OLG Köln: Unzulässige Übermittlung personenbezogener Daten in die USA

Der EuGH erklärte 2020 das „Privacy Shield“-Abkommen für ungültig. Seit Juli diesen Jahres gilt mit dem „Data Privacy Framework“ ein neuer Angemessenheitsbeschluss. Das OLG Köln (Urt. v. 3.11.2023 – 6 U 58/23) entschied nun, dass auch unter Geltung des neuen Angemessenheitsbeschlusses die allgemeinen Anforderungen an eine Datenverarbeitung nach der DSGVO erfüllt sein müssen.

Die Beklagte ist eine Tochtergesellschaft der Deutschen Telekom AG. Die Parteien streiten über die Rechtsmäßigkeit der von der Beklagten in der Vergangenheit verwendeten Datenschutzhinweise und damit korrespondierende Datenübermittlungen und in der Vergangenheit verwendeten Cookie-Bannern. Auf der Seite wurde u.a. ein Cookie-Banner eingesetzt, bei dem die optische Gestaltung der Auswahlmöglichkeiten nicht gleichwertig nebeneinander stand. Zudem wurden beim Aufruf der Website personenbezogene Daten wie die IP-Adresse sowie Browser- und Geräteinformationen aus einer Endeinrichtung eines Website-Besuchers an Google LLC als Betreiberin von Google Analyse- und Marketingdiensten („Google Adservices“) mit Sitz in den USA übermittelt. Der Kläger, die Verbraucherzentrale NRW e.V., sah hierin einen Verstoß gegen § 25 Abs. 1 S. 1 TTDSG und eine unzulässige Übermittlung der personenbezogenen Daten der Verbraucher an Server der Google LLC in den USA durch die Beklagte in ein Drittland ohne angemessenes Schutzniveau i.S.d. Art. 45 DSGVO und ohne geeignete Garantien i.S.d. Art. 46 DSGVO.

Das LG Köln (Urt. v. 23.3.2023 – 33 O 376/22) entschied, dass diese Standardvertragsklauseln eine Datenübermittlung in die USA nicht rechtfertigen können, da sie nicht geeignet seien, ein der DSGVO entsprechendes Datenschutzniveau zu gewährleisten. Gegen diese Entscheidung richtet sich die Berufung beider Parteien. Diese blieb nun vor dem OLG Köln ohne Erfolg.

Hintergrund

Am 12.7.2016 trat das sog. „Privacy Shield“-Abkommen in Kraft. Dieser Beschluss der Europäischen Kommission sollte ein angemessenes Datenschutzniveau für die Datenübermittlung in die USA gewährleisten und einen sicheren Rechtsrahmen für Unternehmen schaffen. Der EuGH (Urt. v. 16.7.2020 – C-311/18) erklärte das Abkommen jedoch für ungültig. Er stellte in seinem Urteil klar, dass bei einer Übermittlung personenbezogener Daten in ein Drittland ein Schutzniveau erforderlich sei, das mit dem in der Union vergleichbar ist. Aufgrund der weitreichenden Zugriffmöglichkeiten der US-Sicherheitsbehörden sei in den USA jedoch kein gleichwertiges Schutzniveau gewährleistet. Außerdem eröffne das Abkommen keinen ausreichenden Rechtsschutz für Betroffene.

Seitdem herrschte große Rechtsunsicherheit hinsichtlich der Datenübertragung in die USA. Im Juli diesen Jahres hat die Europäische Kommission dann einen neuen Angemessenheitsbeschluss, das EU-US Data Privacy Framework, erlassen.

Kein Angemessenheitsbeschluss im Zeitpunkt der Abmahnung

Die Datenübermittlung der Beklagten sei unzulässig und nicht durch die DSGVO gedeckt. Für den auf Widerholungsgefahr gestützten Unterlassungsanspruch müsse die beanstandete Handlung sowohl im Zeitpunkt ihrer Vornahme als auch im Zeitpunkt der gerichtlichen Entscheidung rechtswidrig sein. Nach der Entscheidung der Vorinstanz wurde jedoch der neue Angemessenheitsbeschluss verabschiedet, dieser sei ebenfalls zu berücksichtigen.

