FRANKFURTER INSTITUT FÜR DAS RECHT DER EUROPÄISCHEN UNION
fireu
Education and Culture DG
Jean Monnet Centre of Excellence

24. Frankfurter Newsletter zum Recht der Europäischen Union

(19.10.2015)

Prof. Dr. Heinrich Amadeus Wolff

EuGH, Urt. v. 06.10.2015, Rs. C-362/14 (Schrems)

I. Das o.g. Urteil des EuGH, das in der Öffentlichkeit starke Beachtung gefunden hat, geht auf eine Vorlage irischer Gerichte zurück. Die Datenschutzrichtlinie aus dem Jahr 1995 (Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr) (DSRL) ist danach so auszulegen, dass die nationalen Kontrollstellen (Aufsichtsbehörden) die Möglichkeit haben müssen, die Eingabe einer Person auch dann zu prüfen, wenn die Eingabe sich auf den Schutz ihrer Rechte und Freiheiten bei der Verarbeitung sie betreffender personenbezogener Daten bezieht, die aus einem Mitgliedstaat in ein Drittland übermittelt wurden, und die Person geltend macht, dass das Recht und die Praxis dieses Landes kein angemessenes Datenschutzniveau gewährleisten, obwohl eine anderslautende Entscheidung der Kommission vorliegt, wonach in diesem Land ein angemessener Datenschutzstandard gewahrt ist. Weiter hat der EuGH entschieden, dass die Entscheidung der Kommission aus dem Jahr 2000, mit der diese festgestellt hat, dass bei den Unternehmen in den USA ein angemessener Datenschutzstandard gewährleistet sei, sofern diese die sog. „Grundsätze des sicheren Hafens“ zum Datenschutz akzeptierten, ungültig ist.

Der Entscheidung liegt folgender Sachverhalt zu Grunde: Die Richtlinie lässt die Datenübermittlung in Länder außerhalb der EU nur zu, wenn der dort gewährleistete Datenschutzstandard entweder landesweit oder zumindest bei der Stelle, welche die Daten erhält, angemessen, d.h. vergleichbar mit dem der Europäischen Union ist (Art. 25 Abs. 1 DSRL). Die Kommission kann in Zweifelsfällen verbindlich entscheiden, dass in einem Drittstaat ein angemessenes Schutzniveau besteht (Art. 25 Abs. 6 DSRL). Eine solche Entscheidung hat die Kommission für den Datenverkehr in die USA getroffen, beschränkt auf die Unternehmen, die eine bestimmte vorformulierte Selbstverpflichtungserklärung abgeben (die sog. Safe Harbor-Erklärung).

Doch selbst wenn in dem Drittstaat ein angemessenes Datenschutzniveau nicht besteht, kann die Datenübermittlung zulässig sein. Erstens kennt die Richtlinie

Ausnahmen für bestimmte Fallgestaltungen (Art. 26 Abs. 1 DSRL/§ 4 c Abs. 1 BDSG) und zweitens kann die Kontrollstelle die jeweilige Datenübermittlung gem. Art. 26 Abs. 2 DSRL/§ 4c Abs. 2 BDSG genehmigen, sofern der Empfänger der Daten ausreichende vertragliche Garantien für den Datenschutz abgibt. Die Kommission kann gem. Art. 26 Abs. 4 DSRL feststellen, dass bestimmte Standardvertragsklauseln ausreichende Garantien in diesem Sinne beinhalten. Der Österreicher Maximilian Schrems bat die irische Kontrollstelle (Datenschutzbehörde) nach den sog. Enthüllungen von Edward Snowden darum, zu verhindern, dass seine Daten, die bei Facebook gespeichert waren, von Irland in die USA übermittelt werden. Die irische Kontrollstelle war der Auffassung, dass die Angemessenheit des Datenschutzniveaus in den USA mit der Entscheidung der Kommission verbindlich festgestellt worden ist, und lehnte den Antrag deshalb ab. Dagegen suchte Schrems in Irland um Rechtsschutz. Der zuständige irische High Court stellte daraufhin fest, dass die Safe Harbor-Erklärung in Kombination mit dem Recht der Vereinigten Staaten von Amerika keinen angemessenen Datenschutzstandard gewährleiste und die Entscheidung der Kommission daher rechtswidrig sei. In einem Vorlageverfahren gem. Art. 267 EUV rief der High Court deshalb den EuGH an.

