MAYER·BROWN

Legal Update
June 15, 2010

Safe Harbor: Strengere Anforderungen an den Datentransfer in die USA
Safe Harbor: More Stringent Requirements for the Transfer of Data to the USA

Wenn deutsche Unternehmen personenbezogene Daten an Unternehmen außerhalb der EU übermitteln, so müssen sie die strengen Anforderungen des Bundesdatenschutzgesetzes erfüllen. Für einen zulässigen Datentransfer müssen sie daher regelmäßig Maßnahmen treffen, um ein angemessenes Datenschutzniveau beim Empfänger sicherzustellen. Die Verwendung der Safe Harbor-Grundsätze ist eine dieser Maßnahmen.

Die für den Datenschutz zuständigen Aufsichtsbehörden haben nun neue Anforderungen an die Übermittlung personenbezogener Daten formuliert, die ganz erhebliche Folgen für in Deutschland tätige Unternehmen haben, die Daten in die USA übermitteln. Diese Firmen müssen sich daher darauf einstellen, dass der Datentransfer auf der Grundlage des Safe Harbor-Abkommens nun nur noch unter engeren Voraussetzungen als bislang zulässig ist – und dass die Datenschutz-Aufsichtsbehörden die Einhaltung dieser hohen Anforderungen genau kontrollieren werden.

Safe Harbor-Abkommen als Erlaubnis für Datenübermittlung in die USA

Die USA weisen grundsätzlich kein ausreichendes Schutzniveau für die Verarbeitung und Übermittlung personenbezogener Daten aus Europa auf. Die Übermittlung personenbezogener Daten aus Europa in Drittländer ohne angemessenes Datenschutzniveau ist nur dann erlaubt, wenn sichergestellt wird, dass ein angemessener Schutz der übermittelten Daten gewährleistet ist. Auch das Bereithalten von Daten für einen Abruf aus den USA wird als Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau gewertet.

When German companies transfer personal data to companies outside the EU then they have to fulfill the stringent requirements of the Federal Data Protection Act. Therefore, in order to ensure a permissible data transfer they must regularly take measures in order to ensure an adequate data protection level by the recipient. The application of the Safe Harbor-principles is one of these measures.

The supervisory authorities responsible for data protection have now stated new requirements for the transfer of personal data, which have quite substantial consequences for those companies doing business in Germany which send data to the USA. Therefore, these companies must be prepared for the fact that the transfer of data on the basis of the Safe Harbor Agreement is only permissible now under stricter requirements – and that the data protection supervisory authority will examine these strict requirements thoroughly.

Safe Harbor Agreement as a Permit for Data Transfer into the USA

Generally the USA do not provide a sufficient level of protection for processing and transferring personal data from Europe. The transfer of personal data from Europe to third countries without an adequate level of data protection is only permissible if it is ensured that an adequate protection regarding the transferred data is ensured. Also, keeping data available for a request from the USA is considered to be a data transfer to a third country without an adequate level of data protection.

Die EU und die USA haben im Jahr 2000 das sogenannte „Safe Harbor"-Abkommen abgeschlossen, eine Vereinbarung über die Voraussetzungen für einen erlaubten Datentransfer aus EU-Staaten in die USA.[1] Das Safe Harbour-Abkommen ermöglicht es Unternehmen, einen solchen angemessenen Datenschutzstandard dadurch herzustellen, dass sie diesem Abkommen beitreten und sich den Safe Harbor-Grundsätzen verbindlich unterwerfen. Das Verfahren hierzu ist nicht allzu kompliziert; Unternehmen können sich auf der Website des US-amerikanischen Handelsministeriums online registrieren.[2] Auf dieser Seite ist auch die Liste der Unternehmen, die sich den Safe-Harbor-Regeln unterworfen haben, abrufbar. Dass dieses Abkommen für viele Unternehmen, die aus Geschäftsgründen international Daten übertragen müssen, eine praktikable Lösung darstellt, belegen die Zahlen: nach einer Pressemitteilung des Bundesbeauftragten für den Datenschutz und der Informationsfreiheit vom 25. Oktober 2006 waren zu diesem Zeitpunkt bereits über 1.000 Unternehmen dem Safe Harbor-Abkommen beigetreten.

Neue Anforderungen der Datenschutzaufsichtsbehörden

Nun müssen sich Unternehmen auf verschärfte Anforderungen einstellen. Das gemeinsame Abstimmungsgremium der obersten Aufsichtsbehörden für den Datenschutz in der Privatwirtschaft – der sogenannte Düsseldorfer Kreis – hat kürzlich einen wichtigen Beschluss über die Datenübermittlung nach Safe Harbor-Grundsätzen gefasst.[3] Mit diesem Beschluss stellen die Aufsichtsbehörden deutlich höhere Anforderungen als bisher an die grenzüberschreitende Datenübermittlung unter dem Safe Harbor-Abkommen. Die Aufsichtsbehörden auf Landesebene orientieren sich bei ihrem Vorgehen in aller Regel stark an den Vorgaben des Düsseldorfer Kreises – daher sollten Unternehmen den Beschluss beachten und umsetzen.

