Hinweise zum „Schrems II“-Urteil des EuGH

In seinem Urteil vom 16.07.2020 hat der Europäische Gerichtshof (EuGH) das Datenschutzabkommen “Privacy Shield” für ungültig erklärt. Hier finden Sie die Pressemitteilung und das Urteil C-311/18 des EuGH.

Das Urteil ist relevant für alle Unternehmen, die Daten von Nutzern, Kunden, Mitarbeitern, aber auch Gerätedaten, die auf einzelne Anwender beziehbar sind, mit Partnern oder verbundenen Unternehmen in den USA oder anderen nicht-europäischen Ländern austauschen.

Wie das Gericht ausführt, bleiben die Standardvertragsklauseln (oder auch Standarddatenschutzklauseln, SDK) zum Datenaustausch grundsätzlich wirksam. Allerdings knüpft der EuGH hohe Anforderungen an die rechtmäßige Einbeziehung dieser Klauseln.

Wer personenbezogene Daten von Europa in die USA oder andere Drittländer außerhalb der EU und des Europäischen Wirtschaftsraumes überträgt, muss künftig also noch genauer prüfen, ob der Datenschutz beim Empfänger bzw. Auftragsverarbeiter gewährleistet ist.

Der EuGH hat entschieden, dass das EU-U.S: Privacy Shield für den Datentransfer in die USA ab sofort keine rechtliche Grundlage mehr bilden kann.

Gleichzeitig stellt er in Frage, inwieweit Unternehmen ihre Datentransfers in die USA und in andere Drittländer auf die SDK der Europäischen Kommission stützen können. Damit hat das Urteil massive Auswirkungen auf die Rechtmäßigkeit von Datentransfers in sämtliche nicht-europäische Staaten.

Zur Einordnung

Das durch Max Schrems (daher Schrems I und Schrems II-Urteil) initiierte Verfahren beschäftigt den EuGH bereits seit dem Jahr 2013. Mit einer Beschwerde rügte Schrems damals die Übermittlung von personenbezogenen Daten durch Facebook Irland in die Konzernmutter Facebook Inc. in den USA. Nach Auffassung des Beschwerdeführers biete das Recht und die Praxis der Vereinigten Staaten – insbesondere vor dem Hintergrund der Enthüllungen durch Edward Snowden zur Massenüberwachung – keinen ausreichenden Schutz der übermittelten Daten vor den Überwachungstätigkeiten der US-Behörden.

Der EuGH hatte seinerzeit infolge eines Vorabentscheidungsersuchens des irischen High Court in seinem ersten „Schrems“-Urteil vom 6. Oktober 2015 (C-362/14) die sog. „Safe-Harbor“-Entscheidung der EU-Kommission für unwirksam erklärt. Die EU-Kommission hatte es in dem Beschluss versäumt, Feststellungen zur Gleichwertigkeit des Schutzniveaus in den USA zu treffen. Wegen dieses Fehlers konnte der EuGH „Safe-Harbor“ verwerfen, ohne selbst Feststellungen zum Schutzniveau in den USA treffen zu müssen. Die politisch heikle Frage, ob in den USA trotz der umfassenden Geheimdienstaktivitäten eine ausreichende Achtung der Grundrechte erfolgt, blieb außen vor.

Mit dem EU-US-Privacy-Shield wurde im Jahr 2016 ein Nachfolgeabkommen vereinbart, das auf einem Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DSGVO beruht und einen DSGVO-konformen Datentransfer an entsprechend zertifizierte US-Unternehmen aus der EU ermöglicht. Diesmal stellte die Kommission ausdrücklich und unter Berücksichtigung der im EU-US-Privacy-Shield getroffenen Vereinbarungen fest, dass das Schutzniveau in den USA im Wesentlichen demjenigen in Europa entspreche.

Facebook stützte sich in der Folge bei Datentransfers in die USA sowohl auf die SDK als auch (teilweise) auf den EU-US-Privacy-Shield. Nach einer erneuten Beschwerde von Max Schrems hatte der EuGH nun die Gelegenheit, zu beiden Instrumenten zu entscheiden.

