Sonderinformation
Unwirksamkeit des EU-US Privacy Shields – massive Haftungsrisiken beim Transfer personenbezogener Daten außerhalb der EU

Mit seiner vielbeachteten Entscheidung vom 16.07.2020 hat der Europäische Gerichtshof (EuGH) in der Rechtssache C-311/18 – auch bekannt unter dem Titel „Schrems II“ – ganz aktuell den sog. EU-US Privacy Shield für ungültig erklärt. Unternehmen, die sich bisher bei der Nutzung bestimmter Dienste etwa auf den Privacy Shield berufen haben, verhalten sich demnach rechtswidrig, da für den Datentransfer nunmehr keine wirksame Rechtsgrundlage vorhanden ist. Dies kann bspw. bei dem Einsatz von mit US-Servern verbundenen Plugins oder gängiger Webtracking-Analyse-Tools, über die Daten in die USA transferiert werden, relevant sein. Werden Unternehmen nicht tätig droht die Verhängung massiver Bußgelder oder die Geltendmachung von Schadensersatzforderungen betroffener Personen. Die den Datentransfer auftragsgemäß übernehmenden Dienstleister werden die eigentlich für den Datenverarbeitung verantwortlichen Unternehmen hingegen nicht in Regress nehmen können. Es besteht damit akuter Handlungsbedarf.

Bei dem Privacy Shield handelt es sich um das maßgebliche Abkommen zum Datentransfer zwischen der Europäischen Union und den USA, das durch die Europäische Kommission im Rahmen des Angemessenheitsbeschlusses (EU) 2016/1250 erlassen wurde. Auf Grundlage des etwas mehr als vier Jahre alten Beschlusses hatte die EU-Kommission der USA ein angemessenes Datenschutzniveau bescheinigt.

Der EuGH stellt dem entgegenstehend jedoch klar, dass der EU-US-Privacy-Shield nach Maßgabe der nunmehr seit 2018 geltenden Datenschutzgrundverordnung (DSGVO) im Licht der EU-Grundrechtecharta kein hinreichendes Schutzniveau gewährleistet. Allein auf Grund des vorgenannten Abkommens sei kein dem Unionsrecht entsprechender Schutz betroffener EU-Bürger gewahrt. Zugleich hat das Gericht wichtige Kernaussagen dazu getroffen, inwieweit sich Unternehmen alternativ bei einem Transfer personenbezogener Daten außerhalb der EU etwa auf Standardvertragsklauseln der Europäischen Kommission stützen können.

Die Entscheidung hat angesichts der erheblichen internationalen Vernetzung von Unternehmen (etwa in einer Unternehmensgruppe oder gegenüber sonstigen Kunden/Geschäftspartner, aber auch über die Nutzung der eigenen IT (bspw. über Cloudlösungen)) weitreichende Konsequenzen. Nicht zuletzt unter dem Druck der Corona-Pandemie greifen Unternehmen aktuell bspw. deutlich stärker auf digitale Anwendungen im Arbeitsalltag zurück, Anwendungen, die unweigerlich einen Datentransfer in nicht EU-

Staaten mit sich bringen und denen mit dem Richterspruch des EuGH nunmehr in weiten Teilen die Rechtsgrundlage entzogen ist. Unternehmen kommen demnach nicht umhin, den gesamten internationalen Datenverkehr, insbesondere auf Grundlage von aus den USA stammenden Softwareanwendungen eingehend zu prüfen und ggf. hier umzustrukturieren.

Hintergrund der Entscheidung

Der EuGH hatte bereits im Oktober 2015 in dem Rechtsstreit des Österreichers Max Schrems anlässlich der Zugriffe der NSA auf die europäischen Nutzerdaten von Facebook das bisherige Safe Harbor-Abkommen zum Transfer personenbezogener Daten zwischen Unternehmen aus den USA und der EU für ungültig erklärt (siehe hierzu im Einzelnen Sonderinformation vom 01.12.2015 zum sog. Safe Harbor-Urteil in der Rechtssache C-362/14 (auch „Schrems I“ genannt).

Die Europäische Kommission hatte sich dann 2016 mit der US-Regierung auf ein neues Regelwerk für den transatlantischen Datenaustausch in Form des EU-US Privacy Shields geeinigt (siehe hierzu im Einzelnen Sonderinformation vom 04.02.2016). Alternativ hierzu konnten Unternehmen bisher ihren Datentransfer auf von der EU-Kommission abgesegnete Standardvertragsklauseln (sog. „Standard Contractual Clauses“(SCC)) stützen. Nunmehr musste sich der EuGH in dem erneut von Max Schrems initiierten Verfahren mit der Frage der rechtlichen Zulässigkeit des Privacy Shields sowie der Standardvertragsklauseln auseinandersetzen.

Inhalt der Entscheidung des EuGH

Der EuGH gelangt zu dem Ergebnis, dass trotz des EU-US Privacy Shields auf Grund US-amerikanischer Rechtsvorschriften der Einsatz von Überwachungsprogramme über das erforderliche Maß hinaus gestattet sei. Ferner sei der gerichtliche Rechtsschutz durch das EU-US-Privacy-Shield nicht ausreichend ausgestaltet. Der EU-US-Privacy-Shield biete daher kein hinreichendes, dem Datenschutzrecht der EU entsprechendes Schutzniveau. Solange seitens der Europäischen Kommission kein geeignetes Schutzniveau im Wege eines entsprechenden neuen Abkommens gewährleistet werden kann, sei der Datenexporteur außerdem selbst in der Verantwortung. Durch ihn müssten dann eigenverantwortlich geeignete Schutzmaßnahmen getroffen werden. Diese können sich generell aus den genannten Standarddatenschutzklauseln ergeben.

Durch die Standardvertragsklauseln könne gewährleistet werden, dass das vom Unionsrecht verlangte Schutzniveau eingehalten werde. So werde dies dadurch sichergestellt, dass der Empfänger dem Datenexporteur mitteilen muss, wenn er die Standardvertragsklauseln nicht einhalten kann, woraufhin der Exporteur die Datenübermittlung aussetzen und/oder vom Vertrag mit dem Empfänger zurücktreten muss. Allerdings obliege es gleichwohl dem Datenexporteur, im Einzelfall die Rechtskonformität des Datentransfers zu garantieren. Er

hat die rechtskonforme Verwendung der Standardvertragsklauseln im Detail zu prüfen und müsste ggf. seinerseits zusätzliche Maßnahmen zum Erhalt des erforderlichen Schutzniveaus garantieren können. Kann er dies nicht, muss der Datentransfer an sich eingestellt werden, sofern man sich nicht der Verhängung massiver Bußgelder ausgesetzt sehen will. Eine Antwort auf die Frage, wie derartige zusätzliche Maßnahmen ausgestaltet sein sollen, bleibt der EuGH aber schuldig. Sicher ist mit dem Urteil aus Luxemburg demnach nur, dass im Grunde nichts sicher ist.

Handlungsempfehlungen

Es besteht in jedem Fall akuter Handlungsbedarf. Unternehmen müssen (z.B. anhand ihres ohnehin obligatorischen Datenverarbeitungsverzeichnisses, Art. 30 DSGVO) prüfen, inwieweit bei ihnen ein Datentransfer in Staaten außerhalb der EU stattfindet. Sodann ist im Einzelfall zu analysieren, inwieweit für den Datentransfer ein ausreichendes Schutzniveau garantiert werden kann. Diese Analyse ist anhand der zwischen den Parteien vereinbarten Vertragsgrundlagen, getroffenen technischen und organisatorischen Schutzmaßnahmen sowie der Gesetzeslage im jeweils betroffenen Drittstaat vorzunehmen. Findet ein Datentransfer allein auf Basis des bisherigen Privacy Shields statt, müssen alternative Vertragsgrundlagen gefunden werden. Basiert der Datentransfer auf den vorgenannten Standardvertragsklauseln sind zusätzliche vertragliche Garantien zum Erhalt des Datenschutzniveaus zu vereinbaren.

