THOMAS HOEREN

DATENSCHUTZ IN DER CLOUD

PROBLEME DER WERBEWIRTSCHAFT BEI DER AUSLAGERUNG VON DATEN AUF AMERIKANISCHE CLOUD-ANBIETER

Prof. Dr. Thomas Hoeren, Universität Münster, zur Zeit Stanford Law School (Kalifornien). Von 1980 bis 1987 Studium der Theologie und Rechtswissenschaften, 1989 Promotion und 1994 Habilitation an der Universität Münster. 1995 bis 1997 Universitätsprofessor an der Heinrich-Heine-Universität Düsseldorf. Seit April 1997 Universitätsprofessor an der Juristischen Fakultät der Westfälischen Wilhelms-Universität Münster; Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM).
E-Mail: hoeren@uni-muenster.de

Es scheint ein Muss zu sein. Wer etwas auf sich hält, geht in die Cloud. Seien es die iCloud-Dienste von Apple oder die Datenspeicher von Amazon, gerade kleine und mittelständische Unternehmen lagern ihre zum Teil umfangreichen Daten gerne in den USA aus. Die Gründe sind vielfältig. Man träumt von einer Kostenersparnis, die mit einer solchen Auslagerung verbunden sein könnte. Denn die Dienste von Apple und Co. sind sehr günstig. Daneben lockt auch noch die weltweite Erreichbarkeit der Daten. Gerade wenn man mit anderen Unternehmern zusammenarbeitet, ergibt der Zugriff auf gemeinsame Datenressourcen Sinn.

Selbst wenn man aber diese Kosten- und Nutzenvorteile berücksichtigt, stellt sich die Frage, ob die Nutzung von Cloud-Diensten insbesondere von US-Anbietern überhaupt rechtlich zulässig und damit geboten ist.

DAS DEUTSCHE RECHT UND DIE CLOUD

In der Zwischenzeit dürfte es sich schon herumgesprochen haben, dass an den Einsatz von Cloud-Diensten eine Reihe rechtlicher Vorgaben nach deutschem Verständnis gekoppelt sind.[1] Eine solche Auslagerung gilt als Auftragsdatenverarbeitung im Sinne von § 11 des Bundesdatenschutzgesetzes (BDSG). Es bedarf daher eines besonders sorgfältig entworfenen und unterschriebenen Vertrages zur Auftragsdatenverarbeitung, in dem insbesondere die Weisungsgebundenheit des Cloud-Anbieters verankert ist.

Schon damit fangen die Probleme an, da sich die Cloud-Anbieter gerade in den USA weigern, sich zu Gehilfen deutscher mittelständischer Unternehmen zu machen. Doch ohne eine entsprechende Vereinbarung droht dem deutschen Unternehmen ein sehr hohes Bußgeld seitens der Datenschutzaufsichtsbehörden. Der Abschluss einer solchen Vereinbarung ist im Übrigen dadurch erleichtert, dass entsprechende Muster schon seit einiger Zeit im Netz zu finden sind (z. B. von Bitkom[2] oder den Datenschutzaufsichtsbehörden[3]).

Meist vergessen wir darüber hinaus, dass es nicht nur des Abschlusses einer solchen Vereinbarung bedarf. Denn Papier ist natürlich geduldig. Vielmehr muss sich der deutsche Auftraggeber auch erkundigen und gegebenenfalls überprüfen, welche Datensicherheitsmaßnahmen beim Auftragnehmer zum Schutz der übertragenen Daten vorhanden sind. Vorsicht ist im Übrigen geboten bei dem »Trick«, den Personenbezug der entsprechenden ausgelagerten Daten zu leugnen. Natürlich gilt das BDSG nicht, wenn überhaupt keine personenbezogenen Daten übertragen werden, z. B. bei der Übertragung anonymisierter oder rein sachbezogener Daten ohne jedweden Bezug zu einer natürlichen Person. Doch schon die Übermittlung des jeweiligen Bearbeiters eines Datensatzes macht den Vorgang personenbezogen. Im Übrigen haben die Datenschutzaufsichtsbehörden auch Bedenken, wenn der Auftraggeber sich auf eine »Verschlüsselung« der Daten vor der Übertragung an den Cloud-Anbieter beruft.[4] Denn nicht jede Verschlüsselung ist eine Verschlüsselung. Wenn mit einfachen Mitteln die Verschlüsselung aufgelöst werden kann, gelten die Daten weiterhin als personenbezogen.