KPP Group GmbH • Berliner Str. 112a • 13189 Berlin
Telefon: 030 / 206 73 72 – 0 • E-Mail: info@kpp-group.de • Homepage: http://www.kpp-group.de

Denn problematisch ist, dass US-Behörden Prüfungsrechte zustehen, ohne dass EU-Bürger sich dagegen wehren können. In dem entschiedenen Verfahren berief sich Schrems z. B. auf Section 702 des Foreign Intelligence Surveillance Acts (FISA 702), der Datenzugriffe bei elektronischen Kommunikationsdiensten bei Nicht-US-Bürgern auch ohne einen gerichtlichen Beschluss und Rechtsschutz erlaubt.

Somit verstößt die EU-Kommission mit dem EU-US-Privacy-Shield gegen den Kern der Grundrechte der EU-Bürger auf Privatleben, Datenschutz und auf einen wirksamen Rechtsbehelf, wenn sie trotz FISA 702 und anderer Zugriffsrechte der US-Behörden Datentransfers in die USA zulässt.

Generelle Möglichkeiten zum legalen Datentransfer

Personenbezogene Daten dürfen vom Verantwortlichen zunächst nur dann in ein Drittland wie die USA übertragen werden, wenn es für diese Übertragung eine Rechtsgrundlage erlaubt. Die DSGVO sieht dafür mehrere Möglichkeiten vor, die praktisch relevantesten sind Angemessenheitsbeschlüsse der Europäischen Kommission nach Art. 45 DSGVO sowie geeignete Garantien nach Art. 46 DSGVO.

Anzumerken ist, dass die grundsätzliche Datenverarbeitung des Verantwortlichen schon nach Art. 6 DSGVO unter Berücksichtigung der Anforderungen des Art. 5 DSGVO rechtskonform erfolgen muss.

Angemessenheitsbeschluss

Ein Angemessenheitsbeschluss der Europäischen Kommission ist eine praktische und einfache Möglichkeit, die Übermittlung von personenbezogenen Daten in ein Drittland zu legitimieren (wenn alle anderen Vorgaben zur Weitergabe von Daten erfüllt sind, versteht sich). Die Kommission kann nach genauer Prüfung, deren Details in Art. 45 Abs. 2 DSGVO niedergelegt sind, beschließen, dass in einem bestimmten Land ein angemessenes Datenschutzniveau besteht. Eine Übersicht der Länder, für die ein Angemessenheitsbeschluss vorliegt, findet sich auf der Webseite der EU.

Diesen Beschluss muss sie regelmäßig überprüfen, damit die Entwicklungen in dem Drittland auch berücksichtigt werden und auf Veränderungen reagiert werden kann. Besteht ein solcher Angemessenheitsbeschluss, können personenbezogene Daten in das genannte Land regulär und legal übermittelt werden. Ein Angemessenheitsbeschluss kann auch für eine internationale Organisation oder für bestimmte Wirtschaftssektoren in einem Land erlassen werden, also bspw. für den Bankensektor, aber auch nur für Teile eines Landes, etwa im Falle der USA für bestimmte Bundesstaaten. Der Privacy Shield beruht(e) auch auf einem solchen Angemessenheitsbeschluss.

Geeignete Garantien

Eine andere Rechtsgrundlage sind „geeignete Garantien“ nach Art. 46 DSGVO. Die Norm ermöglicht es sowohl dem für die personenbezogenen Daten Verantwortlichen als auch dem Auftragsverarbeiter, personenbezogene Daten auf Basis geeigneter Garantien für den Schutz der betroffenen Personen in Drittländer zu übermitteln.

Geeignete Garantien können nach Art. 46 Abs. 2 DSGVO bspw. verbindliche interne Datenschutzvorschriften zwischen Konzernteilen in verschiedenen Ländern (sog. Binding Corporate Rules, BCR) sein, von der Europäischen Kommission erlassene Standarddatenschutzklauseln (SDK) oder besonders geregelte Zertifizierungen (die es in der Praxis aber noch nicht gibt).

