www.jusletter.ch

Anhang:

Ausländischer Lawful Access: Wahrscheinlichkeitsbeurteilung und Gegenmassnahmen im Detail

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

Inhaltsübersicht

1. Normalfall: Behörde gelangt an den Berufsgeheimnisträger

[1] Ausgangspunkt der vorliegenden Wahrscheinlichkeitsbeurteilung ist die ausländische Behörde, welche an Daten über einen Kunden des Berufsgeheimnisträgers gelangen will. Nach dem gewöhnlichen Lauf der Dinge wird die Behörde den Berufsgeheimnisträger auffordern, ihr diese Daten zugänglich zu machen. Nicht Gegenstand dieses Anhangs sind hingegen jene Fälle, in denen eine nachrichtendienstliche Informationsbeschaffung ohne Rechtsweggarantie erfolgt (wie z.B. im Rahmen der Section 702 des US Foreign Intelligence Surveillance Act). Sie erfolgt nach anderen Grundsätzen, weshalb die Wahrscheinlichkeit eines solchen Falls separat zu beurteilen ist.

[2] Der Berufsgeheimnisträger wird dies in der Regel unter Verweis auf das Berufsgeheimnis und – sollte die Missachtung der Aufforderung sanktionsbewehrt sein und die Daten in der Schweiz liegen – unter Hinweis auf Art. 271 StGB ablehnen (soweit nicht Bestimmungen wie etwa Art. 42 Abs. 1 oder 2 FINMAG im Finanzbereich oder Sonderbewilligungen greifen). Nach dem gewöhnlichen Lauf der Dinge wird die Behörde daraufhin versuchen, den Rechts- oder Amtshilfeweg zu beschreiten. Gelingt ihr dies trotz etwaiger Mithilfe des Berufsgeheimnisträgers (und der von ihm erlaubterweise mitgeteilten Daten[1]) nicht, wird sie nach der Praxiserfahrung des Autors die-

[1] Vgl. etwa das Bundesgesetz über den internationalen automatischen Informationsaustausch in Steuersachen (AIAG).

ses Beitrags mit verschiedensten Behörden und Gerichten in den USA und Europa in den meisten Fällen auf die Beschaffung der Daten verzichten.

2. Sonderfall: Behörde gelangt an den Provider

a. Einleitung

[3] In besonderen Fällen ist es denkbar, dass die ausländische Behörde auf die von ihr gewünschten Kundendaten nicht verzichten will. Gelangt sie über den Berufsgeheimnisträger selbst nicht an die Kundendaten, könnte sie versucht sein, den Provider des Berufsgeheimnisträgers zur Herausgabe zu bewegen. Wie wahrscheinlich diese Konstellation überhaupt ist, sei hier offengelassen, da sich dies nicht generalisieren lässt. Der Berufsgeheimnisträger wird seine eigenen Erfahrungen mit Anfragen von ausländischen Behörden haben, die in seine Risikobeurteilung einfliessen muss. Ein Ansatz ist hier sich zu fragen, was die Erfahrungen der vergangenen zehn Jahre mit Anfragen ausländischer Behörden waren.

[4] Nach der hier vertretenen Ansicht dürfte es sich jedoch um einen Ausnahmefall handeln, der noch wesentlich seltener vorkommen wird als ein Editionsbegehren gegenüber dem Berufsgeheimnisträger selbst oder ein Zugangsgesuch auf dem Weg der Amts- oder Rechtshilfe. Da die Kundendaten des Berufsgeheimnisträgers eine gewisse Sensitivität aufweisen, sei hier für die Zwecke der vorliegenden Beurteilung trotzdem davon ausgegangen, dass eine ausländische Behörde ein gewisses Interesse daran haben könnte, auf diesem Weg an Kundendaten des Berufsgeheimnisträgers zu gelangen (im Modell wird dies im Rahmen der Vorfragen berücksichtigt).

[5] Wäre die Behörde in einem solchen Fall erfolgreich, käme es zur Offenbarung von Kundendaten und der objektive Tatbestand der Berufsgeheimnisverletzung wäre erfüllt. Dies gilt es seitens des Berufsgeheimnisträgers zu vermeiden, jedenfalls soweit die Sorgfaltspflicht des Berufsgeheimnisträgers dies gebietet. Damit es zu diesem Taterfolg kommt, müssen verschiedene Umstände zusammentreffen. Im vorliegenden Beurteilungsmodell wird davon ausgegangen, dass wenn konkret sieben Voraussetzungen kumulativ erfüllt sind, der Berufsgeheimnisträger davon ausgehen muss, dass der Provider Kundendaten der ausländischen Behörde im Klartext bekanntgibt, wenn sie dies verlangt.

[6] Die Eintrittswahrscheinlichkeit jeder dieser sieben Voraussetzungen lässt sich durch eine oder mehrere Gegenmassnahmen seitens des Berufsgeheimnisträgers reduzieren. Nachfolgend wird dargelegt, welche Voraussetzungen dies sind und wie wirksam mögliche Gegenmassnahmen mit Bezug auf die Eintrittswahrscheinlichkeit der Voraussetzungen sind. Im Anschluss erfolgt im Beurteilungsmodell eine Gesamtwürdigung auf Basis einer Wahrscheinlichkeitsrechnung, die alle Voraussetzungen in Anbetracht der im konkreten Fall getroffenen Massnahmen gesamthaft betrachtet. Aus Sicht der Statistik ist dabei wichtig, dass bei der Schätzung der Wahrscheinlichkeiten keine Doppelzählung erfolgt. Ist beispielsweise der Zugang des Providers zu Daten im Klartext technisch nicht möglich und ist dies im Rahmen von Voraussetzung Nr. 2 und 3 bereits berücksichtigt, so darf dieser Faktor im Rahmen der Beurteilung von Voraussetzung Nr. 5, ob der Provider zur Herausgabe gezwungen werden kann, nicht erneut berücksichtigt werden. Hingegen kann eine bestimmte Gegenmassnahmen auf verschiedenen Ebenen die Gesamtwahrscheinlichkeit beeinflussen.

[7] Die von aufgezählten Gegenmassnahmen – technische und organisatorische Massnahmen der Datensicherheit (**TOMS**) – sind keine rechtlichen Fragstellungen und nicht als abschliessen-

de Darstellung zu verstehen. Insbesondere bei den technischen Vorkehrungen sind auch andere, äquivalente Methoden denkbar. Ohnehin ergeben sich die relevanten Wahrscheinlichkeiten erst aus der Kombination der verschiedenen Methoden. Welche einzelnen Massnahmen gewählt und wie umgesetzt werden, ist denn auch keine Rechtsfrage, sondern ein Geschäftsentscheid. Es müssen nicht alle von mir diskutierten Massnahmen getroffen werden, um einen angemessenen Schutz vor einem *Lawful Access* zu erreichen. In allen Fällen müssen die Massnahmen regelmässig auf ihre Wirksamkeit hin überprüft werden, da sich die eingesetzte Technologie und die möglichen Gegenmassnahmen ebenso weiterentwickeln wie die Bedrohungslage und der Rechtsrahmen.

b. Voraussetzung Nr. 1: Behörde weiss um den Provider des Berufsgeheimnisträgers

[8] Zunächst muss die Behörde wissen, wer dieser Provider ist. Diese Information könnte zwar geheim gehalten werden, doch lässt sich dies im Falle der Auslagerung von IT-Anwendungen eines Unternehmens an einen Provider normalerweise nicht bewerkstelligen. Es sind in solchen Fällen zu viele Stellen und Personen involviert. Der Berufsgeheimnisträger kann trotz allem versuchen, die Tatsache, dass gewisse seiner Kundendaten beim Provider verwaltet werden, vertraulich zu halten (**Gegenmassnahme Nr. 1**). Die Wirksamkeit der Gegenmassnahme Nr. 1 ist gering.

[9] Ergebnis: Die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 1 ist zwar nicht 100 Prozent, nach der hier vertretenen Ansicht aber meistens sehr hoch.

c. Voraussetzung Nr. 2: Technische Zugriffsmöglichkeit des Providers auf Kundendaten im Klartext

1. Zugriffsmöglichkeit im Allgemeinen

[10] Damit der Provider einem Herausgabebefehl Folge leisten kann und es zu einer Verletzung des Berufsgeheimnisses kommen kann, muss der Provider technisch in der Lage sein, auf die Kundendaten im Klartext zuzugreifen.

[11] Sind keine besonderen Vorkehrungen getroffen, wird der Provider ohne Weiteres auf die Kundendaten im Klartext zugreifen können. Wer z.B. seinen Mailserver vom Provider betreiben lässt, wird aus Gründen der Funktionalität meistens diesen Zustand haben. Womöglich wird er den Zugriff seinen Mitarbeitern im Normalfall nicht gestatten, doch wenn eine entsprechende Herausgabeanweisung vorliegt, wird ihm dies unter diesen Umständen möglich sein und er wird es tun, sind doch die Systeme in seinem Besitz und unter seiner Kontrolle. Daran ändert eine etwaige Verschlüsselung der Kundendaten nichts, soweit der Provider selbst Zugang zum Schlüssel hat. Eine solche Verschlüsselung schützt nur vor einem vom Provider selbst als unautorisiert erachteten Zugriff auf die Daten seiner Kunden. Ebenso schützen rein organisatorische Massnahmen des Providers nicht vor einem Zugriff, den der Provider gemäss anwendbarem Recht vornehmen muss (wohl aber können organisatorische Massnahmen die Pflicht des Providers beeinflussen, Zugriff nehmen zu müssen, wenn eine Behörde dies verlangt).

[12] Ergebnis: Werden somit keine Gegenmassnahmen getroffen, die den Zugriff des Providers auf die Daten seiner Kunden im Klartext auch technisch und nicht nur organisatorisch einschrän-

ken, ist die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 2 ist nach der hier vertretenen Ansicht praktisch 100 Prozent.

2. Zugriffsmöglichkeit bei Totalverschlüsselung

[13] Der Berufsgeheimnisträger kann dem Zugriff des Providers wirksam begegnen, indem er seine Kundendaten totalverschlüsselt und diese Verschlüsselung nicht aufhebt, solange sie auf dem Server des Providers sind (**Gegenmassnahme Nr. 2**).[2] Da der Schlüssel in den Händen des Kunden bleibt, wird dies auch «*Hold-your-own-key*» bezeichnet. Verfügt der Provider nicht über den Schlüssel, wird er allerdings manche seiner Dienstleistungen nicht mehr erbringen können, da diese Dienstleistungen die Bearbeitung von Daten im Klartext erfordern (z.B. Verarbeiten des Inhalts eines Dokuments oder Abfrage einer Datenbank nach bestimmten Inhalten). Auch für die Behebung von Störungen kann es für den Provider erforderlich sein, auf die Systeme und ihre Daten im Klartext zugreifen zu können. Die dauerhafte Totalverschlüsselung ist somit für die meisten Anwendungen keine Lösung, weil sie die Funktionalität der Anwendung zu stark einschränkt. Die bereits erwähnte Auslagerung des Mailservers in die Cloud ist ein Beispiel; hier ist es zwar denkbar, Mails innerhalb einer Organisation generell oder in heiklen Fällen so zu verschlüsseln, dass der Provider nicht darauf zugreifen kann, aber spätestens bei einem Versand an oder Empfang mit Dritten wird dieses Konzept durchbrochen werden müssen. Eine Alternative kann es sein, nur Dateianhänge (unabhängig vom Provider) zu verschlüsseln, sollten sie besonders heikel sein.

[14] Ergebnis: Die Wirksamkeit der Gegenmassnahme Nr. 2 ist zwar sehr hoch und die Eintrittswahrscheinlichkeit der Voraussetzung Nr. 2 unter diesen Umständen praktisch null. Sie ist jedoch für die meisten Anwendungsfälle schlicht nicht praktikabel, auch wenn Datenschützer immer wieder auf diese Methode verweisen.

3. Zugriffsmöglichkeit bei Abschottung («sichere Zone»)

[15] Will der Berufsgeheimnisträger seine Kundendaten aus Praktikabilitätsgründen auf dem Server des Providers nicht dauerhaft verschlüsselt lassen («HYOK»), muss er die Daten in dem Zeitpunkt, in welchem sie entschlüsselt sind, auf andere Weise vor dem Zugriff des Providers schützen, d.h. ihm die Möglichkeit nehmen, trotz Administratorenrechten und der Möglichkeit des physischen Zugriffs auf seine Systeme, auf die Kundendaten im Klartext zuzugreifen. Es wird gewissermassen eine «sichere Zone» auf dem Server des Providers verwendet, in welcher die Kundendaten mit einem nur dem Kunden bekannten Schlüssel entschlüsselt und entsprechend für die gewünschte Anwendung bearbeitet werden.

[16] In diesem Zusammenhang wird immer wieder das Verfahren «*Bring-your-own-key*» oder «BYOK» genannt, das auch von zahlreichen Cloud-Dienstleistern unterstützt wird (**Gegenmassnahme Nr. 3**). Es basiert auf der Idee, dass es der Kunde selbst ist, der den Schlüssel erzeugt und verwaltet. BYOK wird jedoch nach der hier vertretenen Ansicht überbewertet, weil es in den meisten Fällen gewisse wichtige Lücken im Schutzkonzept offenlässt. Es kann jedoch helfen, den «gefühlten» Datenschutz zu befriedigen, auch wenn die Umsetzung von BYOK oft mit einigem

[2] In der Annahme, dass die Verschlüsselung dem Stand der Technik entspricht.

Aufwand verbunden ist und Projekte daher erheblich verteuern kann. Es birgt auch technische Risiken, denn im Rahmen eines BYOK muss der Kunde selbst den Schlüssel verwalten und dafür sorgen, dass er auch erhalten bleibt. Ist er darin nicht erfahren, können Fehler zum Datenverlust führen, weil der Zugang zu den eigenen Daten nicht mehr möglich ist.

[17] Ein Vorteil von BYOK ist, dass der Kunde eine grössere Kontrolle über den Zugang zu seinen Daten hat, weil er im Normalbetrieb den Schlüssel kontrolliert: Widerruft er ihn, ohne ihn vorher ersetzt zu haben, kann er dafür sorgen, dass niemand mehr auf die Daten im Klartext zugreifen kann, selbst wenn sie sich noch auf dem Server des Providers befinden. Das kann etwa beim Exit aus einem Cloud-Vertrag oder bei behördlichen Zugriffen von Relevanz sein. Allerdings ist hier auch zu berücksichtigen, dass es seitens des Providers diesbezüglich technische Gegenmassnahmen gibt, sollte der Provider von einer Behörde im unwahrscheinlichen Fall hierzu gezwungen werden. BYOK kann auch in rechtlicher Hinsicht die Argumentation erleichtern (dazu Voraussetzung Nr. 5), dass der Provider keine Kontrolle über die Daten des Kunden hat. BYOK ist somit nicht nutzlos. Die Vorteile sind jedoch nach der hier vertretenen Ansicht nicht sehr gewichtig.

