Zur Information

Herbst 2009, Nr. 1

Das „Safe Harbor“ System

Datenschutz zwischen der EU und den Vereinigten Staaten Mit Vergleich zu Kanada

Die Versendung personenbezogener Informationen aus der EU in die USA ist rechtlich problematisch. Deshalb möchten wir Ihnen das “Safe Harbor” Programm vorstellen, welches einen legalen, ungestörten Datenaustausch zwischen Unternehmen in der EU und in den USA ermöglicht. Die EU erkennt an, dass Daten bei teilnehmenden U.S.-Unternehmen in einem „sicheren Hafen“ sind, daher dass dort ein angemessenes Schutzniveau besteht.

I. Hintergrund

Noch nie gab es Zeiten, in denen es einfacher, schneller und bequemer möglich war, personenbezogene Informationen zu erlangen, zu verarbeiten und weiter zu versenden. Der elektronische Datentransfer über die Grenzen von Ländern und Kontinenten hinaus ist praktisch nicht kontrollierbar.

Hat man sich in Europa schon seit längerem mit dem Thema Datenschutz beschäftigt und aufgrund von EU-Vorgaben entsprechende landesweite Schutzgesetze erlassen, so war dies in den Vereinigten Staaten von Amerika (USA) lange nicht der Fall. Dort ist die Vorstellung eines staatlichen Eingriffs in den Datentransfer auf keine große Akzeptanz gestoßen. Aus diesem Grund existiert hierzu auch keine Gesetzgebung mit der Konsequenz, dass ein Datenaustausch mit den USA in der EU als unsicher betrachtet wurde.

Die EU- Kommission erließ deshalb im Jahre 1995 die Richtlinie 95/46/EG, wonach es bis heute verboten ist, personenbezogene Daten aus EU- Staaten in so genannte Drittstaaten zu übertragen, es sei denn, es kann ein mit den Vorgaben der EU vergleichbares Datenschutzniveau nachgewiesen werden (umgesetzt in § 4b des deutschen Bundesdatenschutzgesetzes). Die Kommission befand die - hauptsächlich auf Selbstregulation basierenden - Datenschutzvorkehrungen der USA als nicht ausreichend und die Mitgliedsstaaten waren mithin verpflichtet, den Datentransfer in die USA einzustellen. So kam es aufgrund der unklaren Rechtslage in den USA zumindest zu Störungen beim Datenfluss. Beispielsweise ist es einem deutschen Unternehmen mit einer amerikanischen Tochterfirma (oder einer deutschen Tochtergesellschaft mit einer amerikanischen Mutter) verboten, Daten von Deutschland in die USA zu exportieren. Dies gilt natürlich auch für nicht verbundene Unternehmen. Eine solche Einschränkung des Datenaustauschs hätte auf Dauer gravierende Auswirkungen auf die engen Handelsbeziehungen zwischen den USA und den EU- Ländern.

Durch etwas Druck der EU haben die USA zur Lösung des Dilemmas im Jahre 2000 in Zusammenarbeit mit der EU- Kommision das “Safe Harbor” Programm entwickelt.[1] Es stellt eine datenschutzrechtliche Sondervereinbarung der USA und der EU dar. Seither ist es seitens der EU anerkannt, dass bei Unternehmen, die dem “Safe Harbor” Programm beigetreten sind, ein ausreichendes, den Vorgaben der EU vergleichbares Datenschutzniveau gewährleistet ist.[2]

[1] http://www.export.gov/safeharbor/eu/sh_en_workbook1.asp (02.03.2009)
[2] Entscheidung 520/200/EC der EU-Kommission

Steven H. Thal and **Florian von Eyb**

PHILLIPS NIZER LLP
Resourceful Representation®

II. Die sieben Prinzipien des "Safe Harbor" Programms

Die "Safe Harbor" Vereinbarung besteht im Wesentlichen aus sieben Prinzipien. Diese werden durch die Erklärungen zu einer Reihe von häufig gestellten Fragen (Frequently Asked Questions FAQ[3]) konkretisiert. Im Folgenden sind die sieben Prinzipien in ihren Grundzügen dargestellt:

1. Information

Betroffene Personen müssen vorab informiert werden, zu welchem Zweck ihre Daten erhoben und gespeichert werden, an wen sie sich bei Nachfragen oder Korrekturen wenden können und welche Rechte sie u.a. bezüglich Nutzung, Veröffentlichung und Weitergabe ihrer Daten haben.

2. Wahlmöglichkeit

Vor der Weitergabe von Informationen an eine dritte Partei besteht die Möglichkeit zu wählen, ob die Informationen an diese weitergegeben oder für einen Zweck verwendet werden dürfen, der nicht dem Zweck entspricht, für den die Informationen ursprünglich erfragt wurden.

