Sonderrundbrief Oktober 2015

Sehr geehrte Damen und Herren,

am 06.10.2015 hat der Europäische Gerichtshof (EuGH) das sogenannte Safe-Harbor-Abkommen für ungültig erklärt. Was es mit dem Abkommen auf sich hat und inwieweit Sie möglicherweise von der aktuellen Entscheidung betroffen sind, erläutern wir Ihnen nachfolgend in unseren aktuellen Sonderrundbrief zum Thema „Safe Harbor“.

Mit freundlichen Grüßen

Ihre SaphirIT GmbH

“Safe Harbor”

1. „Safe Harbor“ – Was ist das?

Bei „Safe Harbor“ (Sicherer Hafen) handelt es sich um ein zwischen der EU und den USA im Jahre 2000 getroffenes Abkommen, das gewährleistet, dass personenbezogene Daten legal in die USA übermittelt werden können. Ausgangspunkt für diese Vereinbarung bilden die Vorschriften der Europäischen Datenschutzrichtlinie. Nach diesen Vorschriften ist ein Datentransfer in Drittstaaten verboten, die über kein dem EU-Recht vergleichbares Datenschutzniveau verfügen. Dies trifft auf die USA zu, da es dort keine umfassenden gesetzlichen Regelungen zum Datenschutz gibt, die dem europäischen Standard entsprechen. Allerdings sieht die Richtlinie auch vor, dass die Kommission der Europäischen Gemeinschaft die Angemessenheit des Datenschutzes in einem Drittland feststellen kann, wenn dieses bestimmte Anforderungen erfüllt.

SaphirIT GmbH
Sutthauser Straße 285
49080 Osnabrück
Geschäftsführer
Amtsgericht Osnabrück

www.saphirit.de
USt.-ID DE 268765300
Frank W. Stroot
HRB 203854

Datenschutz – IT-Sicherheit
Oldenburgische Landesbank AG
IBAN DE29 2802 0050 5042 8200 00
BIC OLBODEH2XXX

Telefon 0541/60079296
Telefax 0541/60079297
datenschutz@saphirit.de

Damit der Datenaustausch zwischen der EU und den USA als einem ihrer wichtigsten Handelspartner nicht zum Erliegen kommt, wurde deshalb nach einem Weg gesucht, wie Daten legal in die USA transferiert werden können, auch wenn dort kein dem Niveau der EU vergleichbarer Datenschutzstandard vorliegt. Zur Überbrückung der Systemunterschiede wurde das Safe-Harbor-Modell entwickelt. Die Europäische Kommission erließ daher am 26. Oktober 2000 eine Entscheidung, nach der in den USA tätige Unternehmen über ein angemessenes Datenschutzniveau verfügen, wenn sie sich gegenüber der Federal Trade Commission (FTC) öffentlich und unmissverständlich zur Einhaltung der von dem US-Handelsministerium zuvor aufgestellten Prinzipien und 15 häufig gestellten Fragen („FAQs“) verpflichten.

In den USA tätige Unternehmen, die unter die Aufsicht der FTC fallen, können gemäß der Vereinbarung dem Safe Harbor beitreten, in dem sie sich öffentlich verpflichten, diese Prinzipien einzuhalten und die dazu gehörenden verbindlichen häufig gestellten Fragen beachten.

Auch wenn der Beitritt freiwillig ist, sind die Unternehmen danach verpflichtet, sich an die Grundsätze des Safe-Harbor-Abkommens zu halten und müssen dies der FTC jährlich mitteilen. In dem Fall, dass ein Unternehmen gegen diese Prinzipien verstößt, kann die FTC entsprechende Maßnahmen ergreifen, wie etwa die Datenverarbeitung stoppen oder Sanktionen verhängen.

Bis dato konnten sich europäische Unternehmen bei der Übermittlung personenbezogener Daten aus einem Land der Europäischen Union in die USA auf dieses Abkommen berufen. Die Verarbeitung der Daten in den USA galt unter den vorgenannten Voraussetzungen als sicher.

2. Kritik an dem Abkommen

Das Abkommen wurde über die Jahre vermehrt kritisiert. Seitens der hiesigen Datenschutzbehörden wurde angenommen, dass US-Unternehmen die Prinzipien nach dem Abkommen nicht einhalten bzw. nicht adäquat umsetzen. Im Zuge des NSA-Skandals folgte sogar die Aufforderung an die Europäische Kommission, ihre Entscheidung zu Safe Harbor bis auf weiteres zu suspendieren.

Endgültig in Europa angekommen war die Debatte, als der irische High Court in Dublin mit Beschluss vom 18.06.2014 dem EuGH die Frage nach der Verbindlichkeit des Safe-Harbor-Abkommens der EU-Kommission aus dem Jahr 2000 vorlegte.

Hintergrund war die Klage des österreichischen Juristen Max Schrems, der nicht länger hinnehmen wollte, dass Facebook persönliche Daten auf Servern in den USA speichert, wo sie seiner Meinung nach nur unzureichend vor dem Zugriff durch die NSA geschützt sind. Deshalb sollten die Richter am EuGH klären, ob sich der europäische Facebook-Ableger mit Sitz in Dublin an die EU-Grundrechtecharta zum Schutz personenbezogener Daten halten muss und womöglich europäisches Datenschutzrecht verletzt.

