EU-US Data Privacy Framework – Gekommen, um zu bleiben?!

ZD-Interview mit Barbara Schmitz und Dr. Axel Spies

■ Die EU-Kommission hat am 10.7.2023 den Angemessenheitsbeschluss für den sicheren Datentransfer zwischen den USA und der EU erlassen. Damit ist es Unternehmen aus der EU wieder möglich, personenbezogene Daten an US-Unternehmen, die sich zur Einhaltung der Anforderungen des Datenschutzrahmens verpflichtet haben, ohne weitere Bedingungen oder Genehmigungen zu übermitteln. Neben der Frage, welches Akronym künftig verwendet werden soll, TADPF, EU-US DPF und ob mit oder ohne Bindestrich, wirft der neue Datenschutzrahmen weitere relevante Fragen auf, die iRe transatlantischen Dialogs behandelt werden sollen.

■ The European Commission adopted the adequacy decision for safe and trusted EU-US data flows on July 10, 2023. This means that it is once again possible for companies from the EU to transfer personal data to US companies that have committed to comply with the requirements of the data privacy framework without any further conditions or approvals. In addition to the question of which acronym should be used in the future, TADPF, EU-US DPF and whether with or without a hyphen, the new data protection framework raises other relevant issues to be addressed in a transatlantic dialogue.

Lesedauer: 8 Minuten

ZD: Frau Schmitz, Herr Dr. Spies, wie haben Sie, jeweils auf Ihrer Seite des Atlantiks, am 10.7.2023 die Mitteilung der EU-Kommission zum neuen Angemessenheitsbeschluss zum sicheren Datentransfer in die USA aufgenommen?

Schmitz: EU-Kommissar für Justiz und Rechtsstaatlichkeit Reynders hatte bereits im Dezember letzten Jahres bei der Veröffentlichung des Entwurfs für den Angemessenheitsbeschluss den Sommer 2023 als Zeithorizont in Aussicht gestellt. Dass es dann tatsächlich so gekommen ist und der Angemessenheitsbeschluss am 10.7.2023 verkündet worden ist, war für mich dann doch überraschend schnell.

Spies: Hier in Washington haben den Angemessenheitsbeschluss die meisten so erwartet. Die US-Regierung hat in den Verhandlungen mit der EU-Kommission über rund zwei Jahre darauf hingearbeitet. Überrascht hat mich, dass bei manchen Kommentatoren in Europa das Pendel stark zur anderen Seite ausgeschlagen ist. Ich lese manchmal: Damit sei jetzt alles im Bereich EU-US Datentransfer im Lot und auch die „lästigen" Folgenabschätzungen für die USA könne man jetzt in den Schredder geben. Das sehe ich nicht so. Das US-Handelsministerium hat in den FAQs klar gemacht: „Das DPF EU-USA ist kein Mechanismus zur Einhaltung der DS-GVO, sondern stellt einen Mechanismus zur Verfügung, der es den teilnehmenden Organisationen ermöglicht, die EU-Anforderungen für die Übermittlung personenbezogener Daten in Drittländer zu erfüllen, die in Kapitel V der DSGVO niedergelegt sind." Bildlich gesprochen: Das EU-US Data Privay Framework (DPF) baut eine weitere Brücke für die Daten aus der EU in die USA an registrierte Datenimporteure.

ZD: Gut ein Drittel des Welthandels wird zwischen den USA und Europa abgewickelt, womit auch personenbezogene Daten ausgetauscht werden. Mit seinem Schrems-II-Urteil v. 16.7. 2020 hatte der EuGH das Datenschutzniveau in den USA als unzureichend eingestuft, mit weitreichenden Folgen für den transatlantischen Datenverkehr. Wie gingen die Unternehmen mit dieser Bewertung um?

Schmitz: Diese Einschränkungen – ausgelöst von Schrems II – kamen nicht überraschend. Das Privacy Shield wurde seit seiner Einführung im Juli 2016 als unzureichend kritisiert. Nicht nur, dass die Trump-Administration es nicht eilig hatte, einen Ombudsmann für Beschwerden von EU-Bürgern einzurichten, was eine wesentliche Voraussetzung für den Erlass des Angemessenheitsbeschlusses seitens der EU war und ist. Darüber hinaus beschäftigten die Datenschutzskandale um Facebook und Google Analytics auch die EU-Kommission. Vor dem Hintergrund der politischen Entwicklungen in den USA und der Verzögerungen bei der Umsetzung der Anforderungen des Privacy Shield mahnte die damalige EU-Justizkommissarin Jourová die Umsetzung an und drohte mit einer Aussetzung des Privacy Shield zum 1.9.2018. Wie aus dem zweiten Prüfbericht der EU-Kommission zum Privacy Shield v. 19.12.2018 hervorgeht, hat die US-Administration Maßnahmen ergriffen, um die Bedingungen des Abkommens umzusetzen. Das Abkommen war zu diesem Zeitpunkt noch zwei Jahre gültig, stand aber die ganze Zeit über unter dem Damoklesschwert der Klagen von Max Schrems. Auf Grund dieser sich abzeichnenden Entwicklung und der damit verbundenen Rechtsunsicherheit hatten Unternehmen bereits auf alternative Übermittlungsmechanismen zum Privacy Shield gesetzt und zusätzlich auf Standardvertragsklauseln (SCC) zurückgegriffen. Aus den Erfahrungen mit Schrems I und den Umsetzungen iRd Dokumentationspflichten aus der DS-GVO hatten die Unternehmen vorgesorgt. Sie kannten im Wesentlichen die kritischen Datenverarbeitungen im Unternehmen und waren in der Lage, schneller auf den Wegfall des Abkommens zu reagieren.

