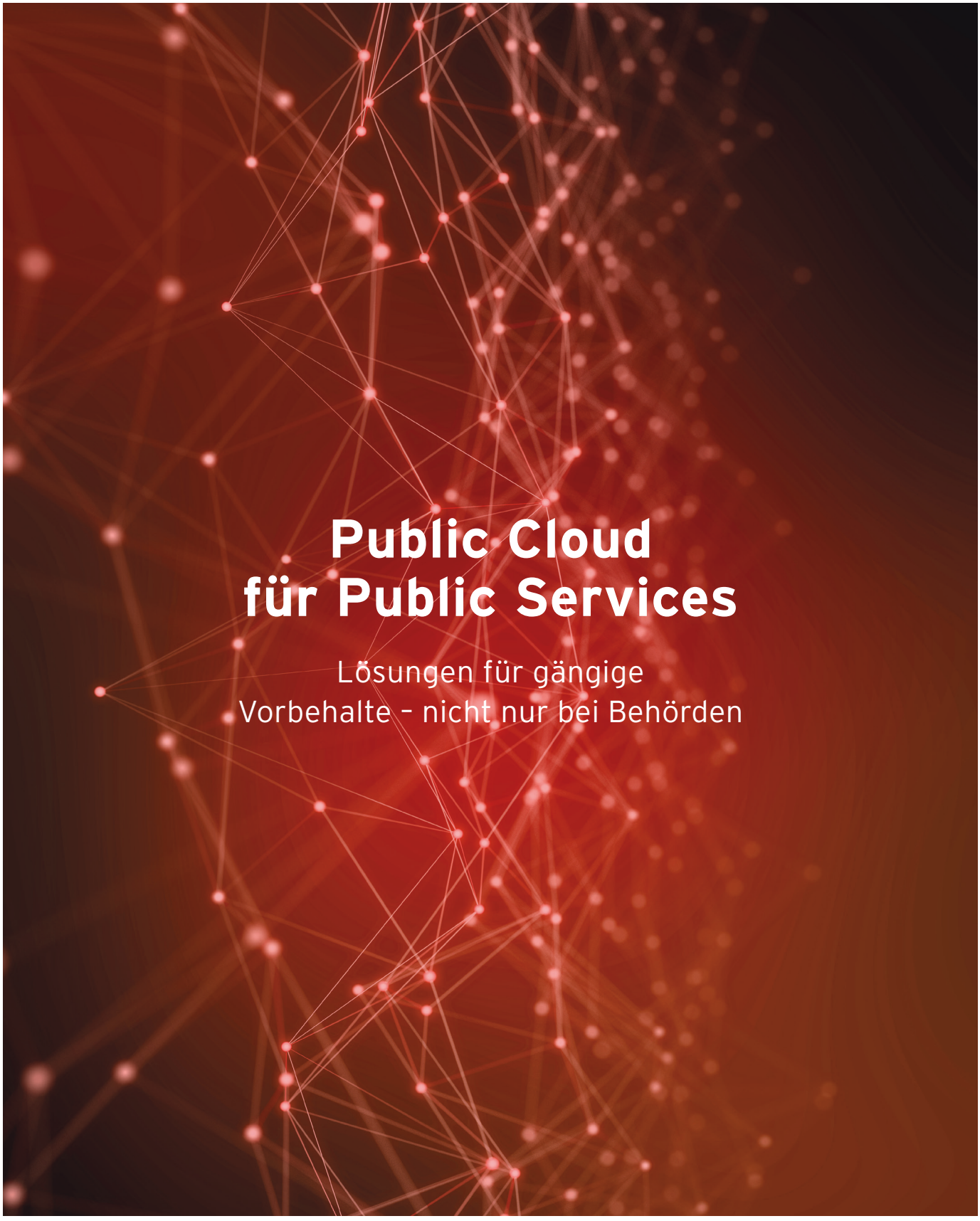
LAUX
LAWYERS AG
ZURICH | BASEL



Public Cloud für Public Services

Lösungen für gängige Vorbehalte – nicht nur bei Behörden

Laux Lawyers AG
August 2021

Auf Initiative und mit freundlicher Unterstützung von aws

I EINLEITUNG

Die Nutzung von Public-Cloud[1]-Services ist mittlerweile weit verbreitet. Cloud-Services halten mit der wachsenden Zahl von leicht zugänglichen Angeboten auch in besonders regulierten Bereichen zunehmend Einzug, so etwa im öffentlichen Sektor (Behörden) oder in der Finanzindustrie.

Die Vorteile sind zahlreich: Cloud-Services können einen signifikanten Beitrag zur Umsetzung von Digitalisierungsinitiativen leisten, sei es in der Privatwirtschaft, dem Service Public oder bei Verbänden und Vereinen. Mit dem Einsatz von Cloud-Services können oft Kosten gesenkt und die Innovationsfähigkeit kann gesteigert werden[2]. Organisationen können durch den Cloud-Einsatz zudem ihre Effizienz steigern, die Flexibilität ihrer IT-Systeme erhöhen, Ressourcen für das Kerngeschäft frei machen und ein zeitgemässes Angebot gegenüber der Öffentlichkeit und Kunden einfacher und schneller aufbauen. Gerade auch kleineren Organisationen bietet der Einsatz von modernen Cloud-Services die Möglichkeit, Leistungen sicherheitstechnisch auf dem modernsten Stand der Technik, digital und medienbruchfrei anzubieten, ohne selbst eine grössere IT-Infrastruktur[3] aufbauen und betreiben zu müssen, und für bestimmte Teile der Informationssicherheit sorgen zu müssen. Dies verbessert die Leistungsfähigkeit, bei hoher Informationssicherheit und relativ effizienten Kosten.

Den Vorteilen können neue oder andersgelagerte Herausforderungen gegenüberstehen. Diesen ist gebührend Rechnung zu tragen: Die Daten liegen beim Cloud-Anbieter – eventuell im Ausland, bleiben aber unter der Kontrolle des Cloud-Kunden.

Man spricht davon, dass die Datenbearbeitung an den Cloud-Anbieter «ausgelagert» wird. Zur Sicherstellung der Kontrolle über die ausgelagerte Datenbearbeitung muss sich der Cloud-Kunde vertieft mit dem Cloud-Service und dem Cloud-Anbieter auseinandersetzen, insbesondere mit Blick auf die Informationssicherheit. Mit steigender Verbreitung von Cloud-Services der grossen internationalen Cloud-Anbieter (sogenannte «Hyperscaler») nimmt das allgemeine Bewusstsein und das Verständnis im Hinblick auf deren Umgang mit den ihnen anvertrauten Daten zu.

Allerdings können gewisse Vorbehalte in der öffentlichen Debatte den Einsatz von Cloud-Services hemmen. Die Vorbehalte lassen sich wie folgt zusammenfassen: Die Cloud (gemeint sind Cloud-Services) sei datenschutzrechtlich problematisch, und Auslandbezüge würden ihrem Einsatz entgegenstehen.

Die nachfolgenden Ausführungen zeigen, dass solche Vorbehalte einer rechtlichen Prüfung nicht standhalten, wenn Cloud-Services, die gewisse Mindeststandards erfüllen, gewählt werden.

