ECC-Rechtstipp

von RA Rolf Becker (rbecker@kanzlei-wbk.de)

Safe Harbor und die Folgen

Der Europäische Gerichtshof (EuGH) hatte die unter dem Stichwort „Sicherer Hafen / Safe Harbor“ bekannte Kommissionsentscheidung der EU-Kommission aus dem Jahr 2000 für ungültig erklärt (EuGH C-362/14 v. 6. Oktober 2015, Maximillian Schrems/ Data Protection Commissioner). Danach galt in Unternehmen in den USA, die sich den Prinzipien verpflichteten, abgestimmt mit den USA, ein angemessenes Datenschutzniveau. Grundlage bilden die Vorschriften der Artikel 25 und 26 der Europäischen Datenschutzrichtlinie, nach denen eine Datenübermittlung in Drittstaaten verboten ist, wenn deren Datenschutzniveau nicht mit dem der EU vergleichbar ist. Allerdings sind entsprechende Feststellungen der EU-Kommission möglich. Als sicher werden z. B. die Schweiz, Andorra, Kanada, Australien, Neuseeland, aber auch Israel, Argentinien und Uruguay angesehen. Die entsprechenden Feststellungen zu den USA wurden jetzt durch das Urteil gekippt.

Zeit bis Ende Januar 2016

Nach dem Urteil gaben die EU-Datenschutzbehörden (Art. 29 Gruppe) der Europäischen Kommission und der amerikanischen Regierung drei Monate Zeit, um bereits schwebende Verhandlungen zu Safe Harbor II abzuschließen.

Das Nach Ablauf der Frist Ende Januar 2016 drohen „alle nötigen und angebrachten Schritte“, um das Urteil des EuGH durchzusetzen. Das bedeutet Bußgelder und sonstige Maßnahmen auch gegen Unternehmen, die nach wie vor Daten ohne ausreichende rechtliche Grundlage in die USA übermitteln. Es geht zwar grundsätzlich nicht um den umgekehrten Weg, also die Nutzung von Daten, die US-Firmen liefern und die im europäischen Raum genutzt werden. Dennoch sind auch viele bekannte Services betroffen. Bis auf Hessen sehen fast alle nationalen Datenschutzbehörden z. B. schon die IP-Adresse als personenbezogenes Datum an. Das betrifft Werbe-Tracker und Social Plugins, bei denen weitaus mehr Daten die Grenzen überschreiten. Natürlich sind auch Public Cloud Lösungen oder hybride Ableger ebenso betroffen, wie andere Dienste, die auf einem Datenaustausch beruhen, wie z. B. E-Mail-Marketing-Services. Über den nachfolgenden Link lassen sich die Firmen ermitteln, die bislang Safe Harbor Prinzipien erfüllt haben und jetzt im Regen stehen: http://safeharbor.export.gov/list.aspx. Viele betroffene Unternehmen in der EU sollen ihre Verträge mit US-Anbietern bereits gekündigt haben.

Daher melden sich Unternehmen wie z. B. Microsoft und betonen, kein Kunde müsse Einschränkungen hinnehmen, wenn Dienste, wie Office 365, Azure Core Services oder Microsoft Intune verwendet werden. Dazu verweist man auf die EU-Standardvertragsklauseln nach Artikel 26, Abs. 2 der EU-Datenschutzrichtlinie von 1995 (EC 95/46). Die Verträge enthalten allerdings Klauseln, die US-Unternehmen eben angesichts der Macht der NSA und deren gesetzlich legitimierten Zugriffsmöglichkeiten eigentlich nicht einhalten können. Erst im April hätten die EU-Datenschutzbeauftragten die Nutzung der Standardverträge gebilligt. Doch sicher ist man sich der Argumentation nicht mehr und kündigt jetzt den Ausbau von Data-Center-Regionen in Großbritannien, den Niederlanden und Irland an. In Deutschland soll es um zwei Rechencentren in Frankfurt und bei Magdeburg gehen und um eine Datentreuhandlösung mit der Telekom. Danach werden Daten allein von der Telekom verwaltet und zwar so, dass die Unternehmen selbst nicht mehr ohne weiteres an diese Daten gelangen. Es geht dabei darum, die Daten dem Zugriff der US-Behörden zu entziehen. Apple wirbt mit Verschlüsselungen, die dem Unternehmen selbst den Zugriff verwehren.