KPP Group GmbH • Berliner Str. 112a • 13189 Berlin
Telefon: 030 / 206 73 72 – 0 • E-Mail: info@kpp-group.de • Homepage: http://www.kpp-group.de

Damit eine Garantie auch eine geeignete Garantie im Sinne der DSGVO ist, muss sie einen Ausgleich für den Mangel an Datenschutz in dem Drittland bieten und Regelungen und Mechanismen vorsehen, damit ein Schutzniveau entsteht, das dem in der EU im Wesentlichen entspricht. Dabei kommt es darauf an, dass die allgemeinen Grundsätze für die Verarbeitung, wie sie in Art. 5 DSGVO niedergelegt sind, eingehalten werden, etwa durch technische Maßnahmen und datenschutzfreundliche Voreinstellungen.

Bedeutsam ist vor allem auch, dass die von der Datenverarbeitung betroffenen Personen ihre Datenschutzrechte auch im Drittland durchsetzen können und sie sich gegen Maßnahmen mit Rechtsbehelfen zur Wehr setzen können. Ist all das gegeben, liegt eine geeignete Garantie für das Schutzniveau vor und die personenbezogenen Daten können in das Drittland übermittelt werden.

Praktisch am relevantesten sind die bereits genannten Standarddatenschutzklauseln (SDK), welche die Kommission vorgibt und die als Vertragszusatz zwischen dem Datenübermittler in der EU und dem Empfänger im Drittland abgeschlossen werden. Dabei ist wichtig, dass von den SDK nur insoweit abgewichen werden darf, als dass das Schutzniveau dadurch erhöht wird. Werden diese standardisierten Klauseln hingegen zum Nachteil der Betroffenen abgeändert, liegt keine geeignete Garantie im Sinne des Art. 46 DSGVO mehr vor.

Für die im Fall vor dem EuGH relevante Datenübermittlung ging es um personenbezogene Daten, die von Facebook in die USA übermittelt werden. Die irische Datenschutzbehörde wollte wissen, ob hierfür das Privacy Shield und/oder die abgeschlossenen Standarddatenschutzklauseln ausreichen und wie diese genau auszulegen sind.

Der EuGH stellte nun klar, dass das Privacy Shield nicht ausreicht.

Daneben hat er aber auch festgestellt, dass es nicht genügt, einfach nur die SDK mit dem Vertragspartner im Drittland abzuschließen und dann sei alles erlaubt. Vielmehr muss auch im Drittland ein Datenschutzniveau bestehen, das in der Sache gleichwertig zu dem in der EU garantierten Schutzniveau ist. Auch sonst hat der EuGH noch ein paar bemerkenswerte Ausführungen zur Auslegung und Anwendung der SDK gemacht.

Standarddatenschutzklauseln

Die SDK an sich wurden vom EuGH nicht beanstandet. Die SDK können eine geeignete Garantie für die Datenübermittlung darstellen.

Nach Art. 46 DSGVO ist eine Übermittlung in Drittstaaten durch einen Verantwortlichen oder Auftragsverarbeiter dann zulässig, wenn geeignete Garantien (das sind hier die Standarddatenschutzklauseln) vorgesehen sind und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Nach dem Urteil des EuGH muss insgesamt gewährleistet sein, dass der Betroffene ein Datenschutzniveau genießt, das dem in der EU garantierten Niveau der Sache nach gleichwertig ist.

Dabei kommt es neben den Vereinbarungen zwischen den Parteien auch auf einen etwaigen Zugriff der Behörden des Drittlands auf die übermittelten Daten sowie die maßgebliche Rechtsordnung des Landes an. Zur Beurteilung des Zugriffs von Behörden sowie zur Beurteilung der Rechtsordnung verweist der EuGH auch in den Fällen des Art. 46 DSGVO auf den Prüfungsmaßstab des Art. 45 Abs. 2 DSGVO, was somit neu ist. Es gelten somit im Kern die gleichen Vorgaben wie beim Privacy Shield.