[1] Der Bund spricht von **«Public Cloud»** wenn die betreffende Cloud-Infrastruktur (siehe FN 3) für die Öffentlichkeit oder einen grossen Industriebereich zugänglich ist und einer Organisation gehört, die Cloud-Services verkauft (Quelle: Cloud-Computing-Strategie der Schweizer Behörden 2012-2020). Der umgangssprachlich geprägte Begriff «Public Cloud» soll mithin zum Ausdruck bringen, dass die Basiskomponenten des Cloud-Anbieters für keinen Kunden individuell-exklusiv («dediziert») nutzbar sind; demgegenüber ist die bereitgestellte Nutzungsmöglichkeit innerhalb eines sog. **«Tenant»** kundenindividuell und abgegrenzt gegenüber anderen Kunden («Isolation»), was mittels Netzwerktechnologie ermöglicht wird. Im Folgenden wird entsprechend generell von **«Cloud-Services»** gesprochen.

[2] Siehe dazu auch den kürzlich veröffentlichen Bericht zur Bedarfsabklärung für eine «Swiss Cloud» des Informatiksteuerungsorgans des Bundes (https://perma.cc/35DP-NL4L).

[3] Der Begriff **«IT-Infrastruktur»** verweist auf die Gesamtheit von Gebäuden, Hardware, Software, Netzwerktechnologie etc., die zum Betrieb eines Cloud-Services eingesetzt werden. Wenn auf die IT-Infrastruktur des Cloud-Anbieters Bezug genommen wird, wird auch von **«Cloud-Infrastruktur»** gesprochen.

Der Gang der Darstellung ergibt sich aus der folgenden Inhaltsübersicht:

II LÖSUNGEN ZU DEN GÄNGIGSTEN VORBEHALTEN

Vorbehalt 1: Datenhaltung im Ausland ist nicht erlaubt.

«Behörden dürfen keine Cloud-Services nutzen, wenn die Daten ausserhalb der Schweiz bearbeitet oder gespeichert werden.»

Nicht zutreffend. Datenbearbeitungen und -speicherungen im Rahmen von Cloud-Services in einem Land, das über ein mit der Schweiz gleichwertiges Datenschutzniveau verfügt[4], sind aus Sicht des Datenschutzgesetzes des Bundes (DSG) und der kantonalen Datenschutzgesetze ohne weitere Massnahmen zulässig. Liegt ein Datentransfer mit Bezug zu einer Rechtsordnung ohne Gleichwertigkeit vor, sind weitere Massnahmen notwendig – beispielsweise müssen sogenannte Standardvertragsklauseln vereinbart werden, gegebenenfalls ergänzt um weitere Schutzbestimmungen (siehe Ausführungen zu Vorbehalt 2 und Vorbehalt 3, insbesondere mit Blick auf die USA). Die grossen internationalen Cloud-Anbieter bieten hierzu rechtlich genügende Angebote an.

Ganz generell – und übrigens unabhängig von einem möglichen Auslandsbezug[5] – muss sich ein Cloud-Kunde bei der Auswahl des Cloud-Anbieters sowie während des Bezugs der Cloud-Services vergewissern, dass er seine Daten gegen Risiken angemessen schützen kann und der Cloud-Anbieter hierfür wirksame technische und organisatorische Massnahmen zur Verfügung stellt.

In Bezug auf technische und organisatorische Massnahmen darf ein Cloud-Kunde auf belastbare Dokumentation abstellen, die er vom Cloud-Anbieter erhält. Diese Dokumentation braucht nicht spezifisch für den Cloud-Kunden erstellt worden zu sein. Auch Zertifizierungen nach Massgabe von ISO-Standards können je nach ihrem Anwendungsbereich eine taugliche Dokumentation zum Nachweis genügender technischer und organisatorischer Massnahmen sein. Eine erhöhte Vertrauenswürdigkeit entsteht, wenn ein Cloud-Anbieter konkret für die eingesetzten Cloud-Infrastrukturen oder für darauf aufbauende Software einen Bericht über sog. Service Organization Controls (SOC) offenlegt. Solche Berichte werden von zugelassenen Prüfgesellschaften ausgestellt und sind im Rahmen der Abschlussprüfung des Cloud-Anbieters relevant. Die Dokumentationen sollten die gesamte Cloud-Infrastruktur mit allen darauf bezogenen technischen und organisatorischen Massnahmen angemessen dokumentieren. Wenn solche Berichte vorliegen und sie die technische Dokumentation stützen, muss sich der Cloud-Kunde nicht eigenhändig von der Existenz der vom Cloud-Anbieter dargelegten technischen und organisatorischen Massnahmen überzeugen.

[4] Dies sind Staaten, welche auf der EDÖB Staatenliste stehen (resp. zukünftig für welche ein Angemessenheitsbeschluss des Bundesrats gemäss revidiertem DSG besteht). Dies sind zurzeit u.a. sämtliche EU- und EFTA-Staaten sowie Grossbritannien, Israel, Japan, Kanada, Argentinien, Uruguay, Neuseeland und unter gewissen Voraussetzungen Australien.

[5] **«Auslandsbezug»** bezeichnet Bezüge entweder des Cloud-Anbieters oder des Cloud-Services ins Ausland. Ein Auslandsbezug liegt z.B. vor, wenn (i) der Cloud-Anbieter seinen rechtlichen Sitz im Ausland hat; (ii) der Cloud-Anbieter IT-Infrastrukturen im Ausland betreibt oder betreiben lässt oder (iii) der Cloud-Anbieter Personal im Ausland oder Subakkordanten im Ausland beschäftigt. Für diese Kategorie (Personal oder Subakkordanten) besteht der Auslandsbezug dann, wenn aus dem Ausland Zugriff auf den Cloud-Service genommen werden kann.

Vorbehalt 2: Eine Behörde kann keinen Cloud-Anbieter aus dem Ausland nutzen.

«Behörden können keine Cloud-Services von Cloud-Anbietern ausserhalb der Schweiz nutzen, z.B. von Cloud-Anbietern mit Sitz in den USA (oder von mit US-Muttergesellschaften verbundenen europäischen oder lokalen Cloud-Anbietern).»

Nicht zutreffend. Aus datenschutzrechtlicher Sicht ist es kein «No Go», dass der Vertrag zur Datenbearbeitung mit einem Cloud-Anbieter mit Sitz im Ausland vereinbart wird.

Dem Aspekt des Auslandbezugs wird im Rahmen der Beurteilung der vom Cloud-Anbieter gewährleisteten Informationssicherheit (siehe Ausführungen zu Vorbehalt 1) und mit Garantien bezüglich Übermittlungen in Länder ohne Angemessenheitsbeschluss (siehe Ausführungen zu Vorbehalt 3) Rechnung getragen. Dasselbe gilt konzeptionell aus Sicht der Geheimnisschutzrechte (z.B. Amts- und Berufsgeheimnisse gemäss Art. 320 und 321 StGB). Auszugehen ist auch diesbezüglich von der grundsätzlichen Zulässigkeit der Nutzung eines ausländischen Cloud-Anbieters, wobei der Cloud-Kunde nach den konkreten Umständen gegebenenfalls zusätzliche Fragen der gebotenen Sorgfalt zu klären hat. Siehe hierzu die Ausführungen zu Vorbehalt 6 und Vorbehalt 7.

Vorbehalt 3: Das «Schrems II-Urteil» verbietet die Nutzung von Cloud-Services mit Bezug zu den USA.

«Das Urteil des EuGHs in der Sache „Schrems II" verbietet den Transfer von Personendaten in die USA.»

Nicht zutreffend. Eine Nutzung von Cloud-Services mit Datentransfer von der Schweiz ins Ausland ist nicht per se verboten, auch nicht bei Transfers von Personendaten in die USA. Ohnehin bindet das Schrems II-Urteil des EuGH Schweizer Behörden nicht.

