www.jusletter.ch

David Schwaninger / Stephanie S. Lattmann

Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke

Cloud Computing ist im Trend. Bei der Nutzung dieser Dienstleistung sind jedoch rechtliche Vorgaben und Risiken mit zu berücksichtigen. Der Artikel behandelt zunächst die datenschutzrechtliche Ausgangslage, bevor auf spezifische Aspekte, nämlich die Auslagerung von Patientendaten eines Arztes, Klientendaten eines Anwalts und Bankkundendaten, eingegangen wird. Schliesslich wird die Rückgabe der Daten an den Cloud Nutzer besprochen, wobei auch auf die Frage eingegangen wird, was mit den Daten geschieht, wenn der Cloud Anbieter in Konkurs fällt.

Rechtsgebiet(e): Datenschutz; Verletzung der Berufs- und Amtspflicht; Beiträge

Zitiervorschlag: David Schwaninger / Stephanie S. Lattmann, Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke, in: Jusletter 11. März 2013

ISSN 1424-7410, www.jusletter.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 Editions Weblaw

Inhaltsübersicht

I. Einleitung

[Rz 1] Cloud Computing erfreut sich aktuell wachsender Beliebtheit. Immer mehr Unternehmen bieten unter diesem Titel Lösungen an, welche dem Benutzer grössere Flexibilität und Kostenersparnisse versprechen.

[Rz 2] Während Cloud Services viele Vorteile bieten, geht damit oft auch ein Kontrollverlust über die Daten einher. Für besonders heikle Daten wie Daten über die Gesundheit, unter dem Anwaltsgeheimnis stehende Daten oder Bankkundendaten gelten besondere rechtliche Rahmenbedingungen betreffend Geheimhaltung, Datenschutz und Datensicherheit. Entsprechend empfiehlt es sich, zu prüfen, ob und für welche Bereiche Cloud Dienstleistungen in Anspruch genommen werden sollen.

[Rz 3] Dieser Beitrag beleuchtet zu diesem Zweck verschiedene Themen, welche bei der Nutzung von Cloud-Lösungen zu beachten sind und je nach Art der Verwendung von Clouds zusätzliche Abklärungen oder Vertragsverhandlungen erforderlich machen. Grundlage bildet dabei die schweizerische Gesetzgebung.

[Rz 4] Zum Begrifflichen: Derjenige, der die Cloud Dienstleistungen beansprucht, wird nachfolgend als «Cloud Nutzer», derjenige der die Cloud Dienstleistungen anbietet, als «Cloud Anbieter» bezeichnet. Die Person, deren Daten in der Cloud gespeichert sind, wird als «Dateninhaber» bezeichnet.

II. Allgemeine Datenschutzrechtliche Vorgaben bei der Auslagerung in eine Cloud

[Rz 5] Bei der Auslagerung von Daten in eine Cloud ist insbesondere den Vorschriften zum Datenschutz Rechnung zu tragen. Je nach Art der Daten und den Standorten der Cloud-Rechenzentren bestehen besondere Informations- und Sorgfaltspflichten, die zu beachten sind.

A. Begriffliches (Personendaten, Datenbearbeitung, Bearbeitungsgrundsätze)

[Rz 6] Sobald eine private Person oder ein Bundesorgan innerhalb einer Cloud Daten von natürlichen oder juristischen Personen[1] bearbeitet, ist das eidgenössische Datenschutzgesetz anwendbar (vgl. Art. 2 DSG).[2] Der Begriff des «Bearbeitens» von Daten ist breit zu verstehen, indem darunter jeder Umgang mit Personendaten fällt, unabhängig von den angewandten Mitteln und Verfahren. So sind darunter insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder das Vernichten von Daten zu subsumieren (Art. 3 lit. e DSG). Damit stellt bspw. allein schon das Speichern von Kundendaten oder die Aktualisierung und Erfassung solcher Daten in der Cloud eine Bearbeitung im Sinne des DSG dar.

[Rz 7] Werden Daten anonymisiert, pseudonymisiert oder verschlüsselt, handelt es sich in der Regel nicht um Personendaten im Sinne des Gesetzes.[3] Dennoch ist auch hier Vorsicht geboten: Werden z.B. Patientennamen durch eine Nummer ersetzt, reicht dies zur Pseudonymisierung (und damit zum Ausschluss des Datenschutzgesetzes) nicht aus, wenn aufgrund anderer individualisierender Merkmale eine personenbezogene Zuordnung nach wie vor möglich ist (was meist der Fall ist).[4]

[Rz 8] Qualifizierte Personendaten sind die sog. besonders schützenswerten Personendaten. Darunter fallen Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen (Art. 3 lit. c DSG).

[Rz 9] Das Datenschutzgesetz sieht folgende Datenbearbeitungsgrundsätze vor (vgl. Art. 4 und 5 DSG): Personendaten dürfen nur rechtmässig erhoben werden (d.h. ohne Gewalt, Arglist, Drohung oder Täuschung gegenüber den betroffenen Personen). Sie müssen nach Treu und Glauben bearbeitet werden. Personendaten dürfen ausserdem nur zu

---

[1] Im Gegensatz zu anderen Staaten (auch innerhalb der EU, welche in ihrer Richtlinie 95/46/EG als Mindeststandard lediglich den Schutz von Daten für natürliche Personen vorsieht) werden nach Schweizer Recht auch Daten von juristischen Personen vom Datenschutzgesetz erfasst.

[2] Das DSG gilt nur für private Rechtssubjekte und Bundesorgane (Art. 2 Abs. 1 DSG). Für Gemeinden oder kantonale Organe gelten die Datenschutzbestimmungen des jeweiligen Kantons.

[3] Philippe Fuchs, Cloud Computing – eine datenschutzrechtliche Betrachtung, in: Jusletter IT, 6. Juni 2012, Rz. 12.