Alternativ können Unternehmen u.U. auf von den europäischen Datenschutzbehörden gesondert genehmigte spezielle Vertragsklauseln (Art. 46 Abs. 3 lit. a DSGVO) oder sog. „Binding Corporate Rules“ (BCRs nach Art. 47 DSGVO)) zurück greifen.

Wichtig ist in jedem Fall die weiteren Entwicklungen, auch ggf. Hinweise der Datenschutzbehörden, zum internationalen Datentransfer zu verfolgen.

Sehr gerne unterstützen wir auch Ihr Unternehmen in der Klärung sämtlicher Fragen rund um den Datenschutz. Wir beraten Sie mit Blick auf die rechtskonforme Umsetzung der mit den nunmehrigen EuGH-Urteil aufgestellten Vorgaben. So lassen sich Haftungsrisiken, mitunter Bußgelder und Schadensersatzforderungen, langfristig vermeiden.

Ihre Ansprechpartner:

Dr. Andreas Katzer

Rechtsanwalt, M.I.L (Lund)
- Individual- und kollektives Arbeitsrecht
- Arbeitsrecht
- Sportrecht
- Unternehmenskauf
- Sozialversicherungs- und Steuerrecht,
- insbesondere im arbeits- und sportrechtlichen
- Zusammenhang
- Europarecht und Internationales Recht

andreas.katzer@sonntag-partner.de
Tel.: + 49 821 57058 - 0

Dr. Viktor Stepien

Rechtsanwalt
- Arbeitsrecht
- Sozialversicherungsrecht im arbeitsrechtlichen Zusammenhang
- Datenschutzrecht

viktor.stepien@sonntag-partner.de
Tel.: + 49 821 57058 - 0

Prof. Dr. Ulrike Trägner

Rechtsanwältin
- Individualarbeitsrecht
- Kollektives Arbeitsrecht, insb.
- Betriebsverfassungsrecht
- Datenschutzrecht

ulrike.trägner@sonntag-partner.de
Tel.: + 49 731 379 58-0

Julian N. Modi

Rechtsanwalt
- Gewerblicher Rechtsschutz (Marken-, Patent- Design- bzw. Geschmacksmusterrecht)
- Urheber- und Wettbewerbsrecht
- IT-Recht/Internetrecht
- Medien- und Presserecht
- Allgemeines Zivil- und Wirtschaftsrecht
- Datenschutzrecht

julian.modi@sonntag-partner.de
Tel.: + 49 821 57058 - 0

Für Rückfragen zum Inhalt dieser Fachnachrichten und zu Ihrem richtigen Ansprechpartner in unserem Hause sowie für eine unverbindliche Kontaktaufnahme stehen wir Ihnen jederzeit gerne zur Verfügung.

Sonntag & Partner

Bei Sonntag & Partner spielen viele Talente zusammen. An unseren süddeutschen Standorten sind wir bundesweit sowie im internationalen Umfeld tätig und stehen unseren Mandanten aus dem gehobenen Mittelstand in den Bereichen Wirtschaftsprüfung, Steuer- und Rechtsberatung mit über 290 Mitarbeitern ganzheitlich zur Seite.

Die jeweilig projektbezogene Teamzusammenstellung sowie der fachübergreifende und integrierte Beratungsansatz zielen auf eine präzise Lösungsentwicklung und Lösungsumsetzung – je nach individuellem Bedarf der Mandanten.

Abgerundet wird unser Kanzleiprofil durch Family Office-Dienstleistungen, Vermögensbetreuung und IT Consulting.

Abschließende Hinweise

Weitere Informationen über unsere Kanzlei und unser Beratungsangebot finden Sie unter https://www.sonntag-partner.de/