Börsen-Zeitung
Zeitung für die Finanzmärkte
Ausgabe 146 vom 01.08.2020, Seite 9

RECHT UND KAPITALMARKT

Wie Unternehmen auf das „Schrems II“-Urteil reagieren sollten

EuGH kippt Privacy Shield – Datentransfers auf dem Prüfstand

Von Christian Tinnefeld und Henrik Hanßen *)

Börsen-Zeitung, 1.8.2020

Für Datenschützer ist es ein turbulenter Sommer: Mit Urteil vom 16. Juli 2020 hat der Europäische Gerichtshof (EuGH) den EU-US Privacy Shield für unwirksam erklärt und damit die Rechtmäßigkeit der Übermittlung personenbezogener Daten von Europa in die Vereinigten Staaten in Frage gestellt. In Zeiten globaler Unternehmensstrukturen und Nutzung der Dienste von IT-Unternehmen aus den USA sind nahezu alle Unternehmen von dem Urteil betroffen. Inzwischen haben sich auch die Datenschutzbehörden zu dem Urteil geäußert und Unternehmen angehalten, ihre Datentransfers in außereuropäische Staaten zu überprüfen.

Das aktuelle „Schrems II“-Urteil ist die Fortsetzung des Verfahrens, das der Österreicher Maximilian Schrems vor dem Irish High Court angestoßen hat und das bereits im Jahr 2015 zur Unwirksamkeit des „Safe Harbor“-Abkommens führte. Im Kern ging es um die Rechtmäßigkeit von Datentransfers in die USA, die Schrems aufgrund der Überwachungsaktivitäten der US-Geheimdienst- und Strafverfolgungsbehörden in Zweifel zog. Der EuGH hatte im Verfahren C-311/18 nun darüber zu entscheiden, ob der 2016 eingeführte Privacy Shield als Nachfolger von „Safe Harbor“ sowie die von vielen Unternehmen genutzten EU-Standardvertragsklauseln (SCC) wirksam sind.

Der EuGH kam zum Ergebnis, dass der Beschluss zum Privacy Shield unwirksam sei, da durch diesen kein mit der EU „gleichwertiges Schutzniveau“ hergestellt würde. In der Folge sind Datentransfers, die bislang allein auf den Privacy Shield gestützt wurden, ab sofort rechtswidrig.

Hingegen befand der EuGH, dass die Verwendung von SCC grundsätzlich zur Legitimierung von Datentransfers in Drittstaaten außerhalb des Europäischen Wirtschaftsraums ausreicht. Er stellte jedoch klar, dass Unternehmen jeweils im Einzelfall prüfen müssen, ob die SCC aufgrund der Rechtslage im Staat des Datenempfängers tatsächlich eingehalten werden können.

Der bisher weit verbreiteten „Paper Compliance“ durch bloßes Unterzeichnen der SCC erteilte der EuGH damit eine klare Absage. Der EuGH stellte zudem fest, dass Unternehmen über die SCC hinaus nötigenfalls „zusätzliche Maßnahmen“ treffen müssten, um ein mit der EU gleichwertiges Schutzniveau zu erreichen.

Ob die SCC aufgrund der Feststellungen des EuGH zum US-Recht überhaupt noch für Datentransfers in die USA genutzt werden können, ist aktuell umstritten. Während einige Behörden die Nutzung von SCC in bestimmten Fällen noch für zulässig halten, stellte zum Beispiel die Berliner Datenschutzbehörde generell Datenübermittlungen in die USA in Frage. Nach der Veröffentlichung des EuGH-Urteils bekräftigten die Datenschutzbehörden umgehend die Pflicht von Unternehmen zur Vornahme von Einzelfallprüfungen und fordern Benachrichtigungen, falls kein gleichwertiges Datenschutzniveau hergestellt werden kann.

Auch wenn die Behörden sich gegenwärtig noch abstimmen, ist mittelfristig, etwa aufgrund von Beschwerden, mit Prüfverfahren gegen Unternehmen zu rechnen – wie auch schon nach dem „Safe Harbor“-Urteil.

Handlungsempfehlungen

Unternehmen sollten kurzfristig tätig werden, um internationale Datentransfers in ihrem Verantwortungsbereich mit dem Urteil des EuGH in Einklang zu bringen:

- Mit einer Bestandsaufnahme („Data Mapping“) sollten alle internationalen Datentransfers mitsamt den angewendeten Rechtsgrundlagen identifiziert werden – unabhängig davon, ob die Transfers konzernintern oder an externe Empfänger (zum Beispiel IT-Dienstleister) stattfinden.
- Datentransfers auf Grundlage des Privacy Shields sollten eingestellt werden, soweit sie nicht auf eine alternative Rechtsgrundlage gestützt werden können. Hierzu sollten Unternehmen auf ihre Dienstleister zugehen und über alternative Regelungen sprechen.
- Sofern SCC als Rechtsgrundlage genutzt werden, sollte deren Anwendbarkeit im Einzelfall geprüft werden, unter Berücksichtigung des lokalen Rechts im Drittstaat und Art und Umfang des konkreten Datentransfers.
- Nötigenfalls sind zusätzliche Maßnahmen umsetzen, wie weitere vertragliche Vereinbarungen und technische Maßnahmen (z. B. Pseudonymisierung und Ende-zu-Ende-Verschlüsselungen).
- Wo möglich sollten alternative Rechtsgrundlagen genutzt werden, wie etwa behördlich genehmigte verbindliche Unternehmensrichtlinien (Binding Corporate Rules) oder Ausnahmen nach Art. 49 Datenschutz-Grundverordnung (DSGVO), z. B. Einwilligungen der betroffenen Personen.
- Zudem sollten Unternehmen die Aktivitäten der Europäischen Kommission beobachten, die angekündigt hat, ein angemessenes Datenschutzniveau bei transatlantischen Datentransfers sicherzustellen und die SCC schnellstmöglich zu überarbeiten.

Wichtig ist schließlich, dass durch das Urteil des EuGH nicht nur Datenübermittlungen in die USA, sondern in sämtliche Länder außerhalb des Europäischen Wirtschaftsraums auf dem Prüfstand stehen.

*) Dr. Christian Tinnefeld ist Partner und Dr. Henrik Hanßen Senior Associate von Hogan Lovells.