[4] Ursula Widmer, Gesundheitsdaten in der Cloud, in: P. Scharter/J. Taeger (Hrsg), "D"A"CH Security 2011, syssec 2011, S. 166-177, S. 176 f.

dem Zweck bearbeitet werden, der bei deren Beschaffung angegeben wurde, der aus den Umständen ersichtlich oder gesetzlich vorgegeben ist (Zweckbindung).[5]

B. Auslagerung in die Cloud grundsätzlich zulässig (Art. 10a DSG)

[Rz 10] Speichert ein Cloud Nutzer Personendaten nicht auf seinem eigenen Server, sondern auf einer Cloud, lässt er Personendaten im datenschutzrechtlichen Sinn durch einen Dritten bearbeiten (sog. Datenbearbeitung durch Dritte, auch Auftragsbearbeitung genannt).[6] Die Weitergabe von Personendaten zur Bearbeitung an Dritte (Cloud Anbieter) ist grundsätzlich zulässig, und zwar auch ohne Einwilligung der betroffenen Personen, *sofern* die Daten vom Dritten (Cloud Anbieter) nur so bearbeitet werden, wie der Cloud Nutzer es selber tun dürfte und keine gesetzliche oder vertragliche Geheimhaltungspflicht die Bearbeitung durch einen Dritten verbietet.[7] Ausserdem muss sich der Cloud Nutzer vergewissern, dass der Cloud Anbieter die Datensicherheit gewährleistet (Art. 10a DSG).[8] Eine Auftragsbearbeitung darf nur für die Zwecke des Auftraggebers, d.h. des Cloud Nutzers, erfolgen, also weder für die Zwecke des Cloud Anbieters noch für die Zwecke anderer Personen.[9]

[Rz 11] Die Konsequenz einer solchen Auftragsbearbeitung (unter den geschilderten Voraussetzungen) ist, dass der Cloud Anbieter im Verhältnis zum Cloud Nutzer nicht als Dritter betrachtet wird.[10]

[Rz 12] Der Cloud Nutzer muss den Cloud Anbieter jedoch sorgfältig auswählen und sicherstellen, dass dieser die notwendigen Voraussetzungen für eine datenschutzkonforme Datenbearbeitung erfüllt und insb. die Datensicherheit gewährleisten kann.[11] Das Mass der Sorgfalt steigt dabei je vertraulicher und schützenswerter die zu bearbeitenden Daten sind.[12] Der Cloud Nutzer muss den Cloud Anbieter entsprechend instruieren, insbesondere über den erlaubten Zweck und den Umfang der Datenbearbeitung sowie die einzuhaltenden Sicherheitsstandards, und sich ein Weisungsrecht in Bezug auf die Datenbearbeitung ausbedingen.[13] Wichtig ist zudem eine gewisse Überwachung des Cloud Anbieters.[14]

[Rz 13] Der Cloud Anbieter kann sich (vertraglich) den Beizug von Sub-Providern vorbehalten, wobei diesfalls wiederum die Regeln betreffend Datenbearbeitung durch Dritte zu beachten sind.[15] Beim Beizug von Sub-Providern muss aus Sicht des Cloud Nutzers sichergestellt werden, dass der Sub-Provider dieselben Pflichten hat wie der Cloud Anbieter. Auch ist es empfehlenswert, eine Geheimhaltungspflicht des Cloud Anbieters und allfälliger Sub-Provider zu statuieren, welche diejenigen Arbeitnehmer des Cloud Anbieters miteinbezieht, die mit den Daten in Berührung kommen.

[Rz 14] Stellt der Cloud Nutzer datenschutzrelevante Verfehlungen des Cloud Anbieters (oder Sub-Providers) fest, muss er Konsequenzen ziehen. Wenn der Cloud Anbieter z.B. keine angemessene Datensicherheit mehr bietet, kann es aufgrund der Sorgfaltspflicht des Cloud Nutzers erforderlich sein, dass keine weiteren Datenbearbeitungen in der Cloud stattfinden bzw. dass die Zusammenarbeit mit dem Cloud Anbieter beendet wird.[16]

C. Cloud Services mit Auslandsberührung (Art. 6 DSG)

[Rz 15] Der Cloud Anbieter stellt dem Cloud Nutzer für die Speicherung der Daten Server zur Verfügung. Im Gegensatz zu einem klassischen Outsourcing ist für Letzteren grundsätzlich nicht erkennbar, wo die Server, auf denen die Daten gespeichert sind, sich befinden.[17] Liegt ein Server ausserhalb der Schweiz, ist dies von zusätzlicher datenschutzrechtlicher Relevanz (selbst bei einer Auftragsbearbeitung).

[Rz 16] Gemäss Art. 6 Abs. 1 DSG dürfen Personendaten nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. Ob aus Schweizer Perspektive ein angemessener Schutz in einem Land besteht, lässt sich anhand der vom Eidg. Datenschutz- und Öffentlichkeitsbeauftragten («EDÖB») publizierten Staatenliste eruieren.[18] Einen angemessenen gesetzlichen Datenschutz für Daten von natürlichen Personen weisen bspw. die Mitgliedstaaten der EU und des EWR sowie Israel und Argentinien auf. Einzelne dieser Staaten (z.B. das Fürstentum Liechtenstein oder Argentinien) sehen auch den Schutz

---

5 EDÖB, Leitfaden für die Bearbeitung von Personendaten im privaten Bereich, August 2009, S. 4.

6 Fuchs, a.a.O., Rz. 13.

7 Siehe dazu hinten Ziff. III.

8 Widmer, a.a.O., S. 171.

9 David Rosenthal/Yvonne Jöhri, in: Handkommentar zum Datenschutzgesetz, Zürich/Basel/Genf 2008, Art. 10a N 14.

10 Fuchs, a.a.O., Rz. 13.

11 Corrado Rampini, in: BSK zum DSG, 2. Aufl. 2006, Art. 14 N 11; David Rosenthal, in: Handkommentar zum Datenschutzgesetz, a.a.O., Art. 10a N 48 f.; Lukas Morscher, Aktuelle Entwicklungen im Technologie- und Kommunikationsrecht, in: ZBJV 147/2011, S. 177–221, S. 218.

