Dr. Martin Bahr

Safe Harbor down! Was tun?

Der Europäische Gerichtshof (EuGH) hat in seinem Urteil vom 06.10.2015 - Az.: C-362/14 bekanntlich das sogenannte Safe-Harbor-Abkommen für unwirksam erklärt, da es gegen geltendes EU-Datenschutzrecht verstößt. Darf man als deutsches Unternehmen nun noch kundenbezogene Daten in der Cloud, z. B. bei Amazon, ablegen oder Software nutzen, die dies tut? Darf man z. B. Google Analytics weiterhin nutzen, ohne gegen geltendes Recht zu verstoßen? Viele Unternehmen sind verunsichert. Der Beitrag von Rechtsanwalt Dr. Martin Bahr zeigt auf, welche praktischen Konsequenzen sich derzeit für deutsche Unternehmen durch diese Entscheidung ergeben, und gibt praktische Handlungsempfehlungen.

A. Was ist überhaupt das Safe-Harbor-Abkommen?

Die Übermittlung personenbezogener Daten in ein außereuropäisches Land ist grundsätzlich nur dann erlaubt, wenn dort ein angemessenes Schutzniveau für die Daten gewährleistet ist.

Um nicht jeden Einzelfall langwierig zu prüfen, hat die EU-Kommission im Jahr 2000 das sogenannte Safe-Harbor-Abkommen statuiert. Danach sollen alle US-Firmen, die sich zur Teilnahme an dieser Regelung verpflichten, automatisch über ein ausreichendes Datenschutz-Niveau verfügen. Das Safe-Harbor-Abkommen war bereits in der Vergangenheit immer wieder Gegenstand zahlreicher Kritik nicht zuletzt deutscher Aufsichtsbehörden. Kritisiert wurde vor allem, dass die einzelnen teilnehmenden US-Unternehmen durch die dortigen Behörden kaum oder gar nicht kontrolliert wurden.

Eben dieses Safe-Harbor-Abkommen hat der EuGH nun für unwirksam erklärt. Es stellt somit keine ausreichende Grundlage mehr dar, dass Unternehmen personenbezogene Daten in die USA übertragen dürfen.

B. Existieren Alternativen zum Safe-Harbor-Abkommen?

Auf dem Papier existieren theoretisch (!) mehrere alternative Möglichkeiten zum Safe-Harbor-Abkommen. Diese sind:

» die Einwilligung durch den User
» EU-Standardvertragsklauseln oder
» Binding Corporate Rules

Um das Ergebnis aber vorwegzunehmen: Es handelt sich dabei um keine wirklich praxistauglichen Lösungen. In Einzelfällen mag dies anders aussehen, aber für die weit überwiegende Anzahl der betroffenen Unternehmen handelt es sich nur um echte Papiertiger.

Im Folgenden soll kurz dargestellt werden, warum das Ganze so schwer ist:

1. Alternative: Einwilligung durch den User

Seit vielen Jahrzehnten stellt die Rechtsprechung an eine wirksame Einwilligung durch den Nutzer kaum erfüllbare Anforderungen. Insbesondere muss der User über Art, Umfang und Reichweite seiner Einwilligung informiert werden. Nur wenn der Nutzer in ausreichender Weise informiert wird, ist die Einwilligung wirksam. Der Einwilligungstext muss daher so konkret wie möglich sein. Pauschale oder allgemeine Aussagen sind nicht ausreichend.

Problematisch an der Einwilligung ist auch, dass der Nutzer seine Einwilligung jederzeit widerrufen kann. In einem solchen Fall muss das Unternehmen dann umgehend reagieren und die Daten löschen.

Aufgrund dieser Umstände ist die Einwilligung keine echte Lösung für die Praxis.

2. Alternative: EU-Standardvertragsklauseln

Unternehmen können auch die sogenannten EU-Standardvertragsklauseln verwenden. Dies ist eine Möglichkeit, die die EU-Kommission neben dem Safe-Harbor-Abkommen geschaffen hat.

DER AUTOR

Die Kanzlei **Dr. Bahr** *(www.Dr-Bahr.com)* ist auf den Bereich des Rechts der Neuen Medien und den gewerblichen Rechtsschutz (Marken-, Urheber- und Wettbewerbsrecht) spezialisiert. Unter Suchmaschinen-und-Recht.de betreibt sie seit 2005 ein eigenes Themenportal zur rechtlichen Dimension von Suchmaschinen.

Es handelt sich um standardisierte Verträge, die, wenn sie so abgeschlossen werden, angeblich ein ausreichendes Datenschutz-Niveau statuieren sollen. Die Vertragsmuster gibt es auf der Webseite der EU-Kommission *(bit.ly/1MbULWZ)*.

