ALTHAMMER & KILL

Sondernewsletter

zum Scheitern des EU-US Privacy Shield (Stand 22.07.2020)

Bereits in der vergangenen Woche haben wir Sie über die Entscheidung des Europäischen Gerichtshof (EuGH) zum EU-US Privacy Shield informiert. Da dies potenziell Auswirkung auf alle europäischen Unternehmen hat, möchten wir Sie in den kommenden Wochen regelmäßig über neue Entwicklungen informieren.

Was ist das EU-US Privacy Shield?

Das EU-US Privacy Shield ist ein transatlantisches Abkommen zwischen der Europäischen Kommission und den Vereinigten Staaten von Amerika. Es legitimiert den Austausch personenbezogener Daten zwischen beiden Staatengemeinschaften, in dem es Versprechungen zu Datenschutz und Datensicherheit manifestiert sowie ein angemessenes Datenschutzniveau gewährleisten soll (Angemessenheitsbeschluss).

Dies sah der EuGH in seinem Urteil vom 16.07.2020 jedoch anders und kippte das Abkommen.

Was ist passiert?

Am vergangenen Donnerstag erklärte der europäische Gerichtshof das transatlantische Abkommen zwischen der EU und den USA für ungültig. Ausschlaggebend für diese Einschätzung ist die „Schnüffelpraxis" der amerikanischen Sicherheitsbehörden. Die Vereinbarungen im EU-US Privacy Shield können aufgrund der gesetzlich eingeräumten Möglichkeiten der US- Geheimdienste nicht durchgesetzt werden – ein Datenschutzniveau nach europäischen Maßstäben ist so nicht gewährleistet.

Neu ist diese Ansicht nicht. Bereits nach dem Scheitern des Safe Harbor-Abkommens und der Neuauflage unter einem anderen Namen (Privacy-Shield) wurden Bedenken laut. Sicherer schien von Anfang an der Abschluss von Standardvertragsklauseln. Diese kann man analog zu den innereuropäischen Verträgen zur Auftragsverarbeitung (AV-Vertrag) betrachten. Der Inhalt wird jedoch von der europäischen Kommission vorgegeben und Änderungen sind nur mit deren Erlaubnis möglich.

Im Grundsatz bestätigte der EuGH am Donnerstag die Gültigkeit der Standardvertragsklauseln – was nur logisch erscheint. Standardvertragsklauseln haben im Gegensatz zu dem EU-US Privacy Shield globale Gültigkeit. Sie regeln den Datenaustausch mit Drittstaaten und internationalen Organisationen weltweit. Und nicht wie das EU-US Privacy Shield, nur den Austausch mit den Vereinigten Staaten und den dort ansässigen Unternehmen.

Identisch zum EU-US Privacy Shield ist jedoch, dass die Standardvertragsklauseln ebenfalls ein Datenschutzniveau nach europäischen Maßstäben sicherstellen sollen. Und hier beißt sich die Katze in den Schwanz:

Standardvertragsklauseln können die Befugnisse der US-Geheimdienste nicht beschneiden. Selbst wenn ein US-amerikanisches Unternehmen zusichert, das europäische Datenschutzniveau zu wahren, unterliegt das Unternehmen weiterhin der amerikanischen Rechtsprechung. US-Geheimdienste können ohne richterlichen Beschluss Daten von z. B. europäischen Bürgerinnen und Bürgern anfragen. Was nun also für das Scheitern des EU-US Privacy Shield sorgt, kann im Zweifel auch für Standardvertragsklauseln mit US-amerikanischen Unternehmen gelten: Sie sind nicht wirksam und damit ungültig.

Was bedeutet das Urteil?

Es bedeutet vor allem, dass mindestens eine Rechtsgrundlage für die Übermittlung von personenbezogenen Daten in die USA weggefallen ist. Sofern die Übermittlung auf Basis von Standardvertragsklauseln beruht, könnte man nun argumentieren, dass diese zunächst weiter Bestand haben. Eine tiefergehende Prüfung könnte dieses Ansicht jedoch zum Wanken bringen.

Im Zweifel bleibt als mögliche Rechtsgrundlage nur noch die informierte Einwilligung eines jeden Betroffenen – theoretisch möglich, in vielen Fällen wohl jedoch praxisfremd.

Was sollte kurzfristig getan werden?

Ruhe bewahren

Zunächst gilt es Ruhe zu bewahren. Die Entscheidung des EuGH in diesem Ausmaß kam überraschend – sowohl für Datenschützer wie auch für die Aufsichtsbehörden, die mit dem Urteil nun ebenfalls umgehen müssen.

Von Seiten der EU wurden bereits Stimmen laut, ein neues Abkommen aushandeln zu wollen. Sofern jedoch die amerikanische Rechtsprechung und die damit einhergehenden Befugnisse der Geheimdienste nicht beschnitten werden, ist ein potenziell neues Abkommen (z.B. ein Privacy Shield 2.0) auch nur ein Konstrukt auf Zeit. Nichtregierungsorganisationen könnten abermals Klage einreichen und ein solches Abkommen für nichtig erklären lassen.