[18] Die Problematik von BYOK liegt darin, dass der Kunde zwar den Grossteil des sog. Schlüsselmanagements bei sich durchführt und daher unter eigener Kontrolle hat. Je nachdem, wie der Begriff definiert wird, findet ein Teil aber trotz allem beim Provider statt: Denn die Ver- und Entschlüsselung der Daten geschieht auch bei BYOK auf den Systemen des Providers, d.h. der Provider hat noch eine gewisse Kontrolle darüber. Wieviel, hängt von der konkreten Ausgestaltung der Lösung ab, aber wenn keine besonderen Vorkehrungen getroffen werden, bleibt es dem Provider technisch möglich, mindestens seine Software so anzupassen, dass er noch eine Entschlüsselung von Daten veranlassen kann.

[19] Die Wirksamkeit von BYOK hängt somit entscheidend davon ab, ob und wie wirksam auf dem Server des Providers eine sichere Zone für das Entschlüsseln (und natürlich die Aufbewahrung des Schlüssels) geschaffen werden kann. Dies muss mit *technischen* Vorkehrungen geschehen, da organisatorische Vorkehrungen (wie Weisungen, Prozesse) für den Fall eines *Lawful Access* typischerweise ausser Kraft gesetzt werden. Ist eine solche sichere Zone nicht gewährleistet, hat die Gegenmassnahme Nr. 3 eine geringe Wirksamkeit mit Bezug auf Voraussetzung Nr. 2, d.h. BYOK schützt jedenfalls technisch nicht viel.

[20] Es sind mehrere Methoden denkbar, wie eine solche sichere Zone mit technischen Vorkehrungen geschaffen werden kann. Jede hat dabei ihre Nachteile und Einschränkungen im praktischen Betrieb, d.h. nicht je nach Cloud-Anwendung kommen unterschiedliche Methoden in Frage.

[21] Die *erste* Methode besteht darin, die sichere Zone softwaremässig durch die Verwendung eines sog. virtuellen Servers zu realisieren. Diese Methode ist in Rechenzentren allgegenwärtig, und zwar nicht primär der Datensicherheit, sondern der Ressourcenoptimierung: Auf dem Server des Providers wird in einem ersten Schritt eine Software installiert, die ihrerseits einen Server simuliert. Die Zugangskontrolle (d.h. das Administratorenbenutzerkonto) zu diesem Server wird in einem zweiten Schritt an den Kunden abgetreten, der die Zugangscodes ändern kann. Der Provider kann diesen virtuellen Server zwar weiterhin stoppen, löschen und mit mehr oder weniger Ressourcen (d.h. Rechenleistung, Speicherplatz etc.) versorgen, aber je nach Konfiguration und Funktionalität der verwendeten Software zur Erzeugung des virtuellen Servers wird der Provider jedenfalls über die Software nicht mehr auf den Inhalt des virtuellen Servers und mithin auf die Kundendaten zugreifen können, solange diese vom virtuellen Server bearbeitet werden (**Gegenmassnahme Nr. 4**). Nicht jeder virtuelle Server wird diesen Schutz vor dem Zugriff des

Providers bieten, doch ist die Software entsprechend ausgelegt und konfiguriert, ist die Wirksamkeit dieser Gegenmassnahme mit Bezug auf Voraussetzung Nr. 2 mittel bis hoch. Es ist trotzdem noch möglich, dass der Provider die im virtuellen Server bearbeiteten Kundendaten im Klartext einsehen kann, nämlich dann, wenn sie im Arbeitsspeicher der physischen Serverhardware für die Zwecke der Bearbeitung gespeichert bzw. zwischengespeichert sind oder an einen der physischen Prozessoren übermittelt werden, was in der Regel im Klartext geschieht. Hierfür müsste der Provider eine Software zum Einsatz bringen, die ihn quasi die Vorgänge auf seiner Hardware «mitlesen» lassen. Da er den Server kontrolliert, kann er eine solche «Lauschsoftware» von Kunden unbemerkt installieren. In gleicher Weise wäre es auch denkbar, dass der Provider die für den virtuellen Server benutzte Software so manipuliert, dass sie ihm über eine «Hintertür» einen Zugang zu den im virtuellen Server bearbeiteten oder von diesem abrufbare Klartextdaten bietet. Wie leicht es für einen bestimmten Provider ist, eine solche Lauschsoftware einzusetzen oder eine Hintertür in die für die Erzeugung des virtuellen Servers verwendete Software einzubauen, soll hier nicht beurteilt werden, ebenso, ob die Abschottung durch virtuelle Server noch weitere Schwächen bietet; dies wäre im Einzelfall durch entsprechende Fachleute zu klären und das Ergebnis in die Bewertung einfliessen zu lassen.

[22] Die *zweite* Methode greift die Schwäche der ersten Methode auf, indem sie hardwaremässig verhindert, dass der Provider durch entsprechende Lauschsoftware oder Hintertüren an die Kundendaten im Klartext herankommt. Dazu kommen spezielle Prozessorchips zum Einsatz mit welchen die Entschlüsselung der Kundendaten bis zum letzten Moment hinausgezögert werden kann, nämlich bis zum Moment, wo sich die Daten im Prozessor befinden (**Gegenmassnahme Nr. 5**). Für den Provider sind die Kundendaten somit zu jedem Zeitpunkt, an welchem er als Besitzer des physischen Servers darauf zugreifen könnte, verschlüsselt. Erst wenn sie innerhalb des Prozessors sind, werden sie mit dem nur dem Kunden bekannten Schlüssel (Gegenmassnahme Nr. 3) entschlüsselt. Ein erster Provider bietet diese Gegenmassnahme Nr. 5 inzwischen für bestimmte Anwendungen an.[3] Ihre Wirksamkeit erscheint mit Bezug auf Voraussetzung Nr. 2 als sehr hoch, d.h. sauber umgesetzt kann sie offenbar den technischen Zugriff des Providers auf Kundendaten im Klartext de facto verhindern und damit die immanente Schwäche von BYOK kompensieren, ohne die Funktionalität des Cloud-Service über Gebühr einzuschränken. Die Schwäche des Verfahrens dürfte in der Praxis darin bestehen festzustellen, ob Gegenmassnahme Nr. 5 überhaupt zum Einsatz kommt und sauber umgesetzt wurde: Hierzu sind erstens genaue Kenntnisse der betreffenden Prozessoren erforderlich (tun sie wirklich das, was versprochen wird?), zweitens müssen diese Prozessoren sicher sein (gibt es keine Möglichkeit, an die Daten im Klartext heranzukommen?), drittens muss sichergestellt sein, dass sie vom Provider tatsächlich benutzt werden (oder kommen auf dem Server herkömmliche Prozessoren zum Einsatz?) und viertens muss das Berechtigungsmanagement vollständig in der Hand des Kunden bleiben (sonst kann sich der Provider auf diesem Wege Zugang verschaffen).

[23] Technisch sind auch weitere Methoden zur Schaffung einer sicheren Zone denkbar. Sie muss letztlich so ausgestaltet sein, dass es dem Provider auch dann nicht möglich ist auf die Kundendaten im Klartext zuzugreifen, wenn er es will – Vertrag hin oder her. Mit Zugriff ist dabei der Zugriff durch einen Menschen gemeint. Eine Hardware-basierte Lösung zur Aufbewahrung des Schlüssels beim Provider kann hier beispielsweise ein Ansatz sein, um das Risiko eines Zugriffs

[3] Microsoft «Confidential Compute».

deutlich zu senken. Der Umstand, dass der Computer des Providers die Kundendaten im Klartext sieht, bedeutet somit noch nicht, dass auch Voraussetzung Nr. 2 erfüllt ist; er stellt nach der hier vertretenen Auffassung auch keine Offenbarung dar.[4] Die Daten müssen für eine Berufsgeheimnisverletzung der ausländischen Behörde tatsächlich zur Kenntnis gebracht worden sein, was entweder dadurch geschieht, dass sie die Daten vom Computer des Providers direkt übermittelt erhält (durch einen Fernzugang, durch eine Übermittlung oder – was für die Zwecke dieser Beurteilung ausgeklammert wird – durch Hacking) oder sie einem Mitarbeiter des Providers zugänglich sind; letzteres genügt, weil jeder Mitarbeiter, sollte er mit unmittelbarem staatlichem Zwang konfrontiert sein, diesem letztlich nachgeben wird. Kann daher ein Mitarbeiter Kundendaten irgendwie im Klartext abrufen, auch wenn dies die internen Regeln oder Verträge verbieten, wird er dies im Fall der Fälle auch tun. Wenn also der Provider behauptet, eine andere als die beiden vorgenannten Methoden implementiert zu haben, so ist zu prüfen, ob es sich dabei um eine technische Methode handelt, die den Zugang zu den Kundendaten im Klartext für (alle) Mitarbeiter des Providers und Behörden – allenfalls in Kombination mit Gegenmassnahme Nr. 3 – tatsächlich technisch unterbindet (**Gegenmassnahme Nr. 6**) oder lediglich eine organisatorische Vorkehrung darstellt, also z.B. eine Weisung oder ein Prozess. Liegt eine technische Methode vor, muss weiter geprüft werden, ob es aufgrund der Tatsache, dass der Provider die eingesetzten technischen Mittel (Hard- und Software) auf seinen eigenen Systemen kontrolliert, ihm möglich ist, auf entsprechenden behördlichen Befehl hin das System, welches den Datenzugang verhindert, anzupassen, d.h. eine Hintertür einzubauen. Ob dies vom Provider verlangt werden kann, ist nicht hier sondern im Rahmen von Voraussetzung Nr. 5 zu prüfen.

[24] Alle genannten Gegenmassnahmen zur Schaffung einer sicheren Zone haben die Schwäche, dass der Berufsgeheimnisträger nur schlecht überprüfen kann, ob sie ungeachtet der vertraglichen Zusage tatsächlich wirksam sind und dem Provider ein technischer Zugang zu den Kundendaten im Klartext faktisch verwehrt ist: Cloud-Dienstleister geben ihren Kunden normalerweise keinen physischen Zugang zu ihren Servern und erlauben ihnen auch nicht, die darauf installierte Hard- und Software zu untersuchen, und selbst wenn sie es täten, wären die Kunden mit der Komplexität der Fragestellung überfordert.

[25] Eine gewisse Abhilfe schaffen können die Dienstleister jedoch dadurch, dass sie nebst der vertraglichen Zusicherung der betreffenden Gegenmassnahmen durch einen fachkundigen und unabhängigen Dritten überprüfen und bestätigen lassen, dass die jeweilige Gegenmassnahme zur Schaffung einer sicheren Zone tatsächlich zum Einsatz kommen (d.h. einschliesslich Massnahmen zur Datensicherheit nach dem Stand der Technik) und keine Hinweise auf eine Umgehung (d.h. Bestehen einer Hintertür oder den Einsatz einer Lauschsoftware) vorliegen. Dies ist jeweils als Teil der Gegenmassnahmen Nr. 3–6 zu betrachten.

[26] Geschieht dies und handelt es sich um einen Provider mit gutem Ruf, ist die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 2 nach der hier vertretenen Ansicht faktisch tief, denn damit Voraussetzung Nr. 2 erfüllt wäre, müsste der Provider sowohl seine vertragliche Zusicherung verletzen als auch den unabhängigen Dritten täuschen. Dass beides zusammentrifft ist bei einem Provider mit gutem Ruf nach dem gewöhnlichen Lauf der Dinge und Erfahrungen des Lebens nicht zu erwarten (vorbehalten bleibt selbstverständlich eine auch aus Sicht des Providers unau-

[4] Der Begriff der Offenbarung setzt u.E. begrifflich die Kenntnisnahme durch einen Menschen voraus; eine Maschine genügt nicht. Vgl. dazu Entscheid BGer 6B_1403/2017, Erw.1.2.2.

torisierte Unterwanderung der Gegenmassnahmen durch externe oder interne Angreifer,[5] doch besteht dieses Risiko einer Verletzung der Datensicherheit immer und wird in der vorliegenden Beurteilung ausgeklammert). Der Provider würde ansonsten seine Geschäftsgrundlage aufs Spiel setzen.

[27] Erfolgt zwar die vertragliche Zusicherung, gelingt jedoch der Nachweis durch den Dritten nicht, so reduziert sich die Wirksamkeit der Gegenmassnahme deutlich und es dürfte nur mit einer mittleren Eintrittswahrscheinlichkeit von Voraussetzung Nr. 2 zu rechnen sein; fehlt es an einer vertraglichen Zusicherung, wird die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 2 mittel bis hoch sein.

[28] Zu beachten ist in diesem Zusammenhang auch, ob sich der Provider zusätzlich vertraglich verpflichtet, ausländischen Behörden keine Kundendaten zugänglich zu machen, es sei denn, der Berufsgeheimnisträger oder das Schweizer Recht erlaube es ihm (was eine weitere Gegenmassnahme darstellt; dazu N 78 ff.). Ist er dazu nicht bereit, kann dies ein Hinweis darauf sein, dass die von ihm behaupteten Gegenmassnahmen zur Beschränkung seines technischen Zugriffs nach seiner eigenen Ansicht nicht wirklich wirksam sind. Lässt er sich hingegen darauf ein, spricht dies für die Wirksamkeit dieser technischen Massnahmen.

[29] In technischer Hinsicht ist im Zusammenhang mit BYOK und der Schaffung von sicheren Zonen die technische Absicherung der eingesetzten Verzeichnisdienste zu prüfen (z.B. *Active Directory*). Denn wenn zwar Schlüssel und Kundendaten sicher aufbewahrt werden, es aber dem Provider möglich ist, sich über die Verzeichnisdienste oder Schlüsselmanagement einen Zugang zu verschaffen (z.B. indem der Provider sich mit Hilfe seiner Administratorenrechte im Active Directory des Kunden ein Nutzerkonto mit Zugangsrechten zur sicheren Zone des Kunden einrichtet und sich parallel dazu über das Schlüsselmanagement mit dem entsprechenden *Private Key* ausstattet), nutzen die Massnahmen nichts. Mit anderen Worten: Wer sein Haus einbruchssicher macht, muss zugleich sicherstellen, dass unbefugte Dritte sich nicht einen Schlüssel dazu verschaffen können. Das wird bei vielen Cloud-Diensten eines der Hauptschwierigkeiten sein: Der Provider wird sich grundsätzlich einen Generalschlüssel bzw. den Zugang zum Kästchen mit dem Generalschlüssel vorbehalten. Auch hier gibt es Massnahmen, wie dieses Risiko reduziert werden kann, aber je nach Art von Service kann es dazu führen, dass ungeachtet von BYOK und anderen Massnahmen davon ausgegangen werden muss, dass der Provider – wenn er es unbedingt will – sich technisch Zugang zu den Kundendaten im Klartext verschaffen kann. Es sollte somit geprüft werden, ob das Unternehmen *entweder* sicherstellen kann, dass es die alleinige Hoheit über den Verzeichnisdienst hat, über welchen die Zugangsberechtigungen zu den einzelnen Ressourcen (Mailboxen, Sharedrives, etc.) gesteuert werden (d.h. wer kann Benutzer anlegen, Rechte zuweisen, Personen in Gruppen verschieben oder daraus entfernen, etc.) (**Gegenmassnahme Nr. 7**), oder es dafür sorgen kann, dass nur das Unternehmen kontrollieren kann, welche Personen bzw. Rollen (auch seitens des Providers) Zugang zu den jeweiligen Schlüsseln erhalten (**Gegenmassnahme Nr. 8**). Etwaige Hintertüren können dabei im Rahmen der hier praktizierten Wahrscheinlichkeitsrechnung typischerweise unbeachtet blieben. Denn können sie ausgeschlossen werden, läge konzeptionell eine sichere Zone im Sinne der Gegenmassnahmen

[5] Gemeint ist damit jedoch nicht der Fall, in welchem der Provider durch die Behörde gezwungen wird, seine Gegenmassnahmen zu unterwandern (in diesem Falle handelt der Provider mindestens mit Wissen und allenfalls auch mit Willen), sondern beispielsweise der Angriff durch einen Hacker, von dem der Provider weder weiss noch nicht ihn will.