12 Fuchs, a.a.O., Fn. 22.

13 Rampini, a.a.O., Art. 14 N 11; Fuchs, a.a.O., Rz. 14; Rosenthal, a.a.O., Art. 10a N 52 ff.

14 Rampini, a.a.O., Art. 14 N 11; Fuchs, a.a.O., Rz. 14; Rosenthal, a.a.O., Art. 10a N 63.

15 Fuchs, a.a.O., Rz. 14 mit Verweis auf Rosenthal, a.a.O., Art. 10a N 77.

16 Fuchs, a.a.O., Rz. 15.

17 Fuchs, a.a.O., Rz. 16.

18 Vgl. Staatenliste unter http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=de, zuletzt besucht am 13. Februar 2013.

von Daten juristischer Personen vor. Die USA fallen gemäss EDÖB nur darunter, wenn der Datenempfänger (Cloud Anbieter) dem Safe Harbor Framework beigetreten und auf der Liste des U.S. Department of Commerce verzeichnet ist. Mit Bezug auf Staaten, die keinen genügenden Datenschutz für natürliche oder juristische Personen vorsehen, müssen zusätzliche Voraussetzungen erfüllt werden (s. dazu anschliessend).[19]

[Rz 17] Fehlt eine Gesetzgebung, die einen angemessenen Datenschutz gewährleistet, können Personendaten dennoch ins Ausland bekannt gegeben werden, sofern eine der Voraussetzungen von Art. 6 Abs. 2 DSG erfüllt ist. Darunter fallen bspw. die Einwilligung der betroffenen Person im konkreten Einzelfall oder «hinreichende Garantien», insbesondere durch Vertrag, die einen angemessenen Schutz im Ausland gewährleisten. Als «hinreichende Garantie» gilt z.B. der vom EDÖB publizierte Muster-Outsourcing-Vertrag: Werden die entsprechenden Standardbedingungen verwendet, hat beim EDÖB lediglich eine Meldung zu erfolgen (Informationspflicht betreffend Abschluss eines solchen Vertrages). Wenn die Standardbedingungen dagegen nicht verwendet werden, muss der Vertrag zur Prüfung und Genehmigung beim EDÖB eingereicht werden (Prüfungspflicht des EDÖB).[20]

[Rz 18] Ob überhaupt eine Datenbekanntgabe ins bzw. Datenbearbeitung im Ausland stattfindet, ist nicht anhand des Sitzes des Cloud Anbieters zu ermitteln, sondern vielmehr aufgrund des tatsächlichen Ortes der Datenbearbeitung. Dies dürfte gemeinhin der Standort des oder der jeweiligen Server sein.[21]

[Rz 19] Der Cloud Nutzer wird dem Cloud Anbieter demnach vertraglich die Pflicht auferlegen wollen, für einen angemessenen Schutz der Daten zu sorgen oder nur Server zu verwenden, die sich in Ländern befinden, welche aus Schweizer Sicht einen angemessenen Datenschutz garantieren oder sonst die zusätzlichen Voraussetzungen gemäss Art. 6 Abs. 2 DSG zu erfüllen.[22]

[Rz 20] Cloud Anbieter ziehen regelmässig Sub-Provider bei (z.B. bei Auslastung der eigenen Speicherkapazitäten). In diesen Fällen besteht die praktische Schwierigkeit, dass alle Teilnehmer in der Cloud, auf deren Servern personenbezogene Daten bearbeitet werden, vertraglich eingebunden werden müssen.[23] Der Cloud Nutzer wird sich daher vergewissern wollen, dass der Cloud Anbieter einem allfälligen Sub-Provider mit Servern im Ausland die gleichen Pflichten auferlegt, wie er sie selbst hat.[24]

[19] EDÖB, Die Datenübermittlung ins Ausland kurz erklärt, April 2011, Ziff. 11.

[20] Widmer, a.a.O., S. 172 f.; EDÖB, Erläuterungen zur Übermittlung von Personendaten ins Ausland nach revidiertem DSG, April 2011, S. 11.

[21] Fuchs, a.a.O., Rz. 18.

[22] Fuchs, a.a.O., Rz. 19.

[23] EDÖB, Erläuterungen zu Cloud Computing, Oktober 2011, S. 4.

[24] Fuchs, a.a.O., Rz. 20.

D. Datensicherheit (Art. 7 DSG)

[Rz 21] Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Art. 7 DSG). Dabei muss für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten gesorgt sein (Art. 8 der Verordnung zum DSG), wobei insbesondere folgende Risiken abgesichert werden müssen:

- unbefugte oder zufällige Vernichtung;
- zufälliger Verlust;
- technische Fehler;
- Fälschung, Diebstahl oder widerrechtliche Verwendung;
- unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen.

[Rz 22] Bei der Auswahl «seines» Cloud Anbieters muss sich der Cloud Nutzer vergewissern, dass der Cloud Anbieter diese Voraussetzungen einhält bzw. dass er die Daten gegen die genannten Risiken schützt. Gemäss EDÖB sind die technischen und organisatorischen Massnahmen periodisch vor Ort zu überprüfen.[25] Eine Vor-Ort-Kontrolle ist aber vielfach unrealistisch, da der Cloud Anbieter für seine Cloud Dienstleistungen unter Umständen Server nutzt, die über die ganze Welt verstreut sind.[26] Eine Antwort auf die Frage, wie diese Pflicht effektiv wahrgenommen werden soll, insbesondere, wenn die Server sich im Ausland befinden, gibt das Gesetz nicht. Allenfalls wären regelmässige Reportings des Cloud Anbieters zumindest ein möglicher Kompromiss.

III. Besonderheiten bei gesetzlich geschützten Daten

[Rz 23] Die Offenbarung von anvertrauten Informationen ist in verschiedenen Berufen und Branchen strafbar. Nachfolgend wird am Beispiel von Patientendaten, Klientendaten von Anwälten und Bankkundendaten aufgezeigt, unter welchen Voraussetzungen diese Daten in eine Cloud ausgelagert werden können.

A. Auslagerung von Patientendaten eines Arztes

1. Allgemeines

[Rz 24] Patientendaten stellen in aller Regel besonders schützenswerte Personendaten i.S.v. Art. 3 lit. c DSG dar. Ärzte, Zahnärzte und deren Hilfspersonen unterstehen einem Berufsgeheimnis, das von Art. 321 StGB geschützt wird. Die Verletzung dieses Berufsgeheimnisses («Arztgeheimnis»)

[25] EDÖB, Erläuterungen zu Cloud Computing, Oktober 2011, S. 3.

[26] Fuchs, a.a.O., Rz. 23.

wird auf Antrag mit Geldstrafe oder Freiheitsstrafe bis zu drei Jahren bestraft.

