Quo vadis?

Der internationale Datenverkehr nach dem Schrems II-Urteil des EuGH

Mag. Dr. Peter Wagesreiter, LL.M. (UPenn) ist Partner bei HSP Rechtsanwälte GmbH in Wien. Er ist Experte für Compliance, Corporate Governance und Datenschutz und in diesen Bereichen auch international tätig. Darüber hinaus ist Dr. Peter Wagesreiter auf M&A, Bank- und Kapitalmarktrecht spezialisiert und auch im Bundesstaat New York als Rechtsanwalt zugelassen.

Mag. Samir Pajalic ist Rechtsanwaltsanwärter bei HSP Rechtsanwälte GmbH und nebenbei Lektor an der Fachhochschule des bfi Wien. Er ist im Team von Dr. Peter Wagesreiter und Dr. Jörg Winkler für Compliance, Corporate Governance und Datenschutz tätig. Darüber hinaus ist Mag. Samir Pajalic auf Niederlassungs- und Gesellschaftsrecht spezialisiert.

Der EuGH hat mit der Entscheidung vom 16.07.20, C-311/18, Schrems II, das EU-US-Privacy Shield-Abkommen mit sofortiger Wirkung für ungültig erklärt. Alternativen der Datenübermittlung in Drittländer sind neu zu evaluieren. *Standarddatenschutzklauseln (SDK)* bleiben wirksam, aber sind keine Zauberformel.

Hintergrund der Entscheidung

Am 16.07.20 erklärte der EuGH den Angemessenheitsbeschluss der EU-Kommission über das EU-US- Privacy Shield durch das ***Schrems II***-Urteil für ungültig.

Maßgebend für diese Entscheidung waren die unverhältnismäßigen Überwachungsprogramme – sicherheitsbehördliche (FBI) und geheimdienstliche (NSA) Befugnisse – in den USA und der daraus resultierende mangelhafte Rechtsschutz für EU-Bürger.

SDK bleiben gültig – sind jedoch keine Zauberformel

Die SDK wurden vom EuGH nicht aufgehoben und die Zulässigkeit als Instrument zur Gewährleistung eines angemessenen Schutzniveaus bei der Übermittlung von personenbezogenen Daten in Drittstaaten bestätigt. Zugleich hat der EuGH aber darauf verwiesen, dass der formale Abschluss der SDK allein nicht ausreichend ist. Vielmehr müssen Datenexporteur und -importeur in jedem Einzelfall sicherstellen und überprüfen, dass die Daten im Drittland den gleichen Schutz genießen, wie sie ihn innerhalb der EU aufgrund der ***DSGVO*** und der EU-GRC erhalten. Ist dieser Schutz nicht gewährleistet, so hat der Datenexporteur die Übermittlung der Daten bis zur Sicherstellung eines angemessenen Schutzniveaus auszusetzen oder zu beenden. Nach den rezenten Stellungnahmen der EU-Aufsichtsbehörden könne eine Datenübermittlung allein auf der Basis von SDK – ohne zusätzliche Maßnahmen – eine mögliche Inanspruchnahme des Unternehmens wegen eines Datenschutzverstoßes auslösen.

Die grundlegende Frage ist, wann ein angemessenes Schutzniveau im Drittstaat gewährleistet ist. Der EuGH fordert einen Art. 47 GRC gleichgestellten Rechtsschutz. Hinzukommend müssen Eingriffe in Privatsphäre und ***Datenschutz*** für die Zweckerreichung notwendig und auf ein verhältnismäßiges Maß beschränkt sein. Diesbezüglich können die Leitlinien der Art. 29 Datenschutzgruppe herangezogen werden.

Was ist jetzt zu tun?

Konkrete und verlässliche Leitlinien oder Empfehlungen gibt es seitens der Behörden bisher nicht. Unternehmen sollten sich daher zunächst selbst Gedanken machen, wie sie Datenübermittlungen in Drittstaaten künftig organisieren, wobei hier auch Unterauftragsverarbeitungsverhältnisse zu beachten sind. Wer also einen Auftragsverarbeiter innerhalb der EU einsetzt, der wiederum einen Unterauftragsverarbeiter in den USA oder einem anderen Drittstaat beauftragt, muss seine Datenverarbeitungsprozesse ebenfalls überprüfen und entsprechend anpassen. Außerdem ist zu berücksichtigen, dass auch die Überarbeitung weiterer Datenschutzmaßnahmen (Datenschutzerklärungen, Datenauskünfte und Verfah-

HSP. LAW

Stichworte

Standarddatenschutzklauseln (SDK)

Schrems II

DSGVO

Datenschutz

Internationale Datenübermittlung

rensverzeichnisse) erforderlich ist. Zudem können ***internationale Datenübermittlung***en auch die Auswahl geeigneter technischer und organisatorischer Maßnahmen gem. Art. 32 DSGVO sowie die Risikobewertung im Rahmen von Datenschutzfolgeabschätzungen oder einer möglichen Datenpanne beeinflussen. Der Einsatz von geeigneten Verschlüsselungstechnologien könnte eine Antwort auf zusätzliche Sicherheit für die Datenübermittlung sein.