Nr. 3–6 vor (das Konzept einer sicheren Zone beinhaltet in diesem Sinne bereits ein Äquivalent von Gegenmassnahme Nr. 7 und 8). Die Gegenmassnahmen Nr. 7 und 8 sind daher vor allem dort ein Thema, wo die Bildung einer sicheren Zone aus technischen oder funktionalen Gründen ausscheidet, es aber mit den vorhandenen Instrumenten des jeweiligen Cloud-Service trotzdem möglich ist, ein Plus an Zugriffssicherung gegenüber dem Provider zu erreichen.

[30] Ergebnis: Werden die Gegenmassnahmen Nr. 3 sowie Nr. 4, 5 oder 6 vertraglich vereinbart und umgesetzt, bestehen keine Hinweise auf eine Umgehung (z.B. Hintertür, Lauschsoftware) und sind die Massnahmen durch einen unabhängigen Dritten bestätigt, so ist die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 2 nach der hier vertretenen Ansicht sehr tief. Auch die Gegenmassnahmen Nr. 3 in Kombination mit der Gegenmassnahme Nr. 7 oder Nr. 8 führt immer noch zu einer eher tiefen Eintrittswahrscheinlichkeit, auch wenn diese Gegenmassnahmen naturgemäss weniger Schutz bieten als eine sichere Zone. Hat der Provider hingegen weiterhin technisch Zugang zu den Kundendaten, auch wenn er «versprechen» mag, diesen nicht zu benutzen und über entsprechende interne Weisungen verfügt, so muss die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 2 als hoch zu beurteilen.

4. Zugriffsmöglichkeit im Supportfall

[31] Die Gegenmassnahmen zur Schaffung einer sicheren Zone haben den Nachteil, dass es Situationen geben kann, in welchen der Provider auf die zur Bearbeitung der Kundendaten benutzten Anwendungen zugreifen können muss, zum Beispiel um technische Probleme zu beurteilen und zu lösen. Der Provider und der Berufsgeheimnisträger werden daher zwangsläufig Fälle vereinbaren müssen, in welchen der Provider technischen Zugang zu den Kundendaten im Klartext bzw. den Anwendungen und virtuellen Servern, die solche bearbeiten, erhalten muss. In diesen Situationen besteht bei solchen Support-Zugriffen somit eine vergleichsweise hohe Wahrscheinlichkeit, dass die Voraussetzung Nr. 2 gegeben sein wird.

[32] Dies basiert auf der Annahme, dass es in gewissen Fällen erforderlich sein kann, dass dem Provider auch Zugriff auf Kundendaten im Klartext gewährt werden muss bzw. er solche im Rahmen seiner Arbeiten wahrnehmen kann, d.h. alle anderen Möglichkeiten des Supports ohne Möglichkeit des Zugangs zu Kundendaten nicht zum Ziel führen (Beispiel: Ein Benutzer hat ein Problem mit seiner Mailbox – ein Support-Mitarbeiter des Providers muss unter Umständen Einblick in die Mailbox nehmen, damit er das Problem lösen kann). Trifft diese Annahme zu, was für jede Anwendung separat zu beurteilen wäre, so ist die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 2 zwar nicht 100 Prozent, aber dennoch so hoch, wie die Wahrscheinlichkeit der Notwendigkeit eines Support-Zugriffs mit der Möglichkeit eines Zugangs zu Kundendaten. Mangels anderer Hinweise ist daher davon auszugehen, dass diese Wahrscheinlichkeit einstweilen sehr hoch ist.

[33] Sollte der Provider hingegen der Ansicht sein, dass er für seinen Support bzw. die Einhaltung seiner Leistungsversprechen nie Zugang zu Kundendaten braucht, wäre dies vertraglich entsprechend zu vereinbaren (**Gegenmassnahme Nr. 9**).

[34] Immerhin sind mit Bezug auf Supportzugriffe Gegenmassnahmen zur Senkung der Eintrittswahrscheinlichkeit von Voraussetzung Nr. 2 möglich. Eine besteht darin, den Mitarbeitern des Providers nur einzelfallweise und für eine beschränkte Zeit Zugang zu bestimmten Bereichen der sicheren Zone zu gewähren oder – falls eine solche sichere Zone technisch nicht geschaffen werden kann – den Mitarbeitern des Providers vertraglich den Zugang zu Kundendaten im Klartext nur zu erlauben, wenn der Kunde dies einzelfallweise gestattet hat und nur so lange er dies

gestattet hat (sog. *Lockbox-Verfahren;* **Gegenmassnahme Nr. 10**). Etwas weiter geht der Berufsgeheimnisträger, wenn er dem Mitarbeiter des Providers zwar Zugang zur sicheren Zone gewährt, ihn während seinen Aktivitäten aber live beobachtet und seinen Zugang unterbinden kann, sobald der Mitarbeiter etwas tut, dass dem Berufsgeheimnisträger nicht mehr passt (sog. *Shoulder Surfing*; **Gegenmassnahme Nr. 11**).

[35] Bezüglich der Wirksamkeit beider Gegenmassnahmen im Rahmen von Voraussetzung Nr. 2 ist zunächst entscheidend, wie sie gegenüber dem Provider erzwungen werden können: Sind sie lediglich durch *organisatorische* Vorkehrungen abgesichert (d.h. durch vertragliche Zusagen, interne Weisungen, definierte Prozesse, Vier-Augen-Prinzip etc.), so sind sie mit Bezug auf Voraussetzung Nr. 2 kaum wirksam, da organisatorische Massnahmen seitens des Providers im Falle eines *Lawful Access* faktisch übersteuert werden können (ob dies der Behörde bzw. dem Provider erlaubt ist, wird im Rahmen von Voraussetzung Nr. 5 und 6 geprüft und nicht hier). Sind sie hingegen durch *technische* Vorkehrungen abgesichert (d.h. durch technische Zugangsbeschränkungen, automatische Protokollierung etc.), kann – analog zu den Gegenmassnahmen Nr. 3–6 – ein unabhängiger Nachweis der Implementation dieser Vorkehrungen erbracht werden und liegen keine Hinweise auf eine Umgehung vor (dazu N 24 ff.), so erscheint die Wirksamkeit beider Gegenmassnahmen auf den ersten Blick mittel bis hoch. In der Praxis ist normalerweise eine Kombination zu sehen, d.h. der Provider stellt Gegenmassnahme Nr. 10 und Nr. 11 zwar nur organisatorisch sicher (d.h. er verbietet seinen Mitarbeitern den Zugriff ohne Erlaubnis der Kunden, unterbindet ihn aber nicht), sorgt jedoch für eine automatische Protokollierung aller Zugriffe, so dass der Kunde feststellen kann, ob die Vorgaben befolgt wurden. Hat der Provider dies nicht getan, liegt eine Vertragsverletzung vor. Selbstverständlich wird vom Berufsgeheimnisträger im Fall von Gegenmassnahme Nr. 10 verlangt werden, dass er die Protokolle regelmässig prüft.

[36] Wird eine sichere Zone verwendet, besteht selbstverständlich auch bei diesen Support-Zugriffen das Risiko, dass der Provider eine Software in die sichere Zone einschleust, die dem Provider eine Hintertür zu dieser öffnet und somit auch die Gegenmassnahme Nr. 10 und 11 mit etwaigen technischen Massnahmen unterlaufen wird. Es kann auf das zu den Gegenmassnahmen Nr. 4 und 6 zum Risiko von Hintertüren Gesagte verwiesen werden.

[37] Beide Gegenmassnahmen lösen freilich nicht das grundsätzliche Problem, dass es je nach Fallkonstellation bei gewissen Supportfällen nötig sein wird, dem Provider einen Zugang zur sicheren Zone zu gewähren, bei welcher dieser Kundendaten wahrnehmen kann oder sogar zur Erfüllung seiner Arbeit bearbeiten muss (z.B. bei Arbeiten auf einer Datenbank). Die Gegenmassnahmen Nr. 10 und 11 sind daher primär dort relevant, wo es darum geht, den Zugang zu Kundendaten im Klartext dort zu verhindern, wo es diesen für den Support-Zugriff nicht braucht.

[38] Ergebnis: Ist es denkbar, dass in gewissen Situationen ein Support-Zugriff durch den Provider nötig ist, bei welchem dieser auch Kundendaten im Klartext sehen können muss oder sich dies nicht vermeiden lässt, ist die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 2 sehr hoch, da der Kunde diese Möglichkeit zwangsläufig vorsehen muss. Sind solche Support-Zugriffe faktisch hingegen nicht denkbar, werden die Gegenmassnahmen Nr. 9 sowie 10 oder 11 umgesetzt, wird dies vom Provider vertraglich zugesichert, liegen keine Hinweise auf eine Umgehung (z.B. Hintertür, Lauschsoftware) vor und wird dies durch einen unabhängigen Dritten im Wesentlichen bestätigt, so ist die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 2 mittel (bei Gegenmassnahme Nr. 10) bis tief (bei Gegenmassnahme Nr. 11).

d. Voraussetzung Nr. 3: Möglichkeit des Providers, nach Kundendaten zu suchen

[39] Damit der Provider einem Herausgabebefehl Folge leisten kann, muss er nicht nur auf Kundendaten im Klartext zugreifen können, sondern er muss dies so tun können, dass er eine Anfrage der Behörde vernünftig beantworten kann. Nach dem gewöhnlichen Lauf der Dinge und der Erfahrungen des Lebens wird eine Behörde nicht alle oder irgendwelche Kundendaten verlangen, sondern bestimmte (z.B. Daten eines bestimmten Kunden, einer bestimmten Kundenkategorie, Daten zu bestimmten Transaktionen oder aus einem bestimmten Bereich des Berufsgeheimnisträgers). Dies setzt wiederum voraus, dass der Provider in der Lage ist, im Rahmen seiner Zugriffsmöglichkeiten nach diesen Kundendaten zu suchen und sie abzufragen.

[40] Dazu muss der Provider entweder (i) selbst Zugang zu den vom Berufsgeheimnisträger auf seinen Servern benutzten Anwendungen haben (um eine entsprechende Anfrage absetzen zu können), (ii) auf die darunterliegenden Datenressourcen und -systeme zugreifen können (z.B. das Datenbankmanagementsystem, die Middleware) oder (iii) alle Kundendaten extrahieren können, damit er sie auf seinen eigenen Systemen replizieren und entsprechend absuchen kann. Ist er zu einem dieser Dinge in der Lage, ist die Voraussetzung Nr. 3 gegeben.

[41] Damit der Provider zu einem dieser Dinge in der Lage ist, muss zunächst Voraussetzung Nr. 2 gegeben sein, d.h. ein technischer Zugriff auf die Kundendaten im Klartext. Die Wahrscheinlichkeit, dass dies der Fall ist, wird in der Gesamtbeurteilung berücksichtigt. Es stellt sich daher vorliegend lediglich die Frage, ob die bereits erläuterten Gegenmassnahmen Nr. 3–11 geeignet sind, die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 3 bei an sich vorhandenem Zugriff auf Kundendaten weiter zu senken, und ob es allenfalls weitere Gegenmassnahmen gibt.

[42] Hierbei ist entsprechend der Beurteilung von Voraussetzung Nr. 2 zwischen dem Szenario mit und ohne Support-Zugriff zu unterscheiden. Der Fall der Totalverschlüsselung kann vorliegend ganz ausgeklammert werden, da in diesem Fall die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 2 praktisch null ist. Ebenso sei hier nicht auf den Fall keiner Gegenmassnahme zur Vermeidung von Voraussetzung Nr. 2 eingegangen, da dies im Falle des Berufsgeheimnisträgers nicht vorkommen wird.

[43] Ausserhalb eines Support-Zugriffs sind die Gegenmassnahmen Nr. 3–8 zwar geeignet, auch die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 3 weiter zu reduzieren, jedoch dürfte diese Reduktion nicht wesentlich sein. Sollte es dem Provider gelingen, die Gegenmassnahmen zur Verhinderung seines technischen Zugriffs zu umgehen, indem er z.B. eine Hintertür einbaut oder eine Lauschsoftware einsetzt, mit der er unbemerkt unverschlüsselte Kundendaten aus der sicheren Zone ausleiten oder aus dem Speicher bzw. auf dem Weg zum Prozessor auslesen kann, so wird es ihm auch möglich sein, entsprechende Abfragefunktionen vorzusehen bzw. die Lauschsoftware dauernd «laufen» zu lassen, um auf diese Weise immer grössere Teile der Kundendaten in seine Kontrolle zu bringen. Es wird ihm bei einer solchen Vorgehensweise auch möglich sein, etwaige Protokollierungsmechanismen der Anwendungen zu umgehen (aus diesem Grund wird sie hier nicht als separate Gegenmassnahme erachtet). Allerdings ist die Komplexität eines solchen koordinierten und gezielten Zugriffs auf die sichere Zone gegenüber einem irgendwie gearteten Zugriff massiv höher, und auch ein konstanter Lauschangriff bietet keine Gewähr, dass die gewünschten Kundendaten «in die Fänge» gehen, da dies bei einem solchen Angriff nur dann geschieht, wenn der Kunde sie selbst bearbeitet.