Der EuGH stellt klar, dass die Standardvertragsklauseln an sich eine geeignete Garantie im Sinne der DSGVO sein können. Allerdings muss – so der EuGH – der verantwortliche Datenexporteur (also das Unternehmen als Verantwortlicher) prüfen, ob das Recht des Bestimmungsdrittlands zusammen mit den Standarddatenschutz-

KPP Group GmbH • Berliner Str. 112a • 13189 Berlin
Telefon: 030 / 206 73 72 – 0 • E-Mail: info@kpp-group.de • Homepage: http://www.kpp-group.de

klauseln nach Maßgabe des Unionsrechts einen angemessenen Schutz der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleistet. Erforderlichenfalls können die Parteien zusätzlich zu den SDK weitere Garantien aufnehmen, um einen angemessenen Schutz zu erreichen. Faktisch muss aber auch geprüft werden, ob das Recht des Bestimmungsdrittlands dem Empfänger überhaupt erlaubt, die Standarddatenschutzklauseln einzuhalten.

In erster Linie ist der Verantwortliche für die Prüfung zuständig, ob im geplanten Empfängerland durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Der EuGH verpflichtet aber auch die Aufsichtsbehörden, die Datentransfers auf Basis der SDK zu prüfen und dabei zu beurteilen, ob eben im konkreten Fall ein Schutzniveau garantiert ist, das dem in der EU gleichwertig ist.

Wenn dem nicht so ist und nicht anderweitig ein angemessener Schutz gewährleistet werden kann, dann – so der EuGH –, müssen die Aufsichtsbehörden diese Datentransfers untersagen.

Umfang der Prüfpflicht des Verantwortlichen

Und es stellt sich dann natürlich die Frage, was konkret der Verantwortliche vor der Übermittlung zu prüfen hat? Reicht der Nachweis durch den Importeur, dass er sich an die SDK halten kann? Muss der Verantwortliche eigene Untersuchungen anstellen?

Die Antwort hierauf ergibt sich nach dem EuGH aus den Klauseln der SDK, konkret Klausel 4 Buchst. a sowie Klausel 5 Buchst. a und b. Diese verpflichten den in der Union ansässigen Verantwortlichen und den Empfänger, sich **vor der Übermittlung personenbezogener Daten in ein Drittland zu vergewissern**, dass das Recht des Bestimmungsdrittlands es dem Empfänger erlaubt, die **SDK einzuhalten**.

Das bedeutet, dass die Prüfungsfrage hier auf erster Stufe lautet: kann der Empfänger die SDK auf Basis des für ihn geltenden Rechts einhalten?

Daraus ergeben sich direkt einige wertvolle Erkenntnisse:

Es geht immer um die in den SDK festgelegte Übermittlung; nicht generell um Übermittlungen in das Drittland.

Das bedeutet, die Einhaltung der SDK ist grundsätzlich vertragsspezifisch zu prüfen.

Die Einhaltung der SDK im Hinblick auf das Recht im Drittland, muss daher wohl auch konkret anhand der zu übermittelnden Daten und des spezifischen Empfängers geprüft werden (und nicht allgemein).

Sowohl der Verantwortliche als auch der Empfänger sind verpflichtet, sich entsprechend zu vergewissern (natürlich insbesondere in Form der Zusammenarbeit).

Inhalt der Prüfpflicht

Und der EuGH gibt zudem noch einen Hinweis darauf, was die Vertragsparteien bei dieser Prüfung als Bewertungskriterien zu berücksichtigen haben, wovon sie sich also „vergewissern“ müssen.

In der Fußnote zu Klausel 5 der SDK wird klargestellt, dass zwingende Erfordernisse des Rechts im Drittland, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft zur Gewährleistung u. a. der Sicherheit des Staates, der Landesverteidigung und der öffentlichen Sicherheit erforderlich ist, nicht den Standarddatenschutzklauseln widersprechen.

KPP Group GmbH • Berliner Str. 112a • 13189 Berlin
Telefon: 030 / 206 73 72 – 0 • E-Mail: info@kpp-group.de • Homepage: http://www.kpp-group.de

Das heißt: Ein angemessenes Schutzniveau kann auf Basis der SDK auch dann bestehen, wenn Behörden des Drittlandes Zugriff auf die übermittelnden Daten nehmen. Das ist eine wichtige Klarstellung des EuGH, die auch in der Praxis Relevanz hat.

