Tobias Straub

Instrumente für Drittstaaten-Transfers

Die Schrems II-Entscheidung des EuGH hat internationale Datentransfers in den Fokus der Aufmerksamkeit gerückt. Im Folgenden soll ein Überblick über die rechtlichen Instrumente für Übermittlungen in Drittländer mit einer Einschätzung ihrer Praktikabilität gegeben werden.

Als „Drittstaat" oder „Drittland" gelten Länder außerhalb des Europäischen Wirtschaftsraums, welcher außer der EU noch Island, Liechtenstein und Norwegen umfasst. Während die DS-GVO hier unmittelbar anwendbares Recht ist und damit ein einheitliches Schutzniveau gewährleistet, gilt dies für Drittländer aufgrund der jeweiligen nationalen Regelungen naturgemäß zunächst einmal nicht. Die DS-GVO anerkennt die Notwendigkeit, personenbezogene Daten für wirtschaftliche Zwecke auch in Drittländer zu übermitteln, verlangt aber, dass das durch die DS-GVO gewährte Schutzniveau nicht „untergraben" wird (Art. 44). Ein gängiger Anwendungsfall besteht darin, dass ein Unternehmen in der EU („Datenexporteur") einen Cloud-Dienst eines Anbieters („Datenimporteur") nutzt und es dabei zur Verarbeitung personenbezogener Daten von Mitarbeitern oder Kunden und – da die meisten dieser Dienste von US-amerikanischen Firmen angeboten werden – eben auch zu einer Übermittlung in ein Drittland kommt.

Der Verantwortliche hat die Zulässigkeit der Verarbeitung nach einem zweistufigen Ansatz zu prüfen: zunächst sind alle Vorgaben der DS-GVO maßgeblich, die auch bei einer Verarbeitung ohne Drittstaaten-Bezug gelten. (Da häufig eine Verarbeitung im Auftrag oder unter gemeinsamer Verantwortung vorliegen dürfte, ist insbesondere Art. 28 bzw. Art. 26 zu berücksichtigen und eine Vereinbarung mit den dort vorgesehenen Inhalten zu treffen.) Zusätzlich sind die für Drittstaaten spezifischen Regelungen der Art. 44 ff. zu berücksichtigen, die die relevanten Grundsätze formulieren und verschiedene rechtliche Instrumente für die Übermittlung anbieten. Da es sich bei Cloud-Diensten häufig um ein Massengeschäft handelt, haben sowohl Dienstleister als auch Auftraggeber verständlicherweise ein Interesse an ebenso standardisierten wie leicht umzusetzenden rechtlichen Instrumenten.

Am unkompliziertesten ist der Mechanismus des *Angemessenheitsbeschlusses* von Art. 45, der ohne weitere Anforderungen Datenübermittlungen in Drittländer erlaubt, die – nach Feststellung durch die EU-Kommission – als Ganzes oder in Teilen über ein angemessenes Datenschutzniveau verfügen. Für die USA galt der Angemessenheitsbeschluss bislang nur für Unternehmen, die sich gemäß Privacy Shield selbst zertifiziert hatten, bevor der EuGH dieses Abkommen jetzt gekippt hat. Verantwortliche können Übermittlungen in die USA nun nicht mehr darauf stützen und müssen auf andere Instrumente für den Transfer ausweichen oder diesen ganz einstellen.

Für Drittländer ohne Angemessenheitsbeschluss kann auf die in Art. 46 beschriebenen Instrumente *geeigneter Garantien* zurückgegriffen werden, wobei unter den in Abs. 2 genannten Regelbeispielen die schon aus der Datenschutz-Richtlinie bekannten *Standardvertragsklauseln* (jetzt: „Standard-Datenschutzklauseln", SCCs) der Kommission die höchste praktische Relevanz haben. Typischerweise werden sie formularmäßig verwendet, dürfen aber prinzipiell um weitere Klauseln oder Garantien ergänzt werden, sofern diese keinen Widerspruch ergeben oder zulasten der Betroffenen gehen (EG 109).