[44] Wie die Resilienz der Gegenmassnahmen Nr. 3–8 gegenüber solchen «Angriffen» einzustufen ist, muss an dieser Stelle offenbleiben. Es muss daher nach dem gewöhnlichen Lauf der Dinge davon ausgegangen werden, dass die Gegenmassnahmen ausserhalb des Support-Zugriffs zwar über eine gewisse Wirksamkeit auch mit Bezug auf die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 3 aufweisen, sie aber letztlich beschränkt sein wird. Allerdings ist auch davon auszugehen, dass die Methoden zur Umgehung der Gegenmassnahmen 3–8 sich nicht kurzfristig umsetzen lassen. Insbesondere der Zugriff durch Auslesen aller Daten erfordert eine langfristige Vorgehensweise. Damit sind diese Methoden für konkrete, nach dem gewöhnlichen Lauf der Dinge kurzfristig (d.h. innert Wochen oder Monaten) zu erfüllende Herausgabebegehren nicht geeignet. Diese Methoden sind auch aufwändig. Es ist davon auszugehen, dass eine Behörde nicht gewillt sein wird, lange auf die von ihr verlangten Kundendaten zu warten und es fraglich ist, ob der Provider verpflichtet werden kann oder die Behörde bereit ist, die entsprechenden Kosten zu tragen – dies bei ungewissem Ausgang der Übung. Dies reduziert die Wahrscheinlichkeit eines solchen Szenarios deutlich.

[45] Eine solche Vorgehensweise wird sich zudem langfristig nicht geheim halten lassen: Gelangen Behörden auf diese Weise an Daten von Kunden des Providers, die sie in ihren Verwaltungs-, Straf-, oder Gerichtsverfahren rechtlich verwerten wollen, werden sie jedenfalls in einem nach rechtsstaatlichen Grundsätzen geführten Verfahren offenlegen müssen, wo und wie sie an diese Angaben gelangt sind und es ist davon auszugehen, dass dies in der Folge öffentlich bekannt werden wird. Wird dies öffentlich bekannt, zieht der Berufsgeheimnisträger seine Daten bei diesem in der Folge ab, dürfte er einer Herausgabe seiner Kundendaten an die Behörde höchstwahrscheinlich zuvorkommen. Hat der Provider besonders viele Kunden, ist die Wahrscheinlichkeit, dass ein solcher Zugriff vor dem Bekanntwerden den Berufsgeheimnisträger trifft, nach der hier vertretenen Ansicht dementsprechend gering. Die Möglichkeit, Kundendaten bei Bekanntwerden einer Unterwanderung der Gegenmassnahmen Nr. 3–8 vom Provider abzuziehen, wird daher die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 3 jedenfalls im Falle eines Providers mit zahlreichen anderen Kunden noch weiter reduzieren. Der Berufsgeheimnisträger sollte daher einen entsprechenden Provider wählen und sich diese Möglichkeit (Kündigung mit Abzug aller Daten ohne Rückbehalt durch den Provider) rechtlich und technisch vorbehalten (**Gegenmassnahme Nr. 12**).

[46] Daher ist nach der hier vertretenen Ansicht davon auszugehen, dass mit den Gegenmassnahmen Nr. 3–8 und Gegenmassnahme Nr. 12 die Eintrittswahrscheinlichkeit auch von Voraussetzung Nr. 3 ausserhalb des Support-Zugriffs mittel ist.

[47] Besteht hingegen keine sichere Zone und kann sich der Provider z.B. über die Verzeichnisdienste und Schlüsselmanagement einen Benutzerzugang zu den Daten des Berufsgeheimnisträgers verschaffen, wird die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 3 auch ohne Support-Zugriff relativ hoch sein; begrenzt ist sie primär dadurch, dass der Provider nicht weiss, wie er die Anwendungen des Kunden zu bedienen hat oder sie proprietäre Zugriffsschutzmechanismen aufweisen, die er nicht kontrollieren kann.

[48] Im Falle eines Support-Zugriffs kommen weitere Aspekte hinzu. Hier erfolgt der Zugriff auf die sichere Zone mit Wissen und Willen des Kunden und je nach Konstellation (vgl. N 31 ff.) kann auch ein Zugang zu Kundendaten des Berufsgeheimnisträgers erforderlich sein, d.h. die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 2 ist in diesen Fällen sehr hoch. Anders verhält es sich mit der Eintrittswahrscheinlichkeit von Voraussetzung Nr. 3: Diese ist nach der hier vertretenen Ansicht tief. Denn erstens kommt es zu einem solchen Zugriff nicht dann, wenn der

Provider oder die Behörde es will, sondern wenn eine entsprechende Störung vorliegt und der Kunde den Zugriff freigibt (was er freilich in aller Regel tun wird). Zweitens erhält der Provider in diesem Fall jedenfalls bei Implementierung von Gegenmassnahme Nr. 10 oder 11 nicht Zugriff auf alle Kundendaten, sondern nur jene, die es für die Behebung der Störung braucht. Die Wahrscheinlichkeit, dass der Provider dabei just auf jene Kundendaten des Berufsgeheimnisträgers im Klartext zugreifen kann, die er für die Beantwortung einer gerade ihm vorliegenden Behördenanfrage benötigt, erscheint gering. Zwar wäre es theoretisch denkbar, dass der Provider die Störung provoziert, um eine solchen Zugriff zu erlangen, doch erscheint es unwahrscheinlich, dass sich der Provider auf ein solches konzertiertes Vorgehen mit der Behörde einlässt (eine andere Frage ist, ob sie dies überhaupt verlangen könnte, vgl. N 63) und sie es technisch und praktisch umsetzen kann, ohne, dass den Berufsgeheimnisträgers dies bemerkt, jedenfalls soweit sie Gegenmassnahme Nr. 11 umgesetzt hat (bei dieser dürfte es sofort auffallen, wenn der Provider beginnt, die Daten bestimmter Kunden gezielt abzurufen, und vor allem in relevanten Mengen). Die Gegenmassnahmen Nr. 10 und insbesondere Nr. 11 sind somit geeignet, die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 3 bei Support-Zugriffen mit Zugang zu Kundendaten tief zu halten. Freilich ist auch hier sicherzustellen, dass die Gegenmassnahmen Nr. 11 nicht nur organisatorisch abgesichert ist, sondern auch technisch, d.h. dass der Provider tatsächlich nur mit Einwilligung und unter Beobachtung des Kunden auf Kundendaten im Klartext zugreifen kann.

[49] Ergebnis: Werden die Gegenmassnahmen Nr. 3 sowie Nr. 4, 5, 6, 7 oder 8 sowie Nr. 10–12 umgesetzt, ist die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 3 – bei Eintritt von Voraussetzung Nr. 2 *ohne* Support-Zugriffs mit Zugang zu Kundendaten – nach der hier vertretenen Ansicht mittel; für den Fall des Support-Zugriffs mit Zugang zu Kundendaten ist die Eintrittswahrscheinlichkeit nach der hier vertretenen Ansicht nur mit Gegenmassnahme Nr. 10 mittel, mit Gegenmassnahme Nr. 11 tief. Besteht keine sichere Zone, ist die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 3 hingegen hoch, es sei denn, es bestehen zusätzliche, nicht vom Provider kontrollierte Massnahmen, die ein Abfragen der gesuchten Daten durch den Provider verhindern.

e. Voraussetzung Nr. 4: Der Provider oder einer seiner Subunternehmer ist im Zuständigkeitsbereich einer an einem Lawful Access interessierten Behörde

[50] Ein Zugriff durch eine Behörde setzt einen entsprechenden Herausgabebefehl voraus. Dies wiederum erfordert, dass der Provider sich im örtlichen Zuständigkeitsbereich einer Behörde befindet, die einen solchen Befehl erlassen kann und daran auch interessiert ist. Dies ist als Voraussetzung Nr. 4 zu prüfen.

[51] Grundsätzlich definiert jeder Staat selbst, welche Personen seiner Hoheit unterworfen sind. Dies ist nicht begrenzt auf das Territorium eines Staates. So gesehen ist die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 4 hoch: Es ist ohne Weiteres denkbar, dass es ein Land gibt, das sowohl an Kundendaten des Berufsgeheimnisträgers gelangen will als auch dazu bereit ist, eine Zuständigkeit seiner Behörden über den Provider zu begründen, der über diese Daten verfügt, um diesem deren Herausgabe zu befehlen.

[52] Nach dem gewöhnlichen Lauf der Dinge genügt dies jedoch nicht. Es stellt sich viel mehr die Frage, ob der betreffende Staat seine Anordnung gegenüber dem Provider auch tatsächlich durchsetzen kann, d.h. seine Anordnung nötigenfalls mit staatlicher Gewalt durchsetzen kann. Dies wird immer dann der Fall sein, wenn der Provider sich auf dem Hoheitsgebiet des betreffen-

den Staats befindet, dort Vermögenswerte unterhält oder ein anderer Konnex zum betreffenden Staat besteht, etwa indem er dort seine Dienstleistungen anbietet.

[53] In den USA ein Dienstleister zum Beispiel im Rahmen des *Stored Communications Acts* (und *CLOUD Act*) nur dann damit rechnen, dass ihn die Strafverfolgungsbehörden zur Herausgabe in seinem Besitz oder unter seiner Kontrolle befindliche Daten seiner Kunden herauszugeben, wenn er seinen Sitz in den USA hat. Eine entsprechende Bestimmung sieht Art. 18 Abs. 1 lit. a des Übereinkommens über die Cyberkriminalität (Cybercrime-Convention, CCC, SR 0.311.43) für alle Staaten der Konvention so vor, was gegenwärtig 64 sind, darunter die USA und die meisten Staaten Europas (mit Ausnahme von Irland, welches die CCC zwar unterzeichnet, aber nicht ratifiziert hat).[6] Anders kann die Situation in jenen Fällen sein, in welchen die USA mit einem anderen Staat im Rahmen eines Executive Agreement vereinbart hat, dass aus den USA auch grenzüberschreitende Herausgabeanweisungen an Provider erlaubt sind (so wie etwa im Falle von Grossbritannien).

[54] Will der Berufsgeheimnisträger die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 4 reduzieren, muss er daher dafür sorgen, dass der Konnex des Providers zum Ausland und insbesondere zu Staaten, aus denen Herausgabebefehle zu erwarten sind, möglichst gering bleibt. Als konkrete Massnahme drängt sich daher auf, dass der Provider seinen Sitz in der Schweiz hat (**Gegenmassnahme Nr. 13**), um nicht von Art. 18 Abs. 1 lit. a CCC erfasst zu werden. Um nicht unter Art. 18 Abs. 1 lit. b CCC zu fallen, welcher die Herausgabe von Randdaten betrifft, bietet es sich zusätzlich an, einen Provider zu wählen, der seine Dienstleistungen nicht in hier relevanten ausländischen Staaten anbietet (**Gegenmassnahme Nr. 14**), aber dieser Punkt dürfte vorliegend weniger relevant sein.

[55] Zieht der Provider zur Erbringung der Cloud-Dienstleistung weitere Gesellschaften hinzu oder wird er selbst von einer weiteren Gesellschaft kontrolliert (z.B. einer Muttergesellschaft), so muss die Voraussetzung Nr. 4 für jede dieser Gesellschaften separat beurteilt werden. Die Frage, ob eine beigezogene Gesellschaft überhaupt einen relevanten Zugang zu Kundendaten hat, ist an sich im Rahmen von Voraussetzung Nr. 2, 3 und 5 zu beurteilen. Daher wäre Voraussetzung Nr. 4 an sich für jeden beigezogenen Dritten mit Sitz ausserhalb der Schweiz im Hinblick auf Art. 18 Abs. 1 lit. a CCC (anders lit. b) automatisch zu 100 Prozent erfüllt, da die Behörden seines Sitzlandes immer zuständig sind, von ihm die Herausgabe von Kundendaten zu verlangen. Mit anderen Worten: Zieht ein Provider mit Sitz in der Schweiz oder der EU eine Konzerngesellschaft in den USA bei der Erbringung ihrer Leistungen bei, so sind die US-Behörden räumlich zuständig, ihr Herausgabebefehle nach Art. 18 Abs. 1 CCC zu senden, egal, ob der Provider oder anderen Konzerngesellschaften einen Konnex zu den USA oder einen Sitz in den USA aufweisen.

[56] Nach der hier vertretenen Ansicht kann im Rahmen von Voraussetzung Nr. 4 der Umstand nicht mehr berücksichtigt werden, wie wahrscheinlich es ist, dass diese Behörden überhaupt ein relevantes Interesse haben, für die Herausgabe von Kundendaten an den Provider zu gelangen statt andere Wege zu versuchen, wie namentlich eine Anfrage an den Berufsgeheimnisträger oder den Amts- und Rechtshilfeweg. Diese anderen Wege werden in manchen Fällen wohl einfacher, rascher und zuverlässiger sein; die Wahrscheinlichkeit, dass es zu einem *Lawful Access* über den Provider kommt reduziert sich in dem Masse, als es für die Behörde einfacher ist, auf anderem

6 Vgl. Complete list of the Council of Europe's treaties (https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185), kontrolliert am 3. Juli 2020.

Weg ans Ziel zu kommen. Dieser Aspekt wird im vorliegenden Beurteilungsmodell normalerweise vorfrageweise geprüft und fällt in diesem Fall hier bei Voraussetzung Nr. 4 weg.

[57] Während daher bei gewissen Staaten wie den USA vernünftigerweise von einem gewissen Interesse an Zugangsversuchen über Dienstleister ausgegangen werden muss, dürfte die Analyse bei anderen Staaten zu einem weniger klaren Ergebnis führen. Vorliegend kann dazu keine Aussage getroffen werden; der Berufsgeheimnisträger kann im Zuge einer Risikoabschätzung allerdings ermitteln, aus welchen Ländern sie bisher selbst Herausgabebegehren erhalten hat. Da eine Behörde es in aller Regel zunächst direkt beim Berufsgeheimnisträger versuchen wird, falls und wenn sie an deren Kundendaten gelangen möchte, sind solche historischen Begehren ein guter Indikator, aus welchen Ländern mit Herausgabebefehlen auch in Zukunft zu rechnen ist.

[58] Ergebnis: Soweit die Gegenmassnahme Nr. 13 für den Provider und alle sonst beteiligten Gesellschaften sichergestellt ist, wird die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 4 tief. Dies wird jedoch selten der Fall sein, da die hier relevanten Provider typischerweise Subunternehmer aus anderen Staaten als der Schweiz beiziehen oder ihrerseits unter der Kontrolle einer ausländischen Muttergesellschaft stehen. In diesen Fällen muss daher davon ausgegangen werden, dass immer eine dieser Gesellschaften in einem Land ist, in welcher eine Behörde potenziell Interesse an einem *Lawful Access* hat und somit die Voraussetzung Nr. 4 zu 100 Prozent gegeben ist. Allerdings kann der Berufsgeheimnisträger separat berücksichtigen, wie gross die Wahrscheinlichkeit ist, dass eine an sich zuständige Behörde überhaupt je in eine Situation kommt, in welcher sie über einen *Lawful Access* nachdenken muss: Kann sie ihren Bedarf an Zugang zu Kundendaten des Berufsgeheimnisträgers normalerweise auf anderem Wege (Rechts- und Amtshilfe, freiwillige Datenlieferungen des Berufsgeheimnisträgers) befriedigen, so wird ein Herausgabebefehl an den Provider unwahrscheinlich. Dieser Aspekt wird im vorliegenden Modell typischerweise vorfrageweise geprüft und nicht im Rahmen von Voraussetzung Nr. 4.

f. Voraussetzung Nr. 5: Behörde ist berechtigt, dem Provider, seinem Subunternehmer oder seiner Mutter zu befehlen, sich technischen Zugang zu den Kundendaten zu verschaffen und diese herauszugeben

1. Grundsätzliches

[59] Die Zuständigkeit einer Behörde über den Provider genügt nicht, damit der Provider die Daten herausgibt. Die Behörde muss auch berechtigt sein, von ihm die Herausgabe zu verlangen. Hierzu ist an sich eine Analyse der Eintrittswahrscheinlichkeit dieser Voraussetzung nach dem jeweiligen ausländischem Recht erforderlich. Handelt es sich um einen Staat, dessen Recht sich im hier relevanten Punkt nach der CCC richtet, so sind hier grundsätzliche Aussagen möglich. Beispiel für ein solches Land sind die USA und der bereits erwähnte *Stored Communications Act* und *CLOUD Act*.

