# Riskanter Datentransfer

## Nun werden die immensen Nachwirkungen des EuGH-Urteils zu Schrems II sichtbar. Was ist zu tun?

Der Europäische Gerichtshof (EuGH) hat das sogenannte Privacy-Shield-Abkommen am 16. Juli 2020 für ungültig erklärt (C-311/18). Die Entscheidung wird für die Wirtschaft gravierende Folgen haben, falls die Datenschutzbehörden und die nationalen Gerichte sie konsequent umsetzen. Denn das Urteil betrifft nicht nur Unternehmen, die Daten auf der Grundlage des Privacy-Shield-Abkommens in die Vereinigten Staaten übermitteln. Es hat auch für die Übermittlung personenbezogener Daten aus der EU beziehungsweise dem Europäischen Wirtschaftsraum (EWR) auf der Basis anderer Rechtsgrundlagen erhebliche Folgen.

Dies gilt etwa für die sogenannten EU-Standardvertragsklauseln. Diese Klauseln sind von der EU-Kommission vorgegebene Musterverträge für Datenübermittlungen. Die Umsetzung der Vorgaben der Standardvertragsklauseln soll beim Empfänger der Daten ein angemessenes Datenschutzniveau sicherstellen. In der Praxis haben diese Standardvertragsklauseln eine enorme Bedeutung. Sie sind die für die Wirtschaft wichtigste rechtliche Grundlage für den internationalen Datenaustausch. Zwar hat der EuGH nur das Privacy-Shield-Abkommen für ungültig erklärt. Viele der in dem Urteil getroffenen Aussagen lassen sich aber auch auf Datenübermittlungen auf Basis der Standardvertragsklauseln übertragen.

Die europäischen Datenschutzbehörden fordern daher vor einer Offenlegung von Daten gegenüber einem Empfänger in einem Drittstaat eine gründliche Risikoprüfung. Unternehmen müssten in jedem Einzelfall prüfen, ob eine Weitergabe von Daten trotz der von den europäischen Richtern bemängelten Kritikpunkte noch zulässig ist. Das Ergebnis dieser Prüfung müsse zudem in einer Form dokumentiert werden, die eine Überprüfung durch die Datenschutzbehörden erlaube.

Die Forderungen des EuGH haben Sprengkraft. Denn sie betreffen eine Vielzahl von Sachverhalten – etwa die Zusammenarbeit mit IT-Anbietern aus den Vereinigten Staaten oder andere Drittstaaten ohne angemessenes Datenschutzniveau oder die konzerninterne Weitergabe.

Einzelne Datenschutzbehörden haben bereits Kontrollen angekündigt. In Irland ist die Datenschutzbehörde gegen Facebook aktiv geworden *(siehe Seite 22)*. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit sieht mit dem Urteil „die Stunde der digitalen Eigenständigkeit Europas gekommen". Zudem weist sie auf die Möglichkeit hin, auch immaterielle Schäden wegen Datenschutzverletzungen vor Gericht einzuklagen. Betroffene Personen könnten dann Schadenersatz verlangen, der eine „abschreckende Höhe" aufweisen muss. Erste Verbraucheranwälte, Prozessfinanzierer und Legal-Tech-Unternehmen haben sich bereits auf solche Datenschutzklagen spezialisiert.

Unternehmen sind gut beraten, wirtschaftlich notwendige Datenübermittlungen durch Risikoprüfungen abzusichern. Fehlt es an der von den Datenschutzbehörden geforderten dokumentierten Risikobewertung, wird die Verteidigung gegen Bußgelder oder Schadenersatzansprüche schwer. Daher geht es vor allem darum, für die grenzüberschreitende Übermittlung von Daten eine belastbare Verteidigungsposition aufzubauen. Hierfür sollten Unternehmen konkrete Maßnahmen und Umstände dokumentieren, die für einen hinreichenden Schutz der übermittelten personenbezogenen Daten sprechen. Teil einer solchen Verteidigungsstrategie ist die Bewertung der Sensibilität der übermittelten Daten. Sofern diese für ausländische Geheimdienste nicht sonderlich relevant sind, spricht dies für die Zulässigkeit der Datenübermittlung. Auch die Verschlüsselung von Daten während der Übermittlung kann ein Baustein sein. Zudem können Unternehmen die Standardvertragsklauseln durch zusätzliche vertragliche Regelungen absichern, etwa durch Informationspflichten und Sonderkündigungsrechte.

Der Autor **Tim Wybitul** ist Partner der Kanzlei Latham & Watkins.

Frankfurter Allgemeine Zeitung, 16.09.2020, Wirtschaft, Seite 16