[Rz 25] Die Auslagerung von Patientendaten an externe Informatikdienstleister wie Cloud Anbieter ist heutzutage gängige Praxis.[27] Aufgrund von Effizienz- und Spezialisierungsüberlegungen besteht bei Ärzten und Ärztenetzwerken, aber auch bei Spitälern ein grosses Bedürfnis nach solchen Dienstleistungen. Gerade selbständige Ärzte können von Datenauslagerungen profitieren, damit sie verstärkt ihrer eigentlichen (Arzt-)Tätigkeit nachgehen können.[28]

2. Schweizer Cloud Anbieter mit Server im Inland: Hilfsperson

[Rz 26] Gemäss Art. 321 StGB unterstehen auch die Hilfspersonen von Ärzten und Zahnärzten der berufsspezifischen Geheimhaltungspflicht. Der Gesetzgeber anerkennt somit, dass es für einen Arzt unmöglich ist, alle administrativen und technischen Arbeiten selber zu erledigen. Da die entsprechenden Hilfspersonen zwangsläufig mit strafrechtlich relevanten Daten im Sinne des Arztgeheimnisses in Berührung kommen, werden sie ebenfalls dem Arztgeheimnis unterstellt.[29]

[Rz 27] Hilfsperson ist bereits, wer bei der Berufstätigkeit des (Haupt-) Geheimnisträgers in einer solchen Weise mitwirkt, dass er grundsätzlich von den dabei wahrgenommenen Tatsachen ebenfalls Kenntnis erhält.[30] Eine besondere Stellung bei der Aufgabenerfüllung ist nicht vorausgesetzt.[31]

[Rz 28] Wer entsprechend für einen Arzt IT-Infrastruktur zur Verfügung stellt, wartet oder betreut und diesen damit bei seiner Berufstätigkeit unterstützt, gilt als Hilfsperson im Sinne von Art. 321 StGB.[32] Dies gilt demnach auch für Cloud Anbieter, die für einen Arzt z.B. einen Server zur Verfügung stellen.[33]

[Rz 29] Die Qualifikation des Cloud Anbieters als Hilfsperson ist von entscheidender Bedeutung. Die Weitergabe von Berufsgeheimnissen an dritte Personen ist nämlich dann nicht strafbar, wenn diese dritte Person (als Hilfsperson) ebenfalls dem Berufsgeheimnis unterliegt.[34] Entsprechend begeht der Arzt keine Geheimnisverletzung, wenn er die Patientendaten einem Cloud Anbieter übergibt, welcher Sitz und Rechenzentren in der Schweiz hat und nicht mit Sub-Providern im Ausland zusammen arbeitet (Swiss Cloud).

[Rz 30] Als Ausfluss der datenschutzrechtlichen Prinzipien gilt es aber zu beachten, dass nur «soviele» und «solche» Patientendaten in die Cloud übertragen werden dürfen, wie dies für den spezifischen Auslagerungszweck notwendig ist und dass nur diejenigen Arbeitnehmer des Cloud Anbieters auf die Patientendaten zugreifen können dürfen, welche einen solchen Zugriff zur Aufgabenerfüllung unmittelbar benötigen.[35] Der Arzt wird daher vor einem Outsourcing von Patientendaten in die Cloud vertraglich sicherstellen wollen, dass der Cloud Anbieter sich an diese Grundsätze hält.

3. Cloud Anbieter oder Cloud-Server im Ausland: Keine Hilfsperson

[Rz 31] Befindet sich der Cloud Anbieter oder zumindest der Cloud-Server im Ausland, kann dieser nicht mehr als «Hilfsperson» im obigen Sinne gelten, da er in einem solchen Fall nicht der schweizerischen Strafgesetzgebung untersteht bzw. das Schweizer Strafrecht nicht (oder nicht gleich effektiv) durchgesetzt werden kann. Diese Meinung wird auch vor dem Hintergrund vertreten, dass ausländische Behörden (welche nicht an das Schweizer Berufsgeheimnis gebunden sind) einen Cloud Anbieter – je nach der lokalen Gesetzgebung – unter Umständen verpflichten können, die in der Cloud gespeicherten Daten heraus-/ bekanntzugeben.[36]

[Rz 32] Sollten Patientendaten in eine ausländische Cloud ausgelagert werden, bedarf es daher als unverzichtbare Voraussetzung der Einwilligung der betroffenen Patienten (unter Hinweis auf sämtliche Risiken). Ansonsten stellt eine solche Datenweitergabe eine Arztgeheimnisverletzung dar.[37] In der Praxis dürfte das Einholen von Einwilligungen aber oftmals kaum möglich sein, so bspw. betreffend Daten, welche lange zurückliegende, abgeschlossene Fälle betreffen. Eine Auslagerung in eine ausländische Cloud kommt damit wohl nur für die aktuellen sowie künftigen Fälle in Frage. Hierbei dürften sich entsprechende, von den Patienten zu unterzeichnende Formulare anbieten, welche diese ausführlich darüber informieren sollten, welche Daten in eine ausländische Cloud ausgelagert werden, zu welchem Zweck, und mit welchen Risiken dies allenfalls verbunden ist.[38] Betreffend Risiken dürfte es aus Sicht des Arztes ratsam sein, auch auf das nicht auszuschliessende Risiko allfälliger Zugriffe durch ausländische Behörden hinzuweisen.

---

[27] Medienmitteilung des Datenschutzbeauftragten des Kantons Zürich vom 26. April 2011, Tätigkeitsbericht 2010 des Datenschutzbeauftragten, S. 2.

[28] Vgl. auch Ursula Uttinger, Regulatorische Anforderungen an IT-Outsourcing: Gesundheits- und Versicherungsbereich, in: R. Weber/M. Berger/R. Auf der Maur, IT-Outsourcing, ICT: Rechtspraxis I, 2003, S. 255–270, S. 258.

[29] Vgl. Christian Peter, Die Zulässigkeit der Auslagerung der Bearbeitung der Patientendaten von Spitälern an externe Informatikdienstleister, in: Jusletter vom 22. Juni 2009, Rz. 3.

[30] Stefan Trechsel, StGB Kurzkommentar, Zürich/St. Gallen 2008, Art. 321 N 13.

[31] Niklaus Oberholzer, BSK-StGB II, Basel 2007, Art. 321 N 6.

[32] Peter, a.a.O., Rz. 8.

[33] Vgl. Uttinger, a.a.O., S. 259.

[34] Peter, a.a.O., Rz. 9.

[35] Vgl. auch Peter, a.a.O., Rz. 15.

[36] Widmer, a.a.O., S. 170; Rampini, a.a.O., Art. 14 N 15; Ursula Widmer, Rechtliche Rahmenbedingungen für das Outsourcing im Spitalbereich – Weitergabe von Patientendaten, in: datamaster, September 2007, S. 19–21, S. 20.