[60] Selbstverständlich ist es jedem Staat freigestellt, seinen Behörden *weitergehende* Zugriffsmöglichkeiten auf Daten einzuräumen, speziell soweit sich diese in ihrem eigenen Land befinden (Beispiel: Beschlagnahmung von Daten, die ein Cloud-Provider in seinem Rechenzentrum in Frankfurt speichert, durch die deutschen Behörden; Kabelaufklärung und Überwachungsmassnahmen der Nachrichtendienste in den USA). Diese Fälle sind vorliegend nicht erörtert, da sie vom lokalen Recht abhängen. Sie führen naturgemäss zu einem höheren Risiko eines *Lawful Ac-*

cess und sollten speziell dann beachtet werden, wenn die Speicherung der Daten nicht in einem Rechenzentrum in der Schweiz, sondern im Ausland erfolgt.

[61] Nach Art. 18 Abs. 1 lit. a CCC kann eine Behörde im Rahmen einer Strafuntersuchung von einem Cloud-Dienstleister in ihrem Territorium (vgl. Voraussetzung Nr. 4) verlangen, dass dieser jene Daten der Kunden seiner Dienstleistung herausgibt, die sich in seinem Besitz oder unter seiner Kontrolle befinden. Hierzu führt der Erläuternde Bericht der CCC[7] in Ziff. 173 aus:

> *«Under paragraph 1(a), a Party shall ensure that its competent law enforcement authorities have the power to order a person in its territory to submit specified computer data stored in a computer system, or data storage medium that is in that person's possession or control. The term «possession or control» refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory (for example, subject to applicable privileges, a person who is served with a production order for information stored in his or her account by means of a remote online storage service, must produce such information). At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute «control» within the meaning of this provision. In some States, the concept denominated under law as «possession» covers physical and constructive possession with sufficient breadth to meet this «possession or control» requirement.*
>
> *Under paragraph 1(b), a Party shall also provide for the power to order a service provider offering services in its territory to «submit subscriber information in the service provider's possession or control». As in paragraph 1(a), the term «possession or control» refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company). The term «relating to such service» means that the power is to be available for the purpose of obtaining subscriber information relating to services offered in the ordering Party's territory.»*

[62] Daraus ergibt sich, dass kein «Besitz» (*possession*) vorliegt, wenn die Kundendaten sich nicht physisch im Rechenzentrum eines Providers mit Sitz im Land der anordnenden Behörde befinden. Sind somit die Kundendaten auf einem Server einer anderen Gesellschaft im Konzern in der Schweiz oder sonst in Europa gespeichert, können sie demnach nicht im Besitz eines Cloud-Dienstleisters in den USA sein. Das US-Zivilprozessrecht verwendet immer wieder auch den Begriff «custody»: Es meint (ebenfalls) den tatsächlichen physischen oder körperlichen Besitz eines Dokuments, jedoch ohne dass es der betreffenden Person rechtlich gehört, wie etwa im Falle einer Verwahrung im Auftrag eines Dritten oder wenn Mitarbeiter Dokumente in ihrer Eigenschaft als

7 Council of Europe, Explanatory Report to the Convention on Cybercrime, Budapest, 23. November 2001.

Angestellte des Unternehmens auf sich tragen.[8] Für vorliegende Zwecke ist die Unterscheidung in der Regel nicht relevant.

[63] Denkbar ist jedoch, dass Kundendaten unter der «Kontrolle» (*control*) des Providers stehen. Allerdings machen die Erläuterungen zu Art. 18 Abs. 1 lit. a CCC klar, dass ein Provider nur dann Kundendaten im Sinne der Bestimmungen kontrolliert, wenn er darüber «frei» verfügen kann. Dies impliziert nicht nur die technische Möglichkeit, dies zu tun, sondern auch die rechtliche Befugnis. Mit der technischen Möglichkeit kann wiederum nicht irgendein theoretisch denkbarer Zugriffsweg gemeint sein, sondern es muss sich nach der hier vertretenen Ansicht um eine Zugriffsmöglichkeit handeln, die dem Provider im üblichen Geschäftsgang zur Verfügung steht. Die Erläuterungen stellen denn auch klar, dass eine bloss technische Fernzugriffsmöglichkeit auf Daten nicht notwendigerweise genügt. Ob es tatsächlich auch auf eine rechtliche Befugnis ankommt, wird umstritten sein. Allerdings ist davon auszugehen, dass nur Kundendaten erfasst sein können, auf die der Provider auch sonst ohne Weiteres zugreifen könnte, wenn er will. Daraus ergibt es sich auch, dass der blosse Umstand, dass Daten bei einer seiner Tochtergesellschaften gespeichert sind, ihm noch keine Kontrolle darüber geben.

[64] Ebenso wenig wird von Kontrolle auszugehen sein, wenn der Provider sich in die Systeme seiner Tochtergesellschaft (oder seine eigenen) «hacken» oder über das Einbauen einer Hintertür oder ähnliche Methoden Zugang zu Kunden im Klartext verschaffen müsste, wenn ihm diese sonst nur verschlüsselt oder gar nicht zugänglich sind. In diesen Fällen kann nicht davon die Rede sein, dass er «frei» über die Kundendaten im Klartext verfügen kann. Diese Auslegung ergibt sich auch aus dem Sinn und Zweck und dem Text der Norm, die letztlich lediglich eine Pflicht zur Herausgabe vorsieht, und nicht eine Pflicht zu weiteren Aktivitäten wie etwa das Knacken einer Verschlüsselung, das Belauschen oder Hacken seines Kunden oder den Einbau einer Hintertür in die von ihm benutzte Software. Sind die Kundendaten verschlüsselt, sind es diese, die er in dieser Form herausgeben muss; das Knacken der Verschlüsselung ist dann Sache der Behörde und nicht die Pflicht des Providers, der den Schlüssel nicht kennt. Betreibt der Kunde einen abgeschotteten virtuellen Server, kann vom Provider verlangt werden, dass er ein Abbild (*image*) desselben der Behörde liefert, mit welchem diese allerdings auch kaum etwas anzufangen wissen wird. Seine Software so auszulegen, dass er stets an den Inhalt der Kundendaten im Klartext kommt, verlangt Art. 18 Abs. 1 lit. a CCC nicht; baut er somit nicht von sich aus eine Hintertür ein, kann dies im Rahmen dieser Bestimmung von ihm nicht verlangt werden.

[65] Die USA haben erklärt, dass die Möglichkeiten eines Zugriffs gemäss CLOUD Act sich in eben diesem Rahmen von Art. 18 Abs. 1 CCC bewegen.[9] Dies entspricht, soweit sich dies feststellen lässt, auch der geltenden Rechtsprechung, die sich in den USA vor allem zu Editionsbegehren im Rahmen von zivilrechtlichen Rechtsstreitigkeiten entwickelt hat.[10] Sie stellt mit Bezug auf den Begriff der Kontrolle entweder darauf ab, ob der Adressat der Herausgabeanordnung rechtlich über die verlangten Daten verfügen darf («legal right test»), oder es wird ein Multifaktoren-Test angewandt um festzustellen, ob «die Fähigkeit eines Unternehmens, im Rahmen des normalen Geschäftsbetriebs Dokumente zu verlangen und Zugang zu diesen zu haben, die Vermutung na-

8 Paul Matthews, Hodge M. Malek, Disclosure, London 2012, S. 164.

9 U.S. Department of Justice, The Purpose and Impact of the CLOUD Act, White Paper, April 2019, http://www.justice.gov/CLOUDAct, S. 15 f., kontrolliert am 3. Juli 2020.

10 Vgl. etwa Hogan Lovells, Demystifying the U.S. CLOUD Act, 16. Januar 2019, https://www.hoganlovells.com/en/news/cloud-act-analysis, kontrolliert am 3. Juli 2020.

helegt, dass sich diese Dokumente unter der Kontrolle der prozessführenden Gesellschaft befinden» («practical ability test»).[11] Auch nach der US-Rechtsprechung genügt die Tatsache der gesellschaftsrechtlichen Kontrolle einer anderen Gesellschaft nicht, dass die kontrollierende Gesellschaft auch Kontrolle über die von der Tochtergesellschaft verwalteten Kundendaten hat.

[66] Ob das US-Recht den Behörden weitergehende Möglichkeiten bietet, einen Provider zur Mitwirkung zur Erlangung von Kundendaten im Klartext zu zwingen, und wie wahrscheinlich ein solches Szenario ist, muss hier offenbleiben. Dies ist im konkreten Fall im Falle von Zweifeln ggf. durch ein entsprechendes Rechtsgutachten zu klären. Dasselbe gilt für andere relevante Staaten, d.h. namentlich jene Staaten, in denen sich eine Gesellschaft befindet, die vom Provider für die Erbringung seiner Leistung beigezogen ist oder gewisse rechtliche oder faktische Kontrollrechte gegenüber dem Provider hat.

[67] Aus dem Gesagten ergeben sich jedoch erstens diverse Ansatzpunkte für Gegenmassnahmen, um die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 5 zu reduzieren, und zweitens ist es möglich, je nach Sachverhalt von einer deutlich reduzierten Eintrittswahrscheinlichkeit der Voraussetzung Nr. 5 auszugehen, was in vielen Fällen bereits genügen wird. Es ist mit anderen Worten für eine vernünftige Risikoeinschätzung gar nicht nötig, Gewissheit über die Möglichkeit eines Zugriffs durch ausländische Behörden zu haben; es kann für die Gesamtbeurteilung bereits genügen, wenn anhand der Umstände beispielsweise die Einschätzung möglich ist, dass die Wahrscheinlichkeit unter 50 Prozent liegt. Im Rahmen von Voraussetzung Nr. 5 sind nur jene Gesellschaften in der Sphäre des Providers (inklusive dem Provider selbst) zu betrachten, welche die Voraussetzung Nr. 4 erfüllen (also z.B. eine Muttergesellschaft oder eine an der Vertragserfüllung mitwirkende Gesellschaft im Ausland).

[68] Um keine Vermengung der Wahrscheinlichkeiten zu erhalten, ist im Rahmen von Voraussetzung Nr. 5 nicht mehr zu prüfen, ob eine solche Gesellschaft technischen Zugang zu Kundendaten im Klartext erhalten kann; dies erfolgt im Rahmen von Voraussetzung Nr. 2 und 3. Im Rahmen von Voraussetzung Nr. 5 ist daher zu prüfen, wie hoch die Wahrscheinlichkeit ist, dass (i) die Behörde von der Gesellschaft verlangen kann, die im Rahmen von Voraussetzung Nr. 2 und 3 diskutierten technischen Massnahmen zu überwinden (z.B. ihre eigenen Systeme zu hacken oder belauschen) und ihr die gewünschten Kundendaten zu verschaffen, und (ii) inwiefern sich organisatorische Schutzmassnahmen (z.B. Verbot des Zugriffs) auf die Abwehr von Herausgabebefehlen auswirken, d.h. die Gesellschaft zwar technisch Zugang verschaffen könnte, sie ihn aber nach dem gewöhnlichen Lauf der Dinge nicht hat oder nach internen Regeln oder aufgrund vertraglicher Verpflichtung nicht verschaffen darf und daher die Voraussetzungen für eine Herausgabe nicht mehr erfüllt sind. Technische Massnahmen können hier allerdings von Relevanz sein, wenn sie wie etwa BYOK zum Ausdruck bringen, dass der Provider bzw. seine Mitarbeiter gerade keine Kontrolle über die Kundendaten haben sollen, auch wenn sie sich diese durch rechts- oder vertragswidrige Methoden verschaffen könnten.

---

11 Jonathan D. Jordan, Out of Control Federal Subpoenas: When Does a Nonparty Subsidiary Have Control of Documents Possesed by a Foreign Parent?, 68 Baylor L. Rev. 189, 200-01 (2016), zitiert in: Demystifying the U.S. Cloud Act (FN 9), S. 13; Tess Blair, Tara S. Lawler, Possession, Custody or Control: A Perennial Question gets more complicated, in: The Legal Intelligencer, 5. Februar 2018 (https://www.morganlewis.com/pubs/possession-custody-or-control-a-perennial-question-gets-more-complicated), m.w.H.; Justin Hemmings, Sreenidhi Srinivasan, Peter Swire, Defining the Scope of Possession, Custody, or Control for Privacy Issues and the Cloud Act, in: Journal of National Security Law and Policy (erscheint 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3469808), Links kontrolliert am 3. Juli 2020.

[69] Ebenfalls nicht im Rahmen von Voraussetzung Nr. 5 sondern Nr. 6 ist zu prüfen, ob die Gesellschaft allenfalls zusätzlich auf Basis von *Schweizer Recht* weitere Argumente zur Verfügung hat, sich im betreffenden ausländischen Staat nach dessen Recht gegen den Herausgabebefehl zu wehren (z.B. durch Berufung auf Schweizer Berufsgeheimnisse oder Art. 271 StGB).

[70] Befindet sich der Provider in der Schweiz und bietet er seine Dienstleistungen nicht im Ausland an, ist die Voraussetzung Nr. 4 wahrscheinlich nicht erfüllt (N 58) und die Frage nach Voraussetzung Nr. 5 stellt sich nicht. Wahrscheinlicher ist jedoch, dass sich lediglich das Rechenzentrum in der Schweiz befindet und von einer lokalen Gesellschaft betrieben wird, die Vertragspartei des Kunden jedoch im Ausland (d.h. Gegenmassnahme Nr. 13 nicht umgesetzt wird).

[71] Es gibt somit den Fall, dass sich (i) der Provider selbst im Ausland befindet (d.h. die Gesellschaft, die mit dem Berufsgeheimnisträger den Vertrag schliesst), (ii) eine von ihm zur Vertragsabwicklung beigezogene Gesellschaft sich im Ausland befindet (d.h. ein Subunternehmer) oder (iii) oder sonst eine Gesellschaft sich im Ausland befindet, die Kontrolle über den Provider ausüben könnte (d.h. eine Muttergesellschaft). Für die Wahrscheinlichkeitsberechnung ist zu beachten, dass die höchste Wahrscheinlichkeit eines Erfolgs zählt, sie sich aber pro Herausgabebefehl nicht addiert.

