RECHTSANWÄLTE DR. MICHAEL RATH UND DR. AXEL SPIES*

CLOUD Act: Selbst für die Wolken gibt es Grenzen

A. Hintergrund

Im März 2018 hat der US-Kongress den sog. CLOUD Act (Clarifying Lawful Overseas Use of Data Act) als Teil des Haushaltsgesetzes (Omnibus Act) verabschiedet. Bisher war rechtlich stark umstritten, ob Anbieter von elektronischen Kommunikations- oder Cloud-Diensten den US-Behörden auch dann Zugang zu den Benutzerdaten gewähren müssen, wenn diese Daten im Ausland gespeichert sind. Das Gesetz legt nun unter anderem fest, dass die bereits bestehende Verpflichtungen unabhängig davon erfüllt werden müssen, ob die betroffene Benutzerdaten, auf welche eine US-Behörde zugreifen will, innerhalb oder außerhalb der Vereinigten Staaten gespeichert ist. Konkret bedeutet das, dass der Stored Communications Act auch auf im Ausland gespeicherte Daten anwendbar ist. Nach diesem bereits seit 1986 bestehenden Gesetz müssen US-Unternehmen den US-Behörden einen direkten Zugriff auf Daten aufgrund eines Rechtsaktes (zB einer Verwaltungsanordnung) gewähren.

B. Microsoft-Verfahren als Anlass für den Cloud Act?

Anlass für das neue Gesetz dürfte das vielbeachtete Verfahren Microsoft v. United States vor dem U. S. Supreme Court gewesen sein. Darin ging es seit 2013 im Grundsatz um die Frage, ob Microsoft verpflichtet ist, auf Grundlage von Verwaltungs- und Justizanordnungen (in diesem Fall aufgrund eines Durchsuchungsbefehls) den US-Behörden Zugriff auch auf im Ausland (in diesem Fall Irland) gespeicherte Benutzerdaten zu gewähren. Unter Benutzerdaten versteht man in diesem Zusammenhang die vollständige Kommunikation, Aufzeichnungen oder andere Informationen. Microsoft hatte zunächst verweigert, den US-Behörden Zugang zu gewähren, und vor dem US Court of Appeals Recht bekommen.[1] Ein Urteil in dieser Sache wurde ursprünglich für Mitte des Jahres erwartet, ist aber mit dem CLOUD Act nun hinfällig. Kurz nach dessen Erlass haben die US-Behörden einen neuen Durchsuchungsbefehl auf Grundlage des neuen Gesetzes erlassen. Der Supreme Court stellte daraufhin am 17.4.2018 das Revisionsverfahren ein und verwies den Fall an das Gericht der Vorinstanz mit der Empfehlung zurück, das Verfahren dort ebenfalls einzustellen.

C. Umfassende Zugriffsrechte – geringe Kontrollmöglichkeiten

Durch den CLOUD Act, den Microsoft und andere US-Unternehmen in den USA propagiert haben, dürfen US-Behörden zukünftig für strafrechtliche Zwecke auch ohne Rückgriff auf internationale Rechtshilfeabkommen Zugriff auf (personenbezogene) Daten von (US-)Unternehmen erhalten, die nicht in der USA gespeichert werden. Dies soll grenzüberschreitende behördliche Ermittlungen vereinfachen, da die weltweit sehr unterschiedlichen und teilweise auch widersprüchlichen Regelungen zur Datenweitergabe im Rahmen von Ermittlungen die Tätigkeit der US-Behörden behindert haben sollen. Gleichzeitig sollen aber auch Rechtsstaat und Bürgerrechte gewährleistet werden.

Rechtliche Mittel gegen ein Vorgehen nach dem CLOUD Act haben US-fremde Personen jedoch kaum. Nur wenn das betreffende Land seinerseits ein Privatsphäre- und Datenaustauschabkommen mit den USA vereinbart hat, was zumindest derzeit für Deutschland nicht der Fall ist, bestehen Zugriffsbeschränkungen und Kontrollmöglichkeiten. US-fremde Personen müssen sich also – solange ihre Heimatstaaten keine solchen Abkommen mit den USA abgeschlossen haben – darauf verlassen, dass der jeweilige Anbieter sich gegen den Rechtsakt der US-Behörde zur Wehr setzt und die Herausgabe der Daten bzw. den Zugriff verweigert. Microsoft deutete bereits an, dass man sich weiterhin gegen die entsprechenden Durchsuchungsbefehle der US-Behörden wehren wolle.[2] Da diese Durchsuchungsbefehle aber oft mit einer Verschwiegenheitsverpflichtung (sog. „gag order") einhergehen, ist zumindest zweifelhaft, wie werthaltig diese Absichtsbekundung des Softwareunternehmens in der Praxis ist.