Nur muss dieser Zugriff legislativ so ausgestaltet sein, dass er den Anforderungen des vormaligen Art. 13 Abs. 1 RL 95/46/EG genügt. Dort wurden Ziele aufgeführt, die einschränkende Gesetzesmaßnahmen verfolgen müssen, damit sie zulässig sind.

Art. 13 RL 95/46/EG existiert jedoch nicht mehr. Da nach Art. 94 Abs. 2 DSGVO Verweise auf die RL 95/46/EG als Verweise auf die DSGVO zu verstehen sind, muss man hier wohl an die Stelle des Art. 13 Abs. 1 RL 95/46/EG nun Art. 23 Abs. 1 DSGVO und die dort benannten Ziele setzen (die jenen des Art. 13 Abs. 1 RL 95/46/EG sehr ähnlich sind. Hierzu gehören:

- die nationale Sicherheit,
- die Landesverteidigung,
- die öffentliche Sicherheit,
- die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit,
- den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren,
- den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen sowie
- die Durchsetzung zivilrechtlicher Ansprüche.

Aber: Es reicht nicht, dass das Recht des Drittlandes bei dem Zugriff auf die Daten ein solches Ziel verfolgt. Der Zugriff muss auch zur Verfolgung dieses Ziels erforderlich sein. Verlangt wird also eine Verhältnismäßigkeitsprüfung. Und hier wird es für europäische Unternehmen allein sehr schwer, diese Prüfung valide vornehmen zu können. Insbesondere sollten hierbei daher die Empfänger im Drittland unterstützen.

Der EuGH stellt klar, dass es als Verstoß gegen die SDK anzusehen ist, wenn einer aus dem Recht des Bestimmungsdrittlands folgenden Verpflichtung nachgekommen wird, die über das hinausgeht, was für Zwecke wie die oben genannten erforderlich ist.

Prüfung in der Praxis

In der Praxis könnte der Verantwortliche etwa über einen vorgefertigten Fragenkatalog an den Empfänger validieren, ob Zugriffe möglich sind und wenn ja, zu welchem Zweck. Sind Zugriffe auf die Daten möglich, so muss dieser Zugriff auf seine Erforderlichkeit hin geprüft werden. Meines Erachtens ergibt sich aus dem Urteil nicht, dass der Verantwortliche selbst diese Prüfung vorzunehmen hat. Es dürfte auch in Ordnung sein, wenn der Importeur (etwa über ein rechtliches Gutachten) dem Verantwortlichen nachweisen kann, dass die Zugriffe durch Behörden die europäischen Anforderungen erfüllen.

Einwilligungslösung?

Es wird diskutiert, ob Datentransfers in Drittstaaten nicht auch durch die Einwilligung der betroffenen Personen legitimiert werden können. Denn Artikel 49 DSGVO sieht die Einwilligung als Rechtsgrundlage für den Drittstaatentransfer beim Fehlen eines Angemessenheitsbeschlusses oder sonstiger geeigneter Garantien ja gerade vor. Technisch könnte die Einwilligung mit der Einwilligung zu Cookies (Cookie-Consent-Management) im Cookie-Banner eingeholt werden.

KPP Group GmbH • Berliner Str. 112a • 13189 Berlin
Telefon: 030 / 206 73 72 – 0 • E-Mail: info@kpp-group.de • Homepage: http://www.kpp-group.de

Problematisch erscheint hier jedoch, dass nach Art. 49 Abs. 1 lit a) die betroffene Person in die vorgeschlagene Datenübermittlung ausdrücklich einwilligen muss , nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde. Wie sollten die betroffenen Personen jedoch über alle Risiken der Zugriffsmöglichkeiten US-amerikanischer Behörden aufgeklärt werden können?

Weiterhin darf eine Übermittlung an ein Drittland nach Art. 49 Abs. 2 nur dann erfolgen,

- wenn die Übermittlung nicht wiederholt erfolgt,
- nur eine begrenzte Zahl von betroffenen Personen betrifft,
- für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen,
- und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung angemessene Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat.

