Ing.MMag. Michael A. Gütlbauer, Rechtsanwalt und Partner bei Gütlbauer Sieghartsleitner Pichlmair Rechtsanwälte, Wels

Datenschutz: „Safe Harbor“ ungültig

Am 06.10.2015 wurde vom EuGH das mit großem Interesse erwartete Urteil in der Rechtssache des österreichischen Datenschutz-Aktivisten Mag. Maximillian Schrems gegen den irischen Datenschutzbeauftragten veröffentlicht. Wie erwartet urteilte der EuGH, dass personenbezogene Daten in den USA nicht ausreichend vor dem Zugriff von Behörden geschützt seien. Der folgende Beitrag gibt einen kurzen Überblick über das der Entscheidung zugrunde liegende Verfahren, einige der Entscheidungsgründe, sowie Folgen und Handlungshinweise für Unternehmer, die Daten auch extern speichern.

1. Ausgangssachverhalt

Maximillian Schrems wandte sich an die irische Datenschutzbehörde mit der Beschwerde, das von ihm genutzte soziale Netzwerk Facebook würde ihn betreffende personenbezogene Daten in die USA übermitteln und nicht entsprechend den europäischen Datenschutzbestimmungen hinreichend (vor Zugriff durch US-amerikanische Geheimdienste) schützen.

Die irische Datenschutzbehörde war in diesem Fall deswegen zuständig, da Benutzer des sozialen Netzwerks Facebook mit Wohnsitz außerhalb der USA und Kanada einen Vertrag nicht mit dem Betreiber des Netzwerks selbst, Facebook Inc mit Sitz in Menlo Park, Kalifornien, (kurz Facebook USA) sondern dessen Tochterunternehmen Facebook Ltd mit Sitz in Dublin, Irland, (kurz: Facebook Irland) abschließt.

Mit seiner Beschwerde will Maximillian Schrems erreichen, dass Facebook Irland jeglicher Transfer von (ihn betreffende) personenbezogenen Daten in die USA untersagt wird. Sofern sich die Unrechtmäßigkeit der bisherigen Datenüberlassung ergeben sollte, müsste Facebook Irland dies für alle seine „Kunden" berücksichtigen, um zu vermeiden, dass auch diese Ansprüche auf Unterlassung geltend machen und allenfalls auch eine Geldstrafe wegen Verstoß gegen den Datenschutz verhängt wird. Ob das soziale Netzwerk Facebook diesfalls überhaupt in seiner aktuellen Form weiter betrieben werden könnte, ist unklar. Die wirtschaftlichen Folgen für beide Facebook-Unternehmen sind nicht absehbar (siehe http://heise.de/-2844968).

Vergleichbare Folgen können jedem Unternehmen drohen, das sich externen Dienstleistern zur Datenverarbeitung bedient (zB Datenspeicherung in der Cloud für Zwecke des Datenaustausches von Mitarbeitern, Nutzung web-basierter Anwendungen, etc).

Nach den Behauptungen von Maximillian Schrems wird der Betrieb des sozialen Netzwerks Facebook durch mehrere Rechenzentren weltweit, unter anderem in den USA aufrechterhalten, welche zumindest auch von Facebook USA betrieben werden würden. Facebook Irland überlasse im Rahmen einer Vertragsbeziehung mit Facebook USA personenbezogene Daten in die USA zur Speicherung und Verarbeitung. Als US-amerikanisches Unternehmen sei Facebook USA aufgrund US-amerikanischer Vorschriften (Stichworte: „Patriot Act", „Freedom Act", „FISA") verpflichtet, in bestimmten Fällen Daten an US-amerikanische Behörden herauszugeben, zumal ohne Verständigung der Betroffenen und ohne dass die Betroffenen sich gegen derartige Maßnahmen vor einer Behörde oder einem Gericht zur Wehr setzen könnten.

2. Entscheidung der irischen Datenschutzbehörde auf Basis von Safe-Harbor

Die irische Datenschutzbehörde erachtete die Beschwerde von Maximillian Schrems als nicht begründet, da eine Überlassung von Daten in Drittstaaten (Nicht-EU/EWR) dann zulässig sei, wenn in den Ziel-Ländern ein zumindest gleichwertiges Datenschutzniveau bestehe. Die Überlassung von personenbezogenen Daten zur Verarbeitung im Rahmen eines Auftrages (sog „Auftragsdatenverarbeitung") an Dienstleister innerhalb von EU/EWR ist ohne besondere Genehmigung zulässig, da aufgrund der Harmonisierung des Datenschutzrechts durch die sog „Datenschutzrichtlinie" (RL 95/46/EG) von einem angemessenen Datenschutzniveau ausgegangen werden kann. Sofern jedoch personenbezogene Daten in Drittstaaten zu übermittelt werden sollen, ist (auch) nach österreichischer Rechtslage die Genehmigung der Datenschutzbehörde einzuholen.

