Ungültigkeit des Angemessenheits-beschluss für den EU-US-Privacy-Shield durch EuGH-Beschluss.

Das Aus für Datenübermittlungen in die USA?

Am 16.07.2020 hat der Europäische Gerichtshof im „Verfahren Schrems II“ eine Entscheidung bezüglich des Angemessenheitsbeschlusses für die Übermittlung personenbezogener Daten an Firmen in den USA auf Basis des EU-US-Privacy-Shield getroffen (EuGH-Urteil vom 16.07.2020, Az: C 311/18). Im Verfahren wurde u.a. festgestellt, dass auf Basis des Privacy-Shields legitimierte Übermittlungen nicht mehr rechtmäßig sind. Hintergrund dieser Entscheidung sind die umfassenden Zugriffsmöglichkeiten, der amerikanischen Geheimdienste und Sicherheitsbehörden (FBI, CIA, NSA, ...) denen diese auch ohne richterliche Anordnung nach verschiedenen US-amerikanischen Rechtsakten (hauptsächlich USA PATRIOT Act, USA Freedom Act) zustehen und die im Gegensatz zu europäischen Vorgaben (Artikel 7, Artikel 8 und Artikel 47 EU-Grundrechte-Charta) stehen.

WAS BEDEUTET DAS NUN FÜR DIE PRAXIS?

Unternehmen müssen alle Ihre Verarbeitungen personenbezogener Daten dahingehend prüfen, ob damit Übermittlungen in die USA verbunden sind, und auf welches Instrument gestützt diese Übermittlungen legitimiert sind. Denkbar sind hier i. d. R. der EU-US-Privacy-Shield (auf Basis des Durchführungsbeschluss (EU) 2016/1250 als Angemessenheitsbeschluss im Sinne des Artikel 45 DS-GVO) oder so genannte Standarddatenschutzklauseln (bisher Standardvertragsklauseln genannt, auch als SVK abgekürzt). Es sind aber auch Ausnahmen, wie die Einwilligung der betroffenen Person denkbar. Handelt es sich dabei um den EU-US-Privacy-Shield so müssen die Übermittlungen eingestellt werden, bis ein anderes Instrument gefunden wurde, mit welchem die Übermittlung legitimiert werden kann. Nach aktueller Sachlage scheint es im Moment am wahrscheinlichsten, dass – bis zu einer möglichen zwischenstaatlichen Nachfolgeregelung zum EU-US-Privacy-Shield – so genannte Standarddatenschutzklauseln als Instrument zukünftig Anwendung finden. Jedoch sind diese, da sie auch Gegenstand des vorgenannten Verfahrens waren, kurzfristig nicht als Alternative geeignet, da auch diese derzeit noch keine Möglichkeit bieten, die Daten betroffener Personen in der EU bei Empfängern in den USA von den Zugriffsmöglichkeiten der Geheimdienste und Sicherheitsbehörden auszunehmen. Dies stellt aber gerade ein grundlegendes Kriterium für die Legitimation einer Drittlandübermittlung dar. Da hier aber im Gegensatz zum Angemessenheitsbeschluss Gestaltungsmöglichkeiten existieren, sind diese zumindest zukünftig ein relevantes Instrument.

WELCHE VERARBEITUNGEN SIND (MÖGLICHERWEISE) BETROFFEN?

Betroffen sind – wie vorstehend beschrieben – Verarbeitungen bei denen Übermittlungen in die USA stattfinden. D. h. insbesondere sind hier Clouddienste, wie sie z. B. von Amazon (Amazon Web Services, AWS), Google (Google Cloud Platform), Microsoft (Microsoft Azure) u.a. anderen angeboten werden, betroffen. Weiterhin ist der Einsatz entsprechender Software (z. B. Google Apps, Microsoft

pb-153_10/20

Office 365, sowie weitere cloudbasierte Online-Apps) und Videokonferenz-Lösungen (z. B. Microsoft Teams, Zoom, Adobe Connect) möglicherweise betroffen, sowie weitere SaaS-Nutzungen und in jedem Fall zu prüfen. In Ausnahmefällen, kann die Nutzung europäischer Rechenzentren hier eine Lösung (zumindest im Sinne der fehlenden Drittlands-Übermittlung) darstellen. Besonders zu prüfen sind auch Webseiten im Hinblick auf den Hosting-Anbieter, aber insbesondere auch auf eingebundene Bestandteile (Social Media Plugins, externe Inhalte (z. B. Google Maps, Instagram- bzw. Twitter-Posts, ...), vor allem aber eingebundene Befehlsbibliotheken oder Design-Templates, aber auch eingebundene Plugins von Content Management Systemen). Ein besonderes Augenmerk sollte hier auch auf gegebenenfalls eingesetzte Tracking und Analysedienste gelegt werden, für die bereits mit einem vorangegangenen EuGH-Urteil („Planet 49") die Spielregeln verschärft wurden.