ZD: Im Zusammenhang mit dem Schrems-II-Urteil standen ja auch die Standardvertragsklausel auf dem Prüfstand. Was bedeutet das EU-US Data Privacy Framework für die bereits vereinbarten Standardvertragsklauseln? Ist es ratsam, sie jetzt zu kündigen?

Schmitz: Im Schrems-II-Urteil hat der EuGH die Anforderungen an die Verwendung von Standardvertragsklauseln deutlich erhöht und den Datenexporteur verpflichtet, iRe Transfer-Impact-Assessment (s. Klau-

sel 14 b) ii) SCC) vor der Übermittlung personenbezogener Daten zu prüfen, ob in dem Drittland ein Schutzniveau für personenbezogene Daten besteht, das dem Schutzniveau in der EU gleichwertig ist. Die Unternehmen sollten die geltenden Rechtsvorschriften und tatsächlichen Praktiken im Drittland prüfen und bewerten, ob diese die Anforderungen an ein angemessenes Schutzniveau erfüllen. Damit haben sich viele Unternehmen verständlicherweise schwergetan. Zukünftig kann für diese Prüfung und Bewertung auf die dem EU-US DPF zu Grunde liegenden Voraussetzungen zurückgegriffen werden. Dies wurde sowohl von Reynders in der Pressekonferenz der EU-Kommission v. 10.7.2023 als auch vom EDSA in den FAQs zum DPF bestätigt. Angesichts dieser Erleichterungen bei der Anwendung der Standardvertragsklauseln und einer bestehenden Unsicherheit hinsichtlich der Bestandskraft des DPF gehe ich davon aus, dass die Unternehmen die Standardvertragsklauseln weiterhin nutzen und anwenden werden.

ZD: Hat das EU-US DPF auch Auswirkungen auf Datenübermittlungen aus dem Vereinigten Königreich oder der Schweiz?

Schmitz: In der Schweiz tritt zum 1.9.2023 ein neues Datenschutzgesetz in Kraft, das in Art. 16 SchwDSG regelt, unter welchen Voraussetzungen „Personendaten ins Ausland bekanntgegeben werden" dürfen. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) hat nach der Veröffentlichung des EU-US DPF am 10.7. 2023 mitgeteilt, dass auch die Schweiz mit den USA zusammenarbeitet, um einen entsprechenden Rahmen, das sog. Swiss-US DPF, zu

erarbeiten. Es wird davon ausgegangen, dass der Schweizer Bundesrat nach Inkrafttreten des neuen SchwDSG das Swiss-US DPF als Grundlage für den Datentransfer anerkennen wird.

Die britische Regierung verhandelt mit den USA eine separate sog. Datenschutzbrücke, die laut Pressemitteilung der Britischen Regierung v. 8.6.2023 als Ergänzung zum EU-US DPF zu verstehen ist.

ZD: Herr Dr. Spies, was werden jetzt die nächsten Schritte sein, die US-Unternehmen, die Daten aus Europa empfangen, ergreifen müssen?

Spies: Man muss unterscheiden, ob die Datenexporteure schon zum 17.7.2023 nach dem Privacy Shield ordnungsgemäß zertifiziert waren oder nicht. An diesem Tag hat das US-Handelsministerium (DoC) die schon zertifizierten Unternehmen in das EU-US DPF automatisch überführt. Diese Unternehmen müssen innerhalb von drei Monaten ihre Datenschutzerklärungen anpassen, können das DPF aber schon jetzt nutzen. Die Anpassung kann das registrierte Unternehmen per Login erledigen – es ist kein neuer Zertifizierungsantrag an das DoC erforderlich. Allerdings gilt auch: Diese Unternehmen müssen gut aufpassen, welche Angaben sie machen, denn falsche oder unrichtige Angaben können von den zuständigen US-Regierungsbehörden wie der FTC (Federal Trade Commission) als Verbraucherschutzbehörde sanktioniert werden. Die FTC-Anforderungen für die Data Privacy haben sich seit dem Privacy Shield 2016 fortentwickelt. Für nicht-registrierte US-Unternehmen ist der Registrierungsprozess ziemlich identisch mit dem des Privacy Shield (s. von dem Bussche/Voigt, Konzerndatenschutz/Spies, 2. Aufl. 2019, Teil 4 Kap. 4). Ich erwarte deshalb jetzt keinen großen Ansturm auf DPF-Registrierungen. Viele US-Unternehmen sind bereits über den Privacy Shield registriert – nur wenige sind nach Schems II abgesprungen. Manche neuen Kandidaten werden sich genau überlegen, ob sie sich gegenüber den Behörden auf der DPF-Liste exponieren wollen. Viele werden weiterhin auf die SCC und vielleicht auf die Ausnahmen nach Art. 49 DS-GVO setzen – nicht zuletzt zur eigenen Absicherung, wenn es einmal zu einem Schrems-III-Urteil des EuGH gegen den Angemessenheitsbeschluss kommen sollte. Oder weil der Datenimporteur nicht der Aufsicht der FTC oder des Department of Transportation untersteht und er das EU-US DPF nicht nutzen kann.

Schmitz: Zur Ergänzung: Alisa Vekeman, Co-Lead, Transatlantic Data Flows, EU-Commission, hat in einer IAPP-Videokonferenz am 18.7. 2023 bestätigt, dass Datenimporteure aus den USA, die nach dem DPF zertifiziert sind, keine SCC mit ihren Unterauftragnehmern vereinbaren müssen, wenn sie diese vertraglich zur Einhaltung der DS-GVO verpflichtet haben.

ZD: Und was müssen die europäischen Datenexporteure jetzt machen, wenn sie personenbezogene Daten an einen so registrierten Datenimporteur in die USA übermitteln?

Spies: Auch hier gelten die DS-GVO-Regