Berlin, 20.07.2020

Stellungnahme
und Handlungsempfehlungen

zum Urteil des EuGH betreffend "Privacy Shield" (C-311/18, "Schrems II")

TeleTrusT - Bundesverband IT-Sicherheit e.V.

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

1. Das Urteil in Kürze

Mit seinem Urteil vom 16.07.2020 hat der EuGH das Privacy-Shield-Abkommen zwischen der EU und den USA für Datenübermittlungen in die USA für unwirksam erklärt, da es kein Schutzniveau auf dem Level der DSGVO sicherstellt. Insbesondere stehe Betroffenen in den USA kein Rechtsweg zur Durchsetzung der im Unionsrecht verankerten Rechtsgarantien offen. So sei die eingerichtete Ombudsperson für Datenschutzbeschwerden nicht befugt, für US-Behörden verbindliche Entscheidungen zu treffen, also letztlich nicht in der Lage, die Rechte der Betroffenen auch durchzusetzen.

Die Standardvertragsklauseln (SCC) für die Übermittlung an Auftragsverarbeiter hat der EuGH dagegen nicht als unwirksam angesehen. Einem Transfer von Daten in Nicht-DSGVO-Staaten kann die Entscheidung dennoch entgegenstehen. Der EuGH betonte nämlich, dass auch bei vereinbarten SCC sicherzustellen ist, dass dem Betroffenen wirksame Mittel zur Durchsetzung der Rechte im Zielland offenstehen.

Nachdem betroffenen EU-Bürgern hinsichtlich der weitreichenden Zugriffsbefugnis von US-Behörden, insbesondere der Geheimdienste, keinerlei wirksamer Rechtsschutz möglich ist, scheint das nach der Entscheidung in den USA nicht der Fall.

2. Die rechtlichen Konsequenzen

Datentransfers in die USA sind ab sofort datenschutzwidrig, wenn sie (ausschließlich) auf Grundlage einer Privacy-Shield-Zertifizierung erfolgen. Erfasst sind nicht nur Übermittlungen an Auftragsverarbeiter, sondern auch solche innerhalb eines Konzerns oder an Geschäftspartner.

Sowohl der Einsatz von Software-Tools, bei denen zumindest ein Teil der Datenverarbeitung in den USA erbracht wird, als auch die konzerninternen Datenflüsse an US-Konzernunternehmen müssen überprüft werden.

Auf den Sitz der beteiligten Unternehmen kommt es nicht an. Entscheidend ist allein, ob die Daten in die USA verbracht werden sollen. Auf Basis des Privacy Shields ist das nicht mehr zulässig.

Ob Transfers in die USA oder andere Rechtsordnungen unter den SCC zulässig sind, dürfte davon abhängen, ob dem Betroffenen auch tatsächliche wirksame Mittel der Ausübung zentraler Rechte nach der DSGVO im Zielland bereitstehen.

Der EuGH deutet an, dass dies in den USA aufgrund der unkontrollierten Überwachungsbefugnisse der Sicherheitsbehörden nicht der Fall sein dürfte. Die Berliner Datenschutzbeauftragte fordert Unternehmen in ihrem Zuständigkeitsbereich bereits auf, umgehend zu Dienstleistern in der Europäischen Union oder in einem Land mit angemessenem Datenschutzniveau zu wechseln.

Entsprechend schutzlos ist ein europäischer Betroffener aber auch in vielen anderen Jurisdiktionen in denen heute Verarbeitungen von Daten in den globalen Outsourcing-Ketten unter SCC erfolgen. Es erscheint nur eine Frage der Zeit, bis auch andere Verarbeitungs-Länder in den Fokus geraten.

Was nicht betroffen ist:

Umgekehrt ist nicht jede Datenübermittlung in die USA von dem EuGH-Urteil betroffen. Zulässig bleibt eine Übermittlung, die zur Erfüllung eines Vertrages (oder Durchführung vorvertraglicher Maßnahmen) mit dem Betroffenen erforderlich ist. Die Kommunikation mit amerikanischen Kunden oder Hotelbuchungen in den USA sind weiter zulässig. Genauso können Mitarbeiterdaten im Konzern im erforderlichen Umfange geteilt werden, wenn der internationale Bezug des Arbeitsverhältnisses bei Abschluss des Arbeitsvertrages bekannt war.

Ebenso nicht unmittelbar betroffen ist die Nutzung von US-Dienstleister, wenn die Leistungserbringung vollständig in europäischen Rechenzentren erfolgt. So bieten die großen Hosting- und Cloud-Anbieter aus den USA mittlerweile Serverstandorte in Europa an. Das Hosting in Deutschland wird teilweise auch als Sonderleistung von deutschen Anbietern wie der Telekom übernommen. Hier ist aber zu beachten, dass alle US-amerikanischen Anbieter den Regelungen des Cloud Act unterliegen und daher auch in Europa gespeicherte Daten an Behörden der USA unter bestimmten Bedingungen herauszugeben haben. Auch diese Vorgänge unterliegen keiner angemessenen Kontrollbefugnis des Betroffenen.

3. Was nun zu tun ist

Unternehmen, die Daten unter dem Privacy Shield in die USA transferieren, haben akuten Handlungsbedarf:

(i) Identifizieren der betroffenen Datenflüsse

Zuerst müssen die von der Entscheidung betroffenen Übermittlungsvorgänge identifiziert werden. Dies sind alle Übermittlungen in die USA, die sich auf das Privacy Shield stützten: Einen Überblick bietet das Verzeichnis der Verarbeitungstätigkeiten. Ist die Grundlage des Transfers unklar, macht ein Abgleich mit der Liste der zertifizierten Unternehmen unter Sinn. Ein besonderer Blick sollte auf den unmittelbaren Einsatz von US-Anbietern, bspw. bei Tracking- und Marketing-Cookies, Newsletter-Diensten sowie Videokonferenz- und Kollaborations-Tools geworfen werden.

(ii) Umstellen auf alternative Garantien

Um eine Übermittlung nach Wegfall des Privacy Shields weiterführen zu können, muss diese auf eine alternative Garantie umgestellt werden bzw. unter eine der Ausnahmetatbestände zu fassen sein. Praktisch verbleiben damit nur zwei Alternativen:

Standardvertragsklauseln (SCC)

Die Übermittlung der personenbezogenen Daten kann nach wie vor auf die sog. Standardvertragsklauseln der EU-Kommission gestützt werden. Diese stellen grundsätzlich ein angemessenes Datenschutzniveau beim Empfänger her, sofern sie unverändert vereinbart werden. Der EuGH hat die SCC in seinem Urteil ausdrücklich als solche nicht beanstandet.

Allerdings hat er zugleich auch darauf hingewiesen, dass der Verantwortliche auch bei Verwendung der SCC prüfen muss, ob das Recht des Ziellandes einen angemessenen Schutz personenbezogener Daten bietet. Die zuständigen Aufsichtsbehörden sind außerdem verpflichtet, eine Übermittlung trotz Verwendung der SCC zu verbieten, wenn die Standardvertragsklauseln in einem bestimmten Land nicht durchsetzbar sind. Der EuGH macht in seinem Urteil sehr deutlich, dass er nicht davon ausgeht, dass die SCC in den USA für ein angemessenes Schutzniveau sorgen können. Dem werden sich die nationalen Aufsichtsbehörden wohl anschließen.

Eine Umstellung der Übermittlung auf die SCC dürfte damit allenfalls eine vorübergehende Zwischenlösung darstellen.

Immerhin setzen sämtliche großen US-IT-Anbieter neben dem Privacy Shield bereits jetzt auf die SCC. Diese werden bereits oft in die Auftragsverarbeitungsvereinbarungen einbezogen. Dies gilt beispielsweise für Facebook, Google, Microsoft, Amazon, Salesforce, Zoom und MailChimp. Eine Umstellung ist hier dann grundsätzlich nicht nötig. Zu beachten ist allerdings, dass die Anbieter die Standardvertragsklauseln häufig modifizieren. Da die Klauseln ihre Garantenfunktion nur erfüllen können, wenn sie uneingeschränkt vereinbart werden, kann dies doch dazu führen, dass sie wirkungslos werden. Die Berliner Aufsichtsbehörde hat dies zuletzt bezüglich Microsoft und Zoom so vertreten. Es sollte daher geprüft sein, ob die Standardvertragsklauseln unverändert sind.

Viele US-Anbieter haben für die Leistungsverträge mit europäischen Kunden eigene Tochterunternehmen mit Sitz im europäischen Datenschutzraum gegründet. Die Datenübermittlung in die USA findet dann erst im Rahmen einer Unterbeauftragung statt. Hier ist zu beachten, dass Aufsichtsbehörden in diesen Fällen fordern, dass die Standardvertragsklauseln vom Verantwortlichen unmittelbar mit dem US-Unternehmen abgeschlossen werden. Die Problematik der unkontrollierbaren Transfers nach dem Cloud Act ist damit aber nicht gelöst. Diesbezüglich existieren aber noch keine Entscheidungen.

