

IT-Sonderticker 22.07.2020

Der Sonderticker informiert Sie über folgendes Thema:

- EuGH erklärt EU-US Privacy Shield für ungültig: Einzelfallprüfung beim Einsatz von EU-Standardvertragsklauseln notwendig
-

Der EuGH hat sein Urteil im „Schrems II“-Verfahren (C-311/18) verkündet und das sogenannte EU-US Privacy Shield gekippt. Von der Entscheidung sind nicht nur Anbieter und Nutzer von Cloud-Diensten und Social-Media-Plattformen betroffen. Auch Unternehmen mit Konzerngesellschaften außerhalb der EU müssen ihren konzerninternen Datenaustausch prüfen und anpassen.

Der österreichische Datenschützer Max Schrems hatte bereits das Safe-Habor-Abkommen zwischen der EU und den USA zu Fall gebracht. Nun hat der EuGH auf seine Klage hin auch das Nachfolgeabkommen über den transatlantischen Datentransfer, das EU-US Privacy Shield, für ungültig erklärt.

Die ebenfalls angegriffenen EU-Standardvertragsklauseln hat der EuGH nicht für ungültig erklärt. Dazu hat der EuGH jedoch entschieden, dass beim Einsatz von EU-Standardvertragsklauseln zusätzlich geprüft werden müsse, ob in dem Drittland tatsächlich angemessene durchsetzbare Rechte und wirksame Rechtsbehelfe bestehen. Sofern dies nicht der Fall ist, dürfen – und müssen – nach der Entscheidung des EuGH die Aufsichtsbehörden entsprechende Datenübermittlungen trotz bestehender EU-Standardvertragsklauseln aussetzen oder verbieten.
Hintergrund der EuGH-Entscheidung

Die DSGVO bildet für personenbezogene Daten in der EU und dem EWR den Rechtsrahmen, der die Grundrechte der Betroffenen schützt und strenge Vorgaben für Art und Umfang von Datenverarbeitungen aufstellt. Werden Daten außerhalb dieses geschützten Raumes verarbeitet, müssen die Unternehmen nach den Vorgaben der DSGVO zusätzliche Schutzmaßnahmen treffen. Die EU-Kommission kann z.B. Länder als sicher einstufen oder Abkommen oder Standardvertragsklauseln über so genannte Angemessenheitsbeschlüsse für ausreichend sicher erklären. Solche Beschlüsse liegen für das EU-US Privacy Shield vor und auch für die aktuell gültigen EU-Standardvertragsklauseln.

Konkret hat der EuGH nun den sogenannten Angemessenheitsbeschluss für das EU-US Privacy Shield für ungültig erklärt. Damit sind alle Datentransfers in die USA, die allein auf das EU-US Privacy Shield gestützt werden unzulässig. Viele US-Unternehmen bieten jedoch zusätzlich den Abschluss von EU-Standardvertragsklauseln an. Diese sind nach der EuGH-Entscheidung weiterhin gültig. Allerdings können die zuständigen Aufsichtsbehörden Datentransfers trotz abgeschlossener EU-Standardvertragsklauseln ab sofort für unzulässig erklären und untersagen.
Was heißt das im Detail?

Der EuGH hat den Angemessenheitsstatus für das EU-US-Privacy Shield in Bezug auf amerikanische Internet Service Provider (ISP) für unzulässig erklärt, da es hier Zugriffsrechte von staatlicher Seite gibt, welche nicht dem Verhältnismäßigkeitsgrundsatz nach europäischen Standards entsprechen. Andere Unternehmen oder Konzerngesellschaften können sich weiterhin auf EU-Standardvertragsklauseln berufen, wenn geeignete Garantien weiter ausgebaut und umgesetzt werden. Ob es auch hier zu Zugriffen staatlicher Stellen kommen kann, muss noch geprüft werden. Darüber müssen Unternehmen ihre Möglichkeiten der Einhaltung der Standardvertragsklauseln auch nach Abschluss regelmäßig überprüfen. Ein Restrisiko wird wohl aber auch hier bestehen bleiben
Wie geht es nun weiter?

