VUD | Verein Unternehmens-Datenschutz

# FAQ zum Einsatz von Cloud-Technologien

26. August 2022

- ✓ *Der risikobasierte Ansatz ist ein Grundsatz des Datenschutzrechts – seit je her und auch nach der Revision des Datenschutzgesetzes. Er gilt auch für die Bekanntgabe von Personendaten ins Ausland.*

- ✓ *Für die Bekanntgabe von Personendaten ins Ausland genügt gemäss Datenschutzgesetz ein "angemessener" und künftig ein "geeigneter" Schutz, was dem risikobasierten Ansatz entspricht. Ein Ausschluss jedes theoretischen Risikos ist nicht verlangt.*

- ✓ *Das mit Cloud-Projekten verbundene Risiko ist jeweils im konkreten Einzelfall zu prüfen. Dabei ergibt sich oft, dass selbst bei Cloud-Diensten unter Mitwirkung von US-Providern das Risiko eines ausländischen Behördenzugriffs bei geeigneten Schutzmassnahmen gering und datenschutzrechtlich tragbar ist.*

***Über den VUD***

Der Verein Unternehmens-Datenschutz (VUD) wurde 2006 gegründet und ist ein Zusammenschluss der Unternehmensdatenschützer vieler KMUs und grossen internationalen Schweizer Unternehmen (vud.ch). Der VUD ist der selbständigen und unabhängigen Meinungsbildung im Bereich Datenschutz verpflichtet ist.

Der guten Ordnung halber weisen wir darauf hin, dass die Aussagen in dieser FAQ nicht notwendigerweise die Meinung aller Mitglieder des VUD wiedergeben.

# FAQ zum Einsatz von Cloud-Technologien

Die Frage, wie Cloud-Lösungen von US-Anbietern im Einklang mit dem Schweizer Datenschutzrecht genutzt werden können, beschäftigt derzeit viele Schweizer Unternehmen. Da das Thema grosse Bedeutung für die meisten Schweizer Unternehmen hat, hat sich der VUD zur Publikation dieser FAQ entschieden.

## *Ist der Einsatz von Cloud-Lösungen von US-Anbietern nach Schweizer Datenschutzrecht zulässig?*

Ja, der Beizug eines Anbieters mit Sitz in den USA oder mit US-Konnex wird weder durch das aktuelle noch das künftige Datenschutzgesetz (**DSG**) untersagt.

Bei der derzeitigen Diskussion geht es um die Gefahr, dass die von einem Cloud-Provider mit US-Konnex verwalteten Daten von US-Behörden durchsucht werden. Selbst wenn gezeigt werden kann, dass das Risiko eines solchen Lawful Access im konkreten Fall nur theoretischer Natur ist, sind einige Datenschutzbehörden der Meinung, dass es nicht tragbar sei und das Datenschutzrecht selbst ein theoretisches Risiko nicht zulasse, weil das im Gesetz nirgends so stehe.

Wir sind der Ansicht, dass im DSG seit je her ein risikobasierter Ansatz gilt, auch im Bereich des Auslandsdatentransfers. Das hat sich mit der Revision nicht verändert – der risikobasierte Ansatz wurde dort sogar als "erste Leitlinie" der Revision bezeichnet.

## *Warum ist der ausländische Behördenzugriff plötzlich ein Problem – dieses Risiko gab es doch immer?*

Das ist richtig. Er ist grundsätzlich auch kein Problem aus Sicht des DSG, da das Datenschutzrecht anerkennt, dass es zur Verfolgung öffentlicher Interessen möglich sein muss, dass Behörden eines ausländischen Staates, in welchen Daten exportiert werden, auf diese zugreifen können. Das kann auch in jedem EWR-Land geschehen. Entscheidend ist, dass hierbei gewisse Grundregeln (wie z.B. Grundlage in einem Gesetz, Verhältnismässigkeit, Rechte für Betroffene, Überprüfung durch eine unabhängige Stelle wie etwa ein Gericht) eingehalten werden müssen. Ist das der Fall, steht das DSG dem Export von Personendaten in ein solches Land normalerweise nicht entgegen.