3. Zum Urteil

Der EuGH entschied nicht nur über die Zulässigkeit von Safe Harbor selbst, sondern auch darüber, inwieweit nationale Aufsichtsbehörden an eine Entscheidung der europäischen Kommission hinsichtlich des angemessenen Datenschutzniveaus in einem Drittland gebunden sind, denn durch das Safe-Harbor-Abkommen wurden die Kontrollrechte der nationalen Datenschutzbehörden in den EU-Ländern ausgehebelt. Diesen Eingriff in die Rechte der Datenschutzbehörden sah der EuGH als zu gravierend an. Zwar dürften die Aufsichtsbehörden keine Maßnahmen ergreifen, die einer Angemessenheitsentscheidung der Kommission entgegenstünden, sie müssen aber selbst beurteilen können, ob eine Datenübermittlung in ein Drittland mit den Vorgaben europäischer Datenschutzgrundsätze konform geht. Die irische Aufsichtsbehörde hätte die erfolgte Eingabe des Betroffenen Max Schrems prüfen müssen, so der EuGH.

Nach dem aktuellen EuGH-Urteil verliert das Safe-Harbor-Abkommen seine Gültigkeit, weil dieses mit EU-Recht nicht vereinbar sei. Dies folgt für das Gericht zum einen aus der fehlenden Bindungswirkung für staatlich veranlasste Datenzugriffe. Zum anderen beziehe sich die Entscheidung der Kommission aus dem Jahre 2000 lediglich auf die Einhaltung der Prinzipien und „FAQs“ und enthalte keine ausreichenden Maßnahmen nach der Europäischen Datenschutzrichtlinie, inwieweit die USA mittels nationaler Rechtsvorschriften oder internationaler Verpflichtungen ein solches Niveau gewährleisten würden.

4. Welche Folgen hat das Urteil?

Das Urteil hat große Auswirkungen auf die Datenübermittlungspraxis international tätiger Unternehmen in die USA. So gibt es derzeit etwa 5.500 US-Unternehmen, die europäische Kundendaten in den USA speichern.

Da die USA nach den Richtern des EuGH kein ausreichendes Schutzniveau vor dem Zugriff der dortigen Behörden bieten, sind Unternehmen nun gezwungen, auf anderem Wege ein angemessenes Datenschutzniveau zu gewährleisten. Ein pauschales Berufen auf das Safe-Harbor-Abkommen ist nicht mehr möglich.

Als Alternative kommt ein Rückgriff auf die EU-Standardvertragsklauseln (Stichwort: Auftragsdatenvereinbarung, abgekürzt „ADV“) oder für internationale Großkonzerne die Einführung konzernweiter "Binding Corporate Rules" in Betracht. Durch diese werden allerdings nur die Unternehmen in den USA, nicht aber die US-Überwachungsbehörden verpflichtet. Daher ist es zweifelhaft, ob das vom EuGH geforderte Schutzniveau allein durch solche Mittel erreicht werden kann.

Nach Einschätzung einiger Juristen könnten nun aber auch die EU-Standardvertragsklauseln grundrechtswidrig geworden sein. Der EuGH habe schließlich festgestellt, dass der faktisch unbeschränkte Zugriff US-amerikanischer Geheimdienste auf elektronische Kommunikation mit den europäischen Grundrechten nicht vereinbar sei. Weder Safe Harbor noch die Standardvertragsklauseln würden die Befugnisse der US-Behörden einschränken, dementsprechend seien beide ungültig.

Allerdings besteht auch eine faktische Übergangsregelung. Der EuGH hat nämlich auch entschieden, dass nur er selbst eine Entscheidung der EU-Kommission für ungültig erklären kann. Bis also ein entsprechendes Verfahren zum EuGH kommt, bleiben die Standardvertragsklauseln weiter gültig. Dessen ungeachtet ist es den nationalen Datenschutzbehörden möglich, die Standardvertragsklauseln als unwirksam anzusehen - auch hier erachtet der EuGH die Kommissionsentscheidung nicht als bindend.

Andere Juristen vertreten die Einschätzung, dass Unternehmen die Nutzer ab sofort vorab in die Datenübermittlung einwilligen lassen und über den genauen Verwendungszweck und die Reichweite der Datenverarbeitung in Kenntnis setzen müssen.

Sie seien nun verpflichtet, in ihren Geschäftsbedingungen darauf hinzuweisen, dass US-Geheimdienste auf gespeicherte Daten zugreifen können. Das ist aber heikel, da ihnen das US-amerikanische Recht verbietet, ihre Zusammenarbeit mit eben jenen Diensten offen zu legen. Möglicherweise könnte das bedeuten, dass Unternehmen wie Facebook, Google, Microsoft oder Amazon neue Rechenzentren in der EU aufbauen müssen, da sie die Daten nicht mehr in den USA speichern dürfen.

