Der nur scheinbar sichere Hafen – Arbeitsrechtliche Folgen der aktuellen EuGH-Entscheidung zu „Safe-Harbor“

EINFÜHRUNG

Mit einer bedeutenden und weitreichenden Entscheidung hat der Europäische Gerichtshof (EuGH) heute, am 06. Oktober 2015 bestehende Regelungen zum Austausch von personenbezogenen Daten zwischen der EU und den USA für ungültig erklärt. Neben zu erwartenden Auswirkungen auf die derzeit laufenden Gespräche zwischen der EU und den USA über ein neues transatlantisches Datenschutzabkommen und die ebenfalls schwebenden Verhandlungen über das Freihandelsabkommen TTIP hat diese Entscheidung weitreichende rechtliche Konsequenzen für die Übermittlung personenbezogener Daten in die USA. Die Konsequenzen betreffen auch den Bereich des Arbeitsrechts bzw. den Umgang von Unternehmen mit personenbezogenen Daten ihrer Arbeitnehmer.

EUGH, URTEIL VOM 06.10.2015, RECHTSSACHE C-362/14

Die Entscheidung erging in der Rechtssache C-362/14, in der sich der österreichische Jurist Maximilian Schrems als Nutzer von Facebook gegen den Umgang dieses Unternehmens mit seinen Daten zur Wehr gesetzt hat. Die Daten europäischer Facebook-Nutzer werden im Allgemeinen von der für Europa verantwortlichen irischen Facebook-Tochtergesellschaft jedenfalls zum Teil auch auf Servern in den USA gespeichert. Genau hiergegen hatte der Kläger zunächst bei den irischen Datenschutzbehörden Beschwerde eingelegt und dabei die Auffassung vertreten, dass Recht und Praxis in den USA - gerade vor dem Hintergrund der von Edward Snowden enthüllten Tätigkeiten der Nachrichtendienste der USA - keinen ausreichenden Schutz seiner in die USA übermittelten Daten gewährleisteten und seine persönlichen Daten dort nicht ausreichend vor staatlichem Zugriff geschützt seien.

Die irische Datenschutzbehörde hat die Beschwerde zunächst unter Hinweis darauf zurückgewiesen, dass die Europäische Kommission in ihrer sog. „Safe-Harbor“-Entscheidung vom 26. Juli 2000 das von den USA gewährleistete Datenschutzniveau als angemessen eingestuft habe und entsprechend die Datenübermittlung in die USA nicht zu beanstanden sei. Gegen diese behördliche Entscheidung klagte Herr Schrems vor einem irischen Gericht, welches wiederum die Angelegenheit dem Europäischen Gerichtshof zur Entscheidung vorlegte.

SCHLUSSANTRÄGE DES GENERALANWALTS

Bereits im September 2015 hat daraufhin der am EuGH tätige Generalanwalt Yves Bot im Rahmen seiner Schlussanträge auf die europäische Datenschutzrichtlinie (Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995) hingewiesen und betont, dass diese Richtlinie die Übermittlung personenbezogener Daten von EU-Bürgern in ein Drittland nur unter der Voraussetzung zulasse, dass das Drittland ein angemessenes Datenschutzniveau biete. Er hat weiterhin darauf hingewiesen, dass die Europäische Kommission nach der Datenschutzrichtlinie zwar allgemein feststellen könne, dass ein bestimmtes Drittland ein im Sinne der Richtlinie angemessenes Schutzniveau bietet (vgl. Art. 25 Abs. 6 der Richtlinie).

Entgegen der Einschätzung der Kommission aus dem Jahr 2000 ging er allerdings davon aus, dass Recht und Praxis in den USA gerade kein den europäischen Standards genügendes Schutzniveau bieten. Insbesondere der Zugang der amerikanischen Nachrichtendienste zu den übermittelten Daten stelle einen unzulässigen Eingriff in Rechte europäischer Bürger dar. Recht und Praxis der Vereinigten Staaten ließen es insbesondere zu, dass personenbezogene Daten von Unionsbürgern in großem Umfang gesammelt würden, ohne dass ein wirksamer gerichtlicher Schutz hiergegen gewährleistet sei. Hieraus hat er weiter geschlossen, dass die „Safe-Harbor“-Entscheidung der Kommission aus dem Jahr 2000 ungültig ist und im Übrigen die Existenz einer solchen Entscheidung der Kommission die Kontrollbefugnisse nationaler Datenschutzbehörden weder beseitigt noch einschränkt.

Wie in der Praxis durchaus üblich, hat sich nun der Europäische Gerichtshof der Auffassung des Generalanwalts angeschlossen, in der US-amerikanischen Praxis ebenfalls eine Verletzung europäischer Grundrechte gesehen und letztlich die „Safe-Harbor“-Entscheidung der Kommission als unwirksam bewertet.