Im Juli 2020 befand der oberste Gerichtshof der EU (**EuGH**) im Fall "Schrems II", dass diese Bedingungen in den USA in Bezug auf die Rechte von US-Nachrichtendiensten (dort festgehalten u.a. in Section 702 des Foreign Intelligence Surveillance Act, FISA) nicht der Fall ist und daher in jedem Einzelfall vor einer Übermittlung von Daten in die USA überprüft werden muss, ob Bestimmungen wie Section 702 FISA im konkreten Fall zur Anwendung gelangen können. Sie zielen auf den Abgriff von Daten bei US-Providern ab. Bei einer Einzelfallprüfung ergibt sich erfahrungsgemäss oft, dass selbst bei Cloud-Diensten unter Mitwirkung von US-Providern das Risiko eines solchen Abgriffs bei geeigneten Gegenmassnahmen sehr gering ist – aber eben nicht null.

Seit kurzem vertreten einige EU-Datenschützer jedoch die Ansicht, dieses Risiko müsse null sein (vgl. die "Google Analytics"-Entscheide). Weil dieses Risiko wie jedes Risiko der Datensicherheit naturgemäss nie null ist, ist die Nutzung der betreffenden Cloud-Lösungen aus ihrer Sicht verboten. Sie verlangen, dass auf rein europäische Cloud-Angebote ausgewichen wird. Einzelne Behörden vertreten sogar die Auffassung, jede Tochtergesellschaft eines US-Providers sei per se mitbetroffen, ganz egal, ob ein Datenzugriff aus den USA vorgesehen oder möglich ist (vgl. dazu den Beitrag auf datenrecht.ch). Die Konzernzugehörigkeit soll genügen, damit die Benutzung von Cloud-Diensten etwa der europäischen Tochtergesellschaften der grossen US-Hyperscaler datenschutzwidrig ist. Wir halten diese Auffassung für unzutreffend.

### *Was hat das mit der Schweiz zu tun?*

Zunächst einmal ist der "Schrems II"-Entscheid für die Schweiz nicht bindend. Rein rechtlich änderte sich für die Schweiz damit also nichts. Das Parlament kannte bei den Arbeiten im Zusammenhang mit der Totalrevision des DSG den Entscheid und die damit verbundene Problematik und hat sich trotzdem nicht dafür entschieden, die Anforderungen an Übermittlungen von Personendaten in unsichere Drittländer wie die USA zu erhöhen. Die Bestimmungen wurden im Gegenteil gelockert. Es gibt also keinen Grund anzunehmen, dass beim Export von Personendaten plötzlich ein Null-Risiko-Ansatz in Bezug auf ausländische Behördenzugriffe gilt. Das entspricht auch der herrschenden Ansicht, notabene auch in der EU.

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (**EDÖB**) hat jedoch seit je her den Standpunkt vertreten, dass die Regelungen der EU zu diesem Thema analog auch unter dem DSG gelten müssen. Er verlangt deshalb wie die EU, dass bei einem Export von Personendaten in die USA zusätzlich zu einer vertraglichen Absicherung auch ein sog. *Transfer Impact Assessment* durchgeführt wird, in welchem die Wahrscheinlichkeit eines problematischen US-Behördenzugriffs ermittelt wird. Gleichzeitig äusserte er "Zweifel" am risikobasierten Ansatz, weil dieser in den betreffenden Bestimmungen des DSG nicht ausdrücklich sei. Ferner schreibt er, behördliche Zugriffe müssten durch zusätzliche Massnahmen "verhindert" werden.

### *Verlangt das Gesetz den Ausschluss jedes theoretischen Risikos?*

Nein, der risikobasierte Ansatz ist ein Grundsatz des Datenschutzrechts, welcher dem gesamten DSG und revidierten DSG zugrunde liegt – nach herrschender Ansicht auch den Bestimmungen über die Bekanntgabe von Personendaten ins Ausland. Die Geltung des risikobasierten Ansatzes wird allerdings auch erst seit kurzem und nur teilweise in Zweifel gezogen.

- In der **Botschaft zum revidierten DSG** wird der risikobasierte Ansatz als die "erste Leitlinie" bezeichnet. Auch in den Beratungen war er unbestritten.
- Die **Geltung des Grundsatzes** ist so klar, dass das heutige DSG das Wort "Risiko" kein einziges Mal erwähnt. Im Aufsatz "Die Tücken spontaner Datenschutzbeurteilungen …" von David Rosenthal werden in Absatz 5-7 diverse Artikel erläutert, welche direkt auf

die Beurteilung des Risikos abstellen. Die zentrale Bestimmung des DSG, die Interessenabwägung nach Art. 13 DSG, gehört dazu.

