

von **Dr. Sebastian Kraska**

USA-Datenschutz nach Safe Harbor: Änderungen nach Entscheidung der Aufsichtsbehörden

Der so genannte „Düsseldorfer Kreis“ hat im April diesen Jahres eine Entscheidung hinsichtlich der Zulässigkeit von Datentransfers von Deutschland in die USA an jene Unternehmen getroffen, die den „Safe-Harbor-Prinzipien“ beigetreten sind. Welche Auswirkungen diese Entscheidung für die Datentransferpraxis hat, soll in diesem Aufsatz erläutert werden.

Was ist der „Düsseldorfer Kreis“?

Der Düsseldorfer Kreis ist der Zusammenschluss der Datenschutz-Aufsichtsbehörden im Unternehmens-Bereich (so genannte „nicht-öffentliche Stellen“). Am 29. April 2010 hat der Düsseldorfer Kreis einen Beschluss hinsichtlich des Datentransfers im Rahmen des Safe-Harbor Abkommens überlassen. Der Düsseldorfer Kreis hat in dem Beschluss unter anderem verschärfte Richtlinien erlassen, die den Unternehmen weitere Pflichten bei Datentransfers an Safe-Harbor zertifizierte US-Unternehmen auferlegen.

Was gilt grundsätzlich beim Export von Daten aus Deutschland heraus?

Gemäß § 4b, c des Bundesdatenschutzgesetzes ist eine Datenübermittlung von deutschen Unternehmen an Unternehmen im Ausland solange unbedenklich, solange sich diese Unternehmen in der Europäischen Union oder im Europäischen Wirtschaftsraum (Norwegen, Island und Liechtenstein) befinden. Sollen die Daten an ein Unternehmen in einem anderen Land übertragen werden, muss gesondert geprüft werden ob die Stelle, welche die Daten erhalten soll, ein angemessenes Datenschutz-Schutzniveau aufweist (hierzu können beispielsweise im Einzelfall so genannte „EU-Standardvertragsklauseln“ oder konzernweite verbindliche Datenschutz-Regeln verwendet werden).

Angemessenes Schutzniveau für manche Länder von EU-Kommission bestimmt

Die EU-Kommission hat für die Länder Kanada, Argentinien, Schweiz, Guernsey und Isle of Man bereits das angemessene Datenschutz-Schutzniveau nach der dortigen Gesetzeslage für das ganze Land bestimmt. Soll in ein anderes Land übertragen werden, dass von der EU-Kommission nicht offiziell anerkannt wurde, muss das angemessene Schutzniveau für den Einzelfall festgestellt werden.

Sonderfall USA

Aufgrund der engen Handelsbeziehungen mit den Vereinigten Staaten wurde seitens der EU eine Sonderlösung bestimmt, obwohl gerade für die USA ein angemessenes Datenschutz-Schutzniveau durch die EU-Kommission nicht festgestellt wurde. Nach dem so genannten „Safe-Harbor-Abkommen“ ist es Unternehmen in den USA möglich, sich bei einer US-Behörde als „Unternehmen mit angemessenem Datenschutzniveau“ zertifizieren zu lassen. Die Unternehmen müssen hierbei dem „Safe-Harbor-Abkommen“ beitreten und sich den darin festgelegten Regeln zum Umgang mit personenbezogenen Daten formal unterwerfen. Der deutsche Datenexporteur darf dann Daten an dieses US-Unternehmen übermitteln (dies natürlich nur, wenn die Übermittlung auch im Übrigen datenschutzrechtlich zulässig ist).

Was galt bisher?

Bisher galt für deutsche Datenexporteure folgende Rechtslage: wenn an ein Unternehmen in den USA, das dem Safe-Harbor-Abkommen beigetreten war, Daten übermittelt werden sollten, war der Datentransfer nach § 4b, c des Bundesdatenschutzgesetzes grundsätzlich gestattet, so dass der deutsche Datenexporteur keine Sanktionen zu befürchten hatte. Durch das Safe Harbor Abkommen konnte ohne die Vereinbarung von EU-Standardvertragsklauseln oder Datenschutz-Unternehmensrichtlinien Daten übertragen werden. Auch für die Unternehmen in den USA war diese Lösung leicht: Dem Safe Harbor Abkommen beizutreten ist nur ein einmaliger Akt, der dann auf alle gewünschten Datenimporte in die USA durch das Unternehmen angewandt werden konnte.

Safe Harbor unter Beschuss

Die zehnjährige Praxis des Safe-Harbor-Abkommens zeigte jedoch aus Sicht der deutschen Datenschutz-Aufsichtsbehörden enorme Datenschutzdefizite. Insbesondere findet praktisch keine Aufsicht oder Kontrolle der Einhaltung der Safe-Harbor Bestimmungen durch die öffentliche Seite statt. Eine Studie hat Ende 2008 größere Defizite aufgedeckt und dokumentiert.