US-Dienstleister identifizieren und Rechtsgrundlage für den Datenexport prüfen

Eine Datenverarbeitung ist zunächst weiterhin in Ordnung, wenn...:

- ein AV-Vertrag (DPA – Data Processing Agreement) mit EU-Standardvertragsklauseln (zumeist im Anhang) vorhanden ist und sofern die EU-Standardvertragsklauseln nicht durch den Dienstleister abgeändert wurden.
- Einwilligungen für den Datenexport von den betroffenen Personen vorhanden sind. Zum Beispiel über Consent Manager für Cookies und Co. Eine Anpassung der Datenschutzerklärung auf der Webseite sollte überprüft werden.

Eine Datenverarbeitung ist nicht mehr in Ordnung, wenn...:

- der Datenexport nur auf das EU-US Privacy Shield gestützt wird; der Dienstleister also keinen AV-Vertrag bzw. DPA mit rechtskonformen EU-Standardvertragsklauseln anbietet. Stoppen Sie, wenn möglich, diese Verarbeitungen (z. B. durch Entfernen der entsprechenden Cookies oder Plugins auf Ihrer Webseite).

Was sollte mittelfristig getan werden?

Die Reaktionen der Behörden und deren Umgang mit der neuen Situation sollten genauestens beobachtet werden. Es ist nicht unwahrscheinlich, dass ein neues Abkommen zwischen der EU und den USA entstehen könnte. Wie jedoch bereits eingangs erläutert, wäre ein neues Abkommen vermutlich ebenfalls nur ein Abkommen auf Zeit.

- Prüfen Sie, ob einzelne Datenverarbeitungen selbst oder durch in der EU ansässige Unternehmen durchgeführt werden könnten.
- Überprüfen Sie alle Datenschutzerklärungen und sonstige Informationspflichten, wie z. B. das Auskunftsersuchen. Da das EU-US Privacy Shield keine legitime Rechtsgrundlage mehr ist, kann sich hierauf nicht mehr berufen werden.
- Fragen Sie Ihre Dienstleister in den USA an, ob zwischenzeitlich EU-Standardvertragsklauseln angeboten werden. Schließen Sie diese ab.
- Prüfen Sie vorhandene EU-Standardvertragsklauseln. Änderungen durch den Dienstleister sollten nicht vorgenommen worden sein. Falls doch gilt es zwingend die Gültigkeit überprüfen zu lassen.

Selbstverständlich halten wir unsere Kunden über die weiteren Entwicklungen auf dem Laufenden.

Stimmen zum EuGH-Urteil

Prof. Ulrich Kelber, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

„Der EuGH macht deutlich, dass internationaler Datenverkehr weiter möglich ist. Dabei müssen aber die Grundrechte der europäischen Bürgerinnen und Bürger beachtet werden. Für den Datenaustausch mit den USA müssen jetzt besondere Schutzmaßnahmen ergriffen werden. Unternehmen und Behörden können Daten nicht mehr auf der Grundlage des Privacy Shield übermitteln, das der EuGH für unwirksam erklärt hat. […] Der EuGH hat die Rolle der Datenschutzaufsichtsbehörden bestätigt und gestärkt. Sie müssen bei jeder einzelnen Datenverarbeitung prüfen und prüfen können, ob die hohen Anforderungen des EuGH erfüllt werden. Das bedeutet auch, dass sie den Datenaustausch untersagen, wenn die Voraussetzungen nicht erfüllt werden. Sowohl Unternehmen und Behörden als auch die Aufsichtsbehörden haben jetzt die komplexe Aufgabe, das Urteil praktisch anzuwenden. Wir werden auf eine schnelle Umsetzung in besonders relevanten Fällen drängen." (vgl. https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/17_Schrems-II-Urteil.html, zuletzt abgerufen am 21.07.2020)

Ausführung des EuGH

„[Die] zuständige Aufsichtsbehörde, sofern kein gültiger Angemessenheitsbeschluss der Kommission vorliegt, [ist] verpflichtet (…), eine auf Standarddatenschutzklauseln, die von der Kommission erarbeitet wurden, gestützte Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten, wenn diese Behörde im Licht aller Umstände dieser Übermittlung der Auffassung ist, dass die Klauseln in diesem Drittland nicht eingehalten werden oder nicht eingehalten werden können (…)." (vgl. http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=9732082, zuletzt abgerufen am 21.07.2020)