- Auch das Kernelement des Datenschutzes, der **Begriff des Personendatums**, basiert auf dem risikobasierten Ansatz. Ohne Personendaten findet das DSG keine Anwendung und es gibt auch keine Einschränkungen beim Transfer von Daten ins Ausland. Die Legaldefinition in Art. 3 Bst. a DSG erwähnt den Begriff des Risikos nicht, doch trotzdem liegen Personendaten nur vor, wenn eine gewisse Wahrscheinlichkeit besteht, dass eine Identifizierung erfolgt. Das stand so schon in der Botschaft von 1988 und das hat das Bundesgericht in BGE 136 II 508 E. 3.2 bestätigt. Das steht so ähnlich auch in Erwägungsgrund Nr. 26 der DSGVO und wurde vom EuGH kürzlich erneut bestätigt. Ist die Wahrscheinlichkeit also klein genug, dass der Empfänger keine Identifizierung von Personen im Klartext vornimmt, liegen keine Personendaten vor und somit erst recht keine Übermittlung ins Ausland.
- Aber auch die **Bestimmungen zur Auslandsübermittlung** sind vom risikobasierten Ansatz geprägt. Die heute relevante Bestimmung für Übermittlungen in die USA ist Art. 6 Abs. 2 DSG. Sie verlangt bei der Bekanntgabe in unsichere Drittstaaten nur einen "angemessenen" Schutz, was dem risikobasierten Ansatz entspricht. Hinzu kommt, dass ein Vertrag als Schutz nach dem Willen des Gesetzgebers genügt, obwohl Verträge bekanntermassen nicht vor einem ausländischen Behördenzugriff schützen. Auch dies ist der risikobasierte Ansatz, wie im Übrigen auch diverse Ausnahmetatbestände des Art. 6 Abs. 2 DSG. So dürfen Daten an ein US-Gericht übermittelt werden, wenn dies für ein dortiges Verfahren nötig ist, was das Ergebnis einer Interessenabwägung und damit des risikobasierten Ansatzes ist. Auch im revidierten DSG ändert sich daran nichts. Die Formulierung ist dort etwas anders, aber im Kern gleich. Es muss ein "geeigneter" Datenschutz vorliegen, den der Datenexporteur wiederum beispielsweise mit einem Vertrag – am besten mit den vom EDÖB genehmigten Standardklauseln – erreichen kann (Art. 16 Abs. 2 Bst. b und d revDSG). In der Botschaft des Bundesrates zum revidierten DSG heisst es dazu, dass eine Datenbekanntgabe in unsichere Drittstaaten erlaubt ist, sobald ein angemessener Vertrag abgeschlossen und dem EDÖB gemeldet ist. Setzt der Datenexporteur vom EDÖB genehmigte Standardvertragsklauseln ein, "wird vermutet, dass er alle notwendigen Massnahmen getroffen hat, um sich eines angemessenen Schutzes zu vergewissern." Das Parlament schloss sich der Regelung an. Der Gesetzgeber verlangt mit dem neuen DSG also nicht einmal ein *Transfer Impact Assessment*. Zum Zeitpunkt der Verabschiedung war "Schrems II", Snowden, der US CLOUD Act und auch sonst das Risiko eines Zugriffs durch ausländische Behörden bekannt und in aller Munde. Der Gesetzgeber wollte die Bekanntgabe von Personendaten ins Ausland trotzdem nicht erschweren. Das ist ihm auch erlaubt, da es an den Entscheid des EuGH nicht gebunden ist (der überdies auf anderen, in der Schweiz nicht geltenden Rechtsgrundlagen beruht und der noch dazu nicht sagt, es gelte ein Nullrisikoansatz).
- Ausdrücklich wird der risikobasierte Ansatz im revidierten DSG ferner in den Bestimmungen zur **Datensicherheit** erwähnt (Art. 8 Abs. 1 revDSG), d.h. u.a. dem Schutz vor ungewollten Zugriffen durch Dritte, also einerseits Cyberkriminelle, aber andererseits auch ausländische Behörden.
- Der risikobasierte Ansatz im Datenschutz ergibt sich im Übrigen aus der **Bundesverfassung**, dort aus dem Verhältnismässigkeitsgrundsatz und dem

Erfordernis des öffentlichen Interesses. Ferner ergibt er sich aus Art. 13 Abs. 2 BV (Stichwort Missbrauchsgesetzgebung).

