von **Daniel Huber**

Legale Datentransfers in die USA nach dem Safe Harbor-Urteil des EuGH

Im Oktober hat der EuGH durch seine sog. Safe Harbor-Entscheidung einen kleinen Aufschrei im E-Business provoziert. Was sind die Folgen des Urteils und wie können insbesondere Online-Händler von nun an Gefahren für den eigenen Betrieb abwenden? Akute praxistaugliche Handlungsmöglichkeiten gibt es nicht. Das ist gegenwärtig jedoch noch kein allzu großes Problem. Die IT-Recht Kanzlei gibt einen Überblick über die Lage und stellt mögliche Lösungen vor.

I. Den sicheren Hafen verlassen

Mit seiner Entscheidung vom **6. Oktober 2015 (Az.C-362/14)** hatte der Europäische Gerichtshof (EuGH) das sog. Safe Harbor-Abkommen zwischen den USA und der EU als Grundlage für den Transfers von personenbezogenen Daten in die USA für unwirksam erklärt. Das hat Auswirkungen für alle Unternehmen, die personenbezogene Daten von Kunden (oder Mitarbeitern) auf Servern in den USA speichern oder zumindest zeitweise auf diese übertragen - und das sind fast alle. Bereits bei der Verwendung von Social Media-Plugins, deren Server in den USA stehen, kann es zur Übertragung entsprechender personenbezogener Daten kommen.

Solche Datentransfers in die USA sind auf Grundlage des geltenden deutschen Bundesdatenschutzgesetzes (kurz: BDSG) an sich überhaupt nicht gestattet, weil die USA vom deutschen und vom europäischen Gesetzgeber mangels Wahrung eines gesetzlichen Mindest-Datenschutzniveaus grundsätzlich nicht als datensicherer Staat angesehen werden. Durch die Sicherung gewisser datenschutzrechtlicher Mindeststandards über das Safe Harbor-Abkommen wollten die EU und die USA im Jahr 2000 das Schutzniveau deshalb anheben, damit Übertragungen personenbezogener Daten in die USA zugelassen werden können. Nun hat der EuGH das Abkommen jedoch gekippt. Datenübertragungen auf Basis von Safe Harbor sind deshalb jedenfalls seit 1. Februar 2016 nicht mehr möglich.

Das hat Folgen für alle, die Kundendaten unmittelbar oder mittelbar auf US-amerikanischen Servern speichern. Im Folgenden ein Überblick über die rechtliche Problematik und über Lösungsmöglichkeiten für betroffene Online-Händler.

II. Das deutsche Datenschutzrecht

Personenbezogene Daten sind (zu Recht) ein hohes Gut. Einmal aus der Hand gegeben, kann der Betroffene nicht mehr kontrollieren, was mit seinen Daten geschieht. Bis hin zum Identitätsdiebstahl und damit verbundenen materiellen und immateriellen Schäden kann Vieles passieren. Daher hat der deutsche Gesetzgeber eine Schutzrolle eingenommen und das Bundesdatenschutzgesetz (kurz: BDSG) geschaffen, nach dem - grob gesagt - die Verwendung (Erhebung, Verarbeitung, Speicherung etc.) von personenbezogenen Daten nur dann erlaubt ist, wenn der Betroffene darin eingewilligt hat oder das Gesetz dies erlaubt (§ 4 Absatz 1 BDSG).

Da die Einholung einer Einwilligung des Betroffenen häufig mit großem Aufwand verbunden ist, da dieser über sämtliche Umstände eines Datentransfers möglichst umfassend im Vorfeld aufgeklärt werden muss, spielen die gesetzlichen Erlaubnistatbestände eine wichtige Rolle, bei der es keiner ausdrücklichen Einwilligung des Betroffenen bedarf. Besonders gefährdet sind personenbezogene Daten zudem dann, wenn sie außerhalb des Einflussbereichs des deutschen Gesetzgebers transferiert werden.