In seinem Urteil vom 16. Juli 2020 (Schrems II) erklärte der EuGH das EU-US Privacy Shield Programm für ungültig und bestätigte gleichzeitig die EU-Standardvertragsklauseln als Mechanismus für einen Drittstaatentransfer. Unter dem Eindruck dieses Urteils überprüfte der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) seine Einschätzung in Bezug auf US-Unternehmen, die Swiss-US Privacy Shield zertifiziert sind. Bislang durfte mit diesem davon ausgegangen werden, dass eine Übermittlung von Personendaten in die USA ohne weitere Garantien gleich wie innerhalb der Schweiz erfolgen kann. Diese Vermutung fällt nun weg.

Der EDÖB verwies in seiner Stellungnahme vom 8. September 2020 pauschal auf die gemäss Schrems II-Urteil des EuGHs problematischen «US-Massenüberwachungsgesetze». Er unterliess es aber, den Anwendungsbereich und die Auswirkungen der konkret für problematisch gehaltenen Überwachungsgesetze zu analysieren und im Lichte des Schweizer Rechts zu begründen, in welchen Fällen die Übermittlung von Personendaten in die USA zu unterlassen ist. Zudem machte er Ausführungen genereller Art zum Einsatz von Standardvertragsklauseln.

Diese Einschätzungen haben Auswirkungen auf Schweizer Cloud-Kunden, die Personendaten an Unternehmen in Staaten ohne Angemessenheitsbeschluss transferieren möchten (nicht nur in die USA):

- Der Cloud-Kunde hat im Rahmen einer Einzelfallprüfung zu beurteilen, ob im Importstaat datenschutzrechtliche Risiken bestehen und ob diesen mit Standardvertragsklauseln[6] oder zusätzlichen,

[6] **Hinweis:** Die Europäische Kommission hat am 4. Juni 2021 neue Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer erlassen (https://ec.europa.eu/commission/presscorner/detail/de/ip_21_2847). Neu ist ein ganzer Abschnitt der Standardvertragsklauseln (Abschnitt III) auf die Anforderungen von «Schrems II» ausgerichtet. Die Europäische Kommission hat erfreulicherweise einen risikobasierten Ansatz gewählt, der im Wesentlichen den hier gemachten Empfehlungen entspricht. Der EDÖB hat sich bislang noch nicht zu den neuen Standardvertragsklauseln geäussert. Es ist aber zu erwarten, dass er sie als genügende Garantien akzeptieren wird. Siehe hierzu auch https://www.lauxlawyers.ch/neue-standardvertragsklauseln-der-eu-einfuehrung-und-erste-einschaetzungen/.

Vorbehalt 3: Das «Schrems II-Urteil» verbietet die Nutzung von Cloud-Services mit Bezug zu den USA.

individuell auszuhandelnden Klauseln oder weiteren Massnahmen begegnet werden kann.

- Bei dieser Prüfung ist insbesondere zu analysieren, ob die Daten an ein Unternehmen übermittelt werden, das besonderen Zugriffen der dortigen Behörden unterworfen ist. In den USA seien dies laut EDÖB insbesondere sogenannte «Electronic Communication Service Providers», die (so der EDÖB) unter «US-Massenüberwachungsgesetze» fallen würden[7].

- Zudem muss der Cloud-Kunde im Rahmen dieser Prüfung auch beurteilen, ob das importierende Unternehmen im Empfängerstaat berechtigt und in der Lage ist, die zur Durchsetzung der schweizerischen Datenschutzgrundsätze nötige Mitwirkung zu leisten.

Die Konsequenzen für Schweizer Cloud-Kunden sind die folgenden:

- Die Prüfpflicht des Schweizer Cloud-Kunden ist grundsätzlich umfassend. Sie erfordert eine Analyse des vom Rechtssystem des Importstaats gewährten Datenschutzniveaus.

- Die Prüfpflicht bezieht sich auf jeden konkreten Einzelfall und muss regelmässig und wohl für jede Datenübermittlung erneut und einzeln vorgenommen werden. Mit anderen Worten müssen die Natur der übermittelten Daten und die sich daraus ergebenden Erkenntnisse im Einzelfall mit gewürdigt werden.

In der Praxis lohnt sich indes ein massvolles und besonnenes Vorgehen. Dies gilt umso mehr, als der EDÖB die Beurteilung des EuGHs ohne daran gebunden zu sein und ohne eigene materielle Prüfung der heute zur Rechtslage in den USA verfügbaren Informationen übernommen hat. Auch stehen die pauschalen Ausführungen des EDÖB im Gegensatz zu der von ihm geforderten Einzelfallprüfung, die Cloud-Kunden (1) nach ihrem erheblichen Interesse und (2) nach eingehender Risikoanalyse sowie (3) unter Berücksichtigung weiterer involvierter Interessen (wirtschaftliche und öffentliche Interessen an der Cloud-Nutzung und am internationalen Datentransfer) vornehmen sollen.

Dazu im Einzelnen:

Erstens: Der EuGH befand in «Schrems II» nicht umfassend und abschliessend über die Angemessenheit des Datenschutzniveaus der USA. Er prüfte lediglich, ob die Europäische Kommission im Jahr 2016 das EU-US Privacy Shield als Schutzmechanismus für den Datentransfer von der EU in die USA genehmigen durfte, was er verneinte. Der EDÖB adaptierte den Entscheid für seine Beurteilung der Angemessenheit des Swiss-US Privacy Shields, ohne daran gebunden zu sein. Wie schon der EuGH, verliess sich der EDÖB sodann auf die Sachverhaltserhebungen des Irischen High Courts.

Zweitens: Der EDÖB unterliess es, den vom Irischen High Court erhobenen Sachverhalt gemäss heute verfügbaren Informationen zum US-Recht zu komplettieren und gemäss Schweizer Datenschutzrecht

[7] Der Fokus liegt dabei in erster Linie auf Anbieter von Telekommunikationsdiensten (z.B. Telefonie, E-Mail, Messenger Dienste etc.). Viele Cloud-Services sind indes ausserhalb des offensichtlichen Fokus dieser Gesetzgebungen. Zudem unterbinden starke Transportverschlüsselungen eine Überwachung der Datenflüsse im Transit.

Vorbehalt 3: Das «Schrems II-Urteil» verbietet die Nutzung von Cloud-Services mit Bezug zu den USA.

zu beurteilen[8]. Insgesamt darf somit die Frage gestellt werden, ob die Einschätzung des EDÖB eine genügende Begründung enthält, insbesondere mit Blick auf die Bedeutung, welche sie in der Praxis beansprucht.

Drittens: Im Gegensatz dazu können Cloud-Kunden, die heute auf der Grundlage von EU-Standardvertragsklauseln Datenübermittlungen in die USA vornehmen möchten, alle derzeit verfügbaren Informationen über das US-Recht berücksichtigen, einschliesslich Informationen, die weder der Irische High Court, der EuGH noch der EDÖB berücksichtigt haben. Sie können nach eigenem Ermessen auch andere Schlüsse zum US-Recht ziehen. Die vertiefte Auseinandersetzung mit den konkreten Cloud-Services wie auch der Beizug erfahrener Spezialisten können in diesen Situationen viel dazu beitragen, Klarheit zu schaffen.

Viertens: Bei realistischer Betrachtung lässt sich die Prüfpflicht des Cloud-Kunden nur mit Wahrscheinlichkeitsüberlegungen erfüllen, wie sie bei Risikobeurteilungen generell üblich sind. Eine Sanktionierung des Cloud-Kunden ist in der Praxis nicht denkbar, wenn der Cloud-Kunde seine Risikoüberlegungen nachweisen und den darauf basierenden Ermessensentscheid nachvollziehbar begründen kann. Dies verlangt in erster Linie nach sorgfältig erstellter Dokumentation.

Fünftens: Die wirtschaftlichen Interessen der Unternehmen, die privaten Interessen der Nutzer von Online-Diensten sowie das Interesse der Allgemeinheit an der internationalen Zusammenarbeit (z.B. in der Forschung und Entwicklung) lassen sich ohne internationalen Datentransfer nicht realisieren. Auch solche Interessen Privater sind grundrechtlich geschützt und müssen in Einklang gebracht werden mit dem Interesse am Schutz der Privatsphäre. Ähnliche Überlegungen gelten für die Cloud-Nutzung durch Behörden. Sie haben die ihnen übertragenen öffentlichen Aufgaben nach Massgabe der Wirtschaftlichkeit zu erfüllen. Zu strenge Anforderungen an die Nutzung, Haltung und den internationalen Transfer von Personendaten würden wichtige Interessenabwägungen in vorgefertigter und somit statischer Art vorwegnehmen, was vom Datenschutzrecht in dieser Weise nicht vorgesehen ist. Datenschutz ist keine statisch-abstrakte Aufgabenstellung, sondern verlangt Angemessenheit und Augenmass.

[8] Eine aktuelle und umfassende Darstellung zum heute geltenden US-Recht in den vom EuGH gerügten Bereichen findet sich z.B. in einem gemeinsamen White Paper des US Department of Justice und des US Department of Commerce: «Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II».

Vorbehalt 4: Behördenzugriffe aus dem Ausland verbieten die Cloud-Nutzung.

«Ausländische staatliche Institutionen können auf Daten zugreifen, die in Cloud-Services gespeichert sind. Dies steht der Nutzung des Cloud-Services durch Behörden entgegen.»

Nicht zutreffend. Der Cloud-Kunde muss eine sorgfältige Risikoabwägung vornehmen und beurteilen, was allfällige Behördenzugriffe im Ausland bedeuten und inwiefern diese der Nutzung des Cloud-Services entgegen stehen. Die Tatsache allein, dass Behördenzugriffe aus dem Ausland theoretisch stattfinden könnten (d.h. sich nicht zu 100% ausschliessen lassen), steht der Nutzung des Cloud-Services durch Schweizer Cloud-Kunden jedoch nicht entgegen, auch nicht bei Behörden.

Generell ist davon auszugehen, dass Strafverfolgungsbehörden weltweit alle in ihrem Zugriffsbereich liegenden Daten herausverlangen bzw. beschlagnahmen können. Grundsätzlich ist keine Behörde, kein Unternehmen und keine Privatperson davor geschützt, dass eine Strafverfolgungsbehörde einen bei ihr gespeicherten Datensatz herausverlangt. Die Schweiz (festgelegt in Art. 246-248 und Art. 263 ff. StPO) ebenso wie ausländische Staaten kennen entsprechende Zwangsmassnahmen. Eine Person, die im Verdacht steht, in den USA eine Straftat ausgeübt zu haben, kann sich dem Zugriff der US-amerikanischen Behörden also auch dann nicht entziehen, wenn die Behörde, die allenfalls Daten über diese Person bearbeitet, nur Cloud-Anbieter ohne Bezug zu den USA einsetzt. Dies scheint aber ein weit verbreitetes Fehlverständnis zu sein. Der Zugriff von staatlichen Institutionen ausserhalb der Schweiz (z.B. in den USA) auf Informationen, die Cloud-Kunden auf Cloud-Infrastrukturen in der Schweiz oder im Ausland bereitstellen lassen, sind somit nicht per se problematisch. Es kann einzig darum gehen, ob im Ausland die aus Sicht der Schweiz geforderten Verfahrensgarantien eingehalten werden. Zugriffe einer ausländischen Strafverfolgungsbehörde sind somit so lange nicht von Belang für die hier behandelte Fragestellung, als der Zugriff im Rahmen eines geordneten Untersuchungs- oder Gerichtsverfahrens in einem Rechtsstaat erfolgt. Dies ist auch für den Zugriff von Strafverfolgungsbehörden der USA heute zu bejahen. Im Resultat führt ein Absehen von Cloud-Anbietern mit Auslandsbezug in die USA somit bestenfalls zu einer Verlangsamung der Strafverfolgung im Ausland. Die Verlangsamung entspricht aber keinem öffentlichen Interesse.

Vorbehalt 4: Behördenzugriffe aus dem Ausland verbieten die Cloud-Nutzung.

Der US CLOUD Act:

Der im Frühjahr 2018 in den USA in Kraft getretene «Clarifying Lawful Overseas Use of Data Act» (kurz: «CLOUD Act») regelt den Zugriff von US-Behörden auf ausserhalb der USA gespeicherte Daten. Der CLOUD Act konkretisiert diesbezüglich den US Stored Communications Act und reduziert die Zahl der Verfahren, für die bislang ein internationales Rechtshilfeverfahren in Strafsachen (auch Multi Lateral Assistance Treaty, MLAT) erforderlich war. Inhaltlich entspricht der CLOUD Act weitgehend der Cybercrime Convention des Europarats (Art. 18), welche seit 2012 auch für die Schweiz gilt.

Der CLOUD Act hat grundsätzlich einen deutlich engeren und weniger weitgehenden Anwendungsbereich als landläufig angenommen wird: Er gilt für Strafuntersuchungen (und explizit nicht für Geheimdienste) und erfordert in jedem Fall einen Gerichtsbeschluss eines zuständigen US-Gerichts. Der CLOUD Act betrifft v.a. die Beschlagnahmung von Material im Ausland für strafrechtliche Untersuchungen in den USA gegen US-Personen. Es geht im Rahmen des CLOUD Acts insbesondere nicht um Wirtschaftsspionage oder die Massenüberwachung von Personen. Ebenso erlaubt der CLOUD Act keine Datenerhebung auf Vorrat und auch keine «fishing expeditions». Die US-Strafverfolgungsbehörden müssen wissen und präzise angeben, wonach sie suchen. Sie können keine Anfragen machen, um zu sehen, ob sich auf den Servern des Cloud-Anbieters eventuell irgendetwas von Interesse befinden könnte.

Der CLOUD Act ändert nichts am Prinzip der Staatenimmunität, wie sie im US Foreign Sovereign Immunities Act (FSIA) festgeschrieben ist. Es ist davon auszugehen, dass Cloud-Inhalte von ausländischen Regierungen, deren Untergliederungen und Behörden nicht herausverlangt werden können, da dies auf eine Umgehung des Schutzes der Immunität eines souveränen Staates nach dem FSIA hinauslaufen würde. Der CLOUD Act erweitert diesbezüglich die Möglichkeiten der US-Strafverfolgungsbehörden nicht.

Die im Kontext des CLOUD Act relevanten Zugriffs-Instrumente Warrant (z.B. Durchsuchungsbefehle) und Subpoena (z.B. Herausgabeverfügungen) sind seit jeher geltendes Recht der USA. Es ist die Praxis der USA, diese Instrumente nicht gegenüber dem Unternehmen (ausserhalb der USA) durchzusetzen, das die Daten direkt hostet (also z.B. die lokalen Tochterfirmen des Cloud-Anbieters in der Schweiz oder Europa). Stattdessen werden die Instrumente gegenüber den entsprechenden Muttergesellschaften der Cloud-Anbieter durchgesetzt, wenn diese über ein ausreichendes Standbein in den USA verfügen.

Die angegangenen US-Cloud-Anbieter haben die Möglichkeit zur Anfechtung einer solchen richterlichen Anordnung, insbesondere wenn die Datenherausgabe eine Verletzung des am Ort der Datenhaltung geltenden nationalen Rechts hervorruft. In der Schweiz (Datenhaltung in der Schweiz) kann dies beispielsweise eine Verletzung von Art. 271 StGB (Verbotene Handlungen für einen fremden Staat) oder Art. 273 StGB (Wirtschaftlicher Nachrichtendienst) betreffen oder auch Bestimmungen des Amts- oder Berufsgeheimnisses. Das angerufene US-Gericht wird dabei nach der in den USA üblichen Vorgehensweise die Interessen der Beteiligten gegeneinander abwägen (sog. «common-law comity analysis»). Die diesbezügliche Gerichtsentscheidung unterliegt sodann der Berufung und Überprüfung durch unabhängige Berufungsgerichte[9].

[9] Dies ist ein weitaus strengeres und unabhängigeres Verfahren, als es in anderen Ländern für Informationsanfragen von Strafverfolgungsbehörden existiert (auch im Vergleich zur Schweiz).

Vorbehalt 4: Behördenzugriffe aus dem Ausland verbieten die Cloud-Nutzung.

Eine Offenlegung von Cloud-Inhalten ausländischer Regierungen oder Behörden würde (spätestens) in einer solchen Comity-Analyse verhindert, da souveräne ausländische Staaten und ihre Untergliederungen und Behörden Immunität gegenüber allen Gerichtsverfahren in den USA geniessen (siehe oben zum FSIA) und dieses Prinzip im Rahmen der richterlichen Abwägungen eine entscheidende Rolle spielt.

Für Anfragen US-amerikanischer Strafverfolgungsbehörden kann man heute mit einer hohen Wahrscheinlichkeit davon ausgehen, dass die US-Strafverfolgungsbehörde den Cloud-Kunden, d.h. die Behörde, direkt kontaktieren würde. Dies wird so in Weisungen von staatlichen Stellen bestätigt[10].

Zu beachten ist dabei ganz generell, dass die Wahrscheinlichkeit des Zugriffs ausländischer Strafverfolgungsbehörden tendenziell überschätzt wird. Oft erfolgt gar keine Beurteilung der Wahrscheinlichkeit solcher Zugriffe. Das Thema des Behördenzugriffs nimmt vor diesem Hintergrund in der öffentlichen Wahrnehmung einen zu gewichtigen Platz ein.

[10] Weisung des US Department of Justice: «Seeking Enterprise Customer Data Held by Cloud Service Providers (December 2017)»; US Department of Justice, Office of the Deputy Attorney General, Memorandum for Heads of Department Law Enforcement Components, Department Litigating Components, the Director, Executive Office for U.S. Attorneys, all United States Attorneys (October 2017) – «Policy Regarding Applications for Protective Orders Pursuant to 18 U.S.C. § 2705(B)».

Vorbehalt 5: Behörden im Ausland könnten Sicherheitsschranken überwinden.

«Strafverfolgungsbehörden können von Cloud-Anbietern verlangen, dass diese Verschlüsselungen brechen oder „Backdoors" einrichten. Dies steht der Nutzung des betroffenen Cloud-Services durch Behörden oder Unternehmen entgegen.»

Nicht zutreffend. Selbst wenn ausländische Strafverfolgungsbehörden Backdoors einrichten liessen und Verschlüsselungen brechen bzw. umgehen könnten, stünde dies der Nutzung des Cloud-Services nicht entgegen.

Nach heutigem Kenntnisstand bestehen weder in der EU noch in den USA Backdoor- oder Entschlüsselungspflichten für Cloud-Anbieter. Insbesondere enthält auch der CLOUD Act keine Bestimmungen zur Entschlüsselung von durch den Cloud-Anbieter für den Cloud-Kunden gespeicherten und verschlüsselten Daten oder zum Zugriff auf Daten über «geheime Backdoors[11]» . Es kann zwar die Offenlegung von verschlüsselten Daten erzwungen werden, diese müssen aber nicht durch den Cloud-Anbieter entschlüsselt werden (die Mitwirkung des Cloud-Kunden wäre dann erforderlich).

Letztlich ist deshalb relevant, wie sich der jeweilige Cloud-Anbieter zum CLOUD Act stellt. Dabei kann man festhalten, dass die grösseren US Cloud-Anbieter sehr gewissenhaft mit den jährlich wenigen Anfragen von US-Strafverfolgungsbehörden mit Bezug zum Regelungsinhalt des CLOUD Act umgehen und diese mitunter auch gerichtlich anfechten. Cloud-Kunden sollten sich darüber beim Cloud-Anbieter ausführlich informieren, z.B. wie sich dieser im Falle von Behördenanfragen standardmässig verhält, welche internen Prozesse er befolgt, wie häufig Anfragen vorkommen und welche Themen diese betreffen. Ebenfalls sollten die Verträge dahingehend geprüft werden, ob sich der Cloud-Anbieter verpflichtet, den Cloud-Kunden frühzeitig zu informieren und in das Verfahren zu involvieren (soweit gesetzlich zulässig) und ob sich der Cloud-Anbieter verpflichtet, Verfügungen aufgrund von allfälligen Kollisionen mit schweizerischen Rechtsnormen anzufechten.

[11] Siehe hierzu z.B. das White Paper des US Department of Justice vom April 2019 zum Zweck und den Auswirkungen des CLOUD Acts; «Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act»: «Does the CLOUD Act require providers to decrypt data in response to law enforcement requests? - No. The CLOUD Act is «encryption neutral». It does not create any new authority for law enforcement to compel service providers to decrypt communications. Neither does it prevent service providers from assisting in such decryption, or prevent countries from addressing decryption requirements in their own domestic laws.»

Vorbehalt 6: In Bezug auf Amts- und Berufsgeheimnisse sind Cloud-Services nicht zulässig.

«Bereits die blosse Nutzung eines Cloud-Services stellt in Bezug auf Informationen, welche dem Amts- oder Berufsgeheimnis unterstehen, eine verbotene Offenbarung dar und ist strafbar.»

Nicht zutreffend. Eine strafbare Offenbarung im Sinne der strafrechtlichen Vorschriften zum Amts- und Berufsgeheimnis (insb. Art. 320 und Art. 321 StGB) liegt vor, wenn ein Aussenstehender die zu schützende Information (z.B. Amtsgeheimnis-relevante Informationen) tatsächlich wahrgenommen hat. Dieses tatsächliche Wahrnehmen kann im digitalen Kontext auch als «Klartextzugriff» bezeichnet werden. Offenbaren bedeutet «Zugänglichmachen» von Informationen, d.h. Angaben, die für sich «sprechend» sind und konkret eingesehen werden. Bei vielen Cloud-Services finden indes keine derartigen Klartextzugriffe statt.

Der Umstand, dass ein Cloud-Anbieter die Cloud-Infrastruktur kontrolliert, verleitet mitunter zum vorschnellen Schluss, jedem Cloud-Anbieter sei stets die Möglichkeit der Kenntnisnahme eröffnet. Im öffentlichen Diskurs entsteht so der Eindruck, eine Cloud-Nutzung führe immer zur Strafbarkeit des Geheimnisträgers (Cloud-Kunde) wegen versuchter Geheimnisverletzung. Dem ist nicht so.

Die im Rahmen einer Reihe von Rechtsgutachten zu Geheimnispflichten in regulierten Sektoren (u.a. Anwaltsgeheimnis[12], Bankkundengeheimnis[13], Arzt- bzw. Patientengeheimnis[14] und Amtsgeheimnis[15]) dargelegte Begründung zeigt, dass nur die aktive Offenbarung oder die schuldhaft und pflichtwidrig unterlassene Sicherung der von der Geheimhaltungspflicht erfassten Informationen gegen Klartextzugriffe strafbar ist. Mit der Speicherung von geheimnisgeschützten Informationen auf den Betriebsumgebungen von Cloud-Anbietern wird zwar im Sinne des natürlichen Kausalzusammenhangs ein Grund gesetzt, warum ein (verbotener) Klartextzugriff – z.B. durch einen Mitarbeitenden des Cloud-Anbieters – überhaupt erst möglich würde (wenn z.B. der Mitarbeitende die aufgesetzten Sicherungs- und Sicherheitsmassnahmen überwinden kann). Mit der Speicherung und Bearbeitung der Daten des Cloud-Kunden in den Cloud-Services findet aber rein tatsächlich noch kein Klartextzugriff statt. Somit scheidet die Strafbarkeit des Cloud-Kunden und dessen Mitarbeitern wegen aktiver Verletzung des Geheimnisstraftatbestands allein wegen der initialen Speicherung aus. Wenn dann andere einen verbotenen Zugriff nehmen, ist im Sinne der Adäquanz zu prüfen, inwiefern der Klartextzugriff dem Cloud-Kunden zurechenbar ist (dazu sogleich).

[12] Schwarzenegger/Thouvenin/Stiller: Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte; Anwaltsrevue 1/2019

[13] Laux/Hofmann/Schieweck/Hess: Nutzung von Cloud-Angeboten durch Banken: Zur Zulässigkeit nach Art. 47 BankG; Isler/Kunz/Müller/Schneider/Vasella: Zulässigkeit der Bekanntgabe von Bankkundendaten durch schweizerische Banken an Beauftragte im Ausland unter Art. 47 BankG.

[14] Steiner: Digitalisierter Arztbesuch und Cloud Nutzung im Lichte des Datenschutzrechts des Bundes und der Kantone, sic! 12/2020

[15] Migration von Daten in die Cloud – Analyse in Bezug auf Amtsgeheimnis; nicht öffentliches Gutachten von Laux Lawyers AG, September 2020

Vorbehalt 6: In Bezug auf Amts- und Berufsgeheimnisse sind Cloud-Services nicht zulässig.

Zwar besagt die Rechtsprechung des Bundesgerichts, dass auch das Schaffen einer Möglichkeit des Zugriffs zur Strafbarkeit führt. Damit sollen Konstellationen des ungehinderten Klartextzugriffs erfasst werden (z.B. «Liegenlassen von Dokumenten im Altpapier»), die auf eine aktive Mitteilung von geheimnisgeschützten Informationen hinauslaufen. In hochskalierenden Cloud-Infrastrukturen für reife Cloud-Services sind hingegen erfahrungsgemäss eine Vielzahl von Massnahmen eingerichtet, die Cloud-Kunden nutzen können und die bewirken, dass gerade kein solch ungehinderter Klartextzugriff besteht. Diese Rechtsprechung greift hier somit nicht.

Solange die Behörde durch die Nutzung der technischen, organisatorischen und vertraglichen Massnahmen, die der Cloud-Anbieter zur Verfügung stellt, für einen angemessenen Schutz der in der Cloud gespeicherten Daten sorgt, kann die Strafbarkeit der Behörde ausgeschlossen werden. Massnahmen technischer, organisatorischer und vertraglicher Art müssen geeignet sein, einen Klartextzugriff im Normalbetrieb zu verhindern. Solange diese Voraussetzung erfüllt ist, kann man selbst dann, wenn es zu einem unbefugten Klartextzugriff kommt, nicht sagen, dass die Mitarbeiter des Cloud-Kunden einen eigentlichen Tatbeitrag zu einer strafbaren Offenbarung geleistet haben.

Anders verhielte es sich nur, wenn der Cloud-Kunde im Sinne des sog. adäquaten Kausalzusammenhangs für ungenügende Sicherungs- und Sicherheitsmassnahmen einstehen muss. Es geht also um die Frage, ob die vom Cloud-Kunden getroffenen vertraglichen, technischen und organisatorischen Sicherungsmassnahmen ausreichend sind. Sind sie es nicht, hat der Cloud-Kunde (bzw. haben die dafür verantwortlichen Mitarbeiter des Cloud-Kunden) für einen allfälligen Klartextzugriff einzustehen. Bildlich gesprochen: Wer das Scheunentor geöffnet hält, muss für Klartextzugriffe durch jenen, der in den eigentlich zu schützenden Bereich hineinspaziert, einstehen. Wer jedoch genügend sichert, ist nicht verantwortlich.

Weder der Cloud-Kunde noch der Cloud-Anbieter müssen für Ereignisse einstehen, die sie nicht mit genügender Sicherheit antizipieren können. Entsprechend ist ihnen widerrechtlicher Zugriff von Dritten auf die zu schützenden Informationen nicht anzulasten, wenn die Cloud-Infrastrukturen mittels hochstehender Massnahmen eben genau gegen solche Zugriffe geschützt waren. Strafbar ist dann vielmehr nur derjenige, der die Sicherungsmassnahmen mit krimineller Energie überwindet, z.B. Art. 143 StGB (Unbefugte Datenbeschaffung), Art. 143bis StGB (Unbefugtes Eindringen in ein Datenverarbeitungssystem) und Art. 179novies StGB (Unbefugtes Beschaffen von Personendaten).

Entscheidend ist also, dass der Cloud-Kunde die vom Cloud-Anbieter eingesetzte Cloud-Infrastruktur und die vom Cloud-Anbieter zugesicherten Abläufe versteht. Denn kontrollieren kann nur, wer versteht, wie die Datenbearbeitung beim Cloud-Anbieter aussehen soll. Dies bedingt im Gegenzug die Bereitschaft des Cloud-Anbieters, sich mit den Bedürfnissen seiner Kunden auseinanderzusetzen. Letzteres ist bei reifen Cloud-Anbietern mittels umfassender Dokumentation und Aufklärung sichergestellt.

Vorbehalt 7: Der ausländische Cloud-Anbieter ist keine Hilfsperson.

«Cloud-Anbieter im Ausland können nicht als Hilfspersonen von Cloud-Kunden im Sinne der einschlägigen strafrechtlichen Geheimhaltungsvorschriften beigezogen werden.»

Nicht zutreffend. Auch Cloud-Anbieter im Ausland können als Hilfspersonen gelten. Dies führt dazu, dass selbst bei beiläufigen Klartextzugriffen durch solche Cloud-Anbieter keine strafbare Offenbarung resultiert. Der Cloud-Anbieter sollte im Kontext solcher Klartextzugriffe zu strenger Geheimhaltung verpflichtet werden.

Teilweise wird die Auffassung vertreten, dass der Cloud-Anbieter im Ausland nicht als Hilfsperson des Geheimnisträgers (Cloud-Kunde) anerkannt werden kann. Im Ausland entfalle der Schutz durch Strafrecht, wie er in der Schweiz greift. Dies wiederum laufe auf eine derart relevante Schutzreduktion hinaus, dass man von Strafbarkeit der Cloud-Nutzung durch Geheimnisträger sprechen müsse. Dieser Auffassung kann nicht gefolgt werden.