Die Landesdatenschutzbehörde in Schleswig-Holstein (ULD) hat nämlich bereits Behörden und Unternehmen aufgefordert, sich dringend Alternativen zu überlegen. Dort sieht man die Standardvertragsklauseln nicht als ausreichend an. Es drohen Bußgelder bis zu 300.000 Euro (§ 43 Abs. 2 Nr. 1 BDSG). Bei der Behörde erwartet man offenbar kein schnelles Ende der schon länger laufenden Verhandlungen über eine Neufassung des Safe-Harbor-Abkommens. Auch der zweiten Möglichkeit, ein angemessenes Schutzniveau herzustellen, wird damit indirekt vom ULD schon jetzt eine Absage erteilt. Hier geht es um die sog. Binding Corporate Rules, an denen sich US-Unternehmen orientieren und sich selbst verpflichten, bestimmte Datenschutzniveaus einzuhalten. Allerdings dürfte das angesichts der Zugriffsmöglichkeiten der NSA auch auf diesem Weg nicht gelingen.

Noch keine unmittelbaren Maßnahmen

Unmittelbar scheinen Unternehmen noch nicht von Konsequenzen bedroht zu sein, aber das kann sich schon Anfang des nächsten Jahres schnell ändern. Die kommende EU-Datenschutzgrundverordnung, die eigentlich zum Dezember 2015 bereits ansteht und den neuen Rechtsrahmen im Datenschutz bilden soll, sieht jedenfalls das Marktortprinzip vor. US-Unternehmen müssten sich dann an EU-Recht halten, wenn nicht über TTIP-Abkommen neue Einfallstore geschaffen werden.

EU-Standardvertragsklauseln

Wer den Partner nicht wechseln kann oder will, sollte zumindest auf den Abschluss von Verträgen mit den EU-Standardvertragsklauseln drängen. Die EU-Kommission geht nämlich davon aus, dass dies noch möglich ist. Ansonsten kommt eine außerordentliche Kündigung eines Vertrages in Betracht. Den Weg über denkbare individuelle Einwilligungen der Betroffenen zu suchen, dürfte schwierig werden. Dann müsste man genau wissen, zu welcher Datenverarbeitung der Betroffene im Detail einwilligen soll. Auch in der Praxis ist die Einholung solcher Einwilligung vielfach nicht möglich bzw. sehr aufwändig.

Es wird noch dauern, bis man wieder rechtssicher mit US-Unternehmen Daten austauschen kann. Der Markt für eine wirklich gute Lösung ist noch offen.

Über den Autor

Rechtsanwalt Rolf Becker (www.rolfbecker.de) ist Partner der Rechtsanwälte WIENKE & BECKER (www.kanzlei-wbk.de) in Köln und Autor von Fachbüchern und Fachartikeln zum Wettbewerbsrecht, Markenrecht und Vertriebsrecht insbesondere im Fernabsatz. Als Mitglied im ECC-Club kommentiert Rechtsanwalt Becker für das ECC Köln regelmäßig aktuelle Urteile zum Online-Handel und gibt Händlern praktische Tipps, wie sie mit den gesetzlichen Vorgaben umgehen sollen.

RA Becker auf Twitter: http://twitter.com/rolfbecker

Er ist auch Autor auf den Informationsdiensten www.Versandhandelsrecht.de und www.fernabsatz-gesetz.de.

Dieser Rechtstipp ist Teil des Informationsangebots des E-Commerce-Center Köln (ECC Köln) an der IFH Institut für Handelsforschung GmbH, Köln.

Kontakt:

E-Commerce-Center Köln
c/o IFH Institut für Handelsforschung GmbH
Dürener Str. 401 b
50858 Köln
Telefon: +49 (0) 221 943607-70
Telefax: +49 (0) 221 943607-59

info@ecckoeln.de | www.ecckoeln.de und www.ifhkoeln.de

Erscheinungsdatum: November 2015