Die Notwendigkeit, einen Vertrag zur Auftragsdatenverarbeitung zu unterzeichnen und die Einhal-

tung von Datensicherheitsstandards zu überprüfen, besteht gegenüber in- und ausländischen Cloud-Anbietern. Im Falle der USA kommt aber noch hinzu, dass es sich hierbei um ein Land handelt, das aus der Sicht der EU-Kommission kein angemessenes Datenschutzniveau hat. Bei einem solchen Drittland hält die EU-Kommission einen Datentransfer regelmäßig für verboten. Von diesem Verbot sind zwar Ausnahmen möglich, angesichts der derzeitigen Sicherheitslage im Verhältnis USA – EU jedoch schwierig. Früher konnte man sich noch auf sogenannte Safe-Harbor-Gütesiegel berufen, die ein US-Unternehmen in den USA erwerben konnte. Mit diesem Siegel konnte das US-Unternehmen den Nachweis führen, dass es intern Vorkehrungen getroffen hat, um europäische Datenschutzstandards zu erfüllen. Solche Safe-Harbor-Siegel[5] werden seit einigen Monaten nicht mehr von der EU-Kommission akzeptiert.[6] Von daher ist Vorsicht geboten, wenn sich ein US-Cloud-Anbieter noch auf Safe-Harbor beruft. Es bedarf heutzutage des Abschlusses eines zusätzlichen Mustervertrages nach EU-Standards. Die EU-Kommission hat hierzu vor einigen Jahren ein entsprechendes Muster für die Auftragsverarbeitung mit US-Anbietern veröffentlicht.[7] Dieses Muster ist eins zu eins zu übernehmen und als Annex dem Auftragsdatenverarbeitungsvertrag beizufügen. Ansonsten riskiert gerade der deutsche Auftraggeber wiederum hohe Geldbußen und eine sicherlich unerwünschte negative Publicity in der deutschen Tagespresse.

DIE RECHTSLAGE AUS DER SICHT DER USA

Die obigen Überlegungen sind meines Erachtens weitgehend in der deutschen Datenlandschaft bekannt. Wenig beachtet werden allerdings die US-Perspektiven. Denn der Datentransfer in die USA kann für deutsche Unternehmen losgelöst vom europäischen Datenschutzrecht fatale Konsequenzen haben, was das US-Recht angeht.[8] Vor einigen Monaten hatte der New York City District Court entschieden, dass Anbieter von Cloud-Dienstleistungen die Daten von amerikanischen und nichtamerikanischen Kunden auf Verlangen einer US-Sicherheitsbehörde aushändigen müssen. Diese Verpflichtung gilt selbst dann, wenn die Daten auf Servern in Europa gespeichert sind.[9] Auf der Grundlage eines in den USA gültigen Durchsuchungsbefehls einer US-Behörde können daher die Anbieter von Internet-, E-Mail- und Cloud-Diensten mit Sitz in den USA zur Herausgabe von Daten gezwungen werden, die außerhalb der USA gespeichert werden können. Zur Begründung verweist der zuständige Richter darauf, dass der Aufwand für die US-Regierung durch die Zusammenarbeit mit anderen Ländern deutlich erhöht werde, wenn der normale Rechtshilfeweg eingehalten würde. Amerikanisches Recht sei deshalb auch außerhalb der USA anwendbar, wenn es um onlinegespeicherte Inhalte gehe. Microsoft werde so gezwungen, Daten aus einem Rechenzentrum in Dublin an die US-Behörden herauszugeben. Auch wenn Microsoft erklärte, gegen diese Entscheidung Rechtsmittel einlegen zu wollen, bleibt der Schaden für die Cloud-Anbieter aus den USA massiv. Dabei gilt es nicht nur, die Begehrlichkeiten der US-Sicherheitsbehörden nach dem Patriot Act zu beachten, sondern auch weitere Herausgabeverlangen anderer Behörden (z. B. im Steuerrecht).

Für US-Unternehmen hat eine Lagerung europäischer Daten in den USA große Vorteile. Denn oft werden die Tücken des US-amerikanischen Prozessrechts seitens deutscher Unternehmen vergessen. Im Zuge einer Zivilklage kann ein US-Unternehmen in den USA Offenlegung aller Daten verlangen, die sein deutscher Konkurrent in den USA gelagert hat. Das sogenannte E-Discovery-Verfahren[10] soll als gerichtliches Vorverfahren die Sachverhaltsfeststellung oder Beweisermittlung ohne Mitwirkung der Richter durch die Parteien selbst bewirken. Das Discovery-Verfahren umfasst auch solche Informationen, die zur Auffindung verwertbarer Beweismittel beitragen können; insofern besteht die Möglichkeit des nach deutschem Recht verbotenen Ausforschungsbeweises. Der jeweilige Prozessgegner kann also vom deutschen Unternehmen umfassende Auskunft und Herausgabe von Daten verlangen, sofern sich das deutsche Unternehmen auf den US-amerikanischen Prozess überhaupt einlässt bzw. einlassen muss.