WICHTIG!

Die Legitimation der Übermittlung personenbezogener Daten in die USA ist lediglich eine zusätzliche Maßnahme bzw. eine „Schutzstufe" der Datenschutz-Grundverordnung. Diese ist nicht zu verwechseln mit der allgemeinen Rechtmäßigkeit der Verarbeitung personenbezogener Daten nach Artikel 6 Absatz 1 DS-GVO bzw. der Rechtmäßigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten nach Artikel 9 Absatz 2 DS-GVO. Auch wenn die DS-GVO die Einwilligung der betroffenen Person als eine legitimierende Ausnahme für eine Datenübermittlung in ein Drittland nennt, ist diese nicht mit einer allgemeinen datenschutzrechtlichen Einwilligung entsprechend gleichzusetzen, da für die Übermittlung in Drittländer deutlich höhere formale Anforderungen an die Einwilligung gestellt werden, die durch allgemeine datenschutzrechtliche Einwilligungen im Sinne der Rechtmäßigkeit der Verarbeitung nicht erfüllt werden. Ein Umschwenken auf eine Einwilligung ist daher kurzfristig nicht möglich – in keinem Fall rückwirkend aufgrund bereits schon abgegebener Einwilligungen. Eine Ausnahme kann, je nach konkreter Gestaltung, für die Einbindung externer Inhalte auf Webseiten bestehen – dies muss aber im Einzelfall sehr genau geprüft werden.

KONSEQUENZEN AUS FORTBESTEHENDEN DATENÜBERMITTLUNGEN OHNE LEGITIMATION

Eine Übermittlung personenbezogener Daten in Drittländer ohne ausreichende Legitimation stellt einen materiellen Verstoß gegen die DS-GVO dar, der mit einer Geldbuße von bis zu 20 000 000 Euro oder (im Fall von Unternehmen mit einem gesamten weltweit erzielten Jahresumsatz im vorangegangen Geschäftsjahr von mehr als 500 000 000 Euro) von bis zu 4 % dieses Umsatzes belegt werden kann. Auch wenn die Einzelumstände des Verstoßes für die tatsächliche Bemessung der Geldbuße Berücksichtigung finden, würde in einem solchen Fall die Fortführung der Verarbeitung als Vorsatz oder zumindest Fahrlässigkeit als erschwerender Fakt in die Geldbußenbemessung einbezogen werden. Vorschlag: Dazu kommt der mögliche Anspruch betroffener Personen auf Schadensersatz, dessen Höhe nach neuester Rechtsprechung auch auf Basis der Ermittlung der Geldbußen festgelegt werden kann. Diese Handhabung kann zu deutlich höheren Beträgen führen, als bisher in der deutschen Schadensersatz-Rechtsprechung in geltend gemachten Einzelfällen verhängt wurden.

HAFTUNG DER UNTERNEHMENSLEITUNG

Dazu kommt, dass nach § 43 GmbHG (insbesondere des Absatz 2) eine persönliche Haftbarkeit für Geschäftsführer von GmbHs, nach § 93 AktG eine persönliche Haftung für Vorstände von Aktiengesellschaften gegenüber der Gesellschaft für Geldbußen und Schadensersatzzahlungen besteht, wenn gesetzliche Vorgaben nicht eingehalten werden.

Es ist also dringender Handlungsbedarf gegeben!

ÜBER DEN AUTOR

Thomas Schwenski ist zertifizierter Datenschutzauditor und externer Datenschutzbeauftragter, sowie Information Security Auditor. Mit über 17 Jahren Erfahrung im IT-Bereich berät er Firmen und Einzelunternehmer zur Umsetzung der Datenschutzgesetze mit besonderen Schwerpunkten in der Etablierung von Datenschutzmanagementsystemen und dem Standard-Datenschutzmodell und ist Dozent und regelmäßiger Fachreferent zu Themen im Bereich Datenschutz, ISO 27000 Normenreihe und BSI IT-Grundschutz.

TÜV Rheinland Akademie GmbH
Alboinstraße 56
12103 Berlin
Tel. 030 7562-0
akademie.tuv.com

TÜVRheinland®
Genau. Richtig.

pb-153_10/20