FOLGEN DER ENTSCHEIDUNG

Das Urteil des EuGH richtet sich sowohl gegen die US-amerikanische Praxis zum Umgang mit Daten von Bürgern der EU als auch gegen die „Safe-Harbor“-Entscheidung der Kommission und das Verhalten der irischen Datenschutzbehörde, welche sich ihrer Verantwortung nach Auffassung des EuGH durch den schlichten Hinweis auf die „Safe-Harbor“-Grundsätze entzogen hat.

Die Entscheidung ist von großer Bedeutung: Wichtig ist zunächst, dass sie keineswegs nur Facebook und das Verhältnis dieses Unternehmens zu den irischen Datenschutzbehörden betrifft. Die aufgestellten Grundsätze sind vielmehr für sämtliche nationalen Datenschutzbehörden der EU und auch für sämtliche Unternehmen relevant, die Daten europäischer Bürger – gleich ob als Kunde, Nutzer oder z.B. eben auch als Arbeitnehmer – in die USA übermitteln. International tätige Unternehmen, die bisher auf diese Weise Nutzer- oder Kundendaten in die USA übermittelt haben,

werden als Folge der Entscheidung vielfach vor der Herausforderung stehen, neue Wege für eine rechtskonforme, transatlantische Datenübermittlung zu finden.

ARBEITSRECHTLICHE FOLGEN

Gerade auch aus arbeitsrechtlicher Sicht muss die Entscheidung Anlass für eine kritische Überprüfung des Umgangs mit Daten im Unternehmen sein. In international tätigen, US-amerikanischen Konzernen findet häufig und in sehr unterschiedlichen Zusammenhängen eine Übermittlung personenbezogener Arbeitnehmerdaten zur Muttergesellschaft in das Hoheitsgebiet der Vereinigten Staaten statt (z. B. zum Zweck einer konzernweit einheitlichen Personaldatenverwaltung). Darüber hinaus arbeiten nicht nur internationale, sondern auch nationale Unternehmen in der Praxis regelmäßig mit externen Providern zusammen, die ihrerseits arbeitnehmerbezogene Daten ihrer Kunden auf im Ausland und eben auch in den USA befindlichen Servern speichern, so etwa beim Betrieb von IT-Systemen durch externe Provider einschließlich der Nutzung eines global einheitlichen Technik-Supports in den USA oder einer Datenspeicherung durch weitere Provider in der sog. „Cloud“ auf in den USA befindlichen Servern.

Aus arbeitsrechtlicher Sicht besteht die Aufgabe nun darin, etwa getroffene Betriebsvereinbarungen zur Datenverarbeitung, geschlossene Vereinbarungen mit verbundenen Konzernunternehmen oder mit externen Providern (z. B. über eine Auftragsdatenverarbeitung oder sonstige sog. „Service-Level-Agreements“) sowie ggf. auch individualvertragliche Einwilligungen in die Übermittlung von Daten in die USA auf ihre Vereinbarkeit mit dem geänderten Rahmenbedingungen zu prüfen und nötigenfalls alternative Lösungen zu finden.

Hierbei ist zu beachten, dass sich die Zulässigkeit der Datenübermittlung in sog. Drittstaaten außerhalb der EU im Grundsatz nach einem zweistufigen Verfahren bestimmt: Neben einer Vereinbarkeit mit nationalen Datenschutzvorschriften (vgl. §§ 4, 28, 32 BDSG, „erste Stufe“) müssen insoweit auch die besonderen Anforderungen bzgl. des Datentransfers in Drittstaaten eingehalten werden (vgl. §§ 4b, 4c BDSG, „zweite Stufe“). Während die erste Stufe durch die Entscheidung des EuGH jedenfalls nicht unmittelbar berührt wird, wird ein einfacher Verweis auf eine „Safe-Harbor“-Zertifizierung des an dem Datentransfer beteiligten Dritten künftig nicht mehr ausreichen, um auch die besonderen Anforderungen eines Datentransfers in Drittstaaten auf der zweiten Stufe zu erfüllen. Alternative Rechtsgrundlagen für einen Datentransfer können in diesen Fällen etwa Binding Corporate Rules oder die Verwendung der EU-Standardvertragsklauseln sein, die auch in der Vergangenheit schon bei Datentransfers in Drittstaaten außerhalb der EU zur Anwendung kamen.

Abhängig vom konkreten Einzelfall kann es dann auch notwendig sein, die zuständige Aufsichtsbehörde des für das jeweilige Bundesland zuständigen Landesdatenschutzbeauftragten in ein ggf. erforderliches Genehmigungsverfahren einzubeziehen. Nach der jüngsten Entscheidung des EuGH und der dadurch entstandenen Rechtsunsicherheit ist jedenfalls auch mit Spannung zu erwarten, wie sich insbesondere die deutschen Aufsichtsbehörden in nächster Zeit zu diesem Thema positionieren werden.

ANSPRECHPARTNER

Dr. Henning Reitz
h.reitz@justem.de

Dr. Daniel Klösel
d.kloesel@justem.de

www.justem.de