security zone newsletter
PLATTFORM FÜR INFORMATIONSSICHERHEIT

Outsourcing – wichtige Datenschutzfragen weiterhin ungelöst?

Das Abrufen von Rechenleistung, Speicherplatz oder sonstigen Diensten über Cloud-Anbieter erfreut sich immer grösserer Beliebtheit, mehr und mehr auch bei Unternehmen. Doch nicht nur Private und seriöse Unternehmen schätzen die Flexibilität und die Skalierbarkeit von Cloud-Diensten. Auch für Cyber-Kriminelle scheint die Cloud zu einem Betätigungsfeld zu werden. Wie kürzlich einem Bericht auf Heise-Online entnommen werden konnte, haben Sicherheitsspezialisten mit einer Investition von lediglich 6 Dollar mittels Cloud-Diensten ganze Webserver ausser Gefecht gesetzt.
Doch braucht es wirklich kriminelle Energie, um bei der Benutzung von Cloud-Diensten mit dem Gesetz in Konflikt zu geraten oder kann dies auch dem seriösen Unternehmen unbeabsichtigt passieren?

Christian Leupi, lic. iur.
Rechtsanwalt, MAS Business IT
Partner bei Grossenbacher Rechtsanwälte, Luzern

Datenverantwortung beim Outsourcing

Die Benutzung von Cloud-Diensten ist in der Regel mit dem Übermitteln von Personendaten auf die Systeme des Cloud-Anbieters, eventuell – sofern weitere Leistungen bezogen werden – auch mit einer Bearbeitung durch den Cloud-Anbieter (Outsourcing) verbunden.

Der Auftraggeber als „Datenherr" muss sich bewusst sein, dass die Verantwortung für die Einhaltung der datenschutzrechtlichen Vorschriften in jedem Falle bei ihm liegt. Ihn trifft deshalb die Pflicht, den Cloud-Dienstleister sorgfältig auszuwählen, zu überwachen und auf die Einhaltung der Schweizer Datenschutzstandards zu verpflichten. Das Datenschutzgesetz schreibt diesbezüglich seit der Revision im Jahre 2008 vor, dass die Datenbearbeitung nur auf Basis einer schriftlichen Vereinbarung oder bei Vorliegen einer entsprechenden gesetzlichen Erlaubnis übertragen werden darf. Ein online abgeschlossener Vertrag, wie dies zum Beispiel bei Standarddiensten wie Amazon S3 oder EC2 der Fall ist, genügt somit den Anforderungen wohl nicht. Der Auftraggeber sollte somit auf einer schriftlichen Vereinbarung beharren. Weiter hat er dafür zu sorgen, dass der Dienstleister die Daten nur in dem Umfang bearbeitet, welcher auch für ihn selbst zulässig ist. Er hat sich – allenfalls auch vor Ort – zu vergewissern, dass der Dienstleister die Datensicherheit einhält.

Beinhalten die Cloud-Dienste nicht nur das Speichern von Daten sondern werden ganze Funktionalitäten ausgelagert (wie im Business Process Outsourcing in der Regel der Fall), so wird der Auftraggeber zudem nicht umhin kommen, bei den betroffenen Personen vor dem Datentransfer eine Einwilligung einzuholen. Beachten muss er zudem, dass der Transfer von besonders schützenswerten Personendaten eine ausdrückliche

Einwilligung der betroffenen Personen erfordert.

Datensicherheit in virtualisierten Umgebungen

Bezüglich Datensicherheit enthält die Datenschutzgesetzgebung diverse technisch-organisatorische Vorgaben, insbesondere Kontrollverpflichtungen, welche der Auftraggeber als Datenherr auch beim Outsourcing in die Cloud respektieren muss. Die Umsetzung bzw. die Einhaltung dieser gesetzlichen Vorgaben stellt im Zusammenhang mit Cloud-Angeboten eine nicht zu unterschätzende Herausforderung für den Auftraggeber dar. Cloud-Dienste zeichnen sich nämlich dadurch aus, dass eine weitreichende Virtualisierung von IT-Ressourcen (Speicherplatz, Rechenleistung etc.) erfolgt, was eine notwendige Grundlage für die Flexibiliät und Skalierbarkeit der Dienste darstellt. Auch in solch technisch komplexen Umgebungen ist in letzter Instanz der Auftraggeber dafür verantwortlich, dass die Daten nicht unberechtigt an Dritte weitergegeben werden; dies insbesondere auch nicht innerhalb der Cloud zwischen den einzelnen Kunden des Cloud-Anbieters. Dabei den Kontrollpflichten nachzukommen, kann den Auftraggeber unter Umständen vor erhebliche Schwierigkeiten stellen.