[37] Widmer, a.a.O., S. 174.

[38] Widmer, a.a.O., S. 174.

B. Auslagerung von Klientendaten eines Anwalts

[Rz 33] Wie verhält es sich, wenn ein Anwalt oder eine Anwaltskanzlei Daten mit Bezug zu Klienten in eine Cloud auslagern möchte?

[Rz 34] Auch Rechtsanwälte und deren Hilfspersonen unterstehen einem Berufsgeheimnis («Anwaltsgeheimnis»), das von Art. 321 StGB geschützt wird.

[Rz 35] Es gelten die gleichen Grundsätze wie beim Arztgeheimnis. So ist der Schweizer Cloud Anbieter, dessen Server sich im Inland befinden, als Hilfsperson im Sinne von Art. 321 StGB zu betrachten, so dass eine Auslagerung von Klientendaten diesfalls als zulässig zu erachten ist. Anders verhält es sich bei Cloud Anbietern im Ausland oder im Fall, dass der Cloud-Server im Ausland steht: Unter Berücksichtigung der dargelegten Grundsätze betreffend Patientendaten ist eine explizite Einwilligung des Klienten notwendig, um ihn betreffende Daten in eine Cloud auszulagern.

[Rz 36] Im Übrigen ist nicht auszuschliessen, dass eine Anwaltsgeheimnisverletzung vorliegt, wenn die Möglichkeit eines Durchgriffs auf die Daten durch ausländische Behörden besteht und der Anwalt dies wusste oder hätte wissen müssen.

C. Auslagerung von Bankkundendaten

[Rz 37] Darf eine Bank Daten in Zusammenhang mit ihren Kunden in eine Cloud auslagern? Diese Frage stellt sich insbesondere vor dem Hintergrund des Bankkundengeheimnisses, welches in Art. 47 des Bundesgesetzes über die Banken und Sparkassen geregelt ist.[39]

[Rz 38] Die Eidg. Finanzmarktaufsicht (FINMA) hat im Jahr 2008 ein Rundschreiben erlassen, welches sich mit dem Thema der Auslagerung von Geschäftsbereichen bei Banken beschäftigt. Als Auslagerungen, die vom Rundschreiben erfasst sind, werden bspw. die Datenaufbewahrung, der Betrieb und Unterhalt von Datenbanken und das Nachführen und Erstellen von Kundenadressen oder Kundenprofilen genannt.[40] Die in dem Rundschreiben formulierten Grundsätze sind auch bei der Auslagerung von Bankkundendaten in eine Cloud zu berücksichtigen.

[Rz 39] Demnach muss eine Bank als Cloud Nutzerin unter anderem Folgendes beachten:

[Rz 40] Der Cloud Anbieter muss sich dem Bankgeheimnis der auslagernden Bank unterstellen. Er hat sich ausdrücklich zu verpflichten, die daraus folgende Vertraulichkeit zu wahren.[41]

[Rz 41] Bankkunden, deren Daten an einen Cloud Anbieter gelangen, müssen über die Auslagerung informiert werden und zwar *vor* der Auslagerung der Daten. Die Information kann z.B. über die Allgemeinen Geschäftsbedingungen, in Depotreglementen, in Kontoauszügen, Informationsbroschüren oder in Briefform erfolgen. Dabei muss auf die getroffenen Sicherheitsvorkehrungen hingewiesen und dem Kunden die Möglichkeit eingeräumt werden, innert einer angemessenen Frist und ohne Nachteile das Vertragsverhältnis zu kündigen.[42]

[Rz 42] Mit dieser grundsätzlichen Informationspflicht geht man bei der Auslagerung von Bankkundendaten also einen Schritt weiter als bei Patienten- und Klientendaten. Bei letzteren beiden entfällt, wie bereits gesehen, zumindest im Falle eines Swiss Cloud Anbieters aufgrund dessen Hilfspersonenstellung eine Informationspflicht. Dafür ist bei der Auslagerung von Bankkundendaten keine explizite Einwilligung des Kunden erforderlich.

[Rz 43] Für das Outsourcing von Geschäftsbereichen (inkl. Kundendaten) ins Ausland gelten gemäss FINMA spezielle Regeln, die auch für das Cloud Computing Geltung haben müssen: Konkret muss der Cloud Nutzer nachweisen, dass er, seine banken- oder börsenrechtliche Prüfgesellschaft sowie die FINMA ihre Prüfrechte wahrnehmen und rechtlich auch durchsetzen können. Der Nachweis kann z.B. mittels Rechtsgutachten oder Bestätigungen einer entsprechenden Aufsichtsbehörde erbracht werden. Die banken- oder börsengesetzliche Prüfgesellschaft hat den Nachweis vor der Auslagerung zu prüfen.[43]

[Rz 44] Die Bank als Cloud Nutzer, deren interne Revision und externe Prüfgesellschaft sowie die FINMA müssen den ausgelagerten Geschäftsbereich vollumfänglich, jederzeit und ungehindert einsehen und prüfen können.[44] Auch darf das Auslagern in die Cloud die Regulierung und Aufsicht durch die FINMA nicht beeinträchtigen, auch nicht bei einer Auslagerung ins Ausland oder durch Gruppengesellschaften im Ausland.[45]

[Rz 45] Der Cloud Anbieter, der nicht der Aufsicht der FINMA untersteht, hat sich gegenüber dem Cloud Nutzer vertraglich zu verpflichten, der FINMA sämtliche Auskünfte und Unterlagen in Bezug auf den ausgelagerten Geschäftsbereich zu geben, die sie für ihre Aufsichtstätigkeit benötigt.[46]

[Rz 46] Ausserdem schreibt die FINMA beim Outsourcing

---

[39] Dasselbe Geheimnis gilt auch für Börsen und Effektenhändler gemäss Art. 43 des Bundesgesetzes über die Börsen und den Effektenhandel.

[40] Eidg. Finanzmarktaufsicht FINMA, Rundschreiben 2008/7 – Outsourcing Banken; Auslagerung von Geschäftsbereichen bei Banken, 20. November 2008 (nachfolgend «FINMA Rundschreiben»), Rz. 5 und 7 des Anhangs.

[41] FINMA, Rundschreiben, Rz. 34.

[42] FINMA Rundschreiben, Rz. 37 ff.

[43] FINMA Rundschreiben, Rz. 49 f.

