USA: Gesetzgeber billigt Datenzugriff außerhalb der USA (CLOUD Act)

Dr. Axel Spies ist Rechtsanwalt in der Kanzlei Morgan Lewis & Bockius, Washington DC und Mitherausgeber der ZD.

Als Teil des Haushaltsgesetzes (Omnibus Act) hat der US-Kongress am 22.3.2018 den CLOUD Act (Clarifying Lawful Overseas Use of Data Act) verabschiedet. Präsident Trump hat das sehr umfangreiche Haushaltsgesetz trotz einiger Bedenken, die nichts mit dem CLOUD Act zu tun haben, am 23.3.2018 unterzeichnet (H.R.4943, S.2383). Sponsoren des CLOUD Act waren Senator Hatch (R-Utah) and Rep. Collins (R-Ga.).

Der CLOUD Act (S. 2201 ff. des Haushaltsgesetzes) enthält neue Vorschriften, wie ausländische Regierungsstellen auf in den USA gespeicherte Daten für Strafverfolgungszwecke zugreifen dürfen. Aus europäischer Warte dürften aber die Vorschriften wichtiger sein, die klarstellen, dass der bestehende Stored Communications Act (SCA) auch auf Daten anwendbar ist, die im Ausland abgespeichert sind, und wie dann vorzugehen ist. Darum geht es im Wesentlichen in dem vor dem *U.S. Supreme Court* anhängigen Revisionsverfahren Microsoft v. USA (vgl. *Spies,* ZD-Aktuell 2017, 05829).

Der Cloud Act stellt mit einem Zusatz zu Titel 18 des United States Code (§ 2713 „Erforderliche Aufbewahrung und Offenlegung von Mitteilungen und Aufzeichnungen") Folgendes klar: „Ein Anbieter von elektronischen Kommunikationsdiensten oder Ferndienstleistungen [Remote Computing Services] muss die in diesem Kapitel enthaltenen Verpflichtungen zur Erhaltung, Sicherung oder Offenlegung des Inhalts einer drahtgebunden oder elektronischen Nachricht sowie aller Aufzeichnungen oder anderer Informationen eines Kunden oder Abonnenten im Besitz oder unter Kontrolle [possession, custody or control] dieses Anbieters erfüllen, [und zwar] unabhängig davon, ob diese Kommunikation, Aufzeichnung oder andere Information innerhalb oder außerhalb der Vereinigten Staaten belegen ist."

1. Beschwerdeverfahren vor dem Richter

Wenn ein solcher Anbieter einen Durchsuchungsbefehl (Warrant) zugestellt bekommt, der (auch) im Ausland (z. B. in der EU) abgespeicherte Daten umfasst, sieht der CLOUD Act ein besonderes Verfahren vor dem Richter vor, um die Rechte der beteiligten Staaten zu wahren, in denen sich die Daten befinden:

Schritt 1: Der Anbieter kann innerhalb von 14 Tagen nach Zustellung eine formelle Beschwerde (motion to modify or quash) beim zuständigen Gericht einreichen und damit die Aufhebung des Warrant mit folgender glaubhaft zu machender Begründung verlangen:

„(i) dass der Kunde oder Abonnent keine US-Person ist und nicht in den Vereinigten Staaten ansässig ist; und

(ii) dass die erforderliche Offenlegung [der Daten] ein wesentliches Risiko darstellt, dass der Anbieter gegen die Gesetze einer qualifizierten ausländischen Regierung verstoßen würde."

Schritt 2: Das Gericht führt dann nach Anhörung der Regierungsseite eine Abwägung unter Zuhilfenahme folgender Leitlinien durch:

„(i) ob die erforderliche Offenlegung den Anbieter dazu veranlasst, die Gesetze einer qualifizierten ausländischen Regierung zu verletzen;

(ii) ob auf Grund der Gesamtheit der Umstände die Gerechtigkeitsinteressen es erfordern [the interest of justice dictate], dass der Warrant geändert oder aufgehoben werden sollte; und

(iii) der Kunde oder Abonnent keine US-Person ist und keinen Wohnsitz in den Vereinigten Staaten hat."

Comity-Analyse: Das Kriterium (ii) wird durch die „Comity-Analyse" wie folgt anhand von acht abwägungsrelevanten Kriterien präzisiert:

„(**A**) die Interessen der Vereinigten Staaten, einschließlich der Untersuchungsinteressen der Regierungsstelle, die die Offenlegung [der Daten] verlangt;

(**B**) die Interessen der qualifizierten ausländischen Regierung zu Gunsten der Verhinderung einer verbotenen Offenlegung;

(**C**) die Wahrscheinlichkeit, der Umfang und die Art der Strafen für den Anbieter oder Mitarbeiter des Anbieters auf Grund von widersprüchlichen rechtlichen Anforderungen an den Anbieter;

(**D**) der Ort und die Staatsangehörigkeit des Abonnenten oder Kunden, auf dessen Kommunikation zugegriffen werden soll, falls bekannt, und die Art und das Ausmaß der Verbindung des Abonnenten oder Kunden mit den Vereinigten Staaten …;

(**E**) die Art und das Ausmaß der Verbindungen und Präsenz des Anbieters in den Vereinigten Staaten;

(**F**) die Bedeutung der Informationen, die offengelegt werden müssen, für die Untersuchung;

(**G**) die Wahrscheinlichkeit eines rechtzeitigen und wirksamen Zugangs zu den Informationen, die offengelegt werden müssen, durch Mittel, die weniger schwerwiegende negative Folgen haben; und

(**H**) wenn das Verfahren im Auftrag einer ausländischen Behörde gem. § 3512 beantragt wurde, die Ermittlungsinteressen der ausländischen Behörde, die die Rechtshilfe beantragt."