Zum Zeitpunkt der Abmahnung jedenfalls habe kein Angemessenheitsbeschluss bestanden. Das Gericht nahm Bezug auf die Schrems-II-Entscheidung des EuGH, mit der er das Privacy-Shield-Abkommen für ungültig erklärte.

Zum Zeitpunkt der Abmahnung bzw. der konkreten Verletzungsform fehlte es

> ***zunächst an einer entsprechenden Grundlage, nachdem der EuGH den zuvor geltenden Beschluss, der auf dem „Privacy Shield“ basierte (eine Übereinkunft der USA mit der EU betreffend die Gewährleistung eines bestimmten Datenschutzniveaus), in seinem Urteil „Schrems II“ (Urteil vom 16.07.2020, Rs. C-311/18 – F… I. u. Schrems, NJW 2020, 2613) für nichtig erklärt hatte, so dass sich Unternehmen wie die Beklagte hierauf allein nicht mehr berufen konnten (hierzu Klein K& R 2023, 553).***

Standarddatenschutzklauseln waren nicht geeignet

Zudem stellte das Gericht klar, dass etwaige Standarddatenschutzklauseln die Datenübermittlung in die USA nicht zu rechtfertigen vermögen, da sie nicht geeignet seien, ein der DSGVO entsprechendes Datenschutzniveau zu gewährleisten, insbesondere da solche Verträge nicht vor einem behördlichen Zugriff in den USA schützen. Auch hierbei berief sich das Gericht auf den EuGH.

> ***Insofern reicht es jedoch nicht aus, dass die Beklagte sich auf Standardvertragsklauseln im Verhältnis zwischen G. und G. I. Ltd. (nunmehr vorgelegt als Anlagen B18 und B19, Bl. 1496 ff., 1518 ff. eA) sowie auf zusätzliche Maßnahmen, die von G. in den sogenannten „G. Ads IDTI“ (Anlage B13, Bl. 604 ff. eA) ausgeführt werden, stützt. Denn der EuGH hat in seiner Entscheidung „Schrems II“ (Urteil vom 16.07.2020, Rs. C-311/18 = NJW 2020, 2613) zunächst klargestellt, dass die Verwendung von Standardvertragsklauseln zwar im Verhältnis der Vertragsparteien relevant sei, aber keinen Schutz vor Maßnahmen der Behörden von Drittstaaten biete, weil diese durch die vertragliche Vereinbarung nicht gebunden seien.*** *Deshalb gebe es Situationen, in denen die in den Klauseln enthaltenen Regelungen kein ausreichendes Mittel darstellten, um den effektiven Schutz von in das betreffende Drittland übermittelten personenbezogenen Daten zu gewährleisten (a.a.O. Rn. 125 f.). Für die USA als Drittland sei zu berücksichtigen, dass die amerikanischen Behörden auf die aus der Union in die Vereinigten Staaten übermittelten personenbezogenen Daten zugreifen und sie verwenden könnten, was sowohl im Rahmen der auf Section 702 des FISA (Foreign Intelligence Surveillance Act) gestützten Überwachungsprogramme PRISM und UPSTREAM als auch auf der Grundlage der Executive Order 12333 geschehen könne (a.a.O. Rn. 165). Diese Überwachungsprogramme genügten jedoch den im Unionsrecht nach dem Grundsatz der Verhältnismäßigkeit bestehenden Mindestanforderungen nicht, so dass nicht angenommen werden könne, dass die auf diese Vorschriften gestützten Überwachungsprogramme auf das zwingend erforderliche Maß beschränkt seien (zusammenfassend Rn. 184).*
>
> ***Aus diesen Ausführungen des Europäischen Gerichtshofs ist zu schließen, dass ein angemessenes Datenschutzniveau bzw. geeignete Garantien im Sinne von Art. 46 Abs. 1 DSGVO im Verhältnis zu den USA nur dann herbeigeführt werden können, wenn sowohl das Fehlen von Rechtsschutzmöglichkeiten des Einzelnen gegen Überwachungsmaßnahmen auf Grundlage der vorgenannten amerikanischen Vorschriften als auch der Datenzugriffsmöglichkeiten allgemein durch zusätzliche Maßnahmen effektiv ausgeschlossen oder auf ein erträgliches Maß zurückgeführt werden können*** *(Lange/Filip, in: BeckOK DatenschutzR, a.a.O., Art. 46 Rn. 2i f.).*

Ein entsprechendes Datenschutzniveau sei vorliegend jedoch nicht erreicht.