In 2000 the EU and the USA signed the so called "Safe Harbor" Agreement, an agreement regarding the requirements for a permitted transfer of data from an EU member state to the USA[1]. The Safe Harbor Agreement enables companies to establish such an appropriate data standard so that they might enter into this agreement and bindingly subject themselves to the Safe Harbor's principles. The procedure for this is not too complicated: companies can register online for this with the US Department of Commerce[2]. This page also contains a list of the companies, which have subjected themselves to the Safe Harbor rules. The numbers prove that this agreement is a practicable solution for many companies which must transfer data internationally for business reasons: according to a press release from the Federal Commissioner for Data Protection and Freedom of Information dated October 25, 2006 more than 1,000 companies had already entered into the Safe Harbor Agreement.

New Requirements by the Data Protection Supervisory Authority

Now companies must prepare for stricter requirements. The joint panel of the highest supervisory authority for data protection in the private industry – the so called Düsseldorfer Kreis –recently passed an important resolution regarding the transfer of data according to the Safe Harbor principles[3]. By way of this resolution the supervisory authorities set stricter requirements than previously for the cross-border transfer of data under the Safe Harbor Agreement. German supervisory authorities generally act on the basis of the resolutions of the Düsseldorfer Kreis – hence, companies are well-advised to heed and implement this resolution.

[1] Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 vom 25.8.2000, abrufbar unter http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:DE:PDF.

[2] Diese Liste ist abrufbar unter https://www.export.gov/safehrbr/list.aspx.

[3] Der Beschluss ist u.a. abrufbar unter: https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2010/Pruefung_der_Selbst-Zertifizierung_des_Datenimporteuers/Beschluss_28_29_04_10.pdf.

[1] Decision 2000/520/EG by the Commission dated July 26, 2000 in accordance with the directive 95/46/EG of the European Parliament and the Council regarding the appropriateness of the protection granted by the "Safe Harbor" principles and the "frequently asked questions" (FAQ) in connection herewith and presented by the US Department of Commerce, ABl. L 215 dated August 25, 2000, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:DE:PDF.

[2] This list is available at https://www.export.gov/safehrbr/list.aspx.

[3] The resolution is available at: https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2010/Pruefung_der_Selbst-Zertifizierung_des_Datenimporteuers/Beschluss_28_29_04_10.pdf.

In Deutschland tätige Unternehmen, die auf der Grundlage von Safe Harbor Daten in die USA übermitteln, sind gut beraten, die Anforderungen der Aufsichtsbehörden für den Datenschutz möglichst zeitnah umzusetzen. Bei Verstößen gegen die Vorschriften des Bundesdatenschutzgesetzes drohen Bußgelder von bis zu 300.000 Euro, die Abschöpfung von Gewinnen, Schadensersatzklagen und erhebliche Rufschäden. Besonders schwere Verstöße gegen das Bundesdatenschutzgesetz sind strafbar; es droht Freiheitsstrafe bis zu zwei Jahren oder Geldstrafen.

Die einzelnen Kontrollbehörden für den Datenschutz orientieren sich in hohem Maß an den Vorgaben des Düsseldorfer Kreises. Durch dessen Beschluss ist der Datentransfer auf der Grundlage des Safe Harbor-Abkommens künftig nur noch unter engeren Voraussetzungen möglich als bislang. Der Düsseldorfer Kreis hat in seinem Papier die folgenden Voraussetzungen aufgestellt:

- Mehr als sieben Jahre zurückliegende Safe Harbor-Zertifizierungen sollen grundsätzlich nicht mehr als gültig betrachtet werden.

- Das Daten in die USA exportierende Unternehmen soll sich vom Datenempfänger nachweisen lassen, wie das importierende US-Unternehmen seinen Informationspflichten gegenüber den von der Datenverarbeitung Betroffenen nachkommt. Dies sei auch deshalb wichtig, damit der Datenimporteur in den USA diese Information an die von der Übermittlung Betroffenen weitergeben kann.

- Daten exportierende Unternehmen müssen eine Prüfung solcher Mindestkriterien dokumentieren und auf Nachfrage der Aufsichtsbehörden nachweisen können.

Folgen der verschärften Aufsichtspraxis

Im Ergebnis werden deutsche Unternehmen, die auf der Grundlage des Safe Harbor-Abkommens personenbezogene Daten in die USA übermitteln, damit verpflichtet, bei ihren Vertragspartnern die Einhaltung der Safe Harbor-Grundsätze zu überprüfen. Falls eine solche Überprüfung nicht möglich ist, empfehlen die Aufsichtsbehörden, das angemessene Datenschutzniveau auf anderem Wege zu gewährleisten, insbesondere durch die Verwendung von EU-Standardvertragsklauseln zur Datenübermittlung.

