PRESSEMITTEILUNG

Stellungnahme des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT) zum Privacy-Shield-Urteil des EuGH

Berlin, 20.07.2020 - Zum Urteil des Europäischen Gerichtshofes betreffend die Unwirksamkeit des "Privacy Shield"-Abkommens zwischen der EU und den USA nimmt der Bundesverband IT-Sicherheit e.V. (TeleTrusT) Stellung und gibt zugleich Handlungsempfehlungen für Unternehmen, wie jetzt verfahren werden sollte.

https://www.teletrust.de/publikationen/stellungnahmen/

Mit seinem Urteil vom 17.06.2020 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. 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. 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.

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. Ebenso nicht unmittelbar betroffen ist die Nutzung von US-Dienstleistern, wenn die Leistungserbringung vollständig in europäischen Rechenzentren erfolgt.

Handlungsempfehlungen:

1. Identifizieren der betroffenen Datenflüsse

2. Umstellen auf alternative Garantien

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.

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

3. Hinweise der Aufsichtsbehörden beachten

Das Urteil schafft für die betroffenen Unternehmen 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.

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.

RA Karsten U. Bartels LL.M., Stellvertretender TeleTrusT-Vorsitzender und Leiter der TeleTrusT-AG "Recht" fasst zusammen: "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."

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

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

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.

Bundesverband IT-Sicherheit e.V. (TeleTrusT), Dr. Holger Mühlbauer, Geschäftsführer, Chausseestraße 17, 10115 Berlin, Tel.: +49 30 40054310, holger.muehlbauer@teletrust.de
www.teletrust.de