> *Dies wird durch die vorgelegten Unterlagen nicht erreicht. G. verpflichtet sich zwar in seinen „G. Ads IDTI“ (Anlage B13, Bl. 604 ff. eA), den Datenexporteur (hier also die Beklagte) über entsprechende Anforderungen von US-Behörden zur Offenlegung personenbezogener Daten zu informieren, stellt dies aber bereits unter den Vorbehalt, dass dies nach US-Recht zulässig ist (Übersetzung S. 50 der Berufungsbegründung, Bl. 548 eA). Entsprechendes gilt für die Benachrichtigung der betroffenen Person. Auch ist ein direkter Zugriff auf personenbezogene Daten nach wie vor nicht ausgeschlossen, wie sich ebenfalls aus diesem Dokument ergibt, weil G. sich auch für diesen Fall (nur) zu einer nachträglichen Information verpflichtet, wenn es von einem solchen Zugriff erfährt. Zwar wird dies später*

insofern relativiert (unterstrichene Passage auf S. 53 der Berufungsbegründung, Bl. 551 eA), als G. der Auffassung ist, dass keine staatliche Stelle in den USA direkten Zugriff auf die Information der G...-Nutzer oder auf Kundendaten habe. Dies schließt es aber gerade nicht aus, dass US-Behörden auf anderem Wege an diese Informationen gelangen, ohne dass G. hiervon zwingend erfährt. Dass G. die Rechtmäßigkeit von Anfragen überprüfen will (S. 51, Bl. 549 eA) und gegebenenfalls von ihm als rechtswidrig erkannte Maßnahmen anfechten will (S. 56 der Berufungsbegründung, Bl. 554 eA), vermag die grundsätzlichen vom EuGH festgestellten Defizite im Rechtsschutzsystem der USA betreffend die in Rede stehenden Überwachungsprogramme nicht zu beseitigen, weil diese zusätzlichen Maßnahmen von G. nur innerhalb des durch die aufgeführten Regelungen begründeten Systems der Überwachungsmechanismen wirken können. Dieses System ist aber in sich bereits, wie der EuGH entschieden hat, in den gebotenen Rechtsschutzmöglichkeiten defizitär, was durch ein Engagement von G. grundsätzlich nicht kompensiert werden kann.

Keine wirksame Einwilligung

Die Beklagte könne sich auch nicht auf eine wirksame Einwilligung gem. Art. 49 Abs. 1 lit. a DSGVO berufen. Die Besucher der Website seien nicht über eine Datenübermittlung an Google informiert worden.

