Philipp Quiel
Schriftleitung
Datenschutz-Berater

Durchsetzbare Rechte und wirksame Rechtsbehelfe

Sehr geehrte Leserinnern und Leser,

Datenübermittlungen in Drittländer werden wohl noch eine Weile im Zentrum datenschutzrechtlicher Beratungen und Diskussionen stehen. Sie gehören zum derzeitigen digitalen Alltag und sind häufig gar nicht auf den ersten Blick als grenzüberschreitendes Handeln zu erkennen.

Sofern für ein Drittland kein Angemessenheitsbeschluss getroffen wurde, sind vor allem geeignete Garantien nach Art. 46 Abs. 2 DSGVO von hoher Praxisrelevanz. Damit Standardvertragsklauseln, Binding Corporate Rules und andere in Art. 46 Abs. 2 DSGVO genannte Garantien als Mechanismus verwendet werden können, müssen betroffenen Personen nach Abs. 1 der Norm auch „durchsetzbare Rechte" und „wirksame Rechtsbehelfe" zur Verfügung stehen. Mit „durchsetzbaren Rechten" sind die Betroffenenrechte aus Kapitel III DSGVO und weitere in der Verordnung garantierte Rechte von Betroffenen gemeint. Die Voraussetzung, dass „wirksame Rechtsbehelfe" vorhanden sein müssen, ist eine Ausprägung des in Art. 47 der Charta der Grundrechte der Europäischen Union garantierten „Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht". Ohne wirksame Rechtsbehelfe würden die Rechte von Betroffenen auch ein Stück weit ins Leere laufen, wenn Uneinigkeiten zwischen Betroffenen und Aufsichtsbehörden und Verantwortlichen bei der Erfüllung dieser nicht gerichtlich überprüft werden könnten.

Für weltweit datenübermittelende Unternehmen ist es problematisch, dass „durchsetzbare Rechte" und „wirksame Rechtsbehelfe" zum überwiegenden Teil von der Rechtsordnung im Drittland abhängig sind. Zwar kann ein Verantwortlicher sich selbst dazu verpflichten, bestimmte Rechte zu erfüllen und die Erfüllung dieser überprüfen zu lassen. Allerdings hilft dies nicht dabei Unzulänglichkeiten in der Rechtsordnung des Drittlandes zu überwinden. Wenn im Drittland beispielsweise Betroffenen aus der EU keine Rechte zum Klagen vor Gerichten im Drittland zustehen, kann ein Unternehmen daran nichts ändern. Wenn in einer Rechtsordnung staatliche Stellen dazu ermächtigt werden, ohne hinreichende Einschränkungen und Bedingungen auf Daten zuzugreifen, können Unternehmen gegen solche Zugriffe keine durchsetzbaren Rechte und wirksamen Rechtsbehelfe garantieren. In solchen Fällen ist es das Drittland selbst, welches das Probleme durch nicht hinreichend an Bedingungen geknüpfte und gerichtlich nicht überprüfbare Zugriffe schafft.

Völkerrechtliche Abkommen, in denen sich alle Vertragsstaaten dazu verpflichten, Rechte unabhängig von der Staatsangehörigkeit und dem Aufenthalt zu garantieren, bieten in diesem Kontext eine Lösungsmöglichkeit. Es ist durchaus denkbar, dass völkerrechtliche Abkommen insgesamt zur Garantie eines Mindestschutzniveaus in Zukunft eine stärkere Rolle spielen werden. Das Übereinkommen Nr. 108 des Europarates zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten ist der erste verbindliche völkerrechtliche Vertrag mit datenschutzrechtlichem Inhalt. Vertragsparteien dieses Übereinkommens müssen nicht zwangsläufig Teil des Europarates, sondern können auch Nicht-Mitgliedstaaten sein.

Bei der Prüfung des Schutzniveaus in Drittländern, die Vertragspartei sind, beeinflussen die im Übereinkommen geregelten Verpflichtungen das Schutzniveau positiv. Carlo Piltz und ich haben auf delegedata.de einen Vorschlag dazu veröffentlicht, wie man die Regeln aus dem Übereinkommen Nr. 108 und der künftig wohl geltenden Version aus 2018 bei der Prüfung des Schutzniveaus in einem Drittland mit beachten kann.

Beim Umgang mit dem Thema Datenübermittlungen in Drittländer wünsche ich Ihnen allen starke Nerven und kreative Lösungsideen sowie beim Lesen dieser Ausgabe viel Spaß.

Ihr

Philipp Quiel