5. Was bedeutet die Entscheidung für Sie?

Die Entscheidung ist insoweit für Sie relevant, falls Sie personenbezogene Daten an Unternehmen/ Dienstleister in den USA übermitteln. Datenübermittlungen in die USA allein auf Basis des Safe-Harbor-Abkommens sind nicht mehr erlaubt. In diesem Fall müssten auf die vorgenannten Alternativen wie die EU-Standardvertragsklauseln oder die „Binding Corporate Rules“ zurückgegriffen bzw. vorab eine Einwilligungserklärung der Betroffenen in die Datenübermittlung eingeholt werden.

Wenn Sie auch bisher mit US-Dienstleistern keine Verträge über eine den EU-Vorgaben entsprechende ADV abgeschlossen hatten, dann handelten Sie ohnehin rechtswidrig, beispielsweise durch Einsetzen von Social Plugins auf Ihrer Website, durch Verwenden von Analysewerkzeugen aus den USA (z.B. Google Analytics), Lagern von Kundendaten in der Dropbox oder durch das Optimieren der Workflows Ihrer Mitarbeiter mittels US-Tools.

Wenn Sie weiter verfahren wie bisher, dürfte sich zwar derzeit praktisch nicht viel ändern. Es ist aber durchaus möglich, dass die Datenschutzbehörden härter durchgreifen, auch wenn deren beschränkte finanzielle Mittel trotz der nun auf sie zukommenden Arbeit, nicht erhöht wurde. Ferner nehmen Datenschutzbehörden in der Regel auch auf die Nachteile der plötzlichen Änderungen Rücksicht. Allerdings ließen einige Landesdatenschutzbeauftragte in jüngerer Vergangenheit bereits erkennen, das Bußgeldverfahren als ein Instrument zum Schutz der informationellen Selbstbestimmung zukünftig stärker zu nutzen, um dagegen vorzugehen, dass Datenschutzverstöße als Teil des unternehmerischen Risikos einkalkuliert und in Kauf genommen werden. Die Entscheidung des EuGH könnte dieser Tendenz weiteren Schub verleihen. Bei Datenschutzverstößen drohen Bußgelder bis zu 300.000,00 EUR pro Verstoß!

Auch Abmahnungen sind nun wahrscheinlicher. Für Unternehmen, die gegen das Datenschutzrecht verstoßen, besteht generell das Risiko, hierfür von Wettbewerbern kostenpflichtig abgemahnt zu werden. Dies gilt beispielsweise im Falle einer fehlenden Datenschutzerklärung auf der unternehmenseigenen Internetseite. Die entsprechende Verpflichtung zur Datenschutzerklärung soll nicht nur datenbezogene Grundrechte gewährleisten, sondern auch den grenzüberschreitenden Verkehr personenbezogener Daten auf ein einheitliches Schutzniveau heben. Ein unterschiedliches Schutzniveau stellt nämlich ein Hemmnis für die Ausübung von Wirtschaftstätigkeiten auf Gemeinschaftsebene dar und kann den Wettbewerb verfälschen. Ebenso können Verstöße gegen alle anderen datenschutzrechtlichen Vorschriften abgemahnt werden, die von der Rechtsprechung als im Sinne des § 4 Nr. 11 UWG (Gesetz gegen den unlauteren Wettbewerb) das Marktverhalten regelnde Normen angesehen werden. Die unzulässige Übermittlung personenbezogener Daten an Unternehmen in unsicheren Drittländern ohne entsprechende Vorkehrungen dürfte eine Verfälschung des Wettbewerbs gegenüber den Unternehmen darstellen, die diese Vorkehrungen getroffen haben. Die streitwertabhängigen Abmahnkosten des von dem Wettbewerber beauftragten Rechtsanwaltes sind von dem Unternehmen zu tragen, das den Verstoß begangen hat. Es drohen zusätzlich erhebliche Schadenersatzforderungen der Wettbewerber.

Sie sollten also rechtlich so viel wie möglich richtig machen, denn je sicherer Ihre Datenverarbeitung rechtlich ist, desto geringer ist das Gesamtrisiko beim Einsatz von rechtlich fragwürdigen US-Anbietern.

SaphirIT Tipp

Sie sollten daher:

- nach Möglichkeit EU- statt US-Anbieter wählen (bzw. US-Anbieter die ADV-Verträge anbieten und Daten in der EU verarbeiten, wie es z.B. bei Amazon Web Services oder Microsoft möglich ist),

- Dienstleister, die Nutzer-/Kunden- und Mitarbeiter-Daten in Ihrem Auftrag verarbeiten, nach ADVs fragen,

- Betroffene im Zweifel um eine Einwilligung bitten,

- eine Datenschutzerklärung anbieten, die über Ihre Datenverarbeitung Auskunft gibt.

Der rechtliche Fokus auf den Datenschutz wird stärker und Sie sollten daher noch mehr als zuvor auf die möglichst genaue Einhaltung der Datenschutzvorschriften achten. Falls Sie für die Umsetzung Unterstützung benötigen, hilft nur eine rechtssichere Beratung!

Sprechen Sie uns jederzeit gerne an!