Data Protection Commission

„So, while in terms of the points of principle in play, the Court has endorsed the DPC's position, it has also ruled that the SCCs transfer mechanism used to transfer data to countries worldwide is, in principle, valid, although it is clear that, in practice, the application of the SCCs transfer mechanism to transfers of personal data to the United States is now questionable. This is an issue that will require further and careful examination, not least because assessments will need to be made on a case by case basis." (vgl. https://www.dataprotection.ie/en/news-media/press-releases/dpc-statement-cjeu-decision, zuletzt abgerufen am 21.07.2020)

Johannes Casper, Hamburgischer Beauftragter für den Datenschutz und Informationsfreiheit

„Nach der heutigen EuGH-Entscheidung befindet sich der Ball wieder einmal im Spielfeld der Aufsichtsbehörden, die nun vor der Entscheidung stehen werden, insgesamt die Datenübermittlung über Standardvertragsklauseln kritisch zu hinterfragen. Das betrifft dann letztlich aber nicht nur Staaten, die sich wie die USA zumindest immerhin bemüht hatten, den Eindruck zu machen, adäquate Strukturen des Datenschutzes zu schaffen. Für Länder wie China sind derartige datenschutzrechtliche Vorkehrungen weit entfernt. Auch mit Blick auf den Brexit wird sich die Frage der zulässigen Datenübermittlung stellen. Für den internationalen Datenverkehr ziehen schwere Zeiten auf. Unter dem Strich bleibt die Erkenntnis: In den vergangenen Jahren ist es den USA, aber auch der EU-Kommission nicht gelungen, eine tragfähige Grundlage für einen angemessenen Schutz von Daten zu implementieren, die dem europäischen Datenschutzstandard entspricht. Die Auswirkungen dieses Urteils betreffen den internationalen Datentransfer insgesamt. Eine Datenübermittlung in Staaten ohne angemessenes Datenschutzniveau wird es daher künftig nicht mehr geben dürfen. Hier sind die Aufsichtsbehörden in besonderer Weise gefordert, eine gemeinsame Strategie zu entwickeln und umzusetzen." (vgl. https://datenschutz-hamburg.de/pressemitteilungen/2020/07/2020-07-16-eugh-schrems, zuletzt abgerufen am 21.07.2020)

Dr. Stefan Brink, Landesbeauftragter für Datenschutz in Baden-Württemberg

„Ich halte die DSGVO für den richtigen Weg und fände es großartig, wenn andere Länder ihrem Vorbild folgen würden. Ich bin allerdings skeptisch, ob der EuGH nicht überschätzt, wie lang der europäische Hebel wirklich ist. Andere Länder lassen sich ungern in ihre Gesetzgebung hineinreden, und wenn wir den Datenaustausch konsequent unterbinden, wäre der Schaden auch für uns massiv." (vgl. https://zeitung.faz.net/faz/politik/2020-07-20/22ea53d809ccc61cfe25da3e213e61e6/?GEPC=s3, zuletzt abgerufen am 21.07.2020)

Maja Smoltczyk, Berliner Beauftragte für Datenschutz und Informationsfreiheit

„Der EuGH hat in erfreulicher Deutlichkeit ausgeführt, dass es bei Datenexporten nicht nur um die Wirtschaft gehen kann, sondern die Grundrechte der Menschen im Vordergrund stehen müssen. Die Zeiten, in denen personenbezogene Daten aus Bequemlichkeit oder wegen Kostenersparnissen in die USA übermittelt werden konnten, sind nach diesem Urteil vorbei. Jetzt ist die Stunde der digitalen Eigenständigkeit Europas gekommen. Die Herausforderung, dass der EuGH die Aufsichtsbehörden ausdrücklich verpflichtet, unzulässige Datenübermittlungen zu verbieten, nehmen wir an. Das betrifft natürlich nicht nur Datenübermittlungen in die USA, für die der EuGH die Unzulässigkeit bereits selbst festgestellt hat. Auch bei der Übermittlung von Daten in andere Staaten wie etwa China, Russland oder Indien wird zu prüfen sein, ob dort nicht ähnliche oder gar größere Probleme bestehen." (vgl. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf, zuletzt abgerufen am 21.07.2020)

Der Beauftragte für den Datenschutz der EKD

„Der BfD EKD wird prüfen, inwiefern das heutige Urteil des EuGHs Einfluss auf die Bewertung datenschutzkonformer Datenübermittlungen gemäß § 10 DSG-EKD und somit auf die Tätigkeit unserer Behörde haben wird." (vgl. https://datenschutz.ekd.de/2020/07/16/eugh-kippt-eu-us-privacy-shield/, zuletzt abgerufen am 21.07.2020)

Der Diözesendatenschutzbeauftragte der (Erz-)Bistümer Hamburg, Hildesheim. Osnabrück und des Bischöflich Münsterschen Offizialats

„Die katholischen Datenschutzaufsichtsbehörden prüfen die Auswirkungen der Entscheidung für die kirchlichen Einrichtungen." (vgl. https://www.datenschutz-kirche.de/node/431, zuletzt abgerufen am 21.07.2020)