[44] FINMA Rundschreiben, Rz. 40.

[45] FINMA Rundschreiben, Rz. 46.

[46] FINMA Rundschreiben, Rz. 47.

explizit eine Formvorschrift vor, indem ein schriftlicher Vertrag zwischen der Bank und dem Anbieter abzuschliessen sei. Dasselbe muss auch für die Auslagerung von Daten in Clouds gelten.[47] Ob und inwiefern die Erfüllung all dieser Vorgaben eine Auslagerung von Bankkundendaten noch lohnenswert macht, ist daher sorgfältig abzuwägen.

[Rz 47] Zu beachten ist, dass die oben genannten besonderen Grundsätze zusätzlich zu den allgemeinen datenschutzrechtlichen Grundsätzen gelten.

IV. Rückgabe von Daten an den Cloud Nutzer

[Rz 48] Durch das Auslagern von Daten in eine Cloud überträgt der Cloud Nutzer dem Cloud Anbieter in den meisten Fällen die Verwaltung dieser Daten. Aktualisierungen und Änderungen im Datenbestand erfolgen mit Ausnahme von Cloud Lösungen, die einzig zur Sicherung von Daten an einem zweiten Ort dienen (Backup), beim Cloud Anbieter. Dies führt zu einer Abhängigkeit des Cloud Nutzers gegenüber dem Cloud Anbieter.

A. Allgemeines

[Rz 49] Es ist denkbar, dass ein Cloud Nutzer den Cloud Anbieter nach einiger Zeit wechseln oder gänzlich auf eine Cloud Lösung verzichten will. In diesen Fällen wird der Cloud Nutzer darauf angewiesen sein, dass er die ursprünglich ausgelagerten Daten vom Cloud Anbieter in der aktuellsten Version «zurück» erhält. Je nach Art der in eine Cloud ausgelagerten Daten würde er ansonsten Gefahr laufen, dass er gesetzliche Aufbewahrungspflichten[48], datenschutzrechtliche Pflichten (z.B. Auskunftspflicht) oder Herausgabepflichten gegenüber eigenen Kunden nicht mehr erfüllen und im Extremfall seine Geschäftstätigkeit zumindest für eine gewisse Zeit nicht mehr betreiben kann.

[Rz 50] Die Daten sollten dem Cloud Nutzer dabei in einem Format übergeben werden, welches ihm erlaubt, diese wieder in eine eigene IT-Umgebung oder in die Cloud eines anderen Anbieters zu integrieren. Ansonsten besteht die Gefahr, dass die Daten wegen nicht vorhandener standardisierter Technologien und Schnittstellen nicht (mehr) oder nur mit grossem finanziellem und/oder technischem Aufwand in das eigene IT-System zurückgeführt oder zu einem anderen Cloud Anbieter migriert werden (Lock-in Effekt).[49] Wie sich die Rückgabemodalitäten gestalten sollen, ist daher bereits bei der Auswahl eines Cloud Anbieters zu klären und vertraglich zu regeln. Da der Cloud Provider nach Ende der vertraglichen Zusammenarbeit mit dem Cloud Nutzer keine Berechtigung mehr zur Datenbearbeitung im Sinne von Art. 10a DSG hat, ist der Cloud Nutzer gehalten, den Cloud Anbieter zu verpflichten, die Daten vollständig und ohne Rückbehalt von Sicherungskopien zurückzugeben bzw. allfällige Kopien der Daten zu vernichten.

B. Konkurs eines Cloud Anbieters

[Rz 51] Wie in jedem anderen Geschäftsbereich auch kann nicht ausgeschlossen werden, dass gegen einen Cloud Anbieter (oder dessen Sub-Provider) ein Insolvenzverfahren eröffnet wird. Für den Cloud Nutzer wird sich in einem solchen Fall die Frage stellen, ob die von ihm genutzte Cloud Lösung weiter betrieben wird oder zu welchen Bedingungen er die aktuellen Daten vom Cloud Anbieter zurück erhält.

[Rz 52] Die Beantwortung dieser Fragen hängt davon ab, welches Insolvenzrecht zur Anwendung gelangt. Dies wiederum bestimmt sich in der Regel danach, wo der insolvente Cloud Anbieter seinen Sitz, allenfalls seine von einem Insolvenzverfahren betroffene Geschäftsniederlassung hat oder wo er sein Rechenzentrum betreibt.[50]

[Rz 53] Die nachfolgenden Ausführungen beschränken sich auf den Fall, dass ein insolventer Cloud Anbieter seinen Sitz sowie Rechenzentren in der Schweiz hat und nicht mit Sub-Providern im Ausland zusammen arbeitet (Swiss Cloud). Dabei zeigt sich, dass sich auch bei einer Swiss Cloud, welche von einem Insolvenzverfahren (bzw. nach schweizerischer Terminologie Konkursverfahren) betroffen ist, Fragen und Risiken ergeben, die bereits bei der Auswahl des Cloud Anbieters zu beachten sind.

1. Kein Anspruch auf Herausgabe von Daten

[Rz 54] Gemäss Art. 211 Abs. 1 SchKG werden im Konkursfall Forderungen, welche nicht eine Geldzahlung zum Gegenstand haben, in Geldforderungen von entsprechendem Werte umgewandelt. Diese so kalkulierte Geldforderung wird dann zusammen mit allen weiteren (Geld-)Forderungen in den Kollokationsplan aufgenommen (vgl. Art. 247 SchKG). Je nachdem, ob und wie viel Geld bei der Verwertung der Konkursmasse noch eingenommen werden kann, erhalten die Gläubiger anteilsweise etwas für ihre Forderung zurück erstattet (Konkursdividende).

[Rz 55] Zwar kann ein Gläubiger Sachen, die in seinem Eigentum stehen oder die in seinem Auftrag von dem konkursiten Schuldner erworben wurden (Art. 401 Abs. 3 OR), mit Hilfe der Aussonderungsklage herausverlangen (Art. 242 SchKG). Diese Möglichkeit gilt jedoch nach ständiger bundesgerichtlicher Rechtsprechung nur für körperliche Gegenstände.[51]

---

[47] FINMA Rundschreiben, Rz. 51 f.

[48] Beispielsweise die Pflicht zur Aufbewahrung der Geschäftsbücher gemäss Art. 958 f. OR.

[49] EDÖB: Erläuterungen zu Cloud Computing, Oktober 2011, S. 2.

