Datenschutz und Cloud-Lösungen

Wurde die IT-Infrastruktur früher fast gänzlich selber betrieben und/oder betreut, ist heutzutage eine klare Tendenz zu einer Auslagerung dieser Tätigkeit zu erkennen. Gewisse Dienstleister haben bereits angekündigt, dass ihre «Offline-Versionen», sprich Versionen ihrer Software, welche lediglich lokal und frei von Abonnementsverträgen sind, nicht mehr lange angeboten werden. Die entsprechenden Kunden müssen in naher Zukunft den (teilweisen) Gang in die Cloud prüfen. Nachfolgend werden die wichtigsten datenschutzrechtlichen Themen in diesem Zusammenhang aufgezeigt, um eine konforme Cloud-Nutzung zu ermöglichen.

Von Florian Müller

Cloud-Lösungen datenschutzrechtlich erlaubt?

Die kurze Antwort ist «JA!». Sowohl das neue Schweizer Datenschutzrecht als auch die Europäische Datenschutz-Grundverordnung verbieten die Nutzung von Cloud-Lösungen nicht. Sie stellen jedoch gewisse Anforderungen, damit die Nutzung eines Cloud-Dienstes datenschutzkonform erfolgen kann. Die wichtigsten Anforderungen sind:

- Beizug von Cloud-Anbietern allenfalls nur möglich, wenn eine gesetzliche oder vertragliche Grundlage besteht (ADV)
- Verantwortung, dass Cloud-Anbieter die Datensicherheit gewährleistet (TOM)
- Sicherstellung eines angemessenen Datenschutzniveaus bei Bearbeitungen im Ausland

Die Wichtigkeit dieser Anforderungen ergibt sich aus Art. 61 DSG, welche bei (eventual-)vorsätzlicher Verletzung der Pflichten eine Busse bis CHF 250 000.– androhen.

Prüfschema Cloud-Lösung

1. Wer ist mein Vertragspartner?
2. Vertragspartner in der Schweiz?
3. Gesetzliche oder vertragliche Vereinbarung für Datenbearbeitung?
4. Datensicherheit gewährleistet?
5. Datenbearbeitung ausschliesslich in der Schweiz?
6. Zusätzliche Massnahmen für Auslandtransfer?

Datenschutzrechtliche Rollen bei Cloud-Lösungen

Gerade bei Cloud-Lösungen, welche als SaaS-Angebote («Software-as-a-Service») vertrieben werden, wird der Dienstleister meist Personendaten im Auftrag des Verantwortlichen bearbeiten. Dies entlastet zwar den Kunden vom Betrieb der entsprechenden Infrastruktur, nicht aber von der Verantwortung. Der Anbieter wird folglich als Auftragsbearbeiter tätig werden, und die entsprechenden gesetzlichen Voraussetzungen (Art. 9 DSG) müssen eingehalten werden. Die Übertragung der Bearbeitung bedarf folglich einer gesetzlichen oder vertraglichen Grundlage. In der Praxis ist dabei der Abschluss eines Auftragsbearbeitungsvertrags (meist «ADV») notwendig, da es an einer gesetzlichen Grundlage fehlt.

Eher selten sind Sachverhalte, bei denen keine datenschutzrechtlich relevante Datenbearbeitung durch den Cloud-Anbieter erfolgt. Dies wäre dann denkbar, wenn der Anbieter über keine Möglichkeit verfügt, die übermittelten Daten so zu verwenden, um einen Rückschluss auf eine natürliche Person zu ziehen. Möglich wäre dies beispielsweise durch eine vorgängige Verschlüsselung der Daten durch den Kunden, wenn der Schlüssel ausschliesslich beim Kunden verbleibt. Obwohl gewisse Anbieter entsprechende Nutzungsmöglichkeiten zur Verfügung stellen, geht diese meist mit drastischen Einschränkungen des Funktionsumfangs einher. Entsprechend selten wird diese Möglichkeit benutzt.