In der Diskussion um den risikobasierten Ansatz ist auch zu differenzieren, von welchem Risiko im Zusammenhang mit einer Bekanntgabe von Personendaten ins Ausland gesprochen wird. Im Kern geht es um die Frage, ob ein problematisches ausländisches Recht, welches den Behördenzugriff erlaubt, *im konkreten Einzelfall* zur Anwendung kommt. Die Antwort darauf besteht aus einer rechtlichen und einer tatsächlichen Komponente: Erlaubt das ausländische Recht im konkreten Fall seinen Behörden einen Zugriff (rechtliche Frage) und werden die ausländischen Behörden sich diese Befugnis im konkreten Einzelfall zu Nutze machen (tatsächliche Frage).

Diese beiden Komponenten werden häufig nicht differenziert. Hinzu kommt, dass die Beantwortung beider Fragen naturgemäss mit Unsicherheiten behaftet ist. Auch die rechtliche Frage wird sich nie mit absoluter Sicherheit beantworten lassen. Selbst wenn eine rechtliche Einschätzung objektiv richtig ist, kann es immer sein, dass ein Gericht sie im konkreten Einzelfall anders beurteilt. Das verbleibende Restrisiko bei der Einschätzung der rechtlichen Frage muss daher auch vom Null-Risiko-Ansatz gedeckt sein, wenn es hinreichend tief ist. Die Vertreter des Null-Risiko-Ansatzes machen diese Unterscheidung aber häufig nicht und verlangen daher Unmögliches, was in der Folge zum Exportverbot führt. Beim risikobasierten Ansatz können und müssen bei der Beantwortung der Frage, ob es zu einem Behördenzugriff kommen kann, alle weiteren Umstände berücksichtig werden – risikoerhöhende Umstände, aber ebenso auch risikosenkende (wie beispielsweise die Frage, ob es in der Vergangenheit bereits zu Zugriffen gekommen ist). Auch dies führt naturgemäss zu einer Wahrscheinlichkeitsrechnung mit einem Restrisiko, dass sich der Beurteilende irrt.

Letzteres ist auch der Ansatz, den das European Data Protection Board (**EDPB**) in seinen Empfehlungen über zusätzliche Schutzmassnahmen für die DSGVO vertreten hat: Eine Übermittlung von Personendaten in ein unsicheres Drittland ist zulässig, wenn "kein Grund zur Annahme" ("no reason to believe") besteht, dass das problematische ausländische Recht "in der Praxis" ("in practice") auf den konkreten Einzelfall angewandt werden wird. In einer früheren Entwurfsfassung der Empfehlungen wurde noch ein Null-Risiko-Ansatz vertreten. Diesen vertreten in jüngster Zeit allerdings wieder vermehrt diverse EU-Datenschutzbehörden. Auch die **Europäische Kommission** hat dies so gesehen, denn auch die von ihr beschlossenen Standardvertragsklausen verlangen nicht mehr als dies – eine Zusicherung, dass die Parteien nicht mit einem problematischen Behördenzugriff rechnen.

An dieser Stelle sei darauf hingewiesen, dass der risikobasierte Ansatz von diversen Schweizer Behörden gestützt wird, so beispielsweise in einer Beurteilung der Staatsanwaltschaft Basel-Stadt bezüglich der Frage des Berufs- und Amtsgeheimnisses und dem Kanton Zürich in seinem Beschluss zu "M365". Vgl. hierzu Q38 der FAQ von David Rosenthal.

### *Kann es denn beim Einsatz der Cloud-Lösungen der US-Hyperscaler zu einem Zugriff aus den USA kommen, wenn wir eine Speicherung der Daten in Europa wählen?*

Ja, das kann vorkommen. Zwar bieten viele Cloud-Provider die Speicherung von Daten in Europa oder sogar in der Schweiz an. Doch selbst wenn der Vertragspartner eine europäische Niederlassung des Providers ist, wird dieser sich im Vertrag typischerweise vorbehalten, für

gewisse Leistungen auf die Hilfe seiner US-Muttergesellschaft oder eines anderen Subunternehmers zurückzugreifen (z.B. zur Lösung eines technischen Problems). In diesen Fällen kann es zu einem Zugriff von ausserhalb Europas kommen. Dies schliessen auch die Verträge in der Regel nicht aus. Doch auch Fernzugriffe gelten rechtlich als Bekanntgabe von Personendaten ins Ausland und müssen die diesbezüglichen Anforderungen erfüllen.