Um für die Überlassung oder Übermittlung von Daten an US-amerikanische Unternehmen dieses Procedere zu vereinfachen, wurde zwischen der EU und den USA das sogenannte Safe-Harbor-Rahmenwerk ausgehandelt (http://www.export.gov/safeharbor/index.asp). US-amerikanische Unternehmen hatten die Möglichkeit, sich freiwillig den Regeln dieses Rahmenwerks zu unterwerfen (Liste der teilnehmenden Unternehmen: https://safeharbor.export.gov/list.aspx). Aufgrund der gemeinsamen Festlegung des Inhaltes dieses Rahmenwerks erging die Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000, wonach für solche Unternehmen ein Datenschutzniveau als gegeben anzunehmen sei, welches dem europäischen Niveau entspricht. Aufgrund dessen war – so die bisherige Rechtslage – keine Einzelgenehmigung notwendig.

Aufgrund dieser Entscheidung der EU-Kommission war aus Sicht der irischen Datenschutzbehörde eine inhaltliche Prüfung der Beschwerde von Maximillian Schrems nicht notwendig, wenn nicht sogar unmöglich. Die Entscheidung der EU-Kommission wurde für bindend angesehen. Gegen diese Entscheidung erhob Maximillian Schrems Rechtmittel an den irischen High Court, welcher ua diese Frage dem EuGH zur Entscheidung vorlegte.

3. Die Entscheidung des EuGH

Der EuGH entschied in seinem Urteil vom 6.10.2015 zu C-362/14 (http://curia.europa.eu/juris/documents.jsf?num=C-362/14), dass dieser **Automatismus rechtswidrig** sei. Auch wenn daher US-amerikanische Unternehmen sich dem Safe-Harbor-Rahmenwerk unterwarfen, ist **im Einzelfall** von der jeweils zuständigen Datenschutzbehörde eine **Prüfung vorzunehmen, ob die übermittelten personenbezogenen Daten hinreichend geschützt sind**.

Vom EuGH wurde nicht entschieden, ob die Datenübermittlung im konkreten Fall von Facebook Irland an Facebook USA zulässig war und ist. Es wurde „lediglich“ die Entscheidung der EU-Kommission mangels Kompetenz zur Einschränkung der Prüfungsbefugnis der nationalen Datenschutzbehörden für ungültig erklärt und die einschlägigen Bestimmungen der Datenschutzrichtlinie dahingehend interpretiert, dass eine Einzelfallprüfung aufgrund einer Beschwerde möglich sei. Es wird nun an den irischen Behörden liegen, den Einzelfall anhand der Beschwerdepunkte von Maximillian Schrems zu prüfen.

Der EuGH weist weiters darauf hin, dass die Unterwerfung des Auftragsdatenverarbeiters unter das Safe-Harbor-Rahmenwerk alleine nicht ausreichend sei, um ein Datenschutzniveau vergleichbar mit jenem in der EU zu gewährleisten. Dies deswegen, da US-amerikanische Behörden an dieses Rahmenwerk nicht gebunden seien, diese daher weder dessen Regeln noch jene der Charta der Grundrechte der Europäischen Union (kurz GRC) zu beachten hätten (insbesondere Recht auf Datenschutz, Achtung des Privatlebens und auf wirksame Beschwerde gegen Eingriffe in diese Rechte vor einem Gericht). US-Behörden sei nach US-amerikanischen Vorschriften Zugriff auf Daten

zu gewähren, wobei die erwähnten Grundrechte in einer mit EU-Recht nicht vereinbaren Weise verletzt werden könnten und sich der Betroffene dagegen nicht wirksam zur Wehr setzen könne.

4. Folgen der Entscheidung und Auswirkungen für die Praxis

4.1. Aufgrund dieser Beurteilung sind auch allfällige Einzelvereinbarungen zwischen europäischen und ausländischen Unternehmen dahingehend zu prüfen, ob trotz entsprechender Vereinbarungen ausländische Behörden Zugriff auf die übermittelten Daten erreichen können, ohne dass die für derartige staatliche Zugriffe in der EU geltenden Beschränkungen einzuhalten sind. **Sofern ausländische Vorschriften den Zugriff auf die Daten weitergehend ermöglichen als dies die EU-Datenschutzregelungen vorsehen, wäre eine Überlassung oder Übermittlung wohl unzulässig.** Dies betrifft auch sogenannte corporate binding rules (CBR), sohin konzerninterne Vereinbarungen zum konzerninternen Datenaustausch, oder sonstige privatrechtliche Vereinbarung da auch an diese nur die daran teilnehmenden Vertragspartner, nicht aber Dritte (zB staatliche Behörden) gebunden sind.

Der Vollständigkeit halber sei ausdrücklich darauf hingewiesen, dass auch die Übermittlung von Daten in eine Cloud eine genehmigungspflichtige Datenübermittlung darstellen kann, sofern auch nur einer der an der Cloud beteiligten Dienstleister oder Zugriffsberechtigter, US-amerikanischen Regelungen unterliegt und/oder der Datenspeicherort (Rechenzentrum) außerhalb der EU liegt.

