternehmen des Auftraggebers ist.

Kern des Verhältnisses zwischen dem Auftraggeber der Datenverarbeitung und dem Auftragnehmer ist der Bestand eines strengen Weisungsverhältnisses, so dass der Auftraggeber jederzeit Weisungen an den Auftragnehmer erteilen kann, die dieser befolgen muss. So soll sichergestellt werden, dass der Auftragnehmer eng an den Auftraggeber gebunden ist und die Daten, für die nach § 11 Absatz 1 BDSG vor allem der Auftraggeber verantwortlich ist, entsprechend gut geschützt werden.

Strenge Anforderungen an das Vorliegen einer Auftragsdatenverarbeitung

Allerdings sind die Hürden für die Etablierung einer Auftragsdatenverarbeitung zwischen Auftraggeber und Auftragnehmer sehr hoch.

In einem Vertrag zwischen dem Auftraggeber und dem Auftragnehmer (d.h. Cloud-Computing-Anbieter und dessen Kunde) müssten derart detaillierte Regelungen vereinbart werden, dass es in der Praxis nach derzeitiger Rechtslage kaum möglich sein dürfte, ein solches Auftragsdatenverarbeitungsverhältnis rechtskonform und rechtssicher zu begründen.

Das Problem mit dem außereuropäischen Ausland

Dazu kommt das Problem, dass die Privilegierung des § 11 BDSG nur in Anspruch genommen werden kann, wenn der Cloud Computing-Anbieter bzw. dessen Server, wo die Daten tatsächlich gespeichert und verarbeitet werden, in Deutschland, in der sonstigen EU oder zuminderst im Gebiet des EWR sind. Denn nur in diesen Staaten geht das BDSG grundsätzlich von einem gleich hohen, angemessenen Datenschutzniveau wie in Deutschland aus, so dass der Schutz personenbezogener Daten gewährleistet ist.

Damit eine Datenübermittlung in sonstige, außereuropäische Länder erfolgen darf, müsste nach § 4b Absatz 2 BDSG in diesen ein angemessenes Datenschutzniveau bestehen. Dies wird nur für wenige Länder angenommen. Ein Cloud Computing-Anbieter müsste hier komplizierte Vereinbarungen mit den Kunden schließen, die schließlich sicherstellen, dass auch im „unsicheren Ausland“ ein der EU entsprechendes Datenschutzniveau gewährleistet wird.

Am sinnvollsten wäre es daher, wenn eine Cloud Computing Anbieter allein im EU- bzw EWR-Gebiet tätig wäre. Dies ist aber rein technisch problematisch. Das Wesen des Cloud Computing besteht gerade darin, dass es – technisch – vollkommen egal ist, wo die Computer und Server tatsächlich stehen, auf denen Daten eines Unternehmens gespeichert und verarbeitet werden.
Dem deutschen bzw. europäischen Datenschutzrecht ist dies jedoch nicht egal. Es stellt eine große Herausforderung dar, hier eine technisch und rechtlich kongruente Lösung zu erarbeiten.

Erlaubnis nach § 28 BDSG

Eine gesetzliche Erlaubnis, auch ohne Einwilligung der Betroffenen Daten zu erheben, zu verarbeiten, zu übermitteln und zu speichern, ist zudem in § 28 BDSG enthalten.

Nach § 28 Absatz 1 Nr. 2 BDSG ist die Datenverarbeitung und Datennutzung etwa als Mittel zur Erfüllung eigner Geschäftszwecke zulässig, soweit dies zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Hier könnte man anführen, dass sowohl dem Kunden, wie auch dem Cloud Computing-Anbieter finanzielle Vorteile entstehen, wenn Cloud Computing (auch im außereuropäischen Ausland) betrieben wird. Denn der Cloud Computing-Anbieter spart Kosten, wenn er seine Server entsprechend günstig im Ausland aufstellen und betreiben kann und der Kunde spart Kosten, weil er die Server nicht bei sich aufstellen, betreiben und warten muss.

Allerdings werden solche finanziellen Interessen nach allgemeiner Ansicht nicht unter § 28 Absatz 1 Nr. 2 BDSG gefasst. Finanzielle Interessen können die Interessen der Betroffenen am ausreichenden Schutz ihrer Daten in der Regel nicht überwiegen, so dass auch diese Vorschrift nicht zu einer Lösung führt.

Fazit

Das Datenschutzrecht ist wohl die größte Hürde für das Cloud Computing.

Eine vollständige und rechtssichere Lösung scheint kaum möglich, da die technischen Vorteile des Cloud Computing nach derzeitiger Rechtslage eingeengt werden müssten, um das Cloud Computing rechtlich auf sichere Beine zu stellen.

Wird jedoch das Cloud Computing technisch zu sehr eingeschränkt, verliert es womöglich seine (wirtschaftliche) Attraktivität.

Cloud Computing und Datenschutz – hier besteht weiter Diskussionsbedarf!

Autor:
RA Dr. Daniel S. Huber
Rechtsanwalt