Verfahrensrechtlich ist es zwar kaum möglich, eine deutsche Gesellschaft mittelbar prozessual zur Herausgabe solcher Daten zu verpflichten. Das deutsche Unternehmen wird allerdings Schwierigkeiten bekommen, wenn die Daten in den USA gespeichert sind. Im Übrigen ist die Weitergabe von Daten im Rahmen der E-Discovery nicht regelmäßig mit deutschem Datenschutzrecht vereinbar. So stehen zum Beispiel die Möglichkeiten des US-Prozessrechts, eingebrachte Dokumente auf Antrag sogar öffentlich zugänglich zu machen, mit dem Zweckbindungsgrundsatz des Datenschutzrechts in Widerspruch, das eine solche Veröffentlichung ausdrücklich verbietet.

FAZIT

In der derzeitigen Situation, insbesondere angesichts des angespannten Verhältnisses zwischen den USA und Europa in Sachen Datenschutz, kann von einer Nutzung von US-amerikanischen Cloud-Diensten nur nachhaltig abgeraten werden. So verlockend die Angebote sind und so kostengünstig die entsprechenden Dienste angeboten werden, so sehr ist ihre rechtliche Zulässigkeit nach europäischem Recht gelinde gesagt ungeklärt. Will man sie nutzen, sollte man auf jeden Fall auf den Transfer personenbezogener Daten komplett verzichten (selbst bei der Möglichkeit einer Verschlüsselung personenbezogener Daten). Im Übrigen gilt es abzuwarten, bis Europa eine »würdevolle« Antwort auf die Herausforderungen der US-Behörden gefunden hat, die in ihrer Datensammelwut offensichtlich keine Grenzen kennen. Es bedarf insofern vor allem der Verabschiedung der schon seit einigen Jahren angemahnten EU-Datenschutzgrundverordnung.[11] So lange die amerikanische Seite aber nicht verstehen will und kann, was Datenschutz bedeutet, ist der deutsche Auftraggeber gefragt, Vorsicht walten zu lassen. Ihn trifft die Haftung, ihn treffen die Bußgelder, Sie trifft eine sicherlich unerwünschte Erwähnung in der deutschen Tagespresse.

Insofern der einfache Ratschlag: Hände weg von iCloud, OneDrive, Drive, CloudDrive & Co.

[1] Eine Übersicht dazu findet sich in Thomas Hoeren/Gottfried Vossen/Till Haselmann, Cloud Computing für Unternehmen, dpunkt.verlag Heidelberg 2012.

[2] Zu finden unter http://www.bitkom.org/de/themen/50792_78385.aspx.

[3] Zum Beispiel http://www.bfdi.bund.de/bfdi_wiki/index.php/Mustervereinbarung_Auftragsdatenverarbeitung.

[4] Das Problem wird anschaulich beschrieben bei: http://uliarmbruster.wordpress.com/2013/09/07/datenschutzprobleme-trotz-verschlsselung/.

[5] Zum Mechanismus siehe Räther/Seitz: Übermittlung personenbezogener Daten in Drittstaaten – Angemessenheitsklausel, Safe Harbor und die Einwilligung, MMR 2002, 425 ff.

[6] Spies, ZD-Aktuell 2013, 03691.

[7] Die Klauseln sind in der englischen Version abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF und in der deutschen Version abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF.

[8] Dazu auch Voigt: Weltweiter Datenzugriff durch US-Behörden – Auswirkungen für deutsche Unternehmen bei der Nutzung von Cloud-Diensten, MMR 2014, 158 ff.

[9] Entscheidung (Richter James C. Francis IV, US Magistrate Judge) vom 25.4.2014 – 13 Mag. 2814; zu finden etwa unter: http://www.bingham.com/Publications/Files/2014/06/Comment-on-US-Court-Decision-SDNY.

[10] Dazu Spies/Schröder: Auswirkungen der elektronischen Beweiserhebung (eDiscovery) in den USA auf deutsche Unternehmen, MMR 2008, 275 ff.; Flägel/von Georg: E-Discovery nach US-Zivilverfahrensrecht und deutsches Datenschutzrecht, RIW 2013, 439 ff.

[11] Schneider/Härting: Datenschutz in Europa – Plädoyer für einen Neubeginn, CR 2014, 306 ff.