Problem ist hier nur: Die deutschen Datenschutzbehörden haben bereits im Jahr 2013 in einer gemeinsamen Presseerklärung *(bit.ly/1XJBsbo)* erklärt, dass ihnen diese Standard-Vertragsklauseln nicht (mehr) ausreichen, solange nicht die genauen Zugriffsmöglichkeiten der amerikanischen Geheimdienste geklärt sind:

> „Deshalb fordert die Konferenz die Bundesregierung auf, plausibel darzulegen, dass der unbeschränkte Zugriff ausländischer Nachrichtendienste auf die personenbezogenen Daten der Menschen in Deutschland effektiv im Sinne der genannten Grundsätze begrenzt wird.
> Bevor dies nicht sichergestellt ist, werden die Aufsichtsbehörden für den Datenschutz keine neuen Genehmigungen für die Datenübermittlung in Drittstaaten (zum Beispiel auch zur Nutzung bestimmter Cloud-Dienste) erteilen und prüfen, ob solche Datenübermittlungen auf der Grundlage des Safe-Harbor-Abkommens und der Standardvertragsklauseln auszusetzen sind."

Schaut man sich diesbzgl. die Entscheidung des EuGH an, so ist relativ schnell erkennbar, dass auch diese Standardvertragsklauseln aus identischen Gründen gegen EU-Datenschutzrecht verstoßen wie das Safe-Harbor-Abkommen. Zwar betrifft die aktuelle Entscheidung nur das Safe-Harbor-Abkommen, aber bei konsequentem Weiterdenken der Gründe, die zur Unwirksamkeit der Regelung geführt haben, führen diese auch zur Unzulässigkeit der EU-Standardvertragsklauseln. Denn auch diese können nicht sicherstellen, dass US-Geheimdienste keinen Zugriff erhalten.

3. Alternative: Binding Corporate Rule

Denkbar ist auch, dass sich ein internationaler Konzern sogenannte Binding Corporate Rules gibt. Dabei handelt es sich um nichts weiter als unternehmensinterne Datenschutzregeln, die dann weltweit gelten.

Die Krux ist aber auch hier: Das betroffene US-Unternehmen kann den Zugriff amerikanischer Geheimdienste rechtlich nicht wirksam ausschließen. Da es seinen Sitz in den USA hat, unterliegt es auch der dortigen Hoheitsmacht. Insofern ist auch diese Lösung von vornherein zum Scheitern verurteilt.

C. Die praktischen Konsequenzen

Die Problematik kann für deutsche Unternehmen in zwei unterschiedlichen Varianten auftreten:

» Das deutsche Unternehmen überträgt personenbezogene Daten selbst an ein Unternehmen in den USA.
» Das deutsche Unternehmen nutzt das Angebot eines Dritten (z. B. ein Online-Tool), das Daten in die USA überträgt.

1. Variante: Eigene Datenübertragung

Übertragen Sie als deutsches Unternehmen selbst personenbezogene Daten an ein USA-Unternehmen, können sie sich ab sofort nicht mehr auf das Safe-Harbor-Abkommen berufen.

Datenübertragungen, die Sie in der Vergangenheit vorgenommen haben, bleiben unberührt, da die Entscheidung nicht rückwirkend, sondern erst ab dem 06.10.2015 gilt.

Schauen Sie die o. g. Alternativen zum Safe-Harbor-Abkommen an und überprüfen Sie, ob eine der dort genannten Möglichkeiten für Sie denkbar ist. In 95 % der Fälle dürfte keine der o. g. Lösungen für Sie möglich sein, sodass faktisch eine legale Datenübertragung in die USA derzeit nicht möglich ist.

2. Variante: Datenübertragung eines Dritten

Derzeit sind auf der Safe-Harbor-Liste 4.469 Unternehmen verzeichnet.

Wenn Sie als Unternehmer nicht genau wissen, ob der Anbieter des Online-Tools, das Sie nutzen, auf dieser Liste steht, können Sie einfach online auf der Webseite *https://safeharbor.export.gov/list.aspx* nachsehen.

Um das Ergebnis aber vorwegzunehmen: Alle gängigen und größeren Anbieter von Online-Tools berufen sich auf Safe Harbor. Bedeutet im Klartext: Diese Anwendungen dürf(t)en Sie aktuell nicht mehr nutzen.

> **Beispiel:** Die bekannte Amazon-Cloud („Amazon Web Services") beruft sich auf Safe Harbor, da hier (teilweise) die Daten in den USA gespeichert werden. Nach dem EuGH-Urteil ist eine solche Datenübertragung in die USA unwirksam und verstößt gegen EU-Datenschutzrecht. Sie dürf(t)en die Amazon-Cloud somit nicht mehr nutzen

Bereits dieses Beispiel zeigt, dass sich Europa bei strikter Einhaltung der datenschutzrechtlichen Vorgaben damit technologisch ins Mittelalter zurückkatapultieren würde.

Für einzelne Dienstleistungen von US-Unternehmen mag es zwar akzeptable europäische Alternativen geben, die Sie als Unternehmer nutzen können. Aber eben nicht für die meisten.

Wichtig dabei zu berücksichtigen ist jedoch, dass nicht jedes Tool eines Anbieters, der sich auf das Safe-Harbor-Abkommen beruft, automatisch und

zwingend datenschutzwidrig ist. Voraussetzung ist nämlich, dass eine Übermittlung personenbezogener Daten in die USA erfolgt.