Sofern der dem Amts- oder Berufsgeheimnis unterliegende Cloud-Kunde die geheimnisrelevanten Informationen gemäss aktuellem Stand der Technik vor unautorisierten Klartextzugriffen durch Mitarbeiter des Cloud-Anbieters auch im Ausland schützt, entsteht gar nicht erst eine Situation, die aus Sicht des Strafrechts sanktionswürdig wäre. Die Frage, ob der beigezogene Dritte (Cloud-Anbieter) sich auch im Ausland strafbar machen könnte, wird somit nicht relevant; denn es kommt gar nicht erst zu einer Offenbarung (siehe vorne Vorbehalt 6). Folglich steht selbst eine fehlende Anerkennung des ausländischen Cloud-Anbieters als Hilfsperson des Cloud-Kunden der Bearbeitung von geheimnisrelevanten Informationen auf Cloud-Infrastrukturen im Ausland nicht entgegen.

Einige Cloud-Anbieter können in gewissen Ausnahmesituationen eingeschränkten Klartextzugriff auf geheimnisrelevante Daten benötigen, um die entsprechenden Cloud-Services für den Cloud-Kunden betreiben zu können, zum Beispiel in gewissen Supportsituationen. In solchen Fällen wird der Cloud-Kunde den Cloud-Anbieter mit vertraglichen und organisatorischen Massnahmen als sog. Hilfsperson in seinen Perimeter (den Kreis derjenigen, die zur Organisationsstruktur des Cloud-Kunden im weiteren Sinne und somit zur Verantwortungssphäre des Cloud-Kunden gehören) einbinden und somit ein Subordinationsverhältnis begründen.

Vorbehalt 7: Der ausländische Cloud-Anbieter ist keine Hilfsperson.

Als Hilfsperson zu qualifizieren ist dabei, wer bei der Tätigkeit des an das Geheimnis gebundenen Cloud-Kunden mitwirkt und hierfür Klartextzugriff benötigt – funktional verstanden somit zum Perimeter des Cloud-Kunden gehört. Cloud-Anbieter (und, durch entsprechende Überbindung der Geheimhaltungspflichten, ihre Mitarbeitenden) sind dann Hilfspersonen der an das Amts- oder Berufsgeheimnis gebundenen Cloud-Kunden.

Dies gilt nicht nur in Bezug auf Cloud-Anbieter, die ihren Sitz in der Schweiz haben, sondern generell. Dem Aspekt des Auslandbezugs trägt mitunter die Beurteilung der vom Cloud-Anbieter gewährleisteten Informations- bzw. Datensicherheit sowie die speziellen Regelungen und Garantien für den Auslandtransfer bereits genügend Rechnung (siehe Ausführungen zu Vorbehalt 1 und Vorbehalt 3).

Vorbehalt 8: Ohne Schweizer Recht und Schweizer Gerichtsstand geht es nicht.

«Der Vertrag zwischen dem Cloud-Kunden und dem Cloud-Anbieter muss Schweizer Recht unterstehen und einen Schweizer Gerichtsstand aufweisen.»

Nicht zutreffend. Dieser Vorbehalt wird meist aus dem Bereich des Datenschutzrechts heraus erhoben. Weder dem Schweizer Datenschutzgesetz noch den kantonalen Datenschutzgesetzen lässt sich aber eine solche Anforderung entnehmen. Der Beizug von Cloud-Anbietern mit Sitz im Ausland oder mit Datenhaltung im Ausland ist auch dann zulässig, wenn der Vertrag über die Nutzung des Cloud-Services nicht dem Schweizer Recht untersteht – dies jedenfalls solange die im Vertrag vereinbarten datenschutzrechtlichen Anforderungen des Cloud-Kunden rechtlich durchsetzbar sind. Auch sonst verlangt das Schweizer Recht dies nicht. Namentlich ergibt sich eine solche Vorgabe auch nicht aus dem Vergaberecht der Schweiz.

Der Problematik wird in der öffentlichen Debatte mehr Gewicht beigemessen, als vernünftigerweise notwendig erscheint. Eine in einem privatrechtlichen Vertrag getroffene Rechtswahl hat nur einen begrenzten Anwendungsbereich. Es wäre falsch, zu glauben, dass die Parteien einer Transaktion durch eine Rechtswahlklausel im Vertrag das Recht, das für ihre Beziehungen zueinander gilt, umfassend wählen könnten. Wenn Schweizerisches Datenschutzrecht grundsätzlich auf eine Datenbearbeitung unter Verantwortung eines Schweizer Cloud-Kunden anwendbar ist, kann die Wahl ausländischen Rechts im zugehörigen Leistungsvertrag daran nichts ändern.

Die im Vertrag vereinbarte Rechtswahl bezieht sich ausschliesslich auf das unmittelbar auf das Vertragsverhältnis anwendbare Recht und damit zusammenhängende Rechtsfragen, wie z.B.:

- die Voraussetzungen für ein rechtsverbindliches Zustandekommen des Vertrages,
- die Rechte und Pflichten der Parteien aus dem Vertrag,
- Verzug und Verzugsfolgen,
- Gewährleistungen,
- Haftung,
- Beendigung des Vertrages usw.

Die im Vertrag getroffene Rechtswahl hat jedoch keinen Einfluss auf das anwendbare Recht zu folgenden Fragen:

- Datenschutz (z.B. ob Schweizer Datenschutzrecht – Datenschutzgesetze des Bundes oder der Kantone – gilt oder nicht, und ob der Cloud-Kunde seine datenschutzrechtlichen Pflichten einhält oder nicht),
- Informationssicherheit (z.B. Informationssicherheitsgesetz ISG, Informationsschutzverordnung ISchV etc.),

Vorbehalt 8: Ohne Schweizer Recht und Schweizer Gerichtsstand geht es nicht.

- Regulatorische Anforderungen (z.B. Vergaberecht, BAG Kreisschreiben etc.)
- Fragen des Geheimnisrechts (z.B. Amtsgeheimnis, Art. 320 StGB; Berufsgeheimnis, Art. 321 StGB)

Umgekehrt unterliegt ein Cloud-Anbieter in Bezug auf das Strafrecht oder regulatorische Anforderungen (einschliesslich der verwaltungsrechtlichen Durchsetzung von Anforderungen an den Datenschutz und die Informationssicherheit) nicht direkt der Gerichtsbarkeit des Cloud-Kunden in der Schweiz, nur weil Schweizer Recht und Gerichtsstand für den Vertrag gewählt wurden.

Der hauptsächliche und offensichtlich greifbare Vorteil einer Rechtswahl zugunsten des Schweizerischen Rechts ist die Vertrautheit der Rechtsfolgen für den hiesigen Cloud-Kunden. Demgegenüber wäre ein allfälliges anderes (ausländisches) Recht dem Cloud-Kunden in der Schweiz primär wenig vertraut. Eine ausländische Rechtswahl könnte für den Cloud-Kunden im Konfliktfall ein Kostentreiber sein, da erst Abklärungen erforderlich werden könnten, bevor der Cloud-Kunde gegenüber dem Cloud-Anbieter rechtliche Schritte durchsetzen kann (sofern sich dazu überhaupt je ein Anlassfall bieten wird). Insgesamt kann die Rechtswahl als Kostenpunkt diskutiert werden. Dies sollte aber mit der richtigen Gewichtung geschehen (wie hoch ist die Wahrscheinlichkeit, dass sich überhaupt ein Anlassfall bieten wird?). Allerdings ist es nicht ungewöhnlich, dass bei standardisierten Massenprodukten und -dienstleistungen der Anbieter das auf den (ebenfalls standardisierten) Vertrag anwendbare Recht vorgibt.