[50] Vgl. u.a. Karl Spühler, Schuldbetreibungs- und Konkursrecht I, 5. Aufl., Zürich 2011, S. 50 mit weiteren Hinweisen.

[51] Marc Russenberger, in BSK zum SchKG II, 2. Aufl., Basel 2010, Art. 242

Elektronische Daten auf Servern, die im Eigentum des Cloud Anbieters stehen, sind keine körperlichen Gegenstände, womit ein Herausgabeanspruch nicht besteht.[52] Zwar hätte ein Gläubiger im Konkurs des Cloud Anbieters die Möglichkeit, eine Sicherheitsleistung zu verlangen und vom Vertrag zurück zu treten, wenn nicht innert angemessener Frist eine Sicherheit geleistet wird (vgl. Art. 83 Abs. 2 OR). Dies hilft einem betroffenen Cloud Nutzer jedoch nicht, wenn er die Daten bereits dem Cloud Anbieter übergeben hat und diese schon auf dessen Servern aktualisiert wurden, da er dann keinen Herausgabeanspruch hat. Vielmehr wird seine Forderung auf Rückleistung wie vorhin beschrieben in eine geldwerte Forderung umgewandelt.[53]

[Rz 56] Für den Cloud Nutzer würde ein Konkurs seines Cloud Anbieters demnach bedeuten, dass er grundsätzlich keinen Anspruch auf Herausgabe seiner Daten hat. Hinzu kommt, dass Konkurse oftmals mit einer sehr tiefen oder gar keiner Konkursdividende enden. Dies gilt vor allem für die nicht privilegierten Forderungen (3. Klasse), welche nur dann befriedigt werden, wenn alle pfandgesicherten und vorrangigen Forderungen der 1. und 2. Klasse vollumfänglich befriedigt werden können (Art. 219 SchKG). Üblicherweise werden Forderungen eines Cloud Nutzers zur 3. Klasse gehören, womit ein Cloud Nutzer bei einem Konkurs des Cloud Anbieters wohl häufig auch keine finanzielle Entschädigung erhält.

[Rz 57] Es ist denkbar, dass die Konkursverwaltung das Geschäft des Cloud Anbieters (zumindest für beschränkte Zeit) weiter führt (Art. 211 Abs. 2 SchKG). Eine Verpflichtung dazu besteht jedoch nicht. Ebenfalls wird ein Cloud Nutzer die Möglichkeit erhalten, seine Daten (gegen zusätzliches Entgelt) noch zu beziehen, aber auch darauf besteht nicht zwingend ein Anspruch. Demnach ist das Risiko eines nie ganz auszuschliessenden Konkurses bei der Auswahl des Cloud Anbieters und bei der Gestaltung der Verträge mit zu berücksichtigen (s. sogleich).

2. Verwertung von Daten

[Rz 58] Im Konkurs eines Cloud Anbieters wird sich auch die Frage stellen, ob Daten auf seinen Servern einen Wert haben und ob diese gar verwertet werden können, indem sie an einen Dritten verkauft werden.

[Rz 59] Die Verwertung von Aktiven, wie sie auch Daten darstellen können, gehört zu den Aufgaben der Konkursverwaltung (Art. 252 ff. SchKG). Die Konkursverwaltungen wiederum sind kantonal organisiert und unterstehen den kantonalen Datenschutzgesetzen (vgl. Art. 2 Abs. 1 DSG e contrario). Der Datenschutzbeauftragte des Kantons Zürich (DSB) hat sich mit der Frage befasst, ob Personendaten im Rahmen eines Konkurses verwertet werden dürfen. Er hat diese Frage grundsätzlich bejaht, sofern es sich bei diesen Daten um Aktiven handelt.[54] In jedem Fall sei jedoch zuerst eine Interessenabwägung vorzunehmen. Liegen keine überwiegenden privaten oder öffentlichen Interessen vor, die gegen eine Verwertung von Personendaten sprechen, sei diese zulässig. Der DSB hat dies beispielsweise für Daten von Kunden eines in Konkurs gefallenen Versandhauses bejaht. Besteht jedoch zwischen dem Kunden und dem konkursiten Anbieter ein besonderes Vertrauensverhältnis, ist gemäss DSB von einer Verwertung abzusehen.[55]

[Rz 60] Für Daten eines Cloud Nutzers bedeutet dies, dass er die ausgelagerten Daten im Konkurs eines Cloud Anbieters gegebenenfalls nicht zurück erhält und das nicht auszuschliessende Risiko einer Verwertung seiner Daten oder von Teilen davon besteht.

C. Vertragliche Vorkehrungen

[Rz 61] Für den Cloud Nutzer kann es sich empfehlen, vertraglich festzuhalten, dass alle Daten, die er dem Cloud Anbieter übermittelt, als vertraulich (oder geheim) gelten und nicht ohne (schriftliche) Zustimmung an Dritte weitergegeben werden dürfen. Im Vertrag wäre auch festzuhalten, dass die Vertraulichkeits- oder Geheimhaltungspflichten des Cloud Anbieters auf sämtliche Personen zu überbinden sind, welche Zugang zu den (Personen-) Daten haben. Im Falle eines Konkurses des Cloud Anbieters kann eine solche Klausel dazu beitragen, dass Daten nicht einer Verwertung zugeführt werden.[56] Durch die Verschlüsselung von Daten kann eine Verwertung ebenfalls verhindert werden. Je nach Cloud Anbieter können durch eine Verschlüsselung von Daten in der Cloud jedoch nicht alle Cloud-Dienstleistungen genutzt werden.

[Rz 62] Vertraglich sollte ausserdem geregelt werden, was bei Beendigung der Zusammenarbeit mit dem Cloud Anbieter mit den Daten in der Cloud geschieht. Hier wird es vorderhand um die vollständige Rückgabe der Daten gehen (oder alternativ um unwiderrufliche Vernichtung der Daten in der Cloud) sowie um das Format der Rückgabe, insbesondere um Inkompatibilitäten mit dem eigenen System zu vermeiden.

N 10 mit weiteren Hinweisen.

[52] Wenn ein Cloud Nutzer dem Cloud Anbieter Daten auf einer Festplatte übergeben hat mit dem Zweck, diese Daten auf den Server des Cloud Anbieters zu übertragen, kann der Cloud Nutzer zumindest die Herausgabe dieser Festplatte fordern. In den meisten Fällen wird dies das Problem des Cloud Nutzers jedoch nur beschränkt oder gar nicht lösen, da die anfänglich auf der Festplatte übergebenen Daten nicht mehr aktuell sein werden.