Companies doing business in Germany which transfer data to the USA on the basis of the Safe Harbor are well advised to quickly implement the requirements by the supervisory authorities for data protection. A violation of the Federal Data Protection Act's regulations can lead to fines of up to 300,000 Euro, disgorgement of profits, claims for damages and substantial damage to reputation. Particularly severe violations of the Federal Data Protection Act are punishable by imprisonment of up to two years or fines.

As a rule, the individual supervisory authorities for data protection largely align themselves in accordance with the requirements of the Düsseldorfer Kreis. By way of its resolution the data transfer on the basis of the Safe Harbor Agreement is – in the future – only possible under stricter requirements than hitherto. In its paper the Düsseldorfer Kreis has established the following requirements:

- *Safe Harbor certifications which are more than seven years old will generally no longer be considered valid.*

- *The company exporting data to the USA must receive proof from the data recipient how the importing US company is fulfilling its information obligation vis-à-vis the persons affected by the data processing. This is also important so that the data importer in the USA can pass on the information to the person affected by the transfer.*

- *Companies exporting data must document an examination of such minimal criteria and provide this to the supervisory authority upon request.*

Consequences of the stricter supervisory practice

As a result, German companies transferring personal data based upon the Safe Harbor Agreement to the USA are thereby obligated to verify the adherence to the Safe Harbor principles by their contractual partners. If such verification is not possible then the supervisory authorities recommend ensuring the appropriate data protection level by other means, in particular by using EU standard contractual terms to transfer data.

Empfehlungen

Unternehmen, die auf der Grundlage des Safe Harbor-Abkommens personenbezogene Daten an US-Unternehmen übermitteln, müssen der geänderten Praxis der Aufsichtsbehörden zeitnah Rechnung tragen, wenn sie Geldbußen, Rufschäden und mögliche Schadensersatzansprüche Betroffener vermeiden wollen.

1. Nachweise fordern

Deutsche Datenexporteure sollten umgehend auf ihre Vertragspartner zugehen und von diesen die entsprechenden Nachweise verlangen, wie sie die zuständigen Aufsichtsbehörden fordern. Diese Nachweise sollten sorgfältig archiviert werden, um sie auf Nachfrage der Aufsichtsbehörde vorlegen zu können.

2. Verträge gestalten

Bei der Gestaltung künftiger Verträge zur Datenübermittlung auf der Grundlage des Safe Harbor-Abkommens sollten deutsche Datenübermittler noch mehr darauf achten, ihre Vertragspartner in den USA auf die Einhaltung der Safe Harbor-Grundsätze zu verpflichten, z. B. durch Regelungen über Vertragsstrafen bei Verstößen gegen den Datenschutz. Zudem ist es zweckmäßig, auch Kontrollrechte des Datenübermittlers zu vereinbaren.

3. Information Betroffener

Zudem sind Klauseln zweckmäßig, nach denen der US-Vertragspartner während der Vertragslaufzeit regelmäßig aktuelle Zertifizierungsbestätigungen nachweist und kontinuierlich Nachweise vorlegt, wie das US-Unternehmen seinen Informationspflichten gegenüber den von der Datenverarbeitung Betroffenen nachkommt.

Recommendations

Companies, which transfer personal data to US companies based upon the Safe Harbor Agreement must allow for the supervisory authorities' changed practice if they want to avoid fines, damage to reputation and possible claims for damages by the affected persons.

1. Demand Proof

German data exporters should approach their contractual partners immediately and demand respective proof as required by the competent supervisory authorities. This proof should be diligently archived in order to be able to provide it to the supervisory authorities upon request.

2. Draft Agreements

When drafting future agreements for the transfer of data based upon the Safe Harbor Agreement German data transferors should be even more diligent in obligating their contractual partners in the USA to abide by the Safe Harbor principles, e.g. by setting up contractual fines when violating data protection principles. Furthermore, it is advisable to agree upon control rights by the data transferor.

3. Informing Affected Persons

Additionally, clauses are advisable according to which US contractual partners must regularly throughout the contractual relation prove current certifications and continuously provide proof of how the US company is fulfilling its information obligation vis-à-vis the persons affected by the data processing.

Sollten Sie zu dieser Publikation noch mehr Informationen wünschen, wenden Sie sich bitte an einen der folgenden Ansprechpartner:

If you have any questions or require specific advice on any matter discussed in this publication, please contact one of the lawyers listed below:

Tim Wybitul
T: +49 69 79 41 2271
twybitul@mayerbrown.com

Dr. Andrea Patzak
T: +49 69 79 41 1471
apatzak@mayerbrown.com