> ***Auch auf eine Einwilligung der von der Datenübertragung betroffenen Personen kann sich die Beklagte nicht stützen. Zwar ist eine Einwilligung grundsätzlich möglich, wenn – wie im Streitfall – weder Angemessenheitsbeschluss (Art. 45 DSGVO) noch geeignete Garantien (Art. 46 DSGVO) für das betroffene Drittland gegeben sind, vgl. Art. 49 Abs. 1 S. 1 DSGVO. […]***
>
> ***Denn jedenfalls wäre eine etwaige Einwilligung, die nach Auffassung der Beklagten dadurch erfolgt, dass auf ihrem Cookie-Banner zwingend die Schaltfläche „Alles akzeptieren" angeklickt werden muss, bevor die streitgegenständliche Übertragung erfolgt (vgl. S. 25 f. der Berufungsbegründung, Bl. 523 f. eA), unwirksam. Die Vorschrift des Art. 49 Abs. 1 S. 1 lit. a) DSGVO setzt nämlich voraus, dass der Einwilligende über die bestehenden möglichen Risiken ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde.*** *Hieran fehlt es, und zwar auch dann, wenn man die gegenüber dem ursprünglichen Cookie-Banner (Anlage K8, Bl. 192 GA) leicht erweiterte Gestaltung in Anlage B11 (Bl 591 ff. eA) zugrunde legt. Dort heißt es in Bezug auf Drittlandtransfers von personenbezogenen Daten: „[Die Beklagte] kann unter Umständen nicht in allen Fällen sicherstellen, dass das europäische Datenschutzniveau eingehalten wird" (diese Passage fehlte zuvor) und verweist wegen Details auf den Datenschutzhinweis (insoweit unverändert gegenüber Anlage K1, Bl. 49 ff. GA). In diesem findet sich zwar einerseits der Hinweis (S. 5 unten, Bl. 53 GA), dass im Falle einer Einwilligung im Sinne von Art. 49 Abs. 1 S. 1 lit. a) DSGVO das Datenschutzniveau in den meisten Ländern außerhalb der EU nicht den EU-Standards entspreche, was insbesondere umfassende Überwachungs- und Kontrollrechte staatlicher Behörden, z.B. in den USA, die in den Datenschutz der europäischen Bürgerinnen und Bürger unverhältnismäßig eingreifen, betreffe. Andererseits ist aber spezifisch für G. Ads ausgeführt, dass insoweit nach Auskunft von G. keine Übermittlung personenbezogener Daten stattfinde (S. 4 der Anlage K1, Bl. 52 GA). Bereits diese widersprüchliche Aussage in Bezug auf die konkrete Datenübertragung steht dem Ziel einer informierten Einwilligung entgegen, weil der angesprochene Verkehr davon ausgehen wird, dass er in die Nutzung u.a. von Marketing-Cookies einwilligen könne, ohne Risiko zu laufen, dass seine hierbei erhobenen Daten in ein Drittland transferiert werden. Dies ist bereits nach Art. 49 Abs. 1 S. 1 lit. a) DSGVO unzulässig, weil hierdurch die nach der Vorschrift gebotene Risikoaufklärung konterkariert wird, weshalb es auf eine Prüfung am Maßstab des § 307 Abs. 1 S. 2 BGB (Transparenzgebot) nicht mehr ankommt.*

Data Privacy Framework zwischenzeitlich in

Kraft getreten

Zwischenzeitlich sei jedoch das Data Privacy Framework in Kraft getreten, auf dessen Grundlage personenbezogene Daten aus der EU an solche US-Unternehmen übermittelt werden können, die an dem DPF teilnehmen.

> ***Der unter dem 10.07.2023 gefasste Beschluss der EU-Kommision mit dem Titel „EU US Data Privacy Framework“ (im Folgenden: DPF, (C(2023) 4745 final, derzeit nur auf Englisch verfügbar, vorgelegt als Anlage B15, Bl. 1258 ff. eA) stellt nunmehr in den USA ein angemessenes Datenschutzniveau fest und entfaltet unmittelbare Wirkung, so dass Datenübermittlungen in das betreffende Land keiner besonderen aufsichtsbehördlichen Genehmigung bedürfen*** *(vgl. Juarez, in: BeckOK DatenschutzR, 44. Ed. 01.05.2023, Art. 45 DSGVO Rn. 1). Auf der Grundlage des neuen Angemessenheitsbeschlusses können personenbezogene Daten aus der EU an solche US-Unternehmen übermittelt werden, die an dem DPF teilnehmen (DPF Rn. 8: „This Decision has the effect that personal data transfers from controllers and processors in the Union to certified organisations in the United States may take place without the need to obtain any further authorisation.“). Eine solche Teilnahme als „certified organisation“, die eine Selbstverpflichtung sowie die Übermittlung verschiedener weiterer Informationen an das USamerikanische Handelsministerium (US Department of Commerce) voraussetzt (vgl. Klein K& R 2023, 553, 554), ist auch für die G. L.festzustellen, wie aus dem Ausdruck der vom Department of Commerce betriebenen Webseite www.dataprivacyframework.gov“ (Anlage B16, dort S. 3, Bl. 1399 eA) hervorgeht, dem der Kläger inhaltlich nicht entgegengetreten ist.*

Allgemeine Anforderungen müssen auch unter dem Data Privacy Framework erfüllt sein

Der neue Angemessenheitsbeschluss lasse den Unterlassungsanspruch jedoch nicht entfallen, denn auch hier müssen die übrigen allgemeinen Anforderungen erfüllt sein. Vorliegend fehle es jedoch an einer wirksamen Einwilligung nach Art. 6 DSGVO.