[53] Russenberger, a.a.O., Art. 211 N 12.

[54] Was gemäss dem DSB bei Daten über Mitarbeiter des konkursiten Schuldners nicht der Fall ist, s. dazu Datenschutzbeauftragter des Kantons Zürich: Kundendaten im Konkursverfahren und Computerverkauf durch ein Konkursamt, beide im Oktober 2011.

[55] Datenschutzbeauftragter des Kantons Zürich, a.a.O.

[56] Erfüllen die Daten jedoch die Kriterien, um verwertet zu werden, namentlich weil keine überwiegenden öffentlichen oder privaten Interessen vorliegen, die gegen eine Verwertung sprechen, wird auch die Vereinbarung einer Geheimhaltungsklausel eine Verwertung nicht gänzlich verhindern können.

[Rz 63] Damit der Cloud Nutzer Zugriff auf aktuelle Daten hat, empfiehlt es sich, in regelmässigen Abständen ausserhalb der Cloud lesbare Sicherungskopien der Daten zu erstellen oder erstellen zu lassen. Dadurch ist auch gewährleistet, dass der Cloud Nutzer seine Daten in Zukunft auch auf einen anderen Provider oder in seine eigene Infrastruktur migrieren kann.

V. Fazit

[Rz 64] Das Auslagern von Daten in eine Cloud stellt datenschutzrechtlich eine Datenbearbeitung durch Dritte dar. Sie ist grundsätzlich (auch ohne Einwilligung der betroffenen Personen) zulässig, sofern der Cloud Anbieter die Daten nur so bearbeitet, wie der Cloud Nutzer es selber tun dürfte (i.c. Abspeichern auf Server unter Einhaltung der Datenschutzgrundsätze) und der Cloud Anbieter die Datensicherheit gewährleistet (die Personendaten müssen insb. gegen unbefugtes Bearbeiten geschützt werden). Der Cloud Anbieter darf daher nichts Weitergehendes mit den Daten unternehmen, insbesondere die Daten auch nicht für eigene Zwecke nutzen.

[Rz 65] Aus datenschutzrechtlicher Sicht dürfen die Patientendaten nur dann auf einen Server im Ausland gespeichert werden (Bekanntgabe ins Ausland), wenn der Cloud Anbieter sich verpflichtet, für einen angemessenen Schutz zu sorgen oder nur Server zu verwenden, die sich in Ländern befinden, welche aus Schweizer Sicht einen angemessenen Datenschutz garantieren. Strafrechtlich ist aber selbst dann Vorsicht geboten: Befindet sich der Cloud Anbieter oder zumindest der Cloud-Server im Ausland, dürfte die Auslagerung der Daten in die Cloud als Verletzung des Berufsgeheimnisses (Art. 321 StGB) zu werten sein. Um dies zu umgehen, müsste von jedem einzelnen Patienten eine umfassende Einwilligung zur Auslagerung der Datenbearbeitung ins Ausland (unter Hinweis auf die Risiken) eingeholt werden.

[Rz 66] Gleiches gilt für Klientendaten bei Anwälten. Hier ist jedoch zu beachten, dass sich unter diesen Daten auch äusserst geheime Informationen befinden können (z.B. geplante Übernahmen von Unternehmen), die nur für einen sehr beschränkten Personenkreis bestimmt und keinesfalls an Dritte gelangen dürfen. Entsprechend ist gerade bei Anwälten genau zu evaluieren ob und bejahendenfalls welche Daten, in welcher Form (z.B. nur verschlüsselt) ausgelagert werden sollen.

[Rz 67] Etwas abweichend gestaltet sich die Rechtslage bei Bankkundendaten. Banken müssen ihre Kunden immer informieren, wenn sie Daten an einen Dritten auslagern, und zwar unabhängig davon, ob der Dritte die Daten im Inland oder im Ausland bearbeitet. Dafür genügt es bei Banken, wenn Kunden vorgängig informiert werden und für die Kunden die Möglichkeit besteht, die Bankbeziehung vor der Auslagerung zu beenden. Eine *ausdrückliche* Zustimmung der Kunden ist für die Auslagerung von Bankdaten hingegen nicht erforderlich.

[Rz 68] Die Rückgabemodalitäten von Daten in einer Cloud an den Cloud Nutzer bedürfen einer sorgfältigen vertraglichen Regelung. Gleiches gilt für den Fall, dass der Cloud Anbieter irgendwann in Konkurs geraten sollte. Ohne vertragliche Regelung und geeignete Vorkehrungen (z.B. regelmässige Lieferung von Sicherungskopien der Datensätze an den Cloud Nutzer) besteht ansonsten das Risiko, dass der Cloud Nutzer die aktualisierten Daten nicht mehr erhältlich machen kann.

[Rz 69] Der EDÖB hält allgemein fest: Je vertraulicher, geheimer, wichtiger (weil geschäftskritisch) oder sensitiver (weil besonders schützenswert) Daten sind, umso eher ist von einer Auslagerung der Daten in eine Cloud, insbesondere in eine ausländische Cloud, abzusehen, und desto strikter und umfassender müssen die (Datenschutz-)Sicherheitsvorkehrungen und deren Kontrolle sein.[57] Wird vorgängig evaluiert, welche Daten ausgelagert werden können und werden die erwähnten Vorkehrungen und Vorsichtsmassnahmen getroffen sowie die Voraussetzungen zur Auslagerung von Daten in eine Cloud eingehalten, kann in vielen Fällen von den Vorteilen einer Cloud-Lösung profitiert werden.

[Rz 70] Schliesslich ist anzumerken, dass dem EDÖB bei Bedarf die konkrete Ausgangslage und Fragestellung zur Prüfung vorgelegt werden kann, um so eine (schriftliche) Stellungnahme zum geplanten Vorhaben erhältlich zu machen.

David Schwaninger, Rechtsanwalt, LL.M., und Stephanie S. Lattmann, Rechtsanwältin, sind bei Blum&Grob Rechtsanwälte AG unter anderem im IT-Recht und den damit zusammenhängenden Rechtsgebieten tätig.

---

* * *

[57] EDÖB, Erläuterungen zu Cloud Computing, Oktober 2011, S. 3.