Binding Corporate Rules gem. Art. 47 können dagegen nur Übermittlungen innerhalb internationaler Konzerne erleichtern. Branchenspezifische Verhaltensregeln (*Code of Conduct*) gem. Art. 40 und *Zertifizierungen* gem. Art. 42 – jeweils in Verbindung mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Datenimporteurs zur Anwendung der geeigneten Garantien – sind neu in die DS-GVO aufgenommene Mechanismen, die aber noch keine größere Verbreitung gefunden haben. Alle drei vorgenannten Instrumente bedürfen der aufsichtsbehördlichen Genehmigung, ebenso individuelle *„ad hoc"-Verträge* gem. Art. 46 Abs. 3 lit a.

Der EuGH hat die SCCs nicht grundsätzlich für ungültig erklärt, jedoch – da sie als privatrechtlicher Vertrag keine Bindungswirkung für Behörden im Drittland haben – die Pflicht des Datenexporteurs betont, zu prüfen, ob durch sie ein effektiver Schutz und insbesondere durchsetzbare Rechte und wirksame Rechtsbehelfe gewährleistet werden. Die Kommission hat jüngst einen Entwurf für neue SCCs vorgestellt, die in einem Paket alle vier möglichen Kombinationen von Verantwortlichen und Auftragsverarbeitern als Vertragsparteien abdecken und auch eine gesonderte Vereinbarung nach Art. 28 entbehrlich machen. Aufgrund aktueller Einschätzungen der Aufsichtsbehörden muss aber angenommen werden, dass auch die neuen SCCs nicht pauschal als alleiniger Mechanismus insbesondere für die USA als ausreichend zu bewerten sind. Vielmehr können in bestimmten Situationen zusätzlich starke *technische Maßnahmen* (wie Pseudonymisierung oder Verschlüsselung ohne Zugriffsmöglichkeit des Datenimporteurs) erforderlich sein. Sollte es der Anwendungsfall aber technisch erfordern, dass dem Datenimporteur gewisse (Meta-)Daten zugänglich sind, so sind solche zusätzlichen Maßnahmen gar nicht umsetzbar.

Schlussendlich bleiben noch die in Art. 49 abschließend aufgeführten und eng auszulegenden *Ausnahmen* (welche ebenfalls unter dem Vorbehalt von Art. 44 stehen). Zuvorderst steht dabei die *ausdrückliche Einwilligung* der betroffenen Person, welche über die möglichen Risiken einer Übermittlung ohne Angemessenheitsbeschluss und ohne geeignete Garantien aufzuklären ist. Verantwortliche haben zu bedenken, dass dieser Weg aufgrund der üblichen Anforderungen an eine Einwilligung (u.a. Freiwilligkeit und Widerrufbarkeit) mit praktischen Schwierigkeiten verbunden sein kann. Auch bei den Tatbeständen der *Erforderlichkeit für die Erfüllung eines Vertrags* ist die Einschränkung zu beachten, dass diese nur für „gelegentliche" Übermittlungen angewandt werden dürfen. Neben anderen Tatbeständen von untergeordneter Bedeutung für wirtschaftliche Tätigkeiten enthält Abs. 1 UAbs. 2 noch die Möglichkeit der *Abwägung mit den zwingenden berechtigten Interessen* des Verantwortlichen. Auch dieses „letzte Mittel" ist für eine breite Anwendung nicht geeignet, sondern explizit nur für nicht wiederholte Übermittlungen, die eine begrenzte Zahl von Personen betreffen. Die Pflicht zur Information der Aufsichtsbehörde dürfte zudem für Verantwortliche eine eher abschreckende Wirkung haben.

Auch ein halbes Jahr nach der EuGH-Entscheidung ist die aufgekommene Unsicherheit hinsichtlich Drittstaatentransfers nicht ausgeräumt, so dass Verantwortliche weiter gefordert sind.