### *In der Diskussion scheint sich alles um den US CLOUD Act und weitere Bestimmungen des US-Rechts zu drehen – warum?*

Die Fixierung auf den US CLOUD Act scheint eine Schweizer Eigenheit zu sein; im europäischen Ausland ist dieser vergleichsweise selten ein Thema. Dies hat vermutlich mit Unwissenheit über die Relevanz und Funktionsweise des US CLOUD Act zu tun. Wir glauben, die Furcht vor dem US CLOUD Act wird mit fortschreitender Aufklärung schwinden.

Er besteht aus zwei Teilen: Im ersten Teil wird (für die Zwecke des US Stored Communication Act, von dem der US CLOUD Act ein Teil ist) klargestellt, dass sich ein US-Provider nicht mit dem Argument wehren kann, dass die Daten eines Kunden auf einem Server im Ausland liegen, wenn er von der dortigen Strafverfolgungsbehörde einen Befehl zur Herausgabe dieser Daten erhält. Dasselbe gilt umgekehrt unter Schweizer Recht und ist an sich nicht ungewöhnlich. Herausgeben muss ein US-Provider Daten im Klartext aber nur, wenn er auf diese Daten normalerweise tatsächlich Zugriff hat.

Der zweite Teil des US CLOUD Act hat mit der Möglichkeit einer Art Staatsvertrag zu tun, den die USA mit anderen Ländern abschliessen können, damit sie gegenseitig Provider im jeweils anderen Land zur Herausgabe von Daten verpflichten können. Das hatten gewisse Kreise in der Schweiz verlangt, kommt derzeit aber für die Schweiz nicht in Frage.

Aus rein datenschutzrechtlicher Sicht stellt der US CLOUD Act nach herrschender Ansicht kein Problem dar, weil er keine rechtsstaatlichen Grundsätze missachtet und deshalb nicht “problematisch” ist. Einige (Schweizer) Datenschutzbehörden teilen diese Ansicht aber nicht und begründen dies damit, dass ein Lawful Access auf in der Schweiz lagernde Daten illegal sei. Das hat nach unserer Ansicht aber nichts mit der im Falle von Datenexporten nach Art. 6 DSG zu klärenden Frage zu tun, ob ein ausländisches Recht den Anforderungen an einen im Rahmen des Datenschutzes angemessenen Lawful Access erfüllt. Hier werden also Äpfel und Birnen verglichen. Der US CLOUD Act ist daher nur für Cloud-Projekte relevant, in denen es um Berufs- oder Amtsgeheimnisse geht.

Im Falle des US-Rechts aus Sicht des DSG (und der DSGVO) relevant sind hingegen Section 702 FISA und der Executive Order 12333, welche Erlasse den Zugriff auf Daten durch US-Nachrichtendienste regeln. Diese Bestimmungen erfüllen die Anforderungen an einen angemessenen Lawful Access nicht, jedenfalls soweit dem "Schrems II"-Urteil auch für die Schweiz gefolgt wird. Es muss daher bei jedem Cloud-Projekt, welches die Möglichkeit eines Zugriffs auf Daten im Klartext aus den USA vorsieht, geprüft werden, ob es im konkreten Fall Grund zur Annahme gibt, dass ein Zugriff durch US-Nachrichtendienste tatsächlich vorkommt. An diesem Punkt findet auch die derzeitige Diskussion statt: Diverse EU-Datenschutzbehörden sind der Ansicht, dass ein strengerer Massstab gelten muss, nämlich dass absolute Gewissheit besteht, dass kein Zugriff erfolgt ("Null-Risiko-Ansatz"). Wir glauben, dies basiert auf einem Missverständnis bzw. einer Fehlinterpretation des EuGH-Entscheids.

Vgl. zu Section 702 FISA und US CLOUD Act Q29 und Q31 der FAQ von David Rosenthal.