Datenübertragungen ins Ausland sind nach dem Bundesdatenschutzgesetz daher nur in eng umgrenzten Ausnahmefällen gestattet, grundsätzlich auch nur ins EU-Ausland oder in Staaten mit vergleichbarem Schutzniveau (§ 4b BDSG), allerdings gibt es hiervon wiederum spezielle Ausnahmen (§ 4c BDSG).

Die USA sind weder ein Mitgliedstaat der EU, noch bilden die dortigen Gesetze dasselbe Schutzniveau für Betroffene wie in Deutschland, so dass ein Datentransfer in die USA an sich von Gesetzes wegen nicht erlaubt ist. Hier setzte das zwischen der EU und den USA ausgehandelte Safe Harbor-Abkommen an, das dazu geführt hat, dass zumindest an diejenigen US-Unternehmen, die die Voraussetzungen aus dem Safe Harbor-Abkommen eingehalten haben, im Ergebnis Daten übertragen werden durften.

III. Was ist Safe Harbor?

Das Safe Harbor-Abkommen zwischen der EU und den USA aus dem Jahr 2000 sollte es Unternehmen aus der EU und damit auch aus Deutschland trotz des aus europäischer und deutscher Sicht mangelhaften US-amerikanischen Datenschutzniveaus ermöglichen, mit US-Unternehmen auch in Bezug auf den Transfer personenbezogener Daten möglichst eng zusammenzuarbeiten.

Gemäß dem Abkommen konnten US-amerikanische Unternehmen bis zum Urteil des EuGH sich selbst verpflichten, gewisse datenschutzrechtlichen Mindeststandards einzuhalten, auch wenn sie nach den für sie geltenden US-Gesetzen an sich nicht dazu verpflichtet wären, ein derart hohes Datenschutzniveau zu gewährleisten. Freiwillig sollten sich die Unternehmen dem Datenschutz-Niveau unterwerfen, das die EU als Mindeststandard ansieht. US-Unternehmen, die eine solche Selbstverpflichtung eingegangen sind, sah

die EU dann als "sichere Häfen" (deswegen: "Safe Harbor") für personenbezogene Daten von EU-Bürgern an.

Oberflächlich hat dieses System funktioniert; viele US-Unternehmen haben die Erklärung abgegeben, so dass formal gesehen der Transfer von personenbezogenen Daten an diese oder auf deren Server nach EU-Datenschutzrecht, und damit auch nach dem deutschen Datenschutzrecht, (zunächst) erlaubt war.

IV. Das EuGH-Urteil

Der EuGH hat das Safe Harbor-Abkommen nun jedoch im Oktober 2015 gekippt; ein Transfer personenbezogener Daten aufgrund des Safe Harbor-Abkommens ist nach der vom EuGH gesetzten Frist jedenfalls seit 1. Februar 2016 nicht mehr zulässig.
Hintergrund der EuGH-Entscheidung ist, dass die US-Unternehmen, an die ein Transfer personenbezogener Daten aus der EU heraus stattgefunden hat, zwar formal gesehen die nach dem Safe Harbor-Abkommen erforderliche Selbstverpflichtung abgegeben hatten, die darin aber akzeptierten Datenschutzstandards häufig tatsächlich gar nicht einhielten. Zudem gab es keinerlei Aufsichtsstelle, die die Einhaltung der Standards unabhängig von sonstiger Einflussnahme, wie der US-Nachrichtendienste, kontrolliert hätte. Die Rechte der EU-Bürger standen lediglich auf einem Blatt Papier, ohne dass sie wirklich etwas wert gewesen wären. Schließlich ist spätestens seit der NSA-Affäre klar, dass US-Unternehmen die bei ihnen gespeicherten personenbezogenen Daten von EU-Bürgern kaum vor fremdem Zugriff schützen können, selbst wenn sie wollten, da die NSA sowie andere Nachrichtendienste alleine schon aufgrund der Gesetzeslage in den USA rechtlich dazu in der Lage ist, die in den USA gespeicherten Daten auszuspähen.