Beispiel: Das Unternehmen Google beruft sich grundsätzlich auf Safe Harbor. Damit wären somit automatisch sämtliche Handlungen von Google datenschutzwidrig. So einfach ist es dann aber doch nicht: Es kommt nämlich darauf an, ob Google personenbezogene Daten in die USA überträgt.

Im Rahmen des bekannten Analyse-Tools „Google Analytics" zum Beispiel werden die relevanten Informationen in Europa verarbeitet und nur in anonymisierter Fassung in die USA geschickt (so jedenfalls der aktuelle Sachstand). Somit ist Google Analytics auch nach dem Ende des Safe-Harbor-Abkommens rechtlich einwandfrei.

Die Problematik in der Praxis ist nun, dass Sie als Unternehmer in aller Regel gar nicht wissen (können), ob und in welcher Form eine Datenübermittlung in die USA erfolgt. Die meisten Anbieter schweigen sich hierüber vollkommen aus.

D. Reaktionen der Datenschutzbehörden

Die Artikel-29-Datenschutzgruppe, die Vereinigung aller nationalen Datenschutzbehörden innerhalb der EU, hat in einer ersten Stellungnahme *(bit.ly/1k4mr5J)* der Europäischen Kommission eine Frist bis Ende 2016 gesetzt, um ein neues Abkommen auszuhandeln. Sollte bis dahin keine neue Vereinbarung vorliegen, heißt es ausdrücklich:

„EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions."

Die deutschen Datenschutzbehörden haben vor Kurzem ein Positionspapier *(bit.ly/1HnO93Y)* herausgegeben. In dem 15-Punkte-Papier zweifeln die Datenschützer ganz erheblich an, ob eine Datenübertragung in die USA derzeit überhaupt möglich ist. So heißt es dort:

„Im Lichte des Urteils des EuGH ist auch die Zulässigkeit der Datentransfers in die USA auf der Grundlage der anderen hierfür eingesetzten Instrumente, etwa Standardvertragsklauseln oder verbindliche Unternehmensregelungen (BCR), in Frage gestellt."

Bis Januar 2016 wollen die Behörden die gesamte Problematik nicht weiter vor Ort bei Unternehmen prüfen, behalten sich jedoch ausdrücklich das Recht vor, im Falle von Beschwerden durch Nutzer aktiv zu werden und zu ermitteln.

E. Unsere praktischen Handlungsempfehlungen

Unsere praktischen Handlungsempfehlungen sind:

1. Don´t Panic!

Verzweifeln Sie nicht allzu sehr. Die EuGH-Entscheidung betrifft nicht nur Sie allein. Die gesamte europäische Internet-Branche steht vor diesem Scherbenhaufen.

Es gilt abzuwarten, wie die deutschen Datenschutzbehörden weiter auf die aktuellen Ereignisse reagieren und welche Empfehlungen von dort kommen.

2. Kontrollieren Sie Ihre Verträge!

Überprüfen Sie Ihre sämtlichen Verträge, ob in diesen Bezug genommen wird auf das Safe-Harbor-Abkommen.

Ist dies der Fall, empfehlen wir Ihnen, alternativ über die EU-Standardvertragsklauseln oder Binding Corporate Rules nachzudenken. Auch wenn diese Instrumente – wie oben beleuchtet – eigentlich kritisch zu sehen sind, bieten sie derzeit die beste Möglichkeit der rechtlichen Absicherung.

3. Existieren Gerichtsurteile gegen Sie?

Überprüfen Sie, ob in der Vergangenheit gegen Sie Gerichtsurteile ergangen sind, in denen Ihnen verboten wurde, unbefugt personenbezogene Daten zu erheben, zu verarbeiten oder zu ermitteln.

Ist dies der Fall, empfehlen wir Ihnen nachdrücklich, bis auf Weiteres von einer Datenübermittlung in die USA Abstand zu nehmen. Auch wenn es schwerfällt, setzen Sie nur Online-Tools von europäischen Anbietern ein bzw. von solchen Unternehmen, bei denen Sie sicher sein können, dass keine US-Übermittlung stattfindet.

4. Existieren behördliche Anordnungen gegen Sie?

Überprüfen Sie, ob in der Vergangenheit gegen Sie eine behördliche Anordnung ergangen ist, die Ihnen verbietet, unbefugt personenbezogene Daten zu erheben, zu verarbeiten oder zu ermitteln.

Ist dies der Fall, lesen Sie unsere Antwort zu Punkt 3.

5. Haben Sie bereits eine strafbewehrte Unterlassungserklärung abgegeben?

Überprüfen Sie, ob Sie in der Vergangenheit eine strafbewehrte Unterlassungserklärung abgegeben haben, in der Sie sich verpflichtet haben, nicht unbefugt personenbezogene Daten zu erheben, zu verarbeiten oder zu ermitteln.

Ist dies der Fall, lesen Sie unsere Antwort zu Punkt 3.¶