Also ist auch bei einer Einwilligung nichts gewonnen, da sich die Prüfung hier als genauso umfangreich erweist, wie bei der Verwendung der SDK. Ferner bedarf es jedes Mal einer neuen Einwilligung und für einen großen Newsletter mit einer großen Anzahl von Empfängern eignet sich die Einwilligung auch nicht.

Darüber hinaus muss der Verantwortliche die Aufsichtsbehörde von der Übermittlung in Kenntnis setzen (Art. 49 Abs. 2 Satz 3 DSGVO).

Insgesamt scheidet also eine Einwilligungslösung zur Legitimierung des Datentransfers in die USA rein praktisch aus.

So sah es schon der Europäische Datenschutzausschuss (EDSA) 2018 in seiner Leitlinie zu Art. 49 DSGVO

Bin ich von dem Urteil überhaupt betroffen?

Von dem Urteil und den Folgen sind alle Verantwortlichen betroffen, die Datentransfers in die USA unterhalten. Dies kann auf vielfältige Weise geschehen:

- Newsletterversender (z.B. Mailchimp),
- CRM-Produkte (z.B. Hubspot, Zoho),
- Produktivitätstools z.B. Trello)
- Einsatz von GoogleFonts oder Trackern
- Nutzung von Social-Media-Kanälen
- Nutzung von Cloud-Diensten

Handlungsempfehlungen

Unternehmen sollten Maßnahmen ergreifen, um die internationalen Datentransfers in ihrem Verantwortungsbereich mit der DSGVO und dem Urteil des EuGH in Einklang zu bringen. Zu den möglichen Schritten zur Risikoreduzierung gehören insbesondere folgende Maßnahmen:

- Data Mapping:
  Falls noch nicht geschehen, sollten Unternehmen die internationalen Datentransfers und implementierten Transfermechanismen in ihrem Verantwortungsbereich identifizieren. Dies umfasst sowohl Da-

KPP Group GmbH • Berliner Str. 112a • 13189 Berlin
Telefon: 030 / 206 73 72 – 0 • E-Mail: info@kpp-group.de • Homepage: http://www.kpp-group.de

tentransfers zwischen einzelnen Konzerngesellschaften, einschließlich der gruppeninternen Übermittlung von Arbeitnehmerdaten, als auch Transfers an Dienstleister, Geschäftspartner oder sonstige Dritte.

- Überprüfen des Schutzniveaus im Einzelfall:
  Unternehmen müssen nach den Vorgaben des EuGH für jeden Einzelfall beurteilen und dokumentieren, ob ausreichende Garantien zur Absicherung der internationalen Datentransfers implementiert wurden. In dieser Hinsicht wird es bei Datenübermittlungen in die USA besonders relevant sein, inwieweit der Datenempfänger Eingriffsbefugnissen der US-Geheimdienste unterliegt.
- Wechsel zu alternativen Garantien:
  Stellt sich beim Data Mapping heraus, dass ausschließlich das Privacy Shield zur Legitimierung der Übermittlung verwendet wurde, müssen Unternehmen aufgrund der Unwirksamkeit des Privacy Shields auf andere Garantien umsteigen.
- Umsetzung von zusätzlichen Schutzmaßnahmen:
  Auch bei Datentransfers auf Grundlage der Standardvertragsklauseln ist zu prüfen, ob durch die Umsetzung zusätzlicher Schutzmaßnahmen, einschließlich des Abschlusses weitere vertraglicher Garantien ("SCC Plus"), das Schutzniveau beim Empfänger angemessen gesichert werden kann.
- Stellungnahmen der Datenschutzbehörden beobachten:
  Die für die nächste Zeit zu erwartenden Stellungnahmen der Aufsichtsbehörden auf nationaler Ebene und des Europäischen Datenschutzausschusses sollten beachtet werden. Einzelne Stellungnahmen der Datenschutzbehörden sind bereits veröffentlicht (z.B. Berlin, Hamburg, Rheinland-Pfalz und Thüringen).