3. Weitergabe von Daten

Die Daten werden nur dann an Dritte weitergegeben, wenn diese selbst an dem "Safe Harbor" Programm teilnehmen oder schriftlich vesichern, dass sie einem vergeichbaren Programm angehören, welches den gleichen Schutz bietet.

4. Zugriff

Es besteht im Rahmen des Programms die Möglichkeit, gesammelte Informationen einzusehen, zu korrigieren, zu ändern oder zu löschen, es sei denn, dass gewisse vorrangige berechtigte Interessen entgegenstehen.

5. Sicherheit

Es werden geeignete Sicherheitsmaßnahmen getroffen, um die gespeicherten Informationen gegen unbefugte Zugriffe, Veränderungen, Verlust und Veröffentlichung zu schützen.

6. Datenintegrität

Die erfassten Informationen sind auf die zur Erreichung eines bestimmten berechtigten Interesses bzw. Zwecks notwendigen Daten zu beschränken. Darüber hinaus sind Maßnahmen zu treffen, die sicherstellen, dass es sich um verlässliche, zur Erreichung dieses Zweckes geeignete Daten handelt.

7. Einhaltungsverpflichtung

Um die Einhaltung der "Safe Harbor" Prinzipien zu gewährleisten, verpflichten sich die teilnehmenden Unternehmen, mit den Datenschutzbehörden der EU- Länder bei der Ermittlung von Beschwerden zusammen zu arbeiten. Ferner müssen sie ein Verfahren zur Überprüfung der Einhaltung der "Safe Harbor" Prinzipien einsetzen und Abhilfe für Probleme schaffen, die aus der Nichteinhaltung der Prinzipien resultieren.

Die Unternehmen akzeptieren, dass für den Fall, dass sie nicht jährlich dem amerikanischen Handelsministerium den Nachweis darüber erbringen, dass sie die Prinzipien des Programms erneut anerkennen, das Unternehmen aus der Liste der teilnehmenden Firmen gestrichen, sowie eine weitere Datenübertragung an sie untersagt wird.

Die Prinzipien des "Safe Harbor" Programms ähneln in Grundzügen dem Konzept des Bundesdatenschutzgesetzes. Datensicherheit, Informationspflichten, Einverständniserfordernisse und Kontrollmöglichkeiten stehen im Vordergrund.

[3] http://www.export.gov/safeharbor/eu/eg_main_018493.asp

III. Vorteile für Unternehmen aus EU- Mitgliedsstaaten

Ein Vorteil des „Safe Harbor“ Programms für die EU-Unternehmen liegt darin, dass ein einheitlicher Schutz personenbezogener Daten in den USA gewährleistet wird. Einmal erhobene Daten können nicht mehr ohne Einverständnis des Datengebers nach Belieben weitergegeben werden. Ein weiterer Vorteil liegt darin, dass die Kontrolle der Daten nicht mehr ausschließlich auf Selbstregulierungsmechanismen beruht, sondern nunmehr durch übergeordnete Schlichtungs- und Überwachungsstellen erfolgt. Kommen diese Stellen ihrer Aufgabe nicht nach, verlieren nicht nur diese ihre Stellung als Schlichtungsstelle, sondern auch die Unternehmen, die diese Stelle als ihre „Überwachungsstelle“ angegeben haben, ihre Zugehörigkeit zu dem „Safe Harbor“ Programm. Während eine Übermittlung personenbezogener Daten an Drittländer grundsätzlich nur im Rahmen von festgelegten Standardvertragsklauseln möglich ist, gilt dies nicht für U.S.- Unternehmen, die an dem „Safe Harbor“ Programm teilnehmen.

Die Unternehmen gewinnen also an Rechtssicherheit und Vertrauen ihrer Kunden, die sich auf ein angemessenes Sicherheitsniveau für ihre Daten in den USA und entsprechende Kontrollmechanismen verlassen können.

IV. Vorteile für die teilnehmenden U.S.- Unternehmen

Die Teilnahme an dem „Safe Harbor“ Programm bietet auch den teilnehmenden U.S.- Firmen weitreichende Vorteile. So sind die Mitgliedsstaaten an die Entscheidung der Kommission gebunden, in wie weit Datenschutzvorkehrungen ausreichend sind. Die Datenschutzbestimmungen der teilnehmenden Unternehmen werden als ausreichend angesehen und der Datenfluss zu solchen Unternehmen findet ungehindert statt. Das Erfordernis, für Datentransfers vorab eine Genehmingung zu verlangen, fällt für Safe-Harbor-Unternehmen weg bzw. die Genehmigungen werden automatisch erteilt. Ansprüche, die von EU- Bürgern gegenüber U.S.- Firmen geltend gemacht werden, werden mit einer begrenzten Anzahl von Ausnahmen von Gerichten in den USA gehört.

“Safe Harbor” schafft Rechtssicherheit und Kundenvertrauen. Die Teilnahme erfolgt durch unbürokratische Selbstzertifizierung, die Einhaltung wird durch staatliche Stellen überwacht.