> *Das neue DPF lässt den Unterlassungsanspruch des Klägers aus ähnlichen Erwägungen wie zuvor ausgeführt nicht entfallen.*
>
> ***Auch bei Vorliegen eines Angemessenheitsbeschlusses müssen die übrigen – allgemeinen – Anforderungen an eine zulässige Datenverarbeitung erfüllt sein, wozu unter anderem das Erfordernis der in Kapitel II der DSGVO geregelten Einwilligung (Art. 6, 7 DSGVO) gehört*** *(vgl. Pauly, in: Paal/Pauly, DSGVO/BDSG, a.a.O., Art. 44 DSGVO Rn. 2).*
>
> *Daran fehlt es im Streitfall. Denn ebenso wie im Kontext des Art. 49 Abs. 1 S. 1 lit. a) DSGVO ist die eingeholte Einwilligung, die nunmehr Art. 6 Abs. 1 S. 1 lit. a) DSGVO unterfällt, unwirksam.* ***Eine Einwilligung im Sinne der letzteren Vorschrift erfordert, dass der für die Verarbeitung Verantwortliche der betroffenen Person eine Information über alle Umstände im Zusammenhang mit der Verarbeitung der Daten in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zukommen lässt, da dieser Person insbesondere die Art der zu verarbeitenden Daten, die Identität des für die Verarbeitung Verantwortlichen, die Dauer und die Modalitäten dieser Verarbeitung sowie die Zwecke, die damit verfolgt werden, bekannt sein müssen. Solche Informationen müssen diese Person in die Lage versetzen, die Konsequenzen einer etwaigen von ihr erteilten Einwilligung leicht zu bestimmen, und gewährleisten, dass die Einwilligung in voller Kenntnis der Sachlage erteilt wird*** *(vgl. EuGH, Urteil vom 11.11.2020, Rs. C-61/19 Rn. 40 – Orange România SA/ANSPDCP, = NJW 2021, 841).*
>
> *Gemessen hieran wird im Datenschutzhinweis, wie oben näher ausgeführt, suggeriert, dass die Verwendung von G. Ads grundsätzlich ohne Übermittlung personenbezogener Daten auskommt. Unabhängig davon, ob diese Übermittlung in ein Drittland mit oder ohne Angemessenheitsbeschluss erfolgt, entspricht es nicht dem Erfordernis einer transparenten und leicht verständlichen Unterrichtung des Nutzers, wenn dieser aufgrund einer*

entsprechenden Aussage von G…, auf die sich die Beklagte beruft, davon ausgeht, es komme erst gar nicht zu einer Verarbeitung seiner personenbezogenen Daten. Deshalb kann auch dahinstehen, ob – wie der Kläger meint – die Einwilligung im Cookie-Banner auch deshalb unwirksam ist, weil sie keine Eingrenzungen bezüglich der Zwecke der Verarbeitungen oder der Zielländer der Übermittlung enthält (vgl. S. 39 der Klageschrift, Bl. 44 GA).

Die Entscheidung ist nicht rechtskräftig. Das OLG Köln hat die Revision zum BGH zugelassen.

Unser Tipp: Im Rahmen unserer **Legal Products** stehen Ihnen umfangreiche Checklisten und Anleitungen rund um das Thema DSGVO zur Verfügung und Sie erhalten Muster-AV-Verträge und Muster-Antwortschreiben. Zudem bietet der **Trusted Shops Consent-Manager** eine Lösung, um die Einwilligung wirksam einzuholen. Selbstverständlich erhalten Sie umfassenden Support bei der Integration. Ebenfalls enthalten ist ein Update-Service – ergeben sich Gesetzesänderungen oder relevante gerichtliche oder behördliche Entscheidungen, die auch Sie betreffen, aktualisieren wir den Consent-Manager entsprechend und informieren Sie darüber natürlich. Unser Consent-Manager ist in allen **Legal Products** enthalten. In unserem **Legal Enterprise** und **Legal Ultimate** übernehmen wir auch eine außergerichtliche Vertretung bei der Geltendmachung von Unterlassungs- und Aufwendungsersatzansprüchen sowie Schadensersatz-/Schmerzensgeldansprüchen nach der DSGVO (z.B. aufgrund eines nicht erteilten Auskunftsersuchens oder einer unzulässigen Datenübermittlung).

Andrey_Popov/Shutterstock.com