Die Entscheidung des EuGH besteht der Sache nach aus zwei Teilen. Sie befasst sich zum einen mit der Frage, wie die Kontrollstellen (Aufsichtsbehörden) handeln dürfen, wenn sie mit einer Entscheidung der Kommission, in einem Drittstaat sei das Datenschutzniveau angemessen, nicht einverstanden sind. In einem zweiten Teil begründet der EuGH, weshalb das „Safe Harbor-System“ nicht mit der Datenschutzrichtlinie und europäischem Verfassungsrecht vereinbar ist.

Im ersten Teil arbeitet der EuGH heraus, dass der Kommission in Art. 25 DSRL das Recht eingeräumt worden sei, verbindlich zu entscheiden, unter welchen Bedingungen die Datenübermittlung in einen Drittstaat angemessen i.S.d. Datenschutzrichtlinie ist. Er leitet weiter her, dass nach der Datenschutzrichtlinie jede Person zum Schutz ihrer Rechte die Kontrollstellen (Aufsichtsbehörden) anrufen könne (Art. 28 Abs. 4 DSRL). Im Falle einer Anrufung müssten die Kontrollstellen die Möglichkeit haben, in voller Unabhängigkeit die Rechtmäßigkeit der gerügten Maßnahme zu prüfen. Das betreffe auch die Frage, unter welchen Bedingungen personenbezogene Daten in Länder außerhalb der EU übermittelt werden dürfen. Diese Kontrolle durch unabhängige Stellen sei nicht nur in der Datenschutzrichtlinie selbst vorgesehen, sondern ergebe sich bereits auf höherer Normenebene aus Art. 8 der Grundrechtecharta (GRCh). Wenn die Kommission die Befugnis hat, ein angemessenes Datenschutzniveau verbindlich festzustellen, wenn zum anderen die Kontrollstellen (Aufsichtsbehörden) die Befugnis haben, in voller Unabhängigkeit die Rechtslage zu prüfen, also ob die Übermittlung in einen Drittstaat rechtmäßig ist, was wiederum ein angemessenes Schutzniveau voraussetzt, „beißen“ sich beide Befugnisse. Der EuGH löst diesen Konflikt rechtstechnisch geschickt. Nur der EuGH darf danach die Kommissionsentscheidung aufheben, er allein besitzt die Verwerfungskompetenz. Die Kontrollstellen müssten aber die Möglichkeit besitzen, die Rechtsfrage vom EuGH entscheiden zu lassen. Möglich sei das nur, wenn ihnen ein Klagerecht vor den nationalen Gerichten eingeräumt würde. Wörtlich heißt es:

> *Hält die Kontrollstelle die Rügen der Person, die sich mit einer Eingabe zum Schutz ihrer Rechte und Freiheiten bei der Verarbeitung ihrer personenbezogenen Daten an sie gewandt hat, dagegen für begründet, muss sie nach Art. 28 Abs. 3 Unterabs. 1 dritter Gedankenstrich der Richtlinie*

95/46 im Licht insbesondere von Art. 8 Abs. 3 der Charta ein Klagerecht haben. Insoweit ist es Sache des nationalen Gesetzgebers, Rechtsbehelfe vorzusehen, die es der betreffenden nationalen Kontrollstelle ermöglichen, die von ihr für begründet erachteten Rügen vor den nationalen Gerichten geltend zu machen, damit diese, wenn sie die Zweifel der Kontrollstelle an der Gültigkeit der Entscheidung der Kommission teilen, um eine Vorabentscheidung über deren Gültigkeit ersuchen.