### *Welche besonderen Anforderungen gelten für Berufs- und Amtsgeheimnisträger?*

Sie können sich nicht darauf beschränken zu prüfen, ob ihre Daten im Rahmen ihrer Cloud-Lösung in Drittländer gelangen, die über keine angemessenen Regelungen zum Lawful Access verfügen (wie den USA). Sie müssen prüfen, ob aus irgendeinem ausländischen Staat ein Lawful Access auf die eigenen Daten im Klartext möglich ist. Das gilt allerdings nur für jene gesetzlichen Geheimnisse, bei welchen ein Zugriff durch einen ausländischen Staat eine Rechtsverletzung darstellen würde, was bei bestimmten Berufsgeheimnissen (wie z.B. dem Arztgeheimnis oder dem Apothekergeheimnis) nicht unbedingt der Fall ist.

Hierbei geht es also nicht nur um Behördenzugriffe aus den USA. Haben beispielsweise im Rahmen eines konzerninternen Cloud-Projekts Administratoren aus Deutschland oder Frankreich Zugang zu den berufsgeheimnisgeschützten Daten der Schweizer Niederlassung, so muss geprüft werden, ob diese Administratoren gezwungen werden können, ihren lokalen Behörden bei deren Bedarf Zugang zu den Daten gewähren zu müssen. Kann dies höchstwahrscheinlich ausgeschlossen werden, ist eine Auslagerung mangels anderer Zusicherungen gegenüber den geschützten Personen (z.B. den Kunden) unter diesem Aspekt in der Regel zulässig.

Vgl. zum Bankgeheimnis das Gutachten von Walder Wyss und zum Berufsgeheimnis generell den Aufsatz von David Rosenthal.

### *Passen die Verträge der grossen Cloud-Anbieter? Kann hier überhaupt verhandelt werden?*

Die Standardverträge passen nicht immer vollständig, d.h. es kann Anpassungen speziell für die Schweiz brauchen, damit die Anforderungen des DSG oder sogar des Berufs- oder Amtsgeheimnisses erfüllt werden. Immer mehr Provider bieten aber Zusatzvereinbarungen an, um die Lücke zu schliessen.

Die wichtigsten Punkte, auf die aus Sicht speziell der Schweiz geachtet werden muss ist, dass die Auftragsdatenbearbeitungsvereinbarungen (also die *Data Processing Agreements*, wie sie oft bezeichnet werden) nicht nur auf die DSGVO verweisen und deren Vorgaben berücksichtigen, sondern auch auf das DSG. In Bezug auf die Übermittlung in unsichere Drittländer sollte darauf geachtet werden, dass beim Einsatz der EU-Standardvertragsklauseln die Anpassungen gemäss den Vorgaben des EDÖB zum Einsatz kommen.

Aus Sicht des Berufs- und Amtsgeheimnisses ist eine umfassende Geheimhaltungspflicht mit einer "Defend your data"-Klausel erforderlich, d.h. der Pflicht des Providers, sich gegen jede Herausgabeforderung, deren Erfüllung gegen Schweizer Recht verstossen könnte, rechtlich soweit möglich zu wehren. Die Datenschutzvereinbarungen genügen diesbezüglich nicht immer, da sie spätestens ab dem revidierten DSG nur noch Daten von natürlichen Personen schützen, aber nicht mehr solche von juristischen Personen. Letztere sind durch das Berufs- und Amtsgeheimnis aber weiterhin geschützt. Ferner sollte geregelt werden, dass ein Zugriff

auf Personendaten im Klartext durch Mitarbeiter im Ausland nur mit Zustimmung des Kunden erfolgen darf.

### *Spielt der Standort der Datenspeicherung und der Sitz des Anbieters eine Rolle?*

Ja, der Sitz des Anbieters sollte sich im EWR oder in der Schweiz befinden. Damit unterliegt er der DSGVO oder dem DSG und es kommt nicht zu einem Transfer von Personendaten in einen unsicheren Drittstaat, wenn er mit dem Betrieb der Cloud-Lösung beauftragt wird. Zudem sollten die Daten mit Vorzug (aber nicht zwingenderweise) in der Schweiz gespeichert werden. Damit wird ein zusätzlicher Schutz vor ausländischem Behördenzugriff geschaffen (vgl. Q37 der FAQ von David Rosenthal).

Wird ein in den USA ansässiger Provider beauftragt, liegt hingegen rechtlich ein Transfer von Personendaten in den USA vor, selbst wenn dieser die Speicherung der Daten in Europa zusichert. Aus verschiedenen Gründen ist der Schutz von Personendaten in der Cloud vor dem Zugriff durch US-Behörden besser, wenn ein Kunde den Cloud-Vertrag mit einer Gesellschaft im EWR oder in der Schweiz abschliesst, selbst wenn dieser wiederum die Dienste einer US-Muttergesellschaft beizieht (vgl. u.a. Q29 und Q32 der FAQ von David Rosenthal).

