Pressemeldung

Transatlantische Datentransfers weiterhin rechtliche Grauzone: Was können Unternehmen tun?

Berlin, 06.12.2016 **Die Datenübermittlung zu Unternehmen in die USA und andere Drittstaaten ist weiterhin ein rechtlich heikles Thema und es herrscht bei vielen Unternehmen, die auf solche Datenübermittlungen „angewiesen" sind, große Unsicherheit.**
Die Datenschutzbehörden der Länder kontrollieren nun stichprobenartig deutsche Unternehmen im Hinblick auf Datentransfers in sogenannte Drittstaaten. Wieso ist ein transatlantischer Datentransfer so brisant und wie können Unternehmen prüfen, ob auch sie davon betroffen sind?

Die Übermittlung von personenbezogenen Daten ist als Unterfall der Verarbeitung von Daten nach dem Grundsatz des Verbotes mit Erlaubnisvorbehalt danach zu beurteilen, ob die Einwilligung des Betroffenen oder eine gesetzliche Erlaubnisnorm gegeben ist. Als gesetzliche Erlaubnisnorm kommt hier § 11 BDSG ins Spiel, wonach im Fall der Auftragsdatenverarbeitung der Empfänger der Daten nicht als „Dritter", sondern quasi als verlängerter Arm des datenverarbeitenden Unternehmens anzusehen ist.

Der Datentransfer innerhalb Deutschlands und auch der innerhalb des Europäischen Wirtschaftsraums ist insofern „privilegiert", als dass durch Abschluss eines entsprechenden Auftragsdatenverarbeitungsvertrages hier keine Übermittlung von Daten an Dritte gegeben ist. Diese Privilegierung entfällt, wenn es um Datentransfer ins EWR Ausland geht und diese Staaten kein vergleichbares Datenschutzniveau aufweisen.
Sollen Daten in solche Drittstaaten übermittelt werden, gilt es ein angemessenes Datenschutzniveau beim Empfänger der Daten zu gewährleisten. Diese Gewährleistung ist nach dem Wegfall des Safe Harbor Abkommens insbesondere mit den USA noch immer nicht abschließend sichergestellt. Zwar ist mit dem „EU-US Privacy Shield" kürzlich ein Folgeabkommen verabschiedet worden, jedoch leidet auch dieses nach Ansicht vieler Datenschützer an den gleichen rechtlichen Schwachstellen wie zuvor das Safe Harbor Abkommen und es ist bereits eine Klage auch gegen dieses Abkommen beim EuG anhängig.

In praktischer Hinsicht bleiben daneben die EU-Standardvertragsklauseln, Binding Corporate Rules (BCR) und die Einwilligung der Betroffenen als weitere Legitimationsmittel für den Datentransfer übrig. Erstere sind auch nicht über jeden Zweifel erhaben (auch gegen die EU-Standardvertragsklauseln ist eine Klage anhängig) und die Einwilligung ist in den meisten Fällen nicht praxisrelevant.

Was die **EU-Standardvertragsklauseln** angeht, so befinden sich die Beschlüsse zu diesen zusammen mit den Beschlüssen zu den Angemessenheitsentscheidungen zum Schutzniveau für personenbezogene Daten in Drittstaaten aktuell in der Überprüfung durch die Europäische Kommission. Mitte Oktober verkündete der Artikel 31 Ausschuss – der zuletzt für den Erlass des Privacy Shield zuständig war, dass nach seiner Ansicht die Standardvertragsklauseln in ihrer jetzigen Form rechtswidrig seien. Am 15.November traf man sich, um die Änderungsentwürfe zu den Standardvertragsklauseln zu diskutieren. Insbesondere sollen auch die Kontrollrechte der nationalen Datenschutzbehörden im Hinblick auf die Angemessenheitsentscheidung

gestärkt werden. Es wird erwartet, dass noch in diesem Jahr angepasste EU-Standardvertragsklauseln (Controller-Processor) veröffentlicht werden.

Für Datenübermittlungen zu Unternehmen in die USA und andere Drittstaaten herrscht nach wie vor keine Rechtssicherheit. **Für Unternehmen bleibt es spannend: Aktuell überprüfen Datenschutzaufsichtsbehörden in Deutschland diese Datenübermittlungen ins Ausland.**

Anfang November wurde bekannt, dass auf Initiative des Hamburger Beauftragten für Datenschutz die Datenschutzaufsichtsbehörden der Länder Bayern, Berlin, Bremen Mecklenburg-Vorpommern, Saarland, Niedersachsen, Sachsen-Anhalt, Rheinland-Pfalz und Nordrhein-Westfalen Fragebögen zu Datentransfers ins Ausland, insbesondere die USA, an 500 Unternehmen in Deutschland verschicken. In diesen Fragebögen werden die betreffenden Unternehmen zu den durch sie ins EWR-Ausland transferierten Daten befragt und insbesondere die Anwendung der einschlägigen, zuvor dargestellten Rechtsgrundlagen, für diese Übermittlung überprüft.

Hinweis für Unternehmen
Simone Rosenthal von ISiCO Datenschutz GmbH: *„Unternehmen, auch wenn sie nicht in den „Genuss" dieses Fragebogens gekommen sein sollten, sollten die aktuelle Lage nutzen, um ihre Datentransfers und insbesondere die Empfänger dieser Daten zu prüfen. Gerade im Hinblick auf die im Mai 2018 wirksam werdende EU-Datenschutzgrundverordnung mit ihren weitreichenden Änderungen und höheren Bußgeldern bei Datenschutzverstößen - so insbesondere auch bei unzulässigen Datentransfers ins EWR-Ausland - ist eine lückenlose Compliance, durch saubere vertragliche Vereinbarungen, in diesem Bereich unerlässlich."*

Firmenporträt:
Die ISiCO Datenschutz GmbH ist ein spezialisiertes Beratungsunternehmen für IT- Sicherheit, Datenschutz und Datenschutz-Compliance. Die Beratungsleistung umfasst die Umsetzung der nationalen, europäischen und internationalen Datenschutzbestimmungen im Unternehmen und die Implementierung von IT-Sicherheits- und Compliance-Systemen. Das Leistungsspektrum umfasst zudem Risikoanalysen, Audits sowie umfangreiche Rechts- und IT-Sicherheits-Gutachten. Weiterhin führt die ISiCO Datenschutz GmbH Schulungen und Seminare durch und begleitet Unternehmen bei Zertifizierungen.

Kontakt:
ISiCO Datenschutz GmbH │Am Hamburger Bahnhof 4 │10557 Berlin Tel +49 (0)30 213002850 Fax +49 (0)30 213002899 │www.isico-datenschutz.de │Geschäftsführung: Simone Rosenthal │ E-Mail: berlin@isico-datenschutz.de │ PR-Anfragen: Deborah Reusch reusch@isico-datenschutz.de