EuGH, Urt. v. 06.10.2015, Rs. C-362/14 (Schrems), Rn. 65

Der zweite Teil ist politisch spektakulär, aber nicht juristisch. Eine Selbstverpflichtung von in den USA ansässigen Unternehmen gemäß der Safe Harbor-Erklärung gewährleistet kein angemessenes Datenschutzniveau. Die Erklärung hierfür ist einfach: Die Datenschutzrichtlinie verbietet eine Verwendung der erhobenen oder übermittelten Daten zu Zwecken, die unvereinbar sind mit den Zwecken, zu denen sie übermittelt wurden. Die Safe Harbor-Entscheidung legt aber einen Vorrang der in den USA geltenden Gesetze fest, so dass ein Zugriff der Sicherheitsbehörden auf Daten auch zu anderen Zwecken, die mit den ursprünglichen Übermittlungszwecken unvereinbar sind, zumindest möglich erscheint. Weiter ist die Reichweite des Zugriffs nicht normenklar geregelt, sie ist nicht auf ein Minimum beschränkt und gegen den Zugriff gibt es keine angemessene Rechtsschutzgewährleistung. Die Angemessenheit sei deshalb nicht gewahrt.

II. Für die Rechtspraxis hat die Entscheidung Sprengkraft. Faktisch bedeutet sie, dass die Übermittlung personenbezogener Daten in die USA bei gegenwärtigem Rechtsstand im Anwendungsbereich der Datenschutzrichtlinie (d.h. sofern es nicht um rein private Kommunikation und nicht um die Sicherheitsbereiche geht) gegen die Datenschutzrichtlinie verstößt, sofern die konkrete Datenübermittlung nicht die Ausnahmevoraussetzungen von Art. 26 Abs. 1/Abs. 2 bzw. § 4c Abs. 1, Abs. 2 BDSG erfüllt. Jede Stelle, die mit einem Unternehmen in den USA kommuniziert und Informationen über eine bestimmte oder bestimmbare natürliche Person übermittelt, verstößt sowohl gegen das BDSG als auch gegen die Richtlinie. Die Kontrollstellen können und müssen (in schweren Fällen) einschreiten, sofern nicht eine Genehmigung der Aufsichtsbehörde, eine Vereinbarung nach den Standardvertragsklauseln oder eine der sechs Ausnahmen des § 4c Abs. 1 BDSG vorliegt (Einwilligung; Vertragserfüllung bezogen auf Daten der Vertragspartner bzw. bezogen auf Daten eines Dritten, sofern der Vertrag in seinem Interesse liegt; Wahrung wichtiger öffentlicher Interessen; Wahrung lebenswichtiger Interessen des Betroffen; öffentlich zugängliche Daten). Dieser wirtschaftlich unbefriedigende Zustand kann nur auf drei Wegen gelöst werden. Der erste Weg wäre, die Datenschutzrichtlinie zu ändern und die Anforderungen an den Datenverkehr in Drittstaaten abzusenken. Das wäre ein unfreundlicher Akt gegenüber dem EuGH und liefe dem Sinn des Datenschutzes gem. Art. 8 GRCh zuwider. Die zweite Möglichkeit bestünde darin, dass mit den Unternehmen Datenschutzverträge geschlossen werden, die von den Aufsichtsbehörden gem. § 4c Abs. 2 BDSG genehmigt werden. Der dritte Weg wäre, eine Vereinbarung mit den USA auf völkerrechtlichem Weg zu treffen, die den Zugriff der Sicherheitsbehörden der USA auf diese übermittelten Daten hinreichend klar regelt. Das dürfte der realistische Weg sein, birgt aber ein sehr hohes Risiko im Falle eines Scheiterns: Der EuGH würde europäische Unternehmen mit Vertragsbeziehungen in den USA großteils in die Illegalität treiben, weil nicht davon auszu-

gehen ist, dass diese ihre Geschäftsbeziehungen sofort abbrechen und noch laufende Verträgen kündigen können, allein weil dort eine Übermittlung personenbezogener Daten vorgesehen ist. Die Annahme, die sechs Ausnahmegründe des § 4c Abs. 1 BDSG würden den gegenwärtigen Datenverkehr abdecken, ist nicht nahe liegend.