2. Der Provider befindet sich selbst im Ausland

[72] Es muss zunächst jeder Eindruck vermieden werden, dass der Provider freien Zugriff auf die Kundendaten im Klartext hat. Hierzu sollte er den eigenen technischen Zugriff im Sinne der Gegenmassnahmen Nr. 3–8 und 10 oder 11 wie oben dargelegt soweit wie möglich zugunsten des Kunden aufgeben. Kann er in der Folge nicht mehr auf Kundendaten im Klartext zugreifen, kann er nach der hier vertretenen Ansicht im Rahmen eines Herausgabebefehls nach Art. 18 Abs. 1 lit. a CCC höchstens zur Herausgabe verschlüsselter Daten ihrer Kunden gezwungen werden, aber weder zum Einbau einer Hintertür, Durchführen eines Lauschangriffs oder sonstiges «Knacken» ihrer eigenen Sicherheit. Daher ist bei entsprechenden technischen Zugriffsbeschränkungen die Wahrscheinlichkeit, dass Voraussetzung Nr. 5 gegeben ist, als sehr tief einzuschätzen. Wenn der Provider obendrein vertraglich zusichert, dass das von ihm bereitgestellte System über keine Hintertüren oder vergleichbare Programmierungen verfügt, mit welchen sich die technischen Massnahmen zur Schaffung einer sicheren Zone umgehen lassen, so wird dies noch bestärkt (**Gegenmassnahme Nr. 16**). Diese Zusicherung dient mithin dem Provider, der sich glaubhaft gegen einen Herausgabebefehl im Sinne von Art. 18 Abs. 1 lit. a CCC wehren muss; wird sie nicht gegeben, kann sie allerdings auch durch andere Zusicherungen kompensiert werden (N 80). Eine tatsächliche Überprüfung, ob die vom Provider bereitgestellte Cloud-Lösung keine Hintertüren oder dergleichen hat, wird in aller Regel nicht möglich sein.

[73] Selbst bei einer Beschränkung der technischen Zugriffsmöglichkeit verbleibt dem Provider aber typischerweise eine Zugriffsmöglichkeit auf Kundendaten im Rahmen eines Support-Falls. Auch hier wird der Provider einen Herausgabebefehl in aller Regel zurückweisen können, es sei denn, er betreffe just jene Daten, auf die der Provider im Rahmen des Support-Zugriffs zufälligerweise zugreifen muss, um die technische Störung zu beheben. Nach der hier vertretenen Ansicht kann eine Behörde nach Art 18 Abs. 1 CCC weder die Herbeiführung einer solchen Störung verlangen, noch das zweckwidrige Ausnutzen eines solchen Support-Zugriffs. Allerdings sollte der Berufsgeheimnisträger in seinem Vertrag festhalten, dass im Rahmen eines solchen Support-Zugriffs und auch sonst der Leistungserbringung allfällig zur Kenntnis genommenen Daten vom

Provider nicht anderweitig verwendet oder preisgegeben werden dürfen (**Gegenmassnahme Nr. 15**), also ein Support-Zugriff nur zu Zwecken des Supports erfolgen und genutzt werden darf nicht (auch) zu Zwecken des *Lawful Access*.

[74] Eine solche Bestimmung findet sich normalerweise in Vereinbarungen über die Auftragsdatenbearbeitung, die in Cloud-Dienstleistungsverträgen üblich sind. Gegenmassnahme Nr. 15 ist damit noch nicht erfüllt, da es im vorliegenden Fall wichtig ist, nicht nur Auftragsdatenbearbeitungen zu erfassen. Ein Zugriff zu Zwecken des Supports stellt nicht unbedingt eine solche dar, und ein Zugriff zum Zwecke eines *Lawful Access* gilt erst recht nicht als Auftragsdatenbearbeitung. Solche Verwendungen müssen dem Provider daher integral untersagt werden, damit das Risiko von Voraussetzung Nr. 5 reduziert werden kann. Das ist speziell dann wichtig, wenn nebst dem Support-Fall auch sonst ein Zugriff auf Kundendaten im Klartext technisch möglich ist, d.h. der Provider jederzeit auf die Kundendaten im Klartext zugreifen könnte, wenn er will (d.h. Gegenmassnahme Nr. 4, 5 oder 6 *nicht* umgesetzt ist, also keine sichere Zone besteht, die mit technischen Vorkehrungen abgesichert ist). Die Regelung, dass ein Provider auf Kundendaten im Klartext nur mit Einwilligung des Kunden zugreifen darf, ist im Rahmen von Gegenmassnahme Nr. 10 abzudecken, die sowohl eine organisatorische Komponente aufweist (z.B. vertragliche Zusicherung seitens des Providers, interne Weisungen und Prozesse) wie auch technische Komponenten (z.B. Protokollierung).

[75] Werden diese beiden Vorkehrungen – d.h. Gegenmassnahme Nr. 10 und 15 – getroffen und nicht durch Herausgabevorbehalte eingeschränkt (dazu N 77 ff.), besteht nach der hier vertretenen Ansicht eine mittlere bis hohe Wahrscheinlichkeit, dass die Kundendaten nicht als «unter der Kontrolle» des Providers im Sinne von Art. 18 Abs. 1 CCC gelten, obwohl er technisch darauf zugreifen kann. Obwohl keine sichere Zone besteht, kann der Provider in solchen Fällen trotzdem nicht «frei» auf die Kundendaten im Klartext zugreifen. Nach der hier vertretenen Ansicht sind im Rahmen von Art. 18 Abs. 1 CCC auch organisatorische Hürden zu berücksichtigen bei der Beurteilung, ob ein Provider «Kontrolle» über die Kundendaten hat. Unter Umständen genügt es nicht, dass der Provider diese Kundendaten nicht für die Zwecke des *Lawful Access* benutzen «darf». Wenn jedoch zusätzliche organisatorische Vorkehrungen getroffen sind, damit die Mitarbeiter des Providers nicht auf die Kundendaten zugreifen können und dürfen, so sind die Daten für den Provider nicht mehr frei verfügbar. Solche organisatorischen Massnahmen sollten eine Kombination aus Weisungen, Vertragspflichten, Prozesse, Zuständigkeiten und Kontrollen sein, damit gezeigt werden kann, dass sie tatsächlich verhindern, dass Mitarbeiter des Providers auf Kundendaten im Klartext zugreifen, wenn der Kunde dies nicht erlaubt hat. Die Messlatte ist dabei nicht der kriminelle oder unter Zwang stehende Mitarbeiter, sondern der normale Geschäftsbetrieb, wo mangels anderer Hinweise von vertragsgemässem Verhalten ausgegangen werden kann; daran knüpft wohl auch Art. 18 Abs. 1 CCC an. Im Rahmen von Gegenmassnahme Nr. 10 sind die Massnahmen ggf. im Vertrag mit dem Provider entsprechend zu spezifizieren und deren Überwachung vorzusehen.

[76] Vom Provider sollte weiter verlangt werden, dass er sich gegen jeden Herausgabebefehl mit allen rechtlich zulässigen Mitteln wehrt und den Berufsgeheimnisträger, soweit zulässig, darüber orientiert, damit er seinerseits entsprechende Vorkehrungen oder Instruktionen vornehmen kann (**Gegenmassnahme Nr. 17**). Namentlich sollte der Provider kein Ermessen haben, einem Herausgabebefehl Folge zu leisten, weil er ihn für zulässig hält oder den Aufwand der gerichtlichen Überprüfung scheut. Das dürfte in der Praxis kein Problem darstellen; die Regelung, wonach Daten nur herausgegeben werden müssen, wenn der Provider dazu verpflichtet ist, wird dies in

der Regel bewirken, auch wenn es im Sinne einer zusätzlichen Absicherung sinnvoll sein kann, vom Provider eine rechtliche Abwehr solcher Herausgabebefehle zu verlangen.

[77] In diesem Zusammenhang stellt sich als nächstes die Frage, welche Bedeutung einer Vertragsklausel zukommt, mit welcher sich der Provider die Herausgabe von Kundendaten gegenüber Behörden vorbehält, sofern diese gesetzlich vorgeschrieben sei. Bezieht sich dieser Vorbehalt der gesetzlichen Pflicht ausschliesslich auf Schweizer Recht, so ist er unproblematisch. Bezieht er sich auch auf ausländisches Recht, so schafft er zum einen das Risiko, dass eine ausländische Behörde den Standpunkt vertritt, dass der Provider sich gegenüber dem Kunden ausdrücklich die Befugnis zur Offenlegung seiner Kundendaten an eine ausländische Behörde im Rahmen deren Recht vorbehalten hat. Zum anderen birgt die Klausel das Risiko, dass dem Kunden der Vorwurf gemacht werden kann, er wisse nicht nur um die Möglichkeit einer Offenbarung seiner Kundendaten gegenüber einer ausländischen Behörde, sondern nehme sie auch billigend in Kauf, handle mithin eventual-vorsätzlich in Bezug auf eine Berufsgeheimnisverletzung. Letzteres ist freilich nicht zwingend der Fall: Das Wissen um die Möglichkeit des Erfolgseintritts führt nicht zwangsläufig zu dessen Inkaufnahme. Entscheidend ist, für wie wahrscheinlich der Täter – hier: der Mitarbeiter des Berufsgeheimnisträgers – den Erfolgseintritt hält. Vertraut er darauf, dass der Erfolg nicht eintritt (z.B., weil zahlreiche andere Gegenmassnahmen getroffen wurden, die er für wirksam hält), liegt kein Vorsatz vor. Hielt er den Erfolgseintritt trotzdem für nach dem gewöhnlichen Lauf der Dinge und Erfahrungen des Lebens möglich und wäre er mit zumutbaren Massnahmen höchstwahrscheinlich vermeidbar gewesen, handelte er immerhin fahrlässig.

[78] Ein Herausgabevorbehalt nach ausländischem Recht im Vertrag schwächt nach der hier vertretenen Ansicht die Möglichkeit der Abwehr entsprechender Herausgabebefehle wesentlich, weshalb er gestrichen bzw. auf Schweizer Recht eingeschränkt werden sollte (**Gegenmassnahme Nr. 18**). Dies gilt übrigens auch mit Hinblick auf Art. 32 lit. b. CCC, welcher ausländischen Behörden den Zugriff auf Daten auf einem Server auch in der Schweiz erlaubt, wenn sie die Einwilligung des Providers haben und dieser rechtmässig über diese Daten verfügen kann. Es ist daher seitens des Berufsgeheimnisträgers sicherzustellen, dass der Provider weder rechtmässig über die Kundendaten verfügen kann (bzw. nur für sehr beschränkte Zwecke des Berufsgeheimnisträgers in gewissen Support-Fällen), noch diese einem Dritten nach eigenem Ermessen bekanntgeben bzw. zugänglich machen darf (Gegenmassnahmen Nr. 15 und 17). Die Gegenmassnahme Nr. 18 in der Praxis zu erhalten dürfte bei einem Provider, der sich im Ausland befindet, freilich oftmals nicht realistisch sein, da ein Provider kaum je einen Vertrag abschliessen wird, der ihn pauschal zur Missachtung seines Heimatrechts verpflichtet; eine solche Klausel hat immerhin dann eine Chance, wenn der Provider selbst davon ausgeht, dass er unter seinem Heimatrecht vernünftigerweise nicht zur Herausgabe verpflichtet werden kann.

[79] Ferner kann der Vertrag zwischen dem Provider und dem Berufsgeheimnisträger Schweizer Recht als Vertragsstatut unterstellt werden (**Gegenmassnahme Nr. 19**). Untersteht der Vertrag ausländischem Vertragsrecht, sieht dieses möglicherweise automatisch einen Vorbehalt zugunsten von Herausgabeanordnungen des betreffenden ausländischen Rechts vor. Untersteht der Providervertrag also beispielsweise irischem Recht, so ist damit zu rechnen, dass ein vertragliches Verbot der Herausgabe an Dritte nach irischem Vertragsrecht nicht gilt, wenn der Provider nach irischem Recht zur Herausgabe gesetzlich verpflichtet ist. Er wird diesfalls keine Vertragsverletzung begehen. Untersteht der Vertrag jedoch Schweizer Recht, dürfte eine Vertragsverletzung vorliegen. Das mag die Herausgabe durch einen Mitarbeiter in Irland zwar nicht verhindern, wird den Provider aber entsprechenden Vertragsfolgen aussetzen. Das Risiko solcher Vertragsfolgen

wird für ihn daher einen entsprechenden Anreiz sein, auch technische Massnahmen vorzukehren, damit er nicht zur Herausgabe der Kundendaten gezwungen werden kann.

[80] Widerstand seitens des Providers ist daher wie erwähnt vor allem mit Bezug auf Gegenmassnahme Nr. 18 und 19 zu rechnen. Am wirksamsten im Hinblick auf Voraussetzung Nr. 5 ist nach der hier vertretenen Ansicht die Gegenmassnahme Nr. 18 (Herausgabeverbot unter Vorbehalt einzig des Schweizer Rechts), denn wenn sie gewährt wird, verletzt der Provider seinen Vertrag auch dann, wenn die Herausgabe über eine Hintertür oder dergleichen erfolgt (sofern deren Einsatz natürlich nicht anderweitig vertraglich vorbehalten ist); insofern ist Gegenmassnahme Nr. 16 (Zusicherung, dass keine Hintertüren bestehen) nicht essentiell. Verweigert sich der Provider der Gegenmassnahme Nr. 18, stellt sich die Frage, ob er trotz allem mit einer Herausgabepflicht rechnet, was wiederum Auswirkungen auf die Vorhersehbarkeit des (erfolgreichen) *Lawful Access* für den Berufsgeheimnisträger hat, oder ob er Gegenmassnahme Nr. 18 einfach aus Prinzip verweigert und in einer besseren Verhandlungsposition ist. In diesem Falle sollte der Grund für den Widerstand abgeklärt und dokumentiert werden, um die Wahrscheinlichkeit einer Herausgabepflicht einzuschätzen. Wird Gegenmassnahme Nr. 18 nicht mit Gegenmassnahme Nr. 19 verknüpft, ist darauf zu achten, dass das Vertragsstatut nicht dem Recht des Landes entspricht, in welchem sich der Provider befindet, oder aber von diesem Staat ein nur geringes Risiko eines Herausgabebefehls ausgeht.