Datenexport in Drittländer als rechtliche Herausforderung

Die grösste Herausforderung aus datenschutzrechtlicher Sicht stellt weiterhin der Export von Personendaten in Drittländer dar, welche nicht das gleiche Datenschutzniveau aufweisen wie die Schweiz. Die Virtualisierung und Skalierbarkeit der IT-Ressourcen bringt mit sich, dass Speicher- und Verarbeitungssysteme eines einzelnen Cloud-Anbieters weltweit verteilt sein können, so insbesondere in den USA oder im asiatischen Raum, wo kein zur Schweiz ebenbürtiges Datenschutzniveau herrscht.

Der Auftraggeber hat dafür zu sorgen, dass der Cloud-Anbieter sich einem der Schweiz vergleichbaren Datenschutzniveau unterwirft. Dies kann beispielsweise durch einen Datenexportvertrag oder – im Falle der USA – durch Safe Harbour-Registrierungen bewerkstelligt werden. Zu beachten ist, was vielfach übersehen wird, dass die Schweiz auch Firmendaten als Personendaten betrachtet. Dies im Gegensatz zur EU, welche ansonsten eine gleichwertige Datenschutzgesetzgebung kennt. Werden also Firmendaten exportiert, muss unter Umständen auch im EU-Raum eine Zusatzvereinbarung über den Umgang mit Firmendaten getroffen werden.

Der Auftraggeber tut zudem gut daran, im Vorfeld abzuklären, ob eine Datenauslagerung in die Cloud – unabhängig von der Frage des Datenexports ins Ausland – überhaupt gesetzlich zulässig ist. Dies kann beispielssweise bei Daten in den Bereichen Arbeit, Gesundheitswesen oder MWSt sowie elektronische Geschäftsbücher nicht oder nur eingeschränkt gegeben sein. Nicht zu unterschätzen ist auch die Problematik, dass je nach Speicherort der Daten unterschiedliche gesetzliche Vorschriften für den Zugriff auf Daten durch Behörden, auch im Hinblick auf Straf- oder Zivilverfahren, bestehen können.

Lösungsansätze

Damit der Auftraggeber jederzeit Gewähr hat, dass er Herr der Daten ist und keine unautorisierten Zugriffe erfolgen, wäre eine durchgängige Verschlüsselung der Daten anzustreben. Es sind bereits erste technische Ansätze vorhanden, eine Datenverarbeitung in der Cloud zu ermöglichen, ohne dass unverschlüsselt auf die Daten zugegriffen werden muss.

Der Auftraggeber kann heute mangels international einheitlicher Datenschutzstandards kaum zuverlässig abschätzen, mit welchen Rechtsordnungen die in die Cloud ausgelagerten Daten in Berührung kommen. Kurz- und mittelfristig dürften deshalb Rahmenvertragswerke bedeutend sein, mit welchen auf privater Basis versucht wird, einheitliche Standards zu etablieren und so für eine gewisse Rechtssicherheit zu sorgen. Solche Rahmenvertragswerke könnten beispielsweise enthalten:

1. Klare Verpflichtung zur Bearbeitung nur zu transparent kommunizierten Zwecken, gemäss Vorgaben des Auftraggebers und unter Berücksichtigung der Datenschutzstandards im Sitzstaat des Auftraggebers;
2. Vereinfachte Möglichkeiten für Audits und Kontrollen;
3. Proaktive Information des Auftraggebers bei Datenlecks, Anfragen von Behörden etc.