

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover (überarbeitete Fassung vom 23.8.2010)

Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen

Seit dem 26. Juli 2000 besteht eine Vereinbarung zwischen der EU und dem Handelsministerium (Department of Commerce) der USA zu den Grundsätzen des sog. „sicheren Hafens“ (Safe Harbor)¹. Diese Vereinbarung soll ein angemessenes Datenschutzniveau bei US-amerikanischen Unternehmen sicherstellen, indem sich Unternehmen auf die in der Safe Harbor-Vereinbarung vorgegebenen Grundsätze verpflichten. Durch die Verpflichtung und eine Meldung an die Federal Trade Commission (FTC) können sich die Unternehmen selbst zertifizieren. So zertifizierte US-Unternehmen schaffen damit grundsätzlich die Voraussetzungen, dass eine Übermittlung personenbezogener Daten aus Europa an sie unter denselben Bedingungen möglich ist, wie Übermittlungen innerhalb des europäischen Wirtschaftsraumes (EU/EWR). Das US-Handelsunternehmen veröffentlicht eine Safe Harbor-Liste aller zertifizierten Unternehmen im Internet.

Solange eine flächendeckende Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist, trifft auch die Unternehmen in Deutschland eine Verpflichtung, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe Harbor-Liste geführtes US-Unternehmen übermitteln.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass sich Daten exportierende Unternehmen bei Übermittlungen an Stellen in die USA nicht allein auf die Behauptung einer Safe Harbor-Zertifizierung des Datenimporteurs verlassen können. Vielmehr muss sich das Daten exportierende Unternehmen nachweisen lassen, dass die Safe Harbor-Selbstzertifizierungen vorliegen und deren Grundsätze auch eingehalten werden. Mindestens muss das exportierende Unternehmen klären, ob die Safe Harbor-Zertifizierung des Importeurs noch gültig ist. Außerdem muss sich das Daten exportierende Unternehmen nachweisen lassen, wie das importierende Unternehmen seinen Informationspflichten nach Safe Harbor² gegenüber den von der Datenverarbeitung Betroffenen nachkommt.

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, S. 7.

² Informationspflicht: Die Organisation muss Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über sie erhebt und verwendet, wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken. Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig gebeten werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt.

Dies ist auch nicht zuletzt deshalb wichtig, damit das importierende Unternehmen diese Information an die von der Übermittlung Betroffenen weitergeben kann.

Diese Mindestprüfung müssen die exportierenden Unternehmen dokumentieren und auf Nachfrage der Aufsichtsbehörden nachweisen können. Sollten nach der Prüfung Zweifel an der Einhaltung der Safe Harbor-Kriterien durch das US-Unternehmen bestehen, empfehlen die Aufsichtsbehörden, der Verwendung von Standard-Vertragsklauseln oder bindenden Unternehmensrichtlinien zur Gewährleistung eines angemessenen Datenschutzniveaus beim Datenimporteuren den Vorzug zu geben.

Stellt ein Daten exportierendes Unternehmen bei seiner Prüfung fest, dass eine Zertifizierung des importierenden Unternehmens nicht mehr gültig ist oder die notwendigen Informationen für die Betroffenen nicht gegeben werden, oder treten andere Verstöße gegen die Safe Harbor-Grundsätze zu Tage, sollte außerdem die zuständige Datenschutzaufsichtsbehörde informiert werden.

Eine Schlüsselrolle im Hinblick auf die Verbesserung der Einhaltung der Grundsätze kommt dabei der Zusammenarbeit der FTC mit den europäischen Datenschutzbehörden zu. Hierfür ist es erforderlich, dass die FTC und die europäischen Datenschutzbehörden die Kontrolle der Einhaltung der Safe Harbor-Grundsätze intensivieren. Die mit der Safe Harbor-Vereinbarung beabsichtigte Rechtssicherheit für den transatlantischen Datenverkehr kann nur erreicht werden, wenn die Grundsätze auch in der Praxis effektiv durchgesetzt werden.