[81] Ergebnis: Soweit die Gegenmassnahmen Nr. 3, Nr. 4, 5, 6, 7 oder 8, Nr. 10 oder 11, sowie Nr. 15, 17, 18 und 19 umgesetzt sind, ist die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 5 in der hier diskutierten Konstellation (Provider im Ausland) nach der hier vertretenen Ansicht sehr tief. Kann der technische Zugriff auf die Kundendaten nicht wirklich beschränkt werden, werden aber organisatorische Massnahmen getroffen, die dafür sorgen, dass die Mitarbeiter im normalen Geschäftsgang nur mit Einwilligung des Kunden auf Kundendaten im Klartext zugreifen können und dürfen und ist dem Provider die Herausgabe an die Behörde nach ausländischem Recht untersagt (d.h. Massnahmen Nr. 4, 5, 6, 7 oder 8 kommen nicht zum Tragen, wohl aber Nr. 10 oder 11 und Nr. 15, 17, 18 und 19), so ist nach der hier vertretenen Ansicht die Wahrscheinlichkeit immer noch tief, dass Voraussetzung Nr. 5 gegeben ist. Verweigert der Provider die Gegenmassnahmen Nr. 18 und 19, sind aber organisatorische und technische Vorkehrungen getroffen, welche den Mitarbeitern des Providers den Zugang zu den Kundendaten im täglichen Betrieb entziehen, so dürfte sich die Eintrittswahrscheinlichkeit damit wohl unter 50 Prozent drücken lassen. Dies gilt jedenfalls soweit Herausgabebefehle gestützt auf Art. 18 Abs. 1 CCC erfolgen, wie etwa im Falle des *Stored Communications Act* bzw. *CLOUD Act*. Kann sich eine Behörde auf eine andere Rechtsgrundlage abstützen, ist die Eintrittswahrscheinlichkeit unter Umständen höher.

3. Ein Subunternehmer des Providers befindet sich im Ausland

[82] Greift der Provider auf einen Subunternehmer im Ausland zurück, so gilt das vorstehend zum Provider Gesagte analog für den Subunternehmer. Dies bedeutet, der Provider muss sicherstellen, dass er entweder (i) dem Subunternehmer keinen Zugriff auf die Kundendaten im Klartext gibt und dies dem Kunden auch vertraglich zusichert (**Gegenmassnahme Nr. 20**) oder (ii) den Zugriff des Subunternehmers wie für sich selbst einschränkt (z.B. im Support-Fall, Gegenmassnahme Nr. 10 oder 11) und sich verpflichtet, seine eigenen diesbezüglichen Pflichten (Ge-

genmassnahme Nr. 15, 17 und 18) dem Provider zu überbinden und deren Einhaltung überwacht (**Gegenmassnahme Nr. 21**).

[83] Nebst den technischen Massnahmen zur Verhinderung eines Zugriffs des Subunternehmers auf Kundendaten im Klartext können seitens des Providers auch organisatorische Massnahmen getroffen werden, so namentlich der Erlass entsprechender Weisungen und Durchführung entsprechender Kontrollen und einem vertraglich gegenüber dem Subunternehmer abgesicherten Verbots, auf Kundendaten im Klartext ohne Instruktion des Providers zuzugreifen (**Gegenmassnahme Nr. 22**): Sollte der Subunternehmer Adressat eines Herausgabebefehls sein, sollte er gegenüber der Behörde glaubhaft darlegen können, dass er keine Befugnisse hat, auf die Kundendaten zuzugreifen und einen solchen Zugriff auch nicht vom Provider (oder einem anderen Subunternehmer) verlangen kann und ihn daher selbst bei technisch möglichem Zugriff nicht erfüllen muss.

[84] Gegenmassnahmen Nr. 21 und 22 entsprechen im Grossen und Ganzen den Vorgaben von Art. 28 DSGVO für den Einsatz von Auftragsdatenbearbeitern, mit Ausnahme der Bestimmungen, welche eine Herausgabe auf behördliche Anordnung nur nach Schweizer Recht vorsehen.

[85] Ergebnis: Soweit die Gegenmassnahmen Nr. 20 oder 21 sowie Nr. 22 umgesetzt sind, ist die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 5 in der hier diskutierten Konstellation (Subunternehmen im Ausland) nach der hier vertretenen Ansicht voraussichtlich tief, jedenfalls soweit Herausgabebefehle gestützt auf Art. 18 Abs. 1 CCC erfolgen (vgl. N 81). Kann sich eine Behörde auf eine andere Rechtsgrundlage abstützen, ist die Eintrittswahrscheinlichkeit unter Umständen höher.

4. Die Muttergesellschaft des Providers befindet im Ausland

[86] Insbesondere im Zusammenhang mit dem *CLOUD Act* ist immer wieder das Risiko diskutiert worden, dass die Schweizer bzw. europäische Tochter eines US-Anbieters aufgrund eben dieser Mutter-Tochter-Beziehung verpflichtet werden könnte, Kundendaten den US-Behörden offenlegen zu müssen. Die Wahrscheinlichkeit einer solchen Herausgabepflicht lediglich aufgrund einer gesellschaftsrechtlichen Verbindung erscheint wie dargelegt als tief, da weitere Umstände hinzutreten müssen (N 63 f.). Sie würde sich technisch zudem gegen die Mutter, nicht die Tochter richten.

[87] Da es im Rahmen von Herausgabebefehlen auf der Basis von Art. 18 Abs. 1 CCC wesentlich darauf ankommt, welche tatsächlichen Kontrollmöglichkeiten eine Muttergesellschaft des Providers diesem gegenüber hat, ist Vorbeugung möglich. Neben den technischen Vorkehrungen zur Beschränkung des Zugriffs kann der Provider – analog dem Fall des Subunternehmers – eine für alle Mitarbeiter verbindliche Weisung erlassen, wonach weder der Muttergesellschaft noch sonst einer Konzerngesellschaft Zugang zu Kundendaten im Klartext zu gewähren ist, ausser der Kunde hätte dies im Einzelfall erlaubt (**Gegenmassnahme Nr. 23**). Eine solche Weisung kann auch gegenüber den Organen des Providers erfolgen bzw. mit ihnen vertraglich vereinbart werden, mithin auch seitens der Muttergesellschaft, da diese selbst ein Interesse an allen Vorkehrungen hat, die sie vor einem Herausgabebefehl nach dem Recht ihres Landes schützt.

[88] Ferner ist darauf zu achten, dass der Vertrag mit dem Provider diesem untersagt, der Muttergesellschaft Kundendaten zugänglich zu machen, was mit einer herkömmlichen Geheimhaltungs- bzw. Datenschutzklausel zu bewerkstelligen ist (**Gegenmassnahme Nr. 24**); soll der Muttergesell-

schaft Zugang zu den Kundendaten gewährt werden, dann nur zu den Bedingungen des Beizugs eines Subunternehmers (N 82 ff.).

[89] Zu beachten ist ferner, dass Schweizer Recht ebenfalls bewirken kann, dass die Organe bzw. Mitarbeiter des Providers – soweit sie Schweizer Recht unterstehen – Kundendaten im Klartext selbst im Falle einer Anweisung der Muttergesellschaft dieser nicht herausgeben dürfen (N 91 ff.). Dies ist jedoch unter Voraussetzung Nr.6 zu prüfen.

[90] Ergebnis: Soweit die Gegenmassnahmen Nr. 23 und 24 umgesetzt sind, ist die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 5 in der hier diskutierten Konstellation (Muttergesellschaft im Ausland) nach der hier vertretenen Ansicht voraussichtlich tief, jedenfalls soweit Herausgabebefehle gestützt auf Art. 18 Abs. 1 CCC erfolgen (vgl. N 81). Kann sich eine Behörde auf eine andere Rechtsgrundlage abstützen, ist die Eintrittswahrscheinlichkeit unter Umständen höher.

g. Voraussetzung Nr. 6: Die Mitarbeiter des Providers oder eines seiner Subunternehmer können in der Schweiz de facto nicht strafrechtlich belangt werden, wenn sie die Kundendaten der ausländischen Behörde herausgeben

[91] Als letzte Voraussetzung ist im Hinblick auf die Vorhersehbarkeit eines *Lawful Access* durch eine ausländische Behörde zu berücksichtigen, ob der Provider bzw. die handelnden Mitarbeiter nach Schweizer Recht befugt sind, die Kundendaten herauszugeben bzw. eine Herausgabe zulassen dürfen.

[92] Zum einen kann die Frage der Rechtmässigkeit der Herausgabe nach Schweizer Recht auch im Rahmen des ausländischen Rechts, unter welchem ein Herausgabebefehl erfolgt, von Relevanz sein. Führt ein Herausgabebefehl unter der Rechtsordnung des einen Staates dazu, dass der Rechtsunterworfene die Rechtsordnung eines anderen Staates verletzen muss, so besagt das Prinzip der *International Comity*, das die gegenläufigen Interessen der beiden Staaten an der Durchsetzung ihres Rechts gegeneinander abgewogen werden müssen. Dieses Prinzip ist in vielen Rechtsstaaten anerkannt, so beispielsweise auch in den USA. Es kann dazu führen, dass ein Gericht einen Herausgabebefehl, der gegen Schweizer Recht verstösst, aufhebt. Wie weit dieses Prinzip in den einzelnen relevanten Staaten geht, sei hier nicht weiter erörtert. Immerhin kann es die Eintrittswahrscheinlichkeit eines *Lawful Access* durch eine ausländische Behörde deutlich senken. Die Praxiserfahrung des Autors dieses Beitrags zeigt jedenfalls klar, dass sowohl Aufsichts- wie Strafbehörden als auch Zivilgerichte im Ausland schweizerisches Recht – entgegen allen Unkenrufen – durchaus beachten, wenn gezeigt werden kann, dass die Befolgung eines Herausgabebefehls tatsächlich gewichtige Konsequenzen für die Rechtsunterworfenen haben kann; die Strafbarkeit nach Art. 271 StGB spielt hier eine zentrale Rolle, ebenso Geheimhaltungspflichten (dazu sogleich). Aus diesem Grund erscheint es auch wenig sinnvoll, dass die Schweiz sich unter dem CLOUD Act um ein *Executive Agreement* bemüht, jedenfalls wenn es den Rechtsunterworfenen diese in der Praxis sehr effektive Abwehrmöglichkeit beraubt. Sie wird im Rahmen von Voraussetzung Nr. 6 beurteilt.

[93] Zum anderen ist die Frage der Rechtmässigkeit einer Herausgabe nach Schweizer Recht relevant für die Anwendung des Vertrauensprinzips, wonach im Rahmen eines arbeitsteiligen Zusammenwirkens jeder davon ausgehen darf, dass sich der andere an das Schweizer Recht hält,

soweit keine Aufsichtspflichten entgegenstehen und keine Hinweise auf ein pflichtwidriges Verhalten vorliegen.[12]

[94] Auf den konkreten Fall angewandt stellt sich zunächst die Frage, ob die Befolgung eines Herausgabebefehls einer ausländischen Behörde Schweizer Recht verletzen würde. In Frage kommen einerseits Geheimhaltungspflichten und andererseits der Schutz der Schweizer Souveränität:

a) **Geheimhaltungspflichten:** Überträgt der Berufsgeheimnisträger dem Provider die Bearbeitung von Kundendaten, untersteht er (mit seinen Mitarbeitern und Subunternehmern) als Beauftragter oder sonst als Hilfsperson in der Regel dem Berufsgeheimnis. Es ist davon auszugehen, dass dies ungeachtet davon gilt, ob zwischen dem Berufsgeheimnisträger und dem Provider eine entsprechend formulierte Geheimhaltungsabrede besteht. Sieht der Vertrag mit dem Provider vor, dass dieser einem Herausgabebefehl einer ausländischen Behörde Folge leisten darf (d.h. wird Gegenmassnahme Nr. 18 *nicht* umgesetzt), so muss der Provider trotzdem mit einem Verstoss gegen das Berufsgeheimnis rechnen. Fraglich ist allerdings, ob sich der Berufsgeheimnisträger in diesem Fall noch auf das Vertrauensprinzip berufen kann, da der Provider ihm gegenüber vertraglich ausbedungen hat, sich gerade *nicht* an das Schweizer Recht zu halten. Wurde Gegenmassnahme Nr. 18 hingegen umgesetzt, würde eine Herausgabe von Kundendaten an eine ausländische Behörde nicht nur eine Vertragsverletzung darstellen, sondern in der Regel auch zu einer Verletzung der jeweiligen Berufsgeheimnisnorm (als auch Art. 162 StGB und Art. 273 StGB, soweit diesen neben dem Berufsgeheimnis als *lex specialis* eine eigenständige Bedeutung zukommt[13]) führen, da es sich bei den Kundendaten nicht nur um Geheimnisse der Kunden sondern auch des Berufsgeheimnisträgers handelt. Letztere sind vom Provider ebenso geheim zu halten.[14]
b) **Souveränitätsschutz:** Speichert der Provider die Kundendaten des Berufsgeheimnisträgers auf einem Server auf Schweizer Boden, so ist dieser im Rahmen von Art. 271 StGB gegen hoheitliche Zugriffe aus dem Ausland durch die Souveränität der Schweiz geschützt. Ordnet eine ausländische Behörde dem Provider die Herausgabe dieser Daten des Berufsgeheimnisträgers an, und gibt dieser dem Befehl nach, so verletzt er wie auch die ausländische Behörde Art. 271 StGB, sofern er dies ohne Bewilligung tut. Art. 18 Abs. 1 CCC stellt hierfür keine Bewilligung dar.[15] Daher muss ein Mitarbeiter des Providers, der einem Herausgabebefehl mit Bezug auf Kundendaten des Berufsgeheimnisträgers nachkommt, mit einer Strafbarkeit nach Art. 271 StGB rechnen. Voraussetzung ist natürlich in dieser Konstellation, dass der Provider die Kundendaten in der Schweiz speichert und hier bearbeitet.

[95] Die Frage, inwieweit das Berufsgeheimnis und die weiteren allenfalls zur Anwendung gelangenden Geheimhaltungspflichten auch im Ausland durchgesetzt werden können, sei an dieser Stelle nicht vertieft; im Falle von Art. 273 StGB gilt immerhin das Weltrechtsprinzip,[16] welches vorliegend Strafbarkeit auch für im Ausland begangene Geheimnisverletzungen vorsieht. Grundsätzlich untersteht jedenfalls derjenige, der einem Berufsgeheimnisträger eine Rechenzentrums-

12 Vgl. BGE 120 IV 300, Erw. 3.d.

13 Vgl. BGE 145 IV 114 E. 4.2.

14 Vgl. BGE 145 IV 114 E. 4.2.

15 Vgl. BGE 141 IV 108, Erw. 6.4.

16 Art. 4 StGB.

leistung erbringt, mit seinen Mitarbeitern als Hilfsperson bzw. Beauftragter dem Berufsgeheimnis. Im Hinblick auf das Vertrauensprinzip stellt sich jedoch die Frage, ob der Berufsgeheimnisträger sich noch auf die Befolgung der Geheimhaltungspflicht verlassen darf, wenn die Mitarbeiter, die dem Herausgabebefehl Folge leisten, sich nicht in der Schweiz befinden und folglich auch nicht ohne Weiteres strafrechtlich verfolgt werden können. Das ist nach der hier vertretenen Ansicht jedenfalls dann zu verneinen, wenn die Mitarbeiter sich persönlich in einer Pflichtenkollision befinden: Unterstehen sie nebst dem Schweizer Recht auch dem ausländischen Recht und verpflichtet sie letzteres trotzdem zur Herausgabe der Daten, so wird der Berufsgeheimnisträger nicht mehr darauf vertrauen können, dass sie sich stattdessen an das Schweizer Recht halten, weil dieses ihnen weniger nah ist.

