Compliance

Rechtliche Fallstricke in der Cloud

Wilfried Platten: Einer der grössten Vorbehalte gegen die Nutzung von Cloud Services sind rechtliche Bedenken. Was ist aus Compliance-Gesichtspunkten bei der Inanspruchnahme von Software as a Service (SaaS), Infrastructure as a Service (IaaS) oder Platform as a Service (PaaS) zu beachten?

Dr. Rolf Auf der Maur: Der zentrale Punkt ist, dass die Verantwortung für die rechtskonforme Erfassung und Bearbeitung von Daten sowie die Datensicherheit beim Kunden bleibt, der Cloud-Services in Anspruch nimmt. Der Kunde muss den Dienstanbieter daher vertraglich in die Pflicht nehmen, damit er dieser Verantwortung gerecht wird. Bei unternehmenskritischen Applikationen und Daten genügt der Vertrag allein nicht. In solchen Fällen ist auch eine Due-Diligence-Prüfung bezüglich Standort und Sicherheit der Server sowie der Backup- und Recovery-Funktionalitäten der Dienstanbieter erforderlich.

Cloud ist nicht gleich Cloud. Die gängigste Differenzierung ist diejenige zwischen Public Cloud und Private Cloud – und dann gibt es ja auch noch Hybrid Cloud. Wie unterscheiden sie sich aus rechtlicher Sicht?

Public-Cloud-Dienste sind in der Regel auf den Bedarf von Konsumenten ausgerichtet und für den Unternehmenseinsatz kaum geeignet. Bei solchen Angeboten lassen sich in der Regel die vertraglichen Bestimmungen auch nicht individuell aushandeln. Für den Unternehmens-einsatz eignen sich eigentlich nur Private-Cloud-Lösungen und gewisse Hybrid-Cloud-Angebote. Wichtig ist es aus Kundensicht, nüchtern zu überlegen, welche Leistungskomponenten individuell geregelt werden müssen. Rechtlich sind es dieselben Regelungspunkte, die auch bei einem IT-Outsourcing-Projekt zu bedenken sind.

Welche allgemeinen regulatorischen Anforderungen – Stichwort Datenschutz – sind bei der Festlegung der Service Level Agreements (SLAs) zu beachten?

Datenschutz steht bei den allgemeinen regulatorischen Anforderungen üblicherweise im Vordergrund. Der Anbieter von Cloud-Dienstleistungen darf Personendaten nur insoweit bearbeiten, als dies der Kunde selbst darf. Er muss die Daten auch gegen unautorisierten Zugriff respektive Manipulation schützen. Dazu dienen Service Level Agreements mit denselben Leistungskriterien, die auch bei Managed Applications zur Anwendung kommen.

«Bei unternehmenskritischen Applikationen und Daten genügt der Vertrag allein nicht», so Anwalt Dr. Rolf Auf der Maur.

Zusätzlich gibt es ja auch noch branchenspezifische Fallstricke. Welche besonderen regulatorischen Anforderungen müssen bei der Vertragsgestaltung für Branchen wie Banken oder Versicherungen berücksichtigt werden?

In zahlreichen Branchen bestehen besondere regulatorische Anforderungen, die aber beispielsweise auch bei einem normalen IT-Outsourcing zur Anwendung kommen. Ein Beispiel ist das Rundschreiben der Eidgenössischen Bankenkommission zum Outsourcing im Bankensektor. Auch im Gesundheitswesen, im Bereich der Telekommunikation oder in der öffentlichen Verwaltung bestehen besondere Anforderungen. Mir ist noch keine Anforderung bekannt, die nicht auch mit Cloud-Lösungen erfüllt werden könnte. Zumindest dann, wenn es sich um eine Private Cloud handelt, bei der der physische Standort der Daten, der Zugang zu den Daten und die geeigneten Sicherheitsmassnahmen individuell vereinbart werden können. ■

VITA DR. ROLF AUF DER MAUR

Rolf Auf der Maur befasst sich seit Beginn seiner Anwaltstätigkeit 1992 vorwiegend mit rechtlichen Aspekten des Internets. Dabei kann er sein Interesse für neue Kommunikationstechnologien mit seiner anwaltlichen Erfahrung in idealer Weise kombinieren. Zu seinen Klienten zählen führende Unternehmen aus den Bereichen der Medien, der Unterhaltungsindustrie, Telekommunikation und der Informationstechnologie. Neben seiner anwaltlichen Tätigkeit publiziert und referiert Rolf Auf der Maur regelmässig zu rechtlichen Fragen im Zusammenhang mit dem Internet und ist auch unternehmerisch tätig.