V. Teilnahme

Die Teilnahme an dem Programm ist freiwillig und erfolgt durch eine Selbstzertifizierung. Das bedeutet für ein Unternehmen, das an dem Programm teilnehmen möchte, dass es öffentlich einen Brief an die **Federal Trade Commission** in Washington, D.C. richtet. In diesem Brief erklärt das Unternehmen, dass es von nun an die Prinzipien des „Safe Harbor“ Programms einhalten wolle.

Hierzu gibt sich das Unternehmen entweder eine eigene Datenschutzpolitik, die den Vorgaben des „Safe Harbor“ entspricht, oder es übernimmt eine fremde „Privacy Policy“ eines Verbandes oder einer privaten Organisation. Organisationen wie **TRUSTe** oder **Better Business Bureau** bieten solche „Privacy Policies“ an.

Das Unternehmen muss sich ferner einer Schlichtungsstelle unterwerfen. Diese Schlichtungsstellen bieten eine Anlaufmöglichkeit, wenn sich Betroffene über die Datenschutzpraktiken eines Unternehmens beschweren möchten. Eine Schlichtungsstelle ist z.B. die **Direct Marketing Association (DMA)**. Auch die oben genannten Organisationen (TRUSTe und das Better Business Bureau) bieten ihre Tätigkeit als Schlichtungsstelle an.

Die Kosten für eine Neuregistrierung belaufen sich derzeit auf 200 USD. Weiterhin wird eine jährliche Gebühr in Höhe von 100 USD für die „Wiederzertifizierung“ erhoben.

Eine Liste der teilnehmenden Unternehmen kann im Internet unter folgender Adresse eingesehen werden: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list

VI. Vergleich mit Kanada

Das Datenschutzrecht in Kanada ist ähnlich ausgeprägt wie in Europa, weshalb ein “Safe Harbor” Programm zwischen Europa und Kanada nicht notwendig ist. Geregelt ist der Datenschutz in dem Bundesgesetz „Personal Information Protection and Electronic Documents Act“ (PIPEDA) und verschiedenen Landesgesetzen in den einzelnen Provinzen. PIPEDA enthält nahezu die gleichen Prinzipien wie das “Safe Harbor” Programm und folgerichtig hat die EU Kommission entschieden, dass dadurch ein mit den europäischen Maßstäben vergleichbares Schutzniveau im Sinne des Artikel 28 der EU Richtlinie 95/46/EG gewährleistet ist. Die Provinzen Alberta, British Columbia, Ontario und Quebec haben Provinzgesetze erlassen, die der Bundesdatenschutzbeauftragte Kanadas als im Wesentlichen vergleichbar mit PIPEDA anerkannt hat. Diese Provinzgesetze haben für Provinz-interne Fragen Vorrang. Das Bundesgesetz gilt jedoch weiterhin für die provinzübergreifende und die internationale Erhebung, Verarbeitung und Weitergabe von personenbezogenen Daten und in allen Fällen, in denen die Provinzen keine Rechtsvorschriften erlassen haben, die ganz oder teilweise dem Bundesrecht entsprechen.

VII. Fazit

Durch die Schaffung des „Safe Harbor“ Programms ist kein europäisches Datenschutzmodell in den USA eingeführt worden. Dennoch kann aufgrund einer Bewertung der EU- Kommision festgehalten werden, dass das „Safe Harbor“ Programm trotz einiger Defizite bei der Umsetzung eine ausreichende Datensicherheit und Rechtssicherheit garantiert. Mit seiner Entwicklung wurde ein einheitlicher Maßstab für die USA erarbeitet. Die teilnehmenden U.S.-Unternehmen können dadurch das Verbot, personenbezogene Daten aus EU- Staaten an sie zu übertragen, auf legale Weise vermeiden und ihren Kunden und Geschäftspartnern in der EU einen sicheren und ungestörten Datenfluss garantieren.

Für weitere Fragen nehmen Sie bitte Kontakt mit uns auf:

Steven H. Thal, J.Dr. Attorney at Law New York; Rechtskundiger für US Recht, OLG Frankfurt/ M.
+1 212 841 0742
sthal@phillipsnizer.com

Florian von Eyb, LL.M., Rechtsanwalt; Attorney at Law, New York
+1 212 841 0720
fvoneyb@phillipsnizer.com

Disclaimer (English)

This information is provided as a public service to highlight matters of current interest and does not imply an attorney-client relationship. It is not intended to constitute a full review of any subject matter, nor is it a substitute for obtaining specific legal advice from competent, independent counsel.

Disclaimer (Deutsch)

Sämtliche Informationen werden ausschließlich als öffentlicher Service zur Verfügung gestellt und begründen kein Mandanten- oder Beratungsverhältnis. Sie stellen ein aktuelles Thema vor, ohne den Anspruch auf Vollständigkeit zu erheben und ersetzen nicht die individuelle, fallspezifische anwaltliche Beratung.