Die Wahl des Gerichtsstands folgt grundsätzlich denselben Prinzipien: Ein Gerichtsstand in der Schweiz hat kurzfristig Vorteile. Diese dürfen jedoch nicht überbewertet werden, da je nachdem die Vollstreckung des Urteils im Ausland durchzuführen ist. Massnahmeverfahren (Verfahren zur schnellen, aber vorläufigen Durchsetzung von besonderen Schutzinteressen) müssen oft trotz Gerichtsstandsvereinbarung im Ausland angehoben werden.

Auf jeden Fall kann nicht gesagt werden, dass ein Vertrag mit Gerichtsstand im Ausland für eine Behörde generell ausgeschlossen wäre.

III ZUSAMMENFASSUNG

Die Cloud bewirkt einen Paradigmenwechsel, soviel steht fest. Und es zeigt sich, dass dieser Paradigmenwechsel teilweise noch auf Zögerlichkeit stösst. Dies ist aus verschiedenen Gründen durchaus nachvollziehbar bzw. darf nicht überraschen. Es wäre jedoch falsch, die Skepsis hinter juristischen Argumenten zu verstecken. Eine transparente Diskussion darüber, inwiefern das Recht tatsächlich Schranken aufstellt, wäre zielführender. Laux Lawyers AG setzt sich für eine derart transparente Auseinandersetzung mit dem Recht der Cloud ein. Dies soll Cloud-Kunden einen unverfälschten Blick auf die Aufgabenstellung ermöglichen und echte sowie sachlich begründete Risikoentscheide zulassen. Solche Risikoentscheide setzen eine vertiefte Auseinandersetzung mit den hier aufgeworfenen Themenkreisen voraus, aber nicht so sehr in rechtlicher, sondern in tatsächlicher Hinsicht. Der Cloud-Kunde hat sich eingehend mit den tatsächlichen Verhältnissen zu beschäftigen, insbesondere mit Datenübermittlungen ins Ausland, mit dem Zugriff durch staatliche Institutionen, mit den technischen und organisatorischen Verhältnissen beim Cloud-Anbieter und mit den anwendbaren Gesetzen. Im Rahmen von Umsetzungsprojekten können Cloud-Kunden Risiken identifizieren und mit geeigneten organisatorischen, technischen und vertraglichen Massnahmen auf ein Minimum reduzieren. So gelingt es, die einleitend erwähnten Kosten-, Effizienz-, Innovations- und Sicherheitsvorteile von Cloud-Services in Übereinstimmung mit gesetzlichen Vorgaben zu realisieren.

IV PRÜFSCHEMEN

Prüfschema Grenzüberschreitender Datentransfer

1 Prüfung auf allfällige Datenübermittlungen ins Ausland[16];

2 Bei Datenübermittlungen in Staaten, welche nicht auf EDÖB Staatenliste stehen resp. für welche kein Angemessenheitsbeschluss des Bundesrates (revDSG) bestehen:

- **a** Prüfung und ggf. Abschluss von zusätzlichen Schutzmassnahmen (z.B. EU-Standardvertragsklauseln oder verbindliche unternehmensinterne Datenschutzvorschriften beim Cloud-Anbieter);

Zusätzliche Risikoanalyse:

- **b** Rechtssituation im Import-Land;
- **c** Verhältnisse beim Datenimporteur (Cloud-Anbieter);
- **d** Art, Menge und Kritikalität der zu übermittelnden Daten (z.B. allg. Personendaten, durch Berufs- oder Amtsgeheimnis geschützte Daten, besonders schützenswerte Personendaten, exponierte Informationen über Personen, Datenformate);
- **e** Zweck der Übermittlung und Bearbeitung im Import-Land (sensible oder kontroverse Bearbeitungstätigkeit, Speicherung oder Ad-Hoc Remote Zugriff, Komplexität des Bearbeitungsablauf und beteiligte Akteure).

3 Je nach Ergebnis der Risikoanalyse Implementierung zusätzlicher Massnahmen:

- **a** Technische Massnahmen auf Kunden- oder Anbieterseite (z.B. Anonymisierung, Pseudonymisierung, Verschlüsselungen etc.);
- **b** Organisatorische Massnahmen auf Kunden- oder Anbieterseite (z.B. Privacy Shield Selbstzertifizierung, Datenminimierung etc.).

Prüfschema Rechtmässiger Zugriff auf Daten durch staatliche Institutionen

1 Analyse, welchen rechtmässigen Zugriffen auf Daten durch welche staatlichen Institutionen der Cloud-Anbieter unterliegt:

- **a** Aufgrund des Sitzes des Cloud-Anbieters oder seiner verbundenen Unternehmen resp. Subunternehmen in gewissen Ländern;
- **b** Aufgrund bestimmter lokaler Regulierungen (z.B. US CLOUD Act betr. «Electronic Communication Service Provider»; weitere lokale Umsetzungen von Art. 18 Cybercrime Convention etc.).

2 Verhalten des Cloud-Anbieters gegenüber Zugriffen durch staatliche Institutionen:

- **a** Umgang des Cloud-Anbieters mit Anfragen;
- **b** Anzahl und Art der Anfragen, die ein Cloud-Anbieter erhält;
- **c** Vertragliche Zusicherungen bezüglich Information des Cloud-Kunden und genereller Umgang mit Anfragen.

3 Wahrscheinlichkeit des Zugriffs durch staatliche Institutionen.

[16] Auch die Möglichkeit eines «Remote Access» aus einem Drittland kann gemäss anwendbarem Recht als Transfer ins Ausland gelten und ist daher als solcher zu behandeln, z.B. in Supportsituationen.

IV PRÜFSCHEMEN

Prüfschema Zugriff auf geheimnisrelevante Daten durch Cloud-Anbieter

1 Prüfung des Cloud-Services auf Zugriffe auf Daten durch den Cloud-Anbieter:

- **a** Notwendigkeit im Normalbetrieb;
- **b** Unterbindung und Kontrolle durch technische und organisatorische Massnahmen;
- **c** Möglichkeit der Unterbindung auf Kundenseite falls gewünscht (Zugriffskontrollen, kundenseitige Verschlüsselungen etc.);
- **d** Vertragliche Regelungen (Vertraulichkeit, Verhalten bei Zugriffen etc.).

2 Eventuell: Spezielle vertragliche Absicherungen bzgl. Geheimnisrechte.

Prüfschema Anwendbarkeit von Gesetzen

1 Adressierung der datenschutzrechtlichen und weitere regulatorischen Anforderungen des Cloud-Kunden im Vertragswerk, sodass der Cloud-Kunde den auf ihn anwendbaren Rechtspflichten gerecht werden kann:

- **a** Genügende Regelung der Auftragsdatenbearbeitung (Art. 10a DSG, Art. 9 revDSG) inkl. Datensicherheit (technische und organisatorische Massnahmen);
- **b** Verständliche und genügende Regelung weiterer vertraglicher Pflichten des Cloud-Anbieters (Klarheit der Rechte und Pflichten aus dem Vertrag).

2 Eventuell (insb., wenn Vertrag unklar oder lückenhaft oder Rechtsordnung in «unbekannten» oder zweifelhaften Staaten): Abklärungen zu den vertragsrechtlichen Rahmenbedingungen in der betreffenden ausländischen Rechtsordnung (inkl. Rechtspflege).

BÜRO ZÜRICH
A Seegartenstrasse 2
P. O. Box · CH 8024 Zürich
T +41 44 880 2424
F +41 44 880 2425
W www.lauxlawyers.ch

BÜRO BASEL
A Steinenring 40 · CH 4051 Basel
T +41 61 283 0606
W www.lauxlawyers.ch

Alle Anwälte in den zuständigen
Anwaltsregistern eingetragen