CLOUD-VERTRÄGE

Kaum ein Unternehmen kann heute noch auf Cloud-Services verzichten. Beim Vertragsabschluss mit dem Provider gibt es jedoch einiges zu beachten. Ein Rechtsworkshop für CIOs im Schnelldurchgang.

→ VON CLAUDIA KELLER & CASPAR HUMM

DER AUTOR

Caspar Humm
ist hauptsächlich in den Bereichen Immaterialgüterrecht, Pharma- & Gesundheitsrecht sowie allgemein im Gesellschafts- und Handelsrecht beratend und prozessierend tätig. Seit 2014 arbeitet er bei der Kanzlei Wenger & Vieli als Rechtsanwalt.
→ **www.wenger-vieli.ch**

Die Palette der Cloud-Computing-Dienstleistungen ist so vielfältig wie die Bedürfnisse des Zielpublikums: Public, Private und Hybrid Clouds decken unterschiedliche Bedürfnisse der Unternehmen ab. Die den Angeboten zugrundeliegenden SaaS-, PaaS- und/oder IaaS-Dienstleistungen müssen entsprechend vertraglich geregelt werden. Dabei sind verschiedene Aspekte zu beachten.

1 VERTRAGSRECHTLICHE ASPEKTE

Zunächst sind beim Abschluss des Vertrags mit dem Cloud-Anbieter dieselben Punkte zu beachten wie bei anderen Verträgen auch. Unbedingt zu regeln sind beispielsweise:

- Welche Leistung erbracht wird, d. h., mit welchen Leistungen, mit welcher Verfügbarkeit und Performance der Nutzer rechnen darf.
- Zu welchem Preis diese Leistung erbracht wird, z. B. welche Leistungen durch einen Pauschalbetrag abgegolten sind und für welche Leistungen weitere, variable Kosten anfallen können.
- Welche Konsequenzen aus einer Nicht- oder Schlechterfüllung des Vertrags folgen. Dies gilt sowohl seitens des Cloud-Nutzers als auch seitens des Cloud-Anbieters. Dazu gehört auch die Regelung der Haftung. Cloud-Nutzer müssen sich bewusst sein, dass die Haftung der Cloud-Anbieter in den Standardverträgen meist stark eingeschränkt oder wegbedungen wird.
- Wie die Kündigungsmodalitäten ausgestaltet sind, insbesondere, mit welcher Frist die Zusammenarbeit beendet werden kann und für Cloud-Verträge besonders relevant, wie die ausgelagerten Daten nach der Kündigung migriert werden können.
- Wie und wo die Rechte aus dem Vertrag durchgesetzt werden können. Einen Anspruch im Ausland durchzusetzen, ist regelmässig mit grösserem Aufwand verbunden.
- Was mit den Daten geschieht, wenn der Cloud-Anbieter Konkurs geht.

2 DATENSCHUTZRECHTLICHE ASPEKTE

Es gibt keine grundsätzlichen rechtlichen Hindernisse für die Nutzung von Cloud-Dienstleistungen. Sie wirft aber datenschutzrechtliche Fragen auf. Wenn von einer Privatperson oder einem Unternehmen Daten von natürlichen oder juristischen Personen bearbeitet werden, ist das Datenschutzgesetz (DSG) anwendbar. Personendaten dürfen nur rechtmässig, nach Treu und Glauben und nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgegeben ist.

Der Begriff «bearbeiten» ist dabei sehr breit zu verstehen. Er umfasst jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren. So gelten zum Beispiel das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten als Bearbeitung im Sinne des Gesetzes. Schon das Speichern von Personendaten in einer Cloud stellt also eine Datenbearbeitung im Sinne des DSG dar.