III. Der EuGH fordert ein Klagerecht für die Kontrollstellen. Wie dieses aussehen soll, sagt er nicht. Das ist schade. Den nationalen Gesetzgeber stellt das vor große Herausforderungen. Unterstellen wir einmal, Facebook hätte seine europäischen Server im Freistaat Bayern aufgestellt, weil es dort besonders schön ist, und das Bayerische Landesamt für Datenschutzaufsicht hielte – noch vor der EuGH-Entscheidung Schrems – die Entscheidung der Kommission zu Safe Harbor für unvereinbar mit der Datenschutzrichtlinie. Welcher Rechtsschutz müsste dem Landesamt in diesem Fall offen stehen, um die Entscheidung vom EuGH prüfen lassen zu können? Gegen wen, soll die Kontrollstelle klagen? Gegen die Kommission kann sie vor nationalen Gerichten nicht vorgehen, als Klagegegner käme deshalb nur Facebook in Deutschland in Betracht. Gegen das Unternehmen zu klagen, wäre aber nicht glücklich, weil das Unternehmen in diesem Fall die Entscheidung der Kommission verteidigen müsste. Denkbar wäre ein objektives Klageerzwingungsverfahren, zuständig wäre der Bund (Art. 74 Abs. 1 Nr. 1 GG). Solange der Bund untätig ist, könnte wohl auch ein Landesgesetzgeber so frech sein, ein Klagerecht durch Gesetz einzuführen. Zwar hat der Bund deutlich gemacht, ein solches Klagerecht nicht einräumen zu wollen, was die Gesetzgebung des Länder gem. Art. 72 Abs. 1 GG unter normalen Bedingungen sperrt. Hier dürfte die Sperre aber wertungsmäßig nicht greifen, weil die Weigerung des Bundes wegen Verstoßes gegen Art. 28 Abs. 3 Spiegelstrich 3 DSRL aufgrund des Anwendungsvorrangs des Unionsrechts unbeachtlich sein dürfte.

IV. Die Entscheidung des EuGH ist sehr gestalterisch. Wie bei rechtsgestaltenden Entscheidungen üblich, wirft das eine ganze Reihe von Fragen auf, die nicht eindeutig zu beantworten sind. Zu nennen sind etwa folgende Unklarheiten: Das Urteil leitet sorgfältig her, dass die Kontrollstellen die Angemessenheit des Datenschutzniveaus trotz einer Entscheidung der Kommission selbstständig prüfen dürfen. Beschränkt sich die Lockerung der Bindung an die Kommissionsentscheidung nur auf ein Prüfrecht oder dürfen die Kontrollstellen (Aufsichtsbehörden) auch bei existenter Entscheidung der Kommission Aufsichtsmaßnahmen gem. Art. 28 Abs. 3 Spiegelstrich 1 und 2 DSRL erlassen und etwa Datenexporte im Einzelfall untersagen? Gelten die Maßgaben des EuGH nur für Entscheidungen über die Angemessenheit gem. Art. 25 Abs. 2 DSRL oder auch dann, wenn die Kommission Standardvertragsklauseln gem. Art. 26 Abs. 4 Datenschutzrichtlinie erlässt? Inwieweit hat der EuGH über US-amerikanische Eingriffsbefugnisse der Sicherheitsbehörden entschieden und inwieweit beschränken sich die Ausführungen auf die konkrete Entscheidung der Kommission? Wie ist das Ineinandergreifen des Grundrechtsschutzes und der Datenschutzrichtlinie dogmatisch zu lösen?
Zusammenfassend lässt sich festhalten: Es handelt sich um eine Grundsatzentscheidung, die in der Rechtspraxis von enormer Bedeutung ist, Druck im Verhältnis Europas zu den USA erzeugt, die Kontrollstellen (Aufsichtsbehörden) und den Datenschutz stärkt und von einem bewundernswerten Selbstbewusstsein des EuGH zeugt. Dogmatisch regt das Urteil zum Denken an, so ganz schlecht ist das ja nicht. Viele Dinge werden allerdings durch Folgeentscheidungen noch zu klären sein.

Frankfurter Institut für das Recht der Europäischen Union
fireu@euroap-uni.de
http://www.fireu.de