Das Ende des transatlantischen Datentransfers?

Der Europäische Gerichtshof (EuGH) stellt fest: „Safe Harbor“ ist ungültig

Am 6. Oktober 2015 hat der EuGH in der Rechtssache C-362/14, Maximillian Schrems gegen Data Protection Commissioner (irischer Datenschutzbeauftragter), sein Urteil verkündet. In der als „Facebook-Urteil“ bekannten Entscheidung geht es zum einen um die Frage, ob der irische Datenschutzbeauftragte einer Beschwerde des österreichischen Jungjuristen und Facebooknutzers Schrems nachzugehen hatte.

Schrems hatte den Datenschutzbeauftragten aufgefordert, im Lichte der gesetzlichen europäischen Datenschutzvorgaben zu prüfen, ob die Weiterleitung und der Transfer der von Facebook in Irland gespeicherten Daten seiner europäischen Nutzer in die USA rechtens sei.

Der Dreh- und Angelpunkt der Entscheidung ist die Frage, ob das sogenannte „Safe- Harbor-Abkommen“, so wie es der irische Datenschutzbeauftragte meinte, eine solche Prüfung überflüssig macht, da Facebook als entsprechend gelistetes amerikanisches Unternehmen, durch dieses Abkommen privilegiert und damit eine datenschutzrechtliche Prüfung obsolet sei.

ZUR ENTSCHEIDUNG

Das Gericht folgt in seinem Urteil der Einschätzung des Generalanwalts beim EuGH, Bot, und erachtet „Safe Harbor“, gerade auch im Lichte der Enthüllungen Edward Snowdens zu den Praktiken und Machtbefugnissen der amerikanischen Geheimdienste, für ungültig.

Es stellt fest, dass angesichts der Charta der Grundrechte der Europäischen Union (dortiger Artikel 8) sowie der europäischen Datenschutzrichtlinie, die Kommission der Europäischen Gemeinschaft nicht befugt war, mit ihrer Entscheidung vom 26.07.2000 (2000/520/EG), dem „Safe-Harbor-Abkommen“, zu unterstellen, US-amerikanische Unternehmen würden allein mit ihrem Beitritt zu diesem vom Handelsministerium der USA (FTC) konzipierten Abkommen, ein angemessenes Schutzniveau für übermittelte personenbezogene Daten gewährleisten.

Auch seien durch dieses Abkommen die Befugnisse der nationalen europäischen Datenschutzbehörden weder beseitigt noch auch nur beschränkt, so wie von der irischen Behörde angenommen.

Der Artikel 8 der Charta der Grundrechte der Europäischen Union lautet wörtlich:

Schutz personenbezogener Daten

1. Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
2. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
3. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Der Gerichtshof führt insoweit aus, der Wesensgehalt des Grundrechts auf Achtung des Privatlebens, wie auch der Wesensgehalt des Grundrechts auf wirksamen gerichtlichen Rechtsschutz, würden durch den umfassenden Zugriff der US-Behörden auf den Inhalt elektronischer Kommunikation und das Fehlen des Rechts für EU-Bürger auf gerichtlichen Einspruch gegen dieses Praxis verletzt.

REAKTIONEN AUF DAS URTEIL

Wie fast immer nach derart gewichtigen Entscheidungen des EuGH fallen die Bewertungen unterschiedlich aus. Sie reichen von der euphorischen Bewertung als „datenschutzrechtliche Sensation“, die der Datensammlungs und -überwachungswut US-amerikanischer Behörden eine Ende setze, bis zur Einschätzung der aktuellen EU-Kommission, dass sich im Ergebnis nichts daran geändert habe, dass der Datentransfer in die USA möglich und zulässig sei.