Unabhängig davon, ob der Betroffene selbst oder der US-Anbieter gegen den Rechtsakt einer US-Behörde vorgeht, soll sich das Vorgehen an den vorhandenen amerikanischen Rechtsinstrumenten orientieren. Diese sind jedoch – im Vergleich zur DSGVO, die vorrangig den Schutz personenbezogener Daten im Blick hat – eher auf die Unterstützung von Ermittlungstätigkeiten gerichtet. So erfolgt vor der Datenübermittlung nach dem CLOUD Act eine „*comity analysis*" genannte Interessenabwägung des US-Richters. Nur wenn diese dazu führt, dass eine Datenübermittlung unbillig erscheint, unterbindet der Richter den Datenzugriff. Gesichtspunkte für die Abwägung sind u.a. das Ermittlungsinteresse der US-Behörde, die Interessen ausländischer Staaten sowie die Wahrscheinlichkeit und das Maß der Strafen im Ausland. Dies ist im Prinzip im strafrechtlichen Bereich nichts Neues, da die *comity analysis* seit vielen Jahren aufgrund der grundlegenden *Aérospatiale*-Entscheidung des US Supreme Court (AZ 85-1695) von 1987 bei den US-Gerichten Gang und Gäbe ist.

D. Kollision mit der DSGVO

Abgesehen von den völkerrechtlichen Fragestellungen (darf ein Staat sich ohne Weiteres das Zugriffsrecht auf in anderen Staaten gespeicherte Daten einräumen und dadurch bestehende Rechtshilfeabkommen umgehen?) ist

* Dr. Michael Rath ist Rechtsanwalt, Fachanwalt für Informationstechnologie-Recht und Partner der Luther Rechtsanwaltsgesellschaft mbH mit Sitz in Köln. Zudem ist er Certified ISO/IEC 27001 Lead Auditor. Dr. Axel Spies ist Rechtsanwalt sowie Special Legal Consultant bei Morgan, Lewis & Bockius LLP in Frankfurt. Er ist anerkannter Experte in den Bereichen internationaler Datenschutz und Telekommunikation.

1 Vgl. www.computerwoche.de/a/sieg-fuer-den-datenschutz,3329629.

2 Vgl. https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow/.

der CLOUD Act jedoch insbesondere vor dem Hintergrund der seit dem 25.5.2018 geltenden DSGVO von Relevanz. Hier stellt sich die Frage, ob die direkte Datenübermittlung eines Unternehmens an eine US-Behörde nach der DSGVO überhaupt zulässig ist. Entscheidend für die Zusammenarbeit mit Drittländern ist Art. 48 DSGVO. Danach dürfen Entscheidungen der Verwaltungsbehörde eines Drittlandes, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, nur dann anerkannt oder vollstreckt werden, wenn sie auf eine internationale Übereinkunft gestützt sind, wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat. Ob ein Durchsuchungsbefehl des FBI, der wie im *Microsoft*-Fall Microsoft in den USA zugestellt wurde, unter Art. 48 DSGVO fällt, ist eine offene Rechtsfrage.

Wenn man annimmt, ein solcher ausländischer Rechtsakt an eine ausländische Gesellschaft sei von Art. 48 DSGVO gedeckt, könnte der Adressat mit Hinweis auf den Erwägungsgrund 115 zur DSGVO verweisen, der ein Unterlaufen des Schutzniveaus der DSGVO durch Rechtsakte von Drittländern (wie etwa dem CLOUD Act) gerade verhindern soll. Danach seien nur Datenübermittlungen zulässig, welche die Bedingungen der DSGVO für einen Drittlandtransfer einhalten. Eine Datenübermittlung wäre dann unzulässig. Eine mögliche Verteidigungslinie in diesem Fall für die Unternehmen, die nach US-Recht die Daten dem FBI etc. liefern müssen, ist, dass Art. 48 DSGVO nur „unbeschadet anderer Gründe für die Übermittlung gemäß diesem Kapitel" gilt. Dies bedeutet, dass Übermittlungen „zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen" nach Art. 49 Abs. 1 lit. e) DSGVO für die Unternehmen weiter möglich sind. Auch dürfte eine Rolle spielen, dass in diesen strafrechtlichen Fällen die EU-Kommission ebenfalls über die Grenze hinweg ermitteln möchte, damit Straftäter sich nicht mit ihren Daten durch eine Flucht in die ausländische Cloud entziehen können. Dies liegt auch im Interesse der Europäer.