Sowohl die deutschen Aufsichtsbehörden als auch die Behörden in den anderen EU-Ländern werden nun zunächst eine eigene Auswertung der Entscheidung vornehmen. Zu erwarten ist, dass sie anschließend – wie bereits nach der Entscheidung zur Ungültigkeit des Safe-Habor-Abkommens – Empfehlungen veröffentlichen werden und den Unternehmen auch eine gewisse Zeit eingeräumt werden wird, ihre Datenverarbeitungen anzupassen oder umzustellen. Bis dato haben sich schon verschiedene Aufsichtsbehörden zu der Entscheidung geäußert.

Das LfDI Rheinland-Pfalz hat bereits FAQs veröffentlicht. Hier wird insbesondere darauf hingewiesen, dass es keine Übergangsfrist gibt und die Datenübermittlung ab sofort unrechtmäßig und zu stoppen ist, wenn keine Alternativen in Betracht kommen. Die Verantwortlichen müssen prüfen, ob die Garantien der Standardvertragsklauseln in dem jeweiligen Drittland eingehalten werden können. Ob das Urteil Auswirkungen auf andere Transferinstrumente der DSGVO hat, werde derzeit noch geprüft.

Auch der Bundesbeauftragte für Datenschutz sieht den internationalen Datentransfer – mit Ausnahme des EU-US-Privacy Shields - immer noch als möglich an.

Der hamburgische Beauftragte für Datenschutz sieht in dem Urteil einerseits eine erhöhte Unsicherheit für den Umgang mit Standardvertragsklauseln und andererseits liege der Ball jetzt bei den Aufsichtsbehörden, die nun die Standardvertragsklauseln insgesamt kritisch hinterfragen müssten.

Auch der thüringische Beauftragte für Datenschutz kann aktuell nicht einschätzen, wie eine Datenübermittlung in die USA DSGVO-konform durchgeführt werden soll, wenn der Datenexporteur und der Datenempfänger vor der Übermittlung prüfen müssen, ob die Standardvertragsklauseln eingehalten werden.

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat datenverarbeitende Stellen in Berlin aufgefordert, in den USA gespeicherte personenbezogene Daten nach Europa zu verlagern. Verantwortliche, die – insbesondere bei der Nutzung von Cloud-Diensten – personenbezogene Daten in die USA übermitteln, werden von der Berliner Behörde angehalten, umgehend zu Dienstleistern in der Europäischen Union oder in einem Land mit angemessenem Datenschutzniveau zu wechseln.

Dauerhafte Lösungen für sichere internationale Datentransfers werden mit hoher Wahrscheinlichkeit neue internationale Abkommen insbesondere mit den USA erfordern.
Was heißt das für die Unternehmenspraxis?

Unternehmen sollten jetzt prüfen, welche Datentransfers in Drittstaaten sie vornehmen, welche dieser Transfers unternehmenskritisch sind und welche Möglichkeiten für Ad-hoc-Maßnahmen bestehen, falls eine Behörde den Transfer kurzfristig untersagt. Sofern Datentransfers in die USA ausschließlich auf das EU-US Privacy Shield gestützt werden, müssen Unternehmen unverzüglich alternative Vereinbarungen treffen. Meist werden sich EU-Standardvertragsklauseln anbieten, wenngleich auch diese keine Garantie für eine dauerhafte Zulässigkeit bieten. Anbieter, die Daten in den USA verarbeiten, sollten insbesondere prüfen, ob sich der Personenbezug von Daten durch Anonymisierung oder Verschlüsselungsmaßnahmen aufheben oder begrenzen lässt.

Des Weiteren müssen Alternativen her. Eine schnelle Möglichkeit für Website- und App-Betreiber ist die Einholung einer ausdrücklichen Einwilligung in den Drittlandstransfer über den Cookie-Banner. Liegen die Voraussetzungen einer wirksamen Einwilligung vor, kann diese einen Datentransfer auch in die USA rechtfertigen. Allerdings müssen die Nutzer z.B. über die Datenschutzhinweise deutlich über die dadurch entstehenden Risiken aufgeklärt werden.

Nikolaus Bertermann
n.bertermann@skwschwarz.de

Dr. Elisabeth von Finckenstein
E.vonFinckenstein@skwschwarz.de

Dr. Stefan Peintinger
s.peintinger@skwschwarz.de