### *Welche Verschlüsselung erfordert das Schweizer Recht?*

Das Schweizer Recht macht bezüglich der Verschlüsselung von Daten keine spezifischen Vorgaben. Es gibt keine Regel, wonach beispielsweise "Bring-your-own-key" (BYOK) Pflicht wäre. Klar ist aber auch, dass der Einsatz von Verschlüsselung heute eine Standard-Massnahme im Bereich der Datensicherheit ist, wobei sie nicht losgelöst von der Frage diskutiert werden kann, wer und unter welchen Umständen Zugriff auf den Schlüssel hat. Es ist heute allerdings akzeptiert und üblich, dass der Schlüssel zur Entschlüsselung von Daten in der Infrastruktur des Providers aufbewahrt wird, weil er dort auch benötigt wird. Eine andere Frage ist, wann und unter welchen Umständen Mitarbeiter des Providers darauf zugreifen dürfen und können.

### *Wie muss eine Risikobeurteilung betreffend US-Recht durchgeführt werden?*

Die Datenschutzbehörden einschliesslich EDÖB schlagen hierzu vor, dass für jeden Transfer von Daten in die USA ein Rechtsgutachten zum US-Recht eingeholt wird. Dies tut in der Praxis aber kaum jemand, weil es zu aufwändig ist und weil das relevante US-Recht bereits gut aufgearbeitet ist. Der EDÖB bietet im Rahmen seiner Anleitung für die Übermittlung von Personendaten in die USA ein Formular an, welches nach unserer Erfahrung selten genutzt wird.

In einigen Fällen bieten die betreffenden Cloud-Anbieter selbst sog. *Transfer Impact Assessments* an um darzulegen, dass ihnen Daten gefahrlos übergeben werden können. Auch verschiedene internationale Anwaltskanzleien bieten Tools für solche Transfer Impact Assessments an, die typischerweise nicht auf einer Analyse der Rechtslage im konkreten Einzelfall basieren, sondern einer generellen Risikoeinschätzung.

Schliesslich gibt es noch die Templates von David Rosenthal, welche für eine Selbsteinschätzung und zur Dokumentation benutzt werden können (siehe dazu den Beitrag auf datenrecht.ch sowie die FAQ von David Rosenthal, welche in Q8 auch die diversen Formen von Risikobeurteilungen näher erläutert).

### *Welche Risiken sind beim Gang in die Cloud sonst zu beachten?*

Aus Sicht des VUD werden die Risiken durch einen ausländischen Behördenzugriff bei den im Markt üblichen Cloud-Projekten überbewertet. Es gibt andere Risiken, denen wesentlich mehr Beachtung geschenkt werden sollte, als es derzeit der Fall ist. Neben der Datensicherheit zum Schutz gegen Cyberkriminelle geht es hierbei unter anderem um die Abhängigkeit, in welche sich ein Kunde begibt, wenn er seine Infrastruktur von einem Cloud-Anbieter betreiben lässt. Diese ist häufig sehr hoch und gute Exit-Konzepte, wie ein Kunde bei Bedarf innert kurzer Frist von einem Cloud-Provider wegkommen kann, bestehen oftmals nicht.

Übersehen wird aus Sicht des Datenschutzes oft auch, welche Daten der eigenen Mitarbeiter des Kunden ein Cloud-Provider allenfalls für eigene Zwecke bearbeitet oder ob er die vom Kunden anvertrauten Daten noch anderweitig nutzt, so etwa für das Training von Systemen der künstlichen Intelligenz. Schliesslich sind sich viele Unternehmen, die in die Welt der Cloud einsteigen, nicht ihrer eigenen Verantwortlichkeiten und Aufgaben bewusst, die verbleiben.

Die Nutzung von Cloud-Lösungen sind zudem nicht "Plug & Play", wie teilweise angenommen wird. So hängt die Datensicherheit bei manchen der Lösungen stark davon ab, wie der Kunde diese konfiguriert und aufsetzt. Auch die Überwachung des Providers und der Lösung kann einiges an Effort und Erfahrung erfordern – und Risiken mit sich bringen, wenn das eine oder andere fehlt.