Auf der Internetseite von noyb, dem Datenschutzverein hinter Max Schrems finden sich weitere Hinweise und Musterfragebögen an die US-Datenimporteure sowie ein FAQ. Auch die GDD bietet Handlungsempfehlungen auf ihrer Webseite zum Nachlesen an. Sehr empfehlenswert sind auch die Hinweise von RA Schwenke.

Bisherige Resonanz der Berliner Aufsichtsbehörde

Mittlerweile haben einige Aufsichtsbehörden und Verbände Stellungnahmen zum Urteil veröffentlicht.

Die Berliner Aufsichtsbehörde fordert konkret:

„Nach der Entscheidung des Europäischen Gerichtshofs, das EU-US Privacy Shield für ungültig zu erklären, fordert die BlnBDI Datenverarbeiter in Berlin auf, in den USA gespeicherte personenbezogene Daten nach Europa zu verlagern.“

Konkrete Empfehlung

Panik ist fehl am Platz. Allerdings sollten alle Datentransfers in die USA sorgfältig auf ihre Rechtsgrundlage hin überprüft werden. Finden sich Übermittlungen, die bisher nur auf der Grundlage des EU-US-Privacy-Shield erfolgen, sollte zu dem Auftragnehmer Kontakt aufgenommen werden, um zumindest Standardvertragsklauseln abzuschließen.

KPP Group GmbH • Berliner Str. 112a • 13189 Berlin
Telefon: 030 / 206 73 72 – 0 • E-Mail: info@kpp-group.de • Homepage: http://www.kpp-group.de

Quellen, Fundstellen und weitere Hinweise

http://curia.europa.eu/juris/document/document.jsf;jsessionid=72510E-BAC1D4E0DCE5A7B90D9A673CFC?text=&docid=228677&pageIndex=0&do-clang=DE&mode=req&dir=&occ=first&part=1&cid=9712389

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf

https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Schrems-II/Schrems-II.html

https://www.tlfdi.de/mam/tlfdi/presse/200716_pressemitteilung.pdf

https://www.datenschutz.rlp.de/de/themenfelder-themen/datenuebermittlung-in-drittlaender/

https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en

https://ico.org.uk/make-a-complaint/eu-us-privacy-shield/

https://iapp.org/news/a/the-show-must-go-on/

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

https://diercks-digital-recht.de/2020/07/der-eugh-das-privacy-shield-und-die-scc-urteil-in-sachen-schrems-ii-c-311-18/

https://drschwenke.de/eugh-urteil-eu-us-privacy-shield-unwirksam/

https://datenschutz-generator.de/eugh-privacy-shield-unwirksam/

https://www.delegedata.de/2020/07/das-schremsii-urteil-des-eugh-folgen-fuer-die-praxis-des-einsatzes-von-standarddatenschutzklauseln/

https://www.dr-datenschutz.de/privacy-shield-gekippt-welche-auswirkungen-hat-das-eugh-urteil/

https://www.pwclegal.de/datenschutz/eugh-erklaert-privacy-shield-fuer-ungueltig/

https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eugh-privacy-shield-unwirksam-standardvertrag/

https://www.haerting.de/neuigkeit/bye-bye-privacy-shield

https://www.skwschwarz.de/details/eugh-us-privacy-shield-eu-standardvertragsklauseln

https://www.engage.hoganlovells.com/knowledgeservices/news/schrems-ii-privacy-shield-invalidated-and-standard-contractual-clauses-under-scrutiny

https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2020%20PDFs/2020_07_21_EU_Data_Exports_After_Schrems_II_Hogan_Lovells.pdf

https://www.dataguidance.com/news/berlin-berlin-commissioner-issues-statement-schrems-ii-case-asks-controllers-stop-data

https://www.emeralddeleeuw.com/home/schremsii

https://www.faz.net/einspruch/datenschutz-wie-es-nach-schrems-ii-weitergehen-kann-16871896.html

KPP Group GmbH • Berliner Str. 112a • 13189 Berlin
Telefon: 030 / 206 73 72 – 0 • E-Mail: info@kpp-group.de • Homepage: http://www.kpp-group.de