(adjuga Information März 2016)

4. EU-US-Datenschutzschild statt Safe Harbor: Aufgaben für die Unternehmen

Auf Grundlage einer Entscheidung der Europäischen Kommission aus dem Jahr 2000 konnten USUnternehmen personenbezogene Daten in die USA übermitteln, wenn sie sich gegenüber dem USHandelsministerium zur Einhaltung der sogenannten „Safe Harbor Privacy Principles" verpflichteten. Damit sollte ein den europäischen Standards entsprechendes Datenschutzniveau zugesichert werden. Die öffentlich bekannt gewordenen Überwachungspraktiken der US-Sicherheitsbehörden, die scheinbar relativ problemlos auf in den USA gespeicherte personenbezogene Daten zugreifen konnten, haben in den vergangenen Jahren zu einer zunehmend kritischen Beurteilung der Sachlage geführt.

Mit Urteil vom Oktober 2015 hat der Europäische Gerichtshof (EuGH) schließlich das „Safe Harbor"-Abkommen für ungültig erklärt. Seit der Entscheidung dürfen personenbezogene Daten nicht mehr auf Grundlage dieses Abkommens in die USA übermittelt werden.

Die Datenschutzbehörden räumten den Unternehmen eine Übergangsfrist für die Anpassung ihrer Praxis bis Ende Januar 2016 ein. Nach einer vorläufigen politischen Einigung zwischen der Europäischen Kommission und den USA auf das sogenannte „EU-US Privacy Shield" Anfang Februar liegt seit 29. Februar nun eine Pressemitteilung über einen neuen „Angemessenheitsbeschluss" der EU-Kommission mit folgenden Eckpunkten vor:

- Selbstverpflichtung und -zertifizierung von Unternehmen auf die vorgeschriebenen EU-Sdatenschutzprinzipien führen zur Aufnahme auf die EU-US-Datenschutzschild-Liste. Verpflichtung zur Reaktion auf Beschwerden innerhalb von 45 Tagen.
- Überwachung der gelisteten Unternehmen durch das US-Handelsministerium. Sanktionierung von Verstößen gegen die Standards z.B. durch Streichung aus der Liste.
- Einrichtung einer kostenlosen Institution zur alternativen Streitbeilegung („Ombudsmann"), an die europäische Unternehmen und Bürger Beschwerden richten können. Bei Nichtabhilfe Möglichkeit der Einleitung eines Schiedsverfahrens mit vollstreckbarem Schiedsspruch.
- Prüfung der Einhaltung des Abkommens durch die Vertragspartner und Dokumentation mittels eines jährlichen Berichts.
- Ausnahmen im Rahmen der nationalen Sicherheit der USA bleiben erlaubt. Für einen massenhaften Datenzugriff gelten strengere Einschränkungen.

Nach diesen Regeln soll „ein neuer solider Rahmen für den Austausch kommerzieller Daten" geschaffen werden. Gerade der letzte Aufzählungspunkt eröffnet aber eine weite Grauzone. Im Einzelfall wären US-Dienstleister wohl weiterhin aufgrund von Ausnahmegenehmigungen verpflichtet Daten herauszugeben – gleich an welchem Standort sich das Rechenzentrum befindet.

Als nächster Schritt soll das neue Datenschutz-Rahmenabkommen durch die EU-Kommission und die EU-Mitgliedstaaten verabschiedet werden. Ob das "EU-US-Datenschutzschild" aber anschließend einer möglichen gerichtlichen Überprüfung standhalten wird, ist offen.

Die Datenschutzbehörden sind mittlerweile auf den Plan getreten. In Rheinland-Pfalz wurden bereits vor Ablauf der Schonfrist mehr als 120 behördliche Auskunftsverfahren eingeleitet. Der Hamburger Datenschutzbeauftragte will nach Zeitungsberichten gegen drei Firmen ein Bußgeldverfahren einleiten, die auch Monate nach dem EuGH-Urteil ihren Datenverkehr noch nicht umgestellt und keine andere

Rechtsgrundlage für den transatlantischen Datenaustausch geschaffen hatten. Theoretisch drohen hier Bußgelder von bis zu 300.000,- Euro.

Ins Visier der Aufsichtsbehörden geraten alle Unternehmen, die personenbezogene Daten in der EU erheben und in die USA übermitteln. Dies gilt für alle Unternehmen unabhängig von ihrer Größe oder Branchenzugehörigkeit, die personenbezogene Daten auf Servern in den USA hosten (lassen), Cloud-Services nutzen, oder Daten an eine US-amerikanische Konzernmutter oder Tochterunternehmen übermitteln. Eine Überraschung kann bei Nutzung bestimmter Software für die Datenverarbeitung drohen: je nach Architektur der Software findet möglicherweise unbemerkt vom Nutzer ein Datenaustausch mit einem Server in den USA statt.

Was müssen Unternehmen jetzt veranlassen?

Das Mindeste, was Datenschutzbehörden derzeit von den Unternehmen erwarten, ist eine Bestandsaufnahme und eine eigene Beurteilung der transatlantischen Übertragung personenbezogener Daten. Falls diese noch alleine auf Grundlage von Safe Harbor Regelungen legitimiert werden soll, besteht dringender Änderungsbedarf.

Neben der gebotenen Risikovermeidung sollte die Situation als Chance verstanden werden, bestehende Datentransfer- und Datenverarbeitungsprozesse zu überprüfen und auf eine langfristig rechtssichere Grundlage zu stellen. Rechtlich vorteilhaft sind Lösungen, bei denen die beteiligten Unternehmen denselben oder anerkannt vergleichbaren Datenschutzbestimmungen unterliegen, weil z. B. ausschließlich europäisches Datenschutzrecht auf sie Anwendung findet.

Dr. Tilo Jung *+49 6221 4340230* tilo.jung@adjuga.com