Der US-Richter kann auf der Grundlage dieser Interessenabwägung den Warrant aufheben oder ändern. Während der Dauer dieses Beschwerdeverfahrens darf der Anbieter die Informationen nicht löschen. Der Anbieter ist in diesem Zeitraum nicht verpflichtet, die Informationen den US-Ermittlungsbehörden zu liefern, es sei denn das Gericht ordnet die Vorlage in dringenden Fällen an.

2. Kurzanalyse

Es ist noch viel zu früh, um die genauen Auswirkungen des CLOUD Act klar abzustecken. Möglicherweise haben Sen. *Hatch* und Rep. *Collins* aber mit den Cloud Act das Feuer eher angefacht als gelöscht. Das Gesetz in der Endfassung dürfte bei der hektischen Verabschiedung des Haushalts kaum einer gelesen haben. Deshalb ist es nicht sicher, das sich damit das Verfahren vor dem *U.S. Supreme Court* erledigt hat, weil der CLOUD Act nur Regeln zum Gerichtsverfahren beinhaltet (vgl. zum Verfahren *Jansen,* ZD 2018, 149 f. und *Spies,* ZD-Aktuell 2017, 05829). Jedenfalls werden sich US-Anbieter nicht auf das Argument stützen können, dass die Daten außerhalb der USA belegen sind, solange technisch die Möglichkeit besteht, die Daten in die USA zu holen und Besitz und Kontrolle über die Daten besteht. „Possession, custody or control" wird in den USA traditionell weit ausgelegt.

Die o.g. Comity Analyse ist ähnlich aufgebaut wie die sog. Aérospatiale-Kriterien des *U.S. Supreme Court* (hierzu *Spies,* in: Forgó/Helfrich Schneider, Betrieblicher Datenschutz, 2. Aufl. 2017, Teil XII,

e-Discovery, Kap. 2, Rdnr. 9). Das Kriterium „G" („mildere Mittel") erwähnt die bestehenden Multilateral Assistance Treaties (Rechtshilfeabkommen – MLATs) nicht. Der Richter braucht danach nicht zu fragen. Es ist nicht erforderlich, dass die US-Ermittlungsbehörde ein Rechtshilfeverfahren mit dem ausländischen Staat über ein MLAT eingeleitet hat, bevor sie den Warrant zustellt. Die USA wollen offensichtlich weg von den bestehenden (bürokratischen und zeitraubenden) MLAT-Verfahren.

Dies zeigt die rechtlich und politisch delikate Leitlinie „(i)": Verletzung der Gesetze einer „qualifizierten ausländischen Regierung". Darunter fällt nach dem Wortlaut des CLOUD Act nur eine Regierung, mit der die USA ein Executive Agreement haben und (nicht „oder") die die Gegenseitigkeit zumindest im Grundsatz verbürgt: „deren Rechtsvorschriften den Anbietern elektronischer Kommunikationsdienste und den Dienstleistern für Fernverarbeitungsdienste substanzielle und verfahrenstechnische Möglichkeiten bieten, die den in den Absätzen 2 und 5 vorgesehenen [Kriterien] ähneln" (Sec. § 2703 (h) (10 (A) und (B)). Diese Vorschrift hat vermutlich politische Hebelwirkung: sie soll andere Ländern dazu bewegen, Executive Agreements mit den USA abzuschließen (das sind wohl einfache Verwaltungsabkommen oder -abreden) – verbunden damit, dass diese anderen Länder eine ähnliche Comity Analyse eines Richters per Gesetz einführen müssen. Das könnte etwa durch geplante E-Rechtshilfe in der EU geschehen, die ebenfalls auf dem Prinzip aufbaut, dass die (US-)Ermittler direkt an den Anbieter herantreten können und der Anbieter dann dagegen eine Beschwerde einlegen kann (vgl. *Jansen*, ZD 2018, 150). Nur eine „qualifizierte ausländischen Regierung" soll Zugang zu Daten erhalten, die in den USA belegen sind, nur eine solche Regierung spielt bei der Comity-Analyse eine Rolle.

Mit dieser Leitlinie (i) gehen die USA vermutlich auf Kollisionskurs mit Art. 48 DS-GVO, der lautet: „Jegliches Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, dürfen unbeschadet anderer Gründe für die Übermittlung gemäß diesem Kapitel jedenfalls nur dann anerkannt oder vollstreckbar werden, wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind." Es fällt auf, dass in Art. 48 DS-GVO der Weg über das MLAT zwingend vorgeschrieben ist, im CLOUD Act nicht. Einfache Verwaltungsabreden lassen sich nur schwer in den Text des Art. 48 DS-GVO hineininterpretieren. Der Anbieter könnte versuchen, die Kooperation mit dem US-Richter mit Art. 49 Abs. 1 lit. e DS-GVO zu rechtfertigen („…Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich"). Ob diese Vorschrift als Ausnahme zu Art. 48 DS-GVO („unbeschadet anderer Gründe…") auf den CLOUD Act passt, ist sehr zweifelhaft, weil das Comity-Verfahren im CLOUD Act vor der Übermittlung eingreift. Ein weiterer sog. Knackpunkt: Der Cloud Act verwendet den Begriff „US-Personen", die DS-GVO den Terminus „Betroffener" – ohne Relevanz der Staatsangehörigkeit oder Wohnsitz. Schon deswegen passen der CLOUD Act und die DS-GVO nicht zueinander.

Erstes Fazit: Mit dem CLOUD Act hat wahrscheinlich kaum einer in Brüssel so (schnell) gerechnet. Viele US-Anbieter bewerten die Klarstellungen positiv. Ob die existierenden MLATs damit zu Gunsten von Executive Agreements (jederzeit widerrufbare „Deals") der Regierungen rechtlich begraben werden, wird sich zeigen.