DIRK-MICHAEL MÜLOT
Sachverständigenbüro Mülot-Graf

Jahrgang 1959, Wirtschaftsinformatiker und seit 1999 Freier Sachverständiger in den Bereichen Datenschutz, Datensicherheit und IT-Forensik. Als Datenschutzbeauftragter, Datenschutzmanager und Datenschutzauditor ist er durch die TÜV-Rheinland Akademie zertifiziert.

FACHGEBIETE:

- Planung und Aufbau von Datenschutzmanagementsystemen, Auditierungen, Machbarkeitsstudien
- Ausbildung von Datenschutzbeauftragten (Fachkunde, Weiterbildung)
- Datenschutz in medizinischen Fachbereichen, Sozialeinrichtungen, Einrichtungen der Kirchen, Wirtschaftsprüfer- und Steuerberatungskanzleien, im Konzern (Wirtschaft / Industrie), im Verein und im Verband, Behördlicher Datenschutz

SPEZIAL-KOMPETENZEN:

- IT-Forensik (Wirtschaft und Ermittlungsbehörden)
- Datenschutz und „digitale Steuerprüfung“ (GdPdU)
- Datenschutz und digitale Archivierung
- Datenschutz und Arbeitsrecht
- Datenschutz in Einrichtungen der forensischen Psychiatrie
- Social Engineering

› www.muelot-graf.de

AUSWIRKUNGEN DES URTEILS

Allein angesichts der gut 5500 US-Unternehmen, die sich zur Einhaltung der Vorgaben von „Safe-Harbor“ verpflichtet haben (vgl. die Listung auf safeharbor.export.gov/list.aspx) wird deutlich, dass von dieser Thematik nicht nur die Big-Player (Facebook, Google, Microsoft, Amazone, pp.) betroffen sind. Richtig formuliert müsste es heißen, dass nicht nur die deutschen europäischen Unternehmen betroffen sind, die zu diesen Big-Playern Daten transferieren, sondern eine riesige Anzahl auch deutscher Unternehmen, die man eben nicht als große Konzerne, sondern als Klein- oder mittelständische Unternehmen bezeichnet und die mit diversen US-Firmen kooperieren (müssen).

Die großen Konzerne verfügen durchweg über gut aufgestellte eigne Rechtsabteilungen oder arbeiten mit versierten Anwaltsfirmen zusammen, die – soweit nicht schon längst geschehen – Alternativen für „Safe-Harbor“ entwickeln.

Alle betroffenen Unternehmen müssen auf der Hut sein und aktiv werden, auch wenn der Datentransfer in die USA auf der Grundlage von „Safe-Harbor“ jetzt nicht automatisch ungesetzlich geworden ist. So wie in dem Rechtsstreit die irische Datenschutzbehörde jetzt zur Einzelfallprüfung angehalten ist, so sind es auch die nationalen deutschen Datenschutzbehörden. Angesichts des Urteils dürfte es diesen Behörden faktisch und rechtlich aber unmöglich sein, entsprechende Datentransfers zu akzeptieren oder tolerieren.

Die Folgen können für betroffene Unternehmen dramatisch sein, denn hier kommen nicht nur die Bußgeld- und Strafvorschriften des Bundesdatenschutzgesetzes (BDSG) ins Spiel, sondern auch das Untersagen dieses Datentransfers durch die Datenschutzbehörde (vgl. § 38 Absatz 5 BDSG). Betroffene, also just jene Bürger, deren personenbezogene Daten bislang „via“ „Safe-Harbor“ von deutschen Unternehmen in die USA transferiert werden, können angesichts ihrer Rechte aus dem BDSG (§§ 33 ff. BDSG), die Datenschutzbehörden zusätzlich zu einem Eingreifen motivieren.