Je nachdem, wie die Richter in Europa Art. 48 und Art. 49 Abs. 1 lit. e) DSGVO gegeneinander ausbalancieren, könnten Unternehmen in Europa, die (personenbezogene) Daten aus der EU direkt an US-Behörden übermitteln, einen Verstoß gegen Art. 48 DSGVO begehen, der nach Art. 83 Abs. 5 lit. d) DSGVO bußgeldbewährt wäre. Im Ernstfall würden einem Unternehmen Bußgelder iHv bis zu 20. Mio. EUR oder bis zu 4 % des gesamten weltweiten Vorjahresumsatzes drohen, je nachdem, was höher ist.

E. Ausweg Datentreuhand?

Einen möglichen Ausweg zeigt Microsoft mit seinem Programm „Office 365 Deutschland".[3] Hierbei betreibt T-Systems als Dienstleister für die Office-Anwendungen von Microsoft den Cloud-Dienst zum Abspeichern von Daten.[4] Als sog. „Datentreuhänder" hat grundsätzlich nur T-Systems Zugriff auf die Daten, welche zudem in Deutschland gespeichert sind. Microsoft erhält ausschließlich im Rahmen der Treuhandvereinbarung für Zwecke der Wartung und des Supports Zugriff auf die Daten, für andere Zwecke jedoch nicht.

Dies könnte einen Ausweg darstellen, um den direkten Datenzugriff der US-Behörden bereits im Vorhinein zu unterbinden. Denn das amerikanische Recht geht für einen Zugriff davon aus, dass die Daten im Besitz oder unter Kontrolle des jeweiligen Anbieters sein müssen. Das ist beim Modell der Datentreuhand jedoch gerade nicht der Fall. Ob die US-Behörden dies auch so sehen, muss sich in der Praxis aber erst noch zeigen. Problematisch ist in diesem Zusammenhang, dass die meisten Anbieter einer Cloud-Treuhand ein Verbindungsbüro oder sonstige Vertreter in den USA haben. Damit könnten sie unter die „Jurisdiction" der USA fallen. Wenn diese Vertreter dann einen Durchsuchungsbefehl zugestellt bekommen würden, müssten sie evt. die Daten aus der Cloud liefern.

F. Nächste Baustellen: Drittlandtransfer und E-Evidence-Verordnung

Die von großen Internet-Unternehmen gelobte Rechtssicherheit[5] herrscht somit nur auf amerikanischer Seite. Auf der europäischen Seite wäre mit Blick auf die Bußgeld- und Verfahrensrisiken[6] hingegen eine baldige, klare Positionierung der Behörden wünschenswert. Allerdings ist noch unklar, wann eine Reaktion der europäischen Datenschutzinstitutionen (zB in Form von Handlungsempfehlungen durch die Artikel 29-Datenschutzgruppe) erfolgt. Andererseits plant die EU zurzeit mit der sog. E-Evidence-Verordnung einen zum CLOUD Act vergleichbares EU-Gesetz, mit dem Justizbehörden erleichterten (Direkt-)Zugriff zu „elektronischen Beweismitteln" erhalten könnten. Vorerst sind Unternehmen mit Bezug zur USA – sei es durch Mutter-/Tochtergesellschaften oder Dienstleister – daher gut beraten, die Vorgaben der DSGVO umzusetzen und die weiteren Entwicklungen hinsichtlich des Drittlandtransfers auf beiden Seiten des Atlantiks genau zu beobachten.

KONTAKT:

Dr. Michael Rath
Luther Rechtsanwaltsgesellschaft mbH
Anna-Schneider-Steig 22
50678 Köln
Tel.: 0221/993725795
Fax: 0221/9937110
michael.rath@luther-lawfirm.com

Dr. Axel Spies
Morgan, Lewis & Bockius LLP
1111 Pennsylvania Avenue NW
20006-1806 Washington DC 20004
United States
Tel.: +1 202/3736145
Fax: +1 202/3736001
axel.spies@morganlewis.com

3 Vgl. www.computerwoche.de/a/datenschutz-in-microsoft-office-365-und-microsoft-azure,3332111.

4 Vgl. www.computerwoche.de/a/daten-treuhand-als-abwehrmittel-gegen-ueberwachung,3222181.

5 Vgl. https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf.

6 Vgl. www.computerwoche.de/a/wo-die-abmahnung-droht,3544586.