In diesem Zusammenhang findet seit einigen Monaten ein Verfahren Beachtung, in dem sich Microsoft (USA) vor US-Gerichten zu Wehr setzt gegen einen Auftrag zur Herausgabe von Daten eines Kunden, welche in einem Rechenzentrum in Irland gespeichert sind (http://heise.de/-2809638). Nach der Argumentation der US-Regierung in diesem Verfahren ändert der Umstand, dass sich der jeweilige Datenspeicherort (Rechenzentrum) physisch auf EU-Territorium befindet, weder etwas am faktischen Zugriff des Dienstleisters, noch an dessen Verpflichtung nach US-amerikanischen Bestimmungen auf Herausgabe der Daten (an US-amerikanische Behörden). Von Microsoft und zahlreichen anderen Unternehmen wurde die Bedeutung des Ausgangs dieses Verfahrens für die Zusammenarbeit zwischen EU- und US-Unternehmen im IT-Bereich erkannt und hat sich eine breite Unterstützungsfront für Microsoft gebildet.

Es darf mit Spannung erwartet werden, welche Nachwirkungen die nunmehr vorliegende Entscheidung des EuGH nach sich ziehen wird, gerade auch im Hinblick auf die laufenden Auseinandersetzungen über die Befugnisse ausländischer Behörden.

4.2. Für die Praxis bedeutet die Abschaffung des Safe-Harbor-Automatismus, dass gerade kleinere und mittlere Unternehmen, welche keine individuellen Datenschutzregelungen mit US-amerikanischen Dienstleistern abgeschlossen haben, sondern sich auf das Safe-Harbor-Rahmenwerk verlassen

mussten, nunmehr entweder um nachträgliche Genehmigung der Datenübertragung ansuchen oder aber die Übermittlung einzustellen und für die „Zurückholung“ (allenfalls Löschung) der bereits übermittelten Daten Sorge tragen müssen. Einige US-amerikanische Dienstleister haben bereits angekündigt und teilweise sogar schon begonnen, Datenspeicherorte aus den USA in die EU „zu verlegen“.

In jedem Fall sollte die letztgültige Fassung der Vereinbarung mit dem/den Dienstleister(n) einer rechtlichen Prüfung unterzogen werden, insbesondere welchen nationalen Regelungen diese (und allenfalls deren Subdienstleister) unterliegen. Es sollte gegebenenfalls die Möglichkeit der „Datenrückholung“ in die EU/EWR überprüft werden und allenfalls ob ein Ausweichen auf Dienstleister, welche ausschließlich EU-Regelungen unterliegen möglich ist.

4.3. Je nach technischer Umsetzbarkeit kann die Vermeidung der Übermittlung personenbezogener Daten (zB durch Verschlüsselung vor Übermittlung) eine Möglichkeit sein, viele Probleme des Datenschutzes zu lösen. Wenn Dritte keinen Zugriff auf die Klardaten haben, stellen sich insoweit (!) keine datenschutzrechtlichen Fragen mehr.

Die Entscheidung des EuGH hat weiters zur Rechtsunsicherheit dahingehend geführt, dass nicht völlig klar ist, unter welchen Voraussetzungen überhaupt die Übermittlung personenbezogener Daten in Drittstaaten oder bloß an ausländische Unternehmen mit Datenspeicherort in der EU/EWR zulässig sein soll (siehe http://heise.de/-2844968). Es ist zu erwarten, dass die nationalen Datenschutzbehörden in den kommenden Wochen sich mit diesen Fragen beschäftigen und wohl auch Hinweise zu rechtskonformen Verhalten veröffentlichen werden (siehe https://www.dsb.gv.at/site/6218/default.aspx). ●

Impressum

Herausgeber, Medieninhaber: derunternehmer.at OG, Edisonstraße 10, 4600 Wels, FN 232043s LG Wels, office@derunternehmer.at. Unternehmensgegenstand ist die Vermittlung von Rechtsinformationen für Unternehmer und Führungskräfte über das Internet. Geschäftsführende Gesellschafter, Redaktion: Dr. Michael Pichlmair (50 %), Thomas Pichlmair (50 %). Grundlegende Richtung: Unabhängige juristische Zeitung für Unternehmer und Führungskräfte. Die Zeitung erscheint viermal im Kalenderjahr. Preis des Jahresabonnements: EUR 96,00 exkl. 20% USt; Preisänderungen vorbehalten; UID ATU56759458. Bankverbindung: Allgemeine Sparkasse OÖ Bank AG (IBAN AT552032020000015685, BIC ASPKAT2L). Graphisches Konzept: Dr. Michael Pichlmair. Das Abonnement verlängert sich automatisch um ein Jahr, sofern es nicht von einem Rechtsanwalt oder sonstigen Kooperationspartner kostenlos und unverbindlich zur Verfügung gestellt wird und wenn es nicht unter Einhaltung einer einmonatigen Kündigungsfrist schriftlich (auch E-Mail) zum Ende eines Vertragsjahres gekündigt wird. Reklamationen die Übermittlung betreffend, werden nur innerhalb von 4 Wochen nach Versand akzeptiert.