Alternative Schutzmechanismen?

Binding Corporate Rules (BCR)

Für die Übermittlung von personenbezogenen Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, kommen verbindliche interne Datenschutzvorschriften (BCR) gem. Art. 47 DSGVO in Betracht. Diese sind vorab von der zuständigen Aufsichtsbehörde in einem Kohärenzverfahren zu genehmigen. Die Bindungswirkung der BCR beschränkt sich auf die Vertragsparteien – Sicherheitsbehörden im Empfängerstaat können nicht verpflichtet werden. Eine Meldeverpflichtung an die Aufsichtsbehörde ist zwingender Bestandteil der BCR, sofern die gebotenen Garantien im Drittstaat in erheblichem Maß beeinträchtigt werden würden. Bei BCR sind zusätzliche Maßnahmen erforderlich, die eine Aushöhlung des angemessene Schutzniveaus durch den Eingriff des Drittstaats verhindern.

Genehmigungen nach § 13 DSG 2000

Eine vor dem 25.05.18 rechtskräftig von der österreichischen Datenschutzbehörde (DSB) gem. § 13 DSG 2000 erteilte Genehmigung gilt weiter, sofern die Datenübermittlung dem Bescheid entspricht und die DSB den Bescheid nicht aufgehoben, abgeändert oder ersetzt hat. Bei einer auf § 13 DSG 2000 gestützten Genehmigung ist diese gegenüber der betroffenen Person offenzulegen sowie die adäquaten und angemessenen Garantien nach Aufforderung zur Verfügung zu stellen.

Ausdrückliche Einwilligung

Eine Einwilligung kann eine Übermittlung in einen Drittstaat legitimieren, wenn diese ausdrücklich und für den bestimmten Fall des betreffenden Datentransfers und in Kenntnis der Sachlage erfolgte. Zudem muss eine Aufklärung über die Risken der fehlenden geeigneten Garantien der Datenübermittlung stattfinden. Eine standardisierte Erklärung mit dem entsprechenden Hinweis, dass der Drittstaat betroffenen Personen keine Datenschutzrechte gewährt und keine Aufsichtsbehörde implementiert ist, ist ebenso möglich. Da dies grundsätzlich eine Ausnahmeregelung ist, eigne sich diese Alternative für die Datenübermittlung nicht für systematische und massenhafte Übermittlungen nach Ansicht des EU-Datenschutzausschusses (EDSA).

Ausnahmen nach Art. 49 DSGVO

Zu beachten ist bei einer Datenübermittlung nach den Ausnahmetatbeständen des Art 49 DSGVO, dass diese nur für einen bestimmten Zweck erforderlich sein muss. Diese Bestimmung ist einschränkend auszulegen (lt. ErwGr DSGVO & EDSA), sodass die Ausnahmen für eine Datenübermittlung zum Zweck der Vertragserfüllung und -anbahnung und zum Zweck der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen zur Anwendung kommen sowie wenn die Übermittlung gelegentlich erfolgt. Da den Leitlinien der EDSA sowie den ErwGr keine normative Wirkung zukommt, wird man sich nach der Rechtsprechung diesbezüglich in Zukunft orientieren müssen. ■

HSP RECHTSANWÄLTE GMBH

HSP Rechtsanwälte GmbH mit Sitz in Wien steht für gedankliche, örtliche und zeitliche Flexibilität. Um einen Rundumservice zu garantieren, sind die Fachbereiche der Kanzlei mannigfaltig und reichen von Immobilienrecht über Gesellschaftsrecht, IP- und IT-Recht, allgemeines Wirtschaftsrecht, Corporate und M&A, Bau-, Niederlassungs- sowie streitiges Recht.
Als Mitglied bei Geneva Group International (GGI), einer der weltweit führenden Allianzen für Anwälte, Wirtschaftsprüfer, Steuer- und Unternehmensberater, hat HSP Zugang zu einem Netzwerk, welches bei Rechtsproblemen im internationalen Raum bestmögliche Beratung garantiert.

HSP Rechtsanwälte GmbH
Gonzagagasse 4, 1010 Wien
T +43 1 533 0 533
office@hsp.law
https://hsp.law

Ansprechpartner:
Mag. Nikolaus Becker
T +43 1 533 0 533
nikolaus.becker@hsp.law