[96] Dieselbe Problematik stellt sich im Rahmen von Art. 271 StGB. Auch hier gilt das Weltrechtsprinzip, d.h. jeder Mitarbeiter des Providers und der beigezogenen Gesellschaften, die an der Erfüllung eines Herausgabebefehls einer ausländischen Behörde für in der Schweiz belegene Daten des Berufsgeheimnisträgers mitwirkt, muss grundsätzlich mit persönlicher Strafbarkeit rechnen, d.h. die Befolgung der Herausgabe erfolgt nach Schweizer Recht pflichtwidrig. Durchgesetzt werden kann allerdings auch diese Bestimmung nur gegenüber Personen, die sich in der Schweiz aufhalten.

[97] Für den Berufsgeheimnisträger bedeutet dies, dass er dafür sorgen muss, dass (i) die Kundendaten in der Schweiz gespeichert und auch sonst hier bearbeitet werden (Support-Zugriffe aus dem Ausland vorbehalten) und (ii) für die Datenspeicherung- und -bearbeitungen verantwortliche Mitarbeiter oder Organe des Providers oder der Subunternehmer in der Schweiz vertreten sind. Hierzu sind zwei Varianten denkbar:

a) **Der Provider hat seinen Sitz in der Schweiz:** Gemeint ist jene Gesellschaft, mit welcher der Berufsgeheimnisträger seinen Vertrag über die Cloud-Dienstleistungen hat. Sie kontrolliert die weiteren, an der Leistungserbringung beteiligten Gesellschaften durch entsprechende Verträge. Der Berufsgeheimnisträger hat mit dem Provider zu vereinbaren, dass mit Ausnahme des definierten Zugriffs in Support-Fällen mit Einzelfalleinwilligung des Kunden (vgl. Gegenmassnahme Nr. 10 und 11), die Speicherung und Bearbeitung der Kundendaten im Klartext ausschliesslich in der Schweiz stattfinden darf, und diese Pflicht mindestens auch der Rechenzentrumsbetreiberin in der Schweiz als Subunternehmerin (und allen weiteren Subunternehmern mit Zugang zu Kundendaten im Klartext) überbunden sein muss (**Gegenmassnahme Nr. 25**). Damit werden der Provider und seine etwaigen Subunternehmer zum vertraglichen Garanten und haften als solcher auch für Unterlassungen. Eine gesetzliche Garantenpflicht lässt sich vermutlich aus der jeweiligen Berufsgeheimnisnorm ableiten (da der Provider typischerweise als Hilfsperson bzw. Beauftragter des Berufsgeheimnisträgers gelten wird). Sollte er zudem durch den Einsatz von Software mit Hintertüren oder eine mangelnde Umsetzung von Massnahmen zum Schutz der Kundendaten eine Gefahr für diese schaffen mit Bezug auf ausländische Behördenzugriffe, kommt auch eine Garantenstellung aus Ingerenz in Frage. Ob es zur Strafbarkeit überhaupt eine Garantenstellung braucht, sei an dieser Stelle offengelassen; denkbar ist auch eine Strafbarkeit im Rahmen einer Teilnahmehandlung durch Bereitstellen einer Infrastruktur, welche ausländischen Behörden einen Zugang zu Kundendaten in der Schweiz ermöglicht. Kommt es vor diesem Hintergrund in der Sphäre des Providers zum Verrat bzw. einer Souveränitätsverletzung, ist jedenfalls davon auszugehen, dass die verantwortlichen Personen des Providers

sich strafbar verhalten und dafür tatsächlich auch verfolgt werden können. Greift hierbei das Vertrauensprinzip, so darf sich der Berufsgeheimnisträger folglich darauf verlassen, dass die Mitarbeiter und Organe des Providers in dessen Sphäre alles tun werden, was nötig ist, um sich pflichtgemäss zu verhalten und eine Herausgabe von Kundendaten zu verhindern – jedenfalls soweit der Berufsgeheimnisträger seinen regulatorischen und datenschutzrechtlichen Aufsichtspflichten nachkommt und ihm keine Hinweise auf ein pflichtwidriges Verhalten vorliegen. Durch den Beizug eines Providers mit Sitz in der Schweiz kann diesem mit anderen Worten durch entsprechende vertragliche Vereinbarungen und einer für Outsourcings üblichen Aufsicht die strafrechtliche Verantwortung, in seinem Bereich einen *Lawful Access* durch eine ausländische Behörde zu verhindern, weitgehend übertragen werden.

b) **Nur die Betreiberin des Rechenzentrums hat ihren Sitz in der Schweiz:** Gemeint ist jene Gesellschaft, die als Subunternehmerin des (im Ausland befindlichen) Providers den technischen Betrieb des Rechenzentrums des Providers in der Schweiz sicherstellt und damit für die Datenspeicherung und -bearbeitung der Kundendaten technisch verantwortlich ist, sofern die Kundendaten auf ihrem Rechenzentrum sind und bleiben. Hier gilt für die Mitarbeiter und Organe der Betreibergesellschaft grundsätzlich dasselbe wie für den Provider in der Schweiz, jedoch erscheint die Geltung des Vertrauensprinzips etwas weniger klar, da der Berufsgeheimnisträger mit der Betreibergesellschaft keine direkte Vertragsbeziehung unterhält und ihr somit auch keine vertragliche Garantenstellung zukommt. Sie ist lediglich Subunternehmerin des Providers. Werden ihr jedoch in Erfüllung von Gegenmassnahme Nr. 25 die Pflichten des Providers zur Datenspeicherung und -bearbeitung überbunden, ist auch sie vertraglich und damit auch strafrechtlich zum Schutz der Daten verpflichtet.

[98] Im Falle des CLOUD Act wird in der Schweiz immer wieder der Abschluss eines sog. *Executive Agreements* gefordert, wie es der CLOUD Act ebenfalls vorsieht. Die Befürworter glauben, dadurch würde Rechtssicherheit geschaffen und der Datenschutz besser gewährleistet werden.[17] Im vorliegenden Kontext würde ein Executive Agreement, wie es realistischerweise möglich ist, jedoch ein risikoerhöhender Faktor sein. Executive Agreements sind vom CLOUD Act vorgesehen, um den US-Behörden den Zugriff auf Provider bzw. Daten im Ausland unter Umgehung der Rechts- und Amtshilfe zu vereinfachen, nicht sie durch zusätzliche Hürden zu erschweren. Es kann für einen ausländischen Staat von Interesse sein, weil er damit Gegenrecht erhält. Vor diesem Hintergrund hat Grossbritannien am 3. Oktober 2019 als erster Staat ein Executive Agreement mit den USA abgeschlossen.[18] Entgegen landläufiger Erwartung schränkte die Vereinbarung die Geltung des CLOUD Act jedoch nicht ein (vgl. Art. 6 Abs. 3 des US-UK Executive Agreement[19]), sondern erlaubt den USA Herausgabebefehle zusätzlich direkt auch an Provider in Grossbritannien zu richten (und umgekehrt). Nur dann greifen auch die Inländer-Schutzmechanismen. Es ist unrealistisch anzunehmen, dass die USA der Schweiz weitergehende Schutzmechanismen oder gar eine Einschränkung der Zugriffsrechte im Rahmen des CLOUD Acts anbieten wird, da ihr dies keinen Vorteil bringt. Ein Executive Agreement nach dem Vorbild

17 Vgl. etwa die Forderung der Schweizerischen Bankiervereinigung vom 1. Oktober 2019 (https://bit.ly/2VoeBZE), mit ihrem Positionspapier (https://bit.ly/2CMFwYK), kontrolliert am 3. Juli 2020.

18 Abrufbar z.B. unter https://bit.ly/3f4kYsT, kontrolliert am 3. Juli 2020.

19 https://europeanlawblog.eu/2019/10/17/21-thoughts-and-questions-about-the-uk-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/ (https://bit.ly/2BOuWQc), kontrolliert am 3. Juli 2020.

jenes von Grossbritannien würde im Gegenteil bedeuten, dass US-Behörden Schweizer Cloud-Providern direkte Herausgabebefehle senden könnten, das Berufsgeheimnis teilweise aufgegeben werden müsste und Art. 271 StGB als Schutzmechanismus wegfällt.

[99] Lässt sich Gegenmassnahme Nr. 25 nicht umsetzen, sollte im Rahmen von Voraussetzung Nr. 6 als Gegenmassnahme mindestens vereinbart werden, dass die Daten des Kunden ausschliesslich in der Schweiz *gespeichert* («data at rest»), auch wenn zwecks Support oder anderer technischer Vorgänge (wie z.B. Malware-Scans) ein Fernzugriff aus dem Ausland erfolgen kann (**Gegenmassnahme Nr. 26**). Jeder Zugriff auf Daten setzt in diesem Falle grundsätzlich immer noch voraus, dass die Daten zuvor von den Systemen des Providers in der Schweiz «geholt» bzw. vom Rechenzentrum in der Schweiz bereitgestellt werden müssen, womit der Geheimnis- wie auch der Souveränitätsschutz nach wie vor tangiert ist und somit greift.

[100] Ergebnis: Ist Gegenmassnahme Nr. 25 oder mindestens Nr. 26 umgesetzt, so trägt der Provider und – soweit anwendbar – seine Rechenzentrumsbetreiberin (falls eine separate Gesellschaft) schon aufgrund des Schweizer Rechts (Geheimhaltungspflichten, Souveränitätsschutz) die Verantwortung, einen *Lawful Access* einer ausländischen Behörde zu verhindern. Dies wiederum ist Grundlage dafür, dass sich der Berufsgeheimnisträger auf das Vertrauensprinzip berufen kann und die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 6 tief ist. Hinzu kommt, dass die Strafbarkeit der Mitarbeiter des Providers im Falle einer Herausgabe unter Schweizer Recht im Rahmen des Prinzips der *International Comity* vom Provider benutzt werden kann, sich vor einem ausländischen Gericht gegen den Befehl zu wehren – und dies oft mit guten Chancen. Die senkt die Eintrittswahrscheinlichkeit von Voraussetzung Nr. 6 noch weiter.

h. Voraussetzung Nr. 7: Dem Berufsgeheimnisträger gelingt es nicht, die relevanten Kundendaten rechtzeitig in Sicherheit zu bringen bzw. den Zugriff des Providers zu entziehen

[101] Liegt ein Herausgabebefehl vor oder droht ein solcher, erfährt der Berufsgeheimnisträger möglicherweise davon. In diesem Fall kann er entsprechende Massnahmen treffen, um die Kundendaten in Sicherheit zu bringen. Hierzu dient ein entsprechendes vertragliches Recht, das als Gegenmassnahme Nr. 12 bereits empfohlen wurde. Im Rahmen der Berechnung der Wahrscheinlichkeit kann daher berücksichtigt werden, dass dem Berufsgeheimnisträger eine solche Rettung seiner Kundendaten gelingt und den Herausgabebefehl vereiteln kann.

[102] Allerdings ist auch zu beachten, dass Herausgabebefehle geheim erfolgen können (d.h. der Provider nicht darüber sprechen darf, ein sog. *gag order*) und es denkbar ist, dass ein Herausgabebefehl zwar einer gerichtlichen Klärung unterliegt, die streitgegenständlichen Daten jedoch bereits vorab gesichert werden mussten (sog. *freeze order*). Gerade letzteres dürfte häufig vorkommen bzw. von den Providern praktiziert werden. Je nach der Art und Weise der Implementation kann sich hierbei BYOK auszahlen, indem dem Provider der Zugang zu den Daten im Klartext technisch entzogen wird.

i. Gesamtbeurteilung

[103] Ob der Berufsgeheimnisträger seine Sorgfaltspflichten im Rahmen einer Auslagerung seiner Kundendaten an den Provider eingehalten hat, ergibt sich im Ergebnis daraus, wie wahrschein-

lich es ist, dass es trotz der von ihm getroffenen Gegenmassnahmen zu einer Herausgabe von Kundendaten im Klartext kommt.

[104] Diese Wahrscheinlichkeit kann berechnet werden, wenn die einzelnen Eintrittswahrscheinlichkeiten der sieben kumulativ erforderlichen Voraussetzungen – unter Berücksichtigung der jeweiligen Gegenmassnahmen und Umstände – miteinander multipliziert werden (sog. Multiplikationssatz). Soweit parallele Eintrittswahrscheinlichkeiten bestehen (z.B. Zugang innerhalb und ausserhalb des Supports), müssen die Wahrscheinlichkeiten addiert werden, ggf. unter Abzug einer doppelt gezählten Eintrittswahrscheinlichkeit (sog. Additionssatz).

[105] Dogmatisch gesehen ist die Voraussetzung Nr. 6 (Vertrauensprinzip) im Falle der Beurteilung der Fahrlässigkeit unter dem Titel der Vorhersehbarkeit zu beurteilen, während die anderen Voraussetzungen je nach Betrachtungsweise die Vorhersehbarkeit des *Lawful Access* «nach dem gewöhnlichen Lauf der Dinge und den Erfahrungen des Lebens» oder aber dessen «höchstwahrscheinlichen» Verhinderung durch entsprechende Gegenmassnahmen beschlagen. Da beides im Ergebnis auf eine Wahrscheinlichkeitsrechnung hinausläuft, wurden die sieben Voraussetzungen der Einfachheit halber in einer Kalkulation kombiniert, ohne der einen oder anderen dogmatischen Betrachtungsweise den Vorzug zu geben.

[106] Die Wahrscheinlichkeit der sieben Voraussetzungen kann schliesslich gewissermassen als Vorfrage um eine Aussage erweitert werden, als wie wahrscheinlich es erachtet wird, dass eine ausländische Behörde ihr Bedürfnis an Kundendaten des Berufsgeheimnisträgers zu gelangen, nicht bereits auf anderem Wege erfüllt werden kann, also über den Berufsgeheimnisträger selbst oder über Amts- und Rechtshilfe. Ist dies einfacher möglich als über einen Herausgabebefehl gegenüber einem Provider, wird eine ausländische Behörde erfahrungsgemäss den direkten Weg über den Berufsgeheimnisträger oder Amts- und Rechtshilfe bevorzugen. Auch dies kann und muss je nach Situation in die Wahrscheinlichkeitsrechnung miteinbezogen werden, ebenso die Wahrscheinlichkeit, dass eine Behörde sich überhaupt für die Daten des Berufsgeheimnisträgers interessiert. Dies kann das Gesamtergebnis deutlich beeinflussen.