V. Welche Datentransfers in die USA sind betroffen?

Betroffen sind letztlich alle Arten von Transfers von personenbezogenen Daten an US-Unternehmen oder auf Server in den USA, die bislang aufgrund des Safe Harbor-Abkommens rechtmäßig waren.

Davon erfasst werden etwa Geldzahlungen, die unter Einbeziehung vertraulicher Kontodaten über US-Server abgewickelt werden; Social Network-Dienstleistungen, die zumindest in Teilen über US-Server laufen, soweit sie personenbezogene Daten betreffen.

Auch mit US-Servern verbundene Plugins- oder Website-Analysetools, die personenbezogene Daten abfragen, übertragen und speichern, sind davon erfasst.

VI. Wie sollen sich Online-Händler nun verhalten?

Nachdem nun zum 1. Februar 2016 Transfers personenbezogener Daten aus Deutschland in die USA auf Grundlage des Safe Harbor-Abkommens nicht mehr möglich ist, stellt sich die Frage, wie Online-Händler von nun an personenbezogene Daten in rechtmäßiger Weise an US-Unternehmen und auf Server in den USA übertragen können. Auf diese Frage wissen selbst die obersten Datenschützer Deutschlands noch keine, zumindest keine einheitliche Antwort.

- Eine Möglichkeit ist und bleibt natürlich die informierte Einwilligung desjenigen, dessen personenbezogene Daten betroffen sind. Jemand, der umfassend über den künftigen Umgang mit seinen personenbezogenen informiert wird, kann nach deutschem (und sonstigen EU-)Datenschutzrecht entsprechende Datentransfers legalisieren. Der Haken an der Sache: Der Einwilligende muss im Vorfeld möglichst umfassend und klar darüber informiert werden, welche Stellen mit welchen seiner personenbezogenen Daten aus welchen Gründen und zu welchen Zwecken in Kontakt kommen. Nur wenn der Betroffene aufgrund einer breiten und umfassenden Informationsgrundlage bewusst in den Transfer seiner personenbezogenen Daten eingewilligt hat, legitimiert seine Einwilligung die entsprechenden Datentransfers. Ein versteckter Hinweis in AGB genügt hierfür nicht.
- Eine weitere Möglichkeit sind **sog. "Binding Corporate Rules"** (kurz: BCR). Dabei handelt es sich um aufwendige, unternehmensinterne Grundsätze zum unternehmensinternen Umgang mit personenbezogenen Daten, etwa von Kunden und Mitarbeitern, die zusammen mit Datenschutzbehörden erarbeitet werden und letztlich auch deren Kontrolle unterliegen. Für insbesondere kleinere und mittelgroße Online-Händler stellen BCR allerdings keine wirkliche Alternative dar, da sie nur unter größerem - auch finanziellem - Aufwand erarbeitet werden können und nicht akut in Kürze auf die Beine zu stellen sind.
- Schließlich können deutsche Online-Händler in ihre vertraglichen Beziehungen mit US-Unternehmen die datenschutzbezogenen sog. EU-Standardvertragsklauseln einbauen. Diese Klauseln hat die EU entwickelt, um einen bestimmten Mindeststandard des Datenschutzes für personenbezogene Daten zu formulieren. Allerdings leiden die Klauseln letztlich unter denselben Problemen, unter denen aus Sicht des EuGH auch das Safe Harbor-Abkommen krankt, so dass gegenwärtig unklar ist, ob Datenschutzvereinbarungen zwischen deutschen und US-Unternehmen unter Einbeziehung der EU-Standardvertragsklauseln vor dem Hintergrund des EuGH-Urteils überhaupt noch Bestand haben können. Zwar hat sich der EuGH in seinem Safe Harbor-Urteil diesbezüglich weder positiv noch negativ geäußert, jedoch sind auch die EU-Standardvertragsklauseln letztlich nur gute Vorsätze der sie einbeziehenden Unternehmen, die auf einem Papier stehen, ohne dass es eine Aufsichtsbehörde oder unabhängige Stelle gibt, die die Einhaltung der gemachten Versprechungen überprüft.