Ausdrückliche Einwilligung des Betroffenen

Besteht keine Garantie für ein angemessenes Datenschutzniveau kann die Übermittlung ins Drittland auch auf eine Einwilligung des Betroffenen gestützt werden, Art. 49 Abs. 1 Satz 1 a) DSGVO. Die Einwilligung muss aber ausdrücklich erfolgen und erfordert, dass der Betroffene auf die Risiken eines fehlenden Angemessenheitsbeschlusses oder der Garantie eines Datenschutzniveaus hingewiesen wurde.

Die Einwilligungslösung ist nicht sehr verbreitet, insbesondere weil hier vieles unklar ist. Gilt Art. 7 DSGVO auch für diese Einwilligung, also insbesondere die freie Widerruflichkeit und die Anforderungen an die Erklärung selbst?

Zumindest der BGH stellt sehr hohe Anforderungen an Freiwilligkeit und Informiertheit von Einwilligungen (zu Cookie-Bannern: I ZR 7/16).

Vor einer Einwilligung sollte dem Betroffenen verdeutlicht werden, welches Risiko für seine Rechte und Freiheiten und welche Einschränkungen des Rechtsschutzes gegenüber dem gewohnten Rahmen in der EU bestehen. Dafür genügt eine Cookie-Einwilligung oder Newsletter-Anmeldung auch dann nicht, wenn ausdrücklich darauf hingewiesen wurde, dass Dienstleister in den USA eingesetzt werden.

(iii) Hinweise der Aufsichtsbehörden beachten

Das Urteil schafft für die betroffenen Unternehmen eine große Rechtsunsicherheit: Eine langfristige und verlässliche Absicherung des Datentransfers in die USA fehlt. In dieser Lage ist zu erwarten, dass sich die Aufsichtsbehörden auf nationaler und europäischer Ebene zeitnah äußern und eigenen Hinweisen und Handlungsempfehlungen veröffentlichen werden. Die Berliner Behörde ist bereits vorgeprescht, obwohl hier eine Abstimmung der Datenschutzbehörden aller EU-Länder angezeigt wäre.

4. Welche Umsetzungsfristen gelten?

Das Urteil des EuGH entfaltet unmittelbar Gültigkeit. Damit sind die betroffenen Datenübermittlungen ab sofort rechtswidrig. Entsprechend sollten die Maßnahmen unverzüglich ergriffen werden. Gleichzeitig ist nicht zu erwarten, dass Aufsichtsbehörden unmittelbar Bußgelder verhängen werden. Als vor gut 5 Jahren das Safe Harbor-Agreement gekippt wurde, setzten die europäischen Datenschutzbehörden die Umsetzung des Urteils zunächst für 3 Monate aus. Nach Ablauf dieser Frist wurden aber durchaus Bußgelder für Datenübermittlungen verhängt.

5. Ausblick

Das Urteil betrifft in erster Linie den Datentransfer in die USA. Bereits hier sind die Auswirkungen für Unternehmen gravierend, da derzeit keine langfristige Möglichkeit der Übermittlung von Daten in die USA ersichtlich ist. Die Auswirkungen sind aber noch weitreichender. Für viele typische Verarbeitungsländer bestehen die

gleichen erheblichen Zweifel an entsprechendem Rechtsschutz, insbesondere nachdem der EuGH diesen ausdrücklich auch für den Arbeitsbereich der Sicherheitsbehörden fordert.

Wer alle Risiken vermeiden möchte, wird daher auf einer Verarbeitung in Europa unter ausschließlicher Kontrolle europäischer Unternehmen bestehen müssen. Nachdem das häufig technisch oder wirtschaftlich nicht als Option erscheint, kann auch abgewartet werden, wie die Aufsichtsbehörden die Risiken einschätzen werden.

Praktisch ist derzeit ein Stopp aller Verarbeitungen in Rechtsordnungen, die keinen wirksamen Datenschutz haben, nicht umsetzbar. Entgegen mehrfacher Bekundungen ist die DSGVO nämlich kein Exportschlager. Wie schon bei der Aufhebung von Safe Harbor wird der europäische Gesetzgeber eine Lösung für den Transfer von Daten in Drittländer präsentieren. Vorbereitungen laufen dazu bereits, denn die Unwirksamkeit des Privacy Shields war allgemein angenommen worden.

Es gibt mehrere Gestaltungsmöglichkeiten - von Angemessenheitsbeschlüssen bis hin zu einem neuen Abkommen mit den USA.

Ansprechpartner für Rückfragen:

RA Karsten U. Bartels LL.M.
Stellvertretender TeleTrusT-Vorsitzender
Leiter der TeleTrusT-AG "Recht"
bartels@hk2.eu

RA Matthias Hartmann
hartmann@hk2.eu

RA Michael Schramm LL.M. (Minnesota)
schramm@hk2.eu