Der Hamburgische Beauftragte für Datenschutz und Informationssicherheit hat bereits am Tag der Urteilsverkündung u. a. wörtlich erklärt: „Bei der Umsetzung dieser Entscheidung werden die nationalen und europäischen Datenschutzbehörden künftig eine Schlüsselrolle einnehmen. Es ist zu prüfen, ob und inwieweit Datentransfers in die USA auszusetzen sind. Dies gilt auch, wenn sie auf anderer Rechtsgrundlage wie Standardvertragsklauseln, Einwilligung oder Binding Corporate Rules gestützt werden. Die Aufsichtsbehörden werden dafür noch in dieser Woche ihr Vorgehen auf nationaler und europäischer Ebene koordinieren.“

Lässt man die vom Gesetz in § 4c Abs. 1 BDSG zugelassenen Ausnahmen (u.a. Einwilligung des Betroffenen), bei deren Vorliegen ein Datentransfer in die USA weiterhin zulässig bleibt, angesichts der

Dirk-Michael Mülot | Freier Sachverständiger für Datenschutz und Datensicherheit
Kontakt *Telefon +49 (0)5248-8235430, Fax +49 (0)5248-8235431, E-Mail buero@muelot-graf.de*
Adresse *Stammsitz Büro Langenberg, Westfalenweg 2, 33449 Langenberg*
Website *www.muelot-graf.de*

geringen Relevanz außen vor, so könnten möglicherweise für einen rechtssicheren Transfer die Nutzung von Standvertragsklauseln oder die Formulierung/Vereinbarung von Binding Corporate Rules Alternativen (§ 4c Abs. 2 BDSG) sein.

Die EU-Kommission hat Standardvertragsklauseln veröffentlicht. Der Verwender ist allerdings gehalten, diese Vorlagen wortgetreu zu verwenden und umzusetzen. Änderungen bereits am Wortlaut führen zur Unwirksamkeit und somit zu einem unerlaubten Datentransfer mit den oben beschriebenen Folgen.

Die Formulierung von Binding Corporate Rules, sprich „verbindliche Unternehmensreglungen", als Möglichkeit dem Gesetz entsprechenden Persönlichkeitsschutz nachzuweisen, ist alles andere als ein einfaches Unterfangen. Allein von der „Artikel-29-Datenschutzgruppe", dem Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes, wurden zu diesem Thema zahlreiche Arbeitspapiere erarbeitet. Auf derartige Regelungen werden sich allenfalls große Konzerne stützen können, denn deren Erstellung ist sehr komplex und setzt umfangreiche qualifizierte rechtliche rechtliche Kenntnisse voraus.

RESÜMEE

Unternehmen, die personenbezogene Daten an US-amerikanische Unternehmen bislang auf der Grundlage von „Safe-Harbor" transferiert haben, müssen sich schleunigst Gedanken darüber machen, wie sie mit diesem Datentransfer zukünftig umgehen. Ansonsten ist die Gefahr sehr groß, dass Datenschutzbehörden diesen Transfer untersagen und ggf. mit einem Bußgeld belegen können.

Ob und in welcher Form die Ausnahmen des § 4c Absatz 1 und 2 BDSG (Einwilligung pp., Standardvertragsklauseln oder Binding Corporate Rules) „Safe-Harbor" ersetzen können, müssen betroffene Unternehmen unverzüglich prüfen bzw. prüfen lassen. Kein Unternehmensverantwortlicher wird sich zukünftig damit herausreden können, er habe die Notwendigkeit entsprechender Prüfungen und die Umsetzung entsprechender Maßnahmen nicht vorhersehen können.

Unternehmen, die Daten auslagern müssen oder wollen, aber nicht gezwungen sind personenbezogene Daten in die USA zu transferieren, weil sie z.B. als Tochter eines US-Unternehmens hierzu rechtlich, faktisch verpflichtet sind, sollten Ernsthaft über europäische, deutsche Alternativen für einen Datentransfer nachdenken (Stichworte: Deutsche Cloud, Trustet Cloud pp.).

Von neuen Verträgen und/oder Vorhaben ist sinnvollerweise erst einmal Abstand zu nehmen, bis sich die Folgen dieser Entscheidung in konkreten Handlungsweisen darstellen.