Gewährleistung der Datensicherheit

Der Kunde als Verantwortlicher der Datenbearbeitung hat durch technische und organisatorische Massnahmen (TOM) sicherzustellen, dass die Datensicherheit gewährleistet werden kann.[1] Bei einer ausgelagerten Datenbearbeitung hat er die entsprechenden Massnahmen beim Cloud-Anbieter sicherzustellen. Es muss folglich abgeklärt werden, welche Massnahmen beim jeweiligen Anbieter getroffen werden. Nicht genügend ist es, dabei lediglich auf Marketingaussagen wie «Wir halten den Datenschutz ein» oder «Wir sind ISO-zertifiziert» abzustellen. Im Rahmen eines ADV sollten folglich auch die Mindestanforderungen an die Massnahmen vertraglich vereinbart werden. Diese dienen dem Kunden bei einer allfälligen Kontrolle gleichzeitig als Prüfliste bzw. Nachweis.

Die TOM sollten dabei mindestens über folgende Punkte objektiv informieren:

- Passwort- und Benutzerrichtlinien
- Zugriffsmöglichkeiten innerhalb des Anbieters
- Verschlüsselung der Daten, und wer über Schlüssel verfügt

1 Siehe Beitrag Florian Müller: Mindestanforderung in der September-Ausgabe.

- Sicherungsmassnahmen und Wiederherstellungsmöglichkeiten

Ort der Datenbearbeitung

Nicht immer leicht erkennbar ist der Ort der eigentlichen Datenbearbeitung. Sowohl Schweizer als auch ausländische Anbieter bieten oft die (teilweise) Wahlmöglichkeit, wo der Ort der Datenbearbeitung sein soll. Meist kann der Kunde den eigentlichen Speicherort («Data at rest») bestimmen und mindestens teilweise die Region der eigentlichen Datenbearbeitung («Data in use»). Handelt es sich zusätzlich um einen ausländischen Anbieter, ist es wichtig zu prüfen, ob dieser aus dem Ausland auf die Daten zugreift (z. B. für Supportaufträge) und somit allenfalls eine Datenbearbeitung in einem weiteren Land erfolgt.

Die Transparenz der Anbieter wird in der Praxis zwar immer besser, doch ist nicht immer auf den ersten Blick erkennbar, wo der Ort der Datenbearbeitung liegt. Kunden sind somit gut beraten, im Zweifel bei den Anbietern nachzufragen. Gleichzeitig muss intern oder mit einem Partner sichergestellt werden, dass die gewünschten Einstellungen betreffend Speicher- und Bearbeitungsort gewählt werden.

Datenbearbeitung im Ausland

Wird festgestellt, dass eine Datenbearbeitung im Ausland erfolgt, muss der Kunde einer Cloud-Lösung prüfen, ob der Bearbeitungsort innerhalb eines Landes erfolgt, welches ein angemessenes Datenschutzniveau gewährleistet.[2] Ist das entsprechende Land dort nicht aufgeführt, so müssen zusätzliche Massnahmen getroffen werden. In der Praxis werden in diesen Fällen oft die sogenannten EU-Standardvertragsklauseln (mit den für die Schweiz notwendigen Anpassungen) verwendet.[3] In der Praxis zeigt sich immer wieder, dass Cloud-Anbieter noch auf veraltete Transfermechanismen setzen und selbst noch «Safe Harbour» oder «Privacy Shield» in ihren Verträgen aufführen. Beide Transfermechanismen sind seit mehreren Jahren nicht mehr zulässig. Betreffend USA dürfte sich in den nächsten Monaten noch eine Änderung ergeben, da die Einführung eines neuen Schweiz-US-Datenschutzrahmenabkommens wohl kurz bevorsteht. Damit wäre ein Datentransfer aus der Schweiz an Anbieter, welche über eine entsprechende Zertifizierung verfügen, wieder unter einem angemessenen Datenschutzniveau möglich.

2 Länder in Anhang 1 der Datenschutzverordnung.

3 Siehe Beitrag von Herr Lukas Lezzi in der Mai-Ausgabe.

Das Wichtigste in Kürze

- Cloud-Lösungen dürfen verwendet werden.
- Kunde trägt weiterhin Verantwortung für Datensicherheit
- Prüfschema für Cloud-Lösung einhalten
- nicht auf Marketingaussagen blind vertrauen

AUTOR

Florian Müller berät als Technologie-Anwalt und Notar kleinere und mittlere Unternehmen in den Bereichen IT, Datenschutz, Immaterialgüterrecht (IP), Blockchain sowie weiteren wirtschaftsrechtlichen Bereichen. Er war in einer auf IT-Recht und Datenschutz spezialisierten Kanzlei tätig, bevor er als Senior Associate LEXcellence beitrat.