Inbesondere wurde festgestellt, dass viele Unternehmen angeben, Safe Harbor zertifiziert zu sein, ohne tatsächlich beigetreten zu sein. Daneben wurden auch die Mindestbestimmungen des Abkommens weitgehend nicht eingehalten. Auch wurde festgestellt, dass in zehn Jahren nur ein einziger Fall überhaupt von einem Gericht überprüft wurde. Faktisch war damit ein angemessenes Datenschutzniveau gerade nicht gewährleistet.

Was ändert sich nun?

Nach dem Beschluss des Düsseldorfer Kreises müssen deutsche Unternehmen, die Daten an US-Unternehmen übermitteln, nun auch Folgendes beachten: Sollen Daten aus Deutschland in die USA exportiert werden, so sind die datenexportierenden Stellen auch dann, wenn das Daten empfangende US-Unternehmen dem Safe Harbor Abkommen beigetreten ist, zu einer aktiven Überprüfung der Einhaltung der datenschutzrechtlichen Mindeststandards verpflichtet.

Der Düsseldorfer Kreis nennt in seinem Beschluss auch, was er unter einer aktiven Überprüfung versteht:

1. Schriftlicher Nachweis über Beitritt zum Abkommen muss vorgelegt werden

Zum einen muss dem deutschen Datenexporteur ein schriftlicher Nachweis über die Tatsache vorgelegt werden, dass dem Safe-Harbor-Abkommen tatsächlich beigetreten wurde. Dieser Nachweis darf nicht älter als sieben Jahre sein und muss die wesentlichen Verpflichtungen des Safe Harbor Abkommens enthalten. Der Erhalt dieser Bescheinigung sollte sorgfältig dokumentiert werden, da die verantwortliche Stelle auf Anforderung der Datenschutzbehörden verpflichtet ist, dieses vorzulegen.

2. Nachweis über Einhaltung der Informationspflichten muss eingeholt werden

Daneben muss der deutsche Datenexporteur sich von dem potentiellen Datenempfänger auch nachweisen lassen, dass dieser seine Informationspflichten gegenüber den Betroffenen wahrnimmt, welche im Safe Harbor Abkommen selbst festgelegt werden.

Informationspflichten nach Safe Harbor

Nach diesen muss das Unternehmen die betroffenen Datensubjekte darüber informieren, zu welchem Zweck Daten erhoben werden, wie diese die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel den Privatpersonen zur Verfügung gestellt werden, damit diese die Verwendung und Weitergabe der Daten einschränken können.

Auch der Nachweis, dass dies geschehen ist, muss die verantwortliche Stelle der Aufsichtsbehörde vorlegen können.

3. Verstoß gegen Safe Harbor soll der Aufsichtsbehörde angezeigt werden

Der Düsseldorfer Kreis schlägt daneben vor, einen Verstoß gegen die Safe Harbor Voraussetzungen der Aufsichtsbehörde direkt anzuzeigen. Eine Verpflichtung der Praxis kann sich dem Beschluss jedoch nicht entnehmen lassen.

Bußgelder drohen nun vermehrt auch für den deutschen Datenexporteur

Mit dem Beschluss der Aufsichtsbehörde werden dessen Empfehlungen zu faktischen Voraussetzungen für den Datentransfer in die USA. Bei Verstößen gegen das Bundesdatenschutzgesetz können Bußgelder bis zu 300.000,- Euro drohen, daneben können darüber hinaus gehende Gewinne abgeschöpft und Schadensersatzklagen erhoben werden. Das Haftungsrisiko ist damit relativ hoch.

Empfehlungen für die Praxis

Die oben angegebenen Forderungen des Düsseldorfer Kreises sollten unbedingt beachtet werden. Die Datenschutz-Aufsichtsbehörden auf Länderebene orientieren sich im Regelfall sehr stark an der Meinung des Gremiums.

Datenschutz nicht nur formal sondern auch tatsächlich gewährleisten

Um den sicheren Datenschutzstandard nicht nur formal sondern auch tatsächlich zu gewährleisten empfehlen wir den Unternehmen, noch zusätzlich datenschutzfördernde Maßnahmen zu ergreifen, beispielsweise durch die Vereinbarung von Vertragsstrafen zur Absicherung von Imageverlust durch negative Presseberichterstattung bei „Datenschutzskandalen“ (hierbei lässt sich die exakte Höhe des Schadens häufig schwer nachweisen).

Fazit

Deutsche Unternehmen, die an US-Unternehmen mit Safe Harbor Zertifizierung personenbezogene Daten exportieren, müssen nun die im Artikel beschriebenen erweiterten Regelungen beachten (Schriftlicher Nachweis über Safe Harbor Beitritt, Nachweis über Einhaltung der Informationspflichten, ggfs. Hinweispflichten gegenüber der Aufsichtsbehörde etc.).

Autor:

Dr. Sebastian Kraska

Rechtsanwalt