Alle Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen, sind durch das DSG geschützt. Bei vielen Daten, die ein Unternehmen bearbeitet, beispielsweise bei HR- oder Kundendaten, handelt es sich um geschützte Personendaten. Auch Daten, welche die Beziehung zu einem anderen Unternehmen betreffen, gelten als Personendaten, da juristische Personen vom schweizerischen DSG ebenfalls erfasst werden. Soll für die Bearbeitung solcher Daten eine Cloud-Applikation verwendet werden, ist zu prüfen, ob die datenschutzrechtlichen Vorgaben eingehalten werden können. Als besonders schützenswert gelten Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten; aber auch solche, die Gesundheit, Intimsphäre oder Rassenzugehörigkeit betreffen, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen. Für die Bearbeitung solcher Daten gelten strengere Vorgaben und entsprechend erhöhte Sorgfaltspflichten.

3 SONDERFALL CLOUD COMPUTING

Das Datenschutzrecht kennt den Begriff «Cloud Computing» nicht, sondern regelt die «Datenbearbeitung durch Dritte» in allgemeiner Form. Sobald ein Cloud-Nutzer Personendaten auf den Server eines anderen Unternehmens einspeist, handelt es sich datenschutzrechtlich gesehen um eine Bearbeitung durch einen Dritten.

Das Bearbeiten von Personendaten darf durch Vereinbarung grundsätzlich einem Dritten übertragen werden, ohne dass dafür eine Einwilligung der betroffenen Personen erforderlich wäre. Der Auftraggeber ist aber dafür verantwortlich, dass der Dritte die Daten nur so bearbeitet, wie er es selbst tun dürfte. Der Cloud-Nutzer muss sich auch vergewissern, dass der Anbieter die Datensicherheit gewährleistet, indem er die Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten schützt (Art. 7 DSG). Will der Cloud-Anbieter Sub-Provider beiziehen, muss der Cloud-Nutzer sicherstellen, dass diese in dieselben Pflichten eingebunden werden wie der Cloud-Anbieter.

Ein Unternehmen, das Cloud-Services nutzt, ist dafür verantwortlich, dass der Cloud-Anbieter sich vollumfänglich an das schweizerische Datenschutzrecht hält. Der Cloud-Nutzer bleibt auch selbst für die Erfüllung seiner gesetzlichen Aufbewahrungs- und Archivierungspflichten verantwortlich, wie sie etwa das Buchführungs- und das Steuerrecht vorsehen. Die Verantwortung kann also nicht an den Service-Provider delegiert werden. Deshalb sollte darauf geachtet werden, dass der Cloud-Anbieter den notwendigen Standard zumindest vertraglich zusichert. Je vertraulicher, geheimer oder wichtiger die Daten für ein Unternehmen sind und je sensitiver im Hinblick auf die betroffene Person, desto strikter müssen die Sicherheitsvorkehrungen und deren Kontrollmöglichkeiten sein.

4 STANDORT VON ANBIETERN UND SERVERN

Datenschutzrechtlich ist es nicht einerlei, in welchem Land oder in welchen Staaten die Datenbearbeitung stattfindet. Personendaten dürfen grundsätzlich nur ins Ausland bekannt gegeben werden, wenn die dortige Gesetzgebung einen angemessenen Schutz der Daten gewährleistet. Der Eidgenössische Datenschutzbeauftragte führt eine Liste von Staaten, für die das zutrifft. Im EU-Raum ist dies zumindest für die Daten von natürlichen Personen grundsätzlich der Fall, nicht aber beispielsweise in den USA. Damit Daten rechtmässig auch in solchen Staaten bearbeitet werden können, sind zusätzliche Garantien notwendig. Für die USA genügt grundsätzlich eine Selbstzertifizierung gemäss dem U.S.-Swiss Safe Harbour Framework.

Zu berücksichtigen ist, dass weder Datenschutzrecht noch Safe-Harbour-Zertifizierung verhindern, dass Behörden auf Basis hoheitlicher Untersuchungsbefugnisse einen Cloud-Anbieter zur Herausgabe der Daten verpflichten (in den USA beispielsweise gestützt auf den Patriot Act). Das Datenschutzrecht regelt nur, was der Cloud-Anbieter mit den Daten machen darf. Es hat aber keinen Einfluss darauf, wozu Behörden den Cloud-Anbieter allenfalls zwingen können.

5 VERTRAGLICHE REGELUNG IT-SPEZIFISCHER RISIKEN

Vor der Implementierung einer Cloud-Lösung sollte eine Risikoanalyse durchgeführt werden. Dabei sind – abhängig von der konkret vorgesehenen Datenbearbeitung in der Cloud – die Schutzziele (bezüglich Vertraulichkeit, Verfügbarkeit, Integrität, Zurechenbarkeit und Nachvollziehbarkeit) zu bestimmen. Im Hinblick auf die organisatorischen, technischen und rechtlichen Anforderungen an den Cloud-Anbieter und die konkreten Cloud-Service-Dienstleistungen ist die explizite Regelung der Rechte und Pflichten der Vertragspartner notwendig. Folgende Punkte sollten hiervon abgedeckt sein:

- **Aufteilung der Verantwortung** für die Datenbearbeitung zwischen den Parteien.
- **Kontrolle** über die Daten und ihre Bearbeitung darf nicht verloren gehen oder verunmöglicht werden.
- **Überprüfbarkeit** der Abläufe und Prozesse.
- **Auskunfts-, Löschungs- und Berichtigungsansprüche** der betroffenen Personen müssen gewährleistet sein.
- **Serverstandorte:** Für Auslandstandorte muss ein der Schweiz gleichwertiges Datenschutzniveau gewährleistet sein und das Risiko eines Zugriffs von ausländischen Behörden auf die Daten geprüft werden. Dies bedingt Transparenz seitens des Cloud-Anbieters hinsichtlich der Serverstandorte.
- **Gewährleistung der notwendigen Datensicherheit:** Vertraulichkeit, Schutz vor Missbrauch, Integrität, Authentizität, Nachvollziehbarkeit der Datenbearbeitungen, Identity- und Accessmanagement, Schutz vor Datenverlust und Management von Notfällen und anderen Einschränkungen der Dienstleistungen durch System- oder Netzwerkausfälle, Backup-Systeme; bei sensiblen Daten eventuell Private Server statt Shared Server, sodass Attacken auf einen anderen Nutzer die eigenen Daten nicht gefährden.
- **Portabilität und Interoperabilität:** Der Cloud-Nutzer muss bei einer Beendigung der Nutzung der Cloud seine Daten in einem Format erhalten, das ihm erlaubt, die Daten wieder in eine eigene IT-Umgebung oder in eine Cloud-Lösung eines anderen Anbieters zu migrieren. Auch die Rückgabemodalitäten sind bereits bei der Auswahl des Cloud-Anbieters vertraglich zu regeln.

Bis zu welchem Grad ein Cloud-Anbieter diese Vorgaben erfüllen soll, hängt auch vom Verwendungszweck ab. Daten zur Terminfindung oder zur Verwaltung des Versands von Werbematerial sind weniger sensitiv als die Verwaltung von Personaldossiers oder Gesundheitsdaten der Mitarbeiter. Für Berufsgeheimnisträger wie Ärzte oder Anwälte gelten besonders strenge Anforderungen.

Eine regelmässige Kontrolle des Cloud-Anbieters durch Datenschutz-Audits vor Ort wäre wünschenswert, ist aber kaum praktikabel. Alternativen könnten regelmässige, unabhängige Datenschutz-Audits sein, die der Cloud-Anbieter selbst vornehmen lässt – oder eine einschlägige Zertifizierung (Norm ISO/IEC 27001). ←

DIE AUTORIN

Claudia Keller
ist seit 2006 als Anwältin mit Schwerpunkt auf IP/IT- und Datenschutzrecht tätig. Sie publiziert und referiert regelmässig zu diesen Themen. Seit 2013 arbeitet sie bei der Kanzlei Wenger & Vieli als Rechtsanwältin.
→ **www.wenger-vieli.ch**

«Datenschutzrechtlich ist es keinesfalls einerlei, in welchem Staat die effektive Datenbearbeitung stattfindet»