VII. Beschränkte Reaktionsmöglichkeiten sind kein Grund zu großer Sorge

Wirklich praxistaugliche Lösungen gibt es für das gegenwärtige Datenschutzproblem somit nicht. Streng genommen dürfte ein weit überwiegender Großteil der täglichen Transfers von personenbezogenen Daten aus Deutschland an US-Unternehmen bzw. US-Server wegen Verstoßes gegen das deutsche Datenschutzrecht rechtswidrig sein. Abmahnungen durch Konkurrenten oder Verbraucherschutzverbände wären daher grundsätzlich genauso denkbar und möglich wie Sanktionen durch Datenschutzbehörden. Allerdings wird es dazu zumindest in nächster Zeit aller Wahrscheinlichkeit nach kaum kommen. Denn auch die Datenschutzbehörden sind sich momentan uneins darüber, was sie deutschen Unternehmen zu der Thematik raten sollen. Es gibt schlichtweg gegenwärtig keine offiziell abgesegnete, praxistaugliche Vorgehenswese, was die Datenschutzbehörden dazu veranlasst, den Ball ebenfalls flach zu halten. Den Datenaufsehern fehlen zudem die Mittel, gegen die zahlreichen Verstöße nachhaltig vorzugehen. Darüber hinaus haben sie sich in der Vergangenheit meist gerade in Bezug auf kleinere und mittlere Unternehmen verständnisvoll gezeigt und diese verschont, wenn es darum ging, datenschutzrechtliche Exempel zu statuieren. Hierfür sind tatsächlich Facebook, Google & Co deutlich besser geeignet, so dass die Breitenwirkung des Einsatzes der zur Verfügung stehenden personellen und finanziellen Mittel gegen die genannten Großunternehmen für Datenschutzbehörden deutlich vielversprechender sein dürfte.
Schließlich befinden sich die EU und die USA zudem gegenwärtig in aussichtsreichen Verhandlungen über ein Nachfolgeabkommen zu Safe Harbor, das die Vorgaben des EuGH-Urteils umsetzen soll. Zwar ist noch unklar, wann und mit welchem genauen Inhalt das Nachfolgeabkommen in Kraft treten wird, doch dürften die Datenschutzbehörden solange die Füße weitestgehend still halten, bis hier auf höchster Ebene Klarheit hergestellt worden ist.

VIII. Fazit

Das Safe Harbor-Urteil des EuGH verwirrt viele Online-Händler. Unklar ist, auf welcher Rechtsgrundlage nun der Transfer von personenbezogenen Daten an US-Unternehmen bzw. auf US-Server im Rahmen von Cloud-Diensten, Social Networks oder sonstigen webbasierten Diensten stattfinden darf. Zwar ist streng genommen nun Vieles, was alltäglich an Datentransfers stattfindet, rechtswidrig, doch sind die Datenschutzbehörden und Verbände nach derzeitigem Stand weit davon entfernt, die von der Politik verschuldete Rechtsunsicherheit auf dem Rücken kleinerer und mittlerer Unternehmen auszutragen. Dafür spricht auch das recht moderate Vorgehen der Datenschutzbehörden aus der Vergangenheit, das sich häufig von der eigenen PR unterschied.
Am Horizont zeichnet sich zudem eine Lösung in Form eines Nachfolgeabkommens ab. Die IT-Recht Kanzlei bleibt am Thema dran und wird über die weiteren Entwicklungen stets zeitnah und ausführlich

berichten.

Bei Problemen, Rückfragen und weiteren Fragen zu diesem Thema hilft Ihnen das Team der IT-Recht Kanzlei selbstverständlich gerne auch persönlich und im Einzelfall weiter.

Autor:
Daniel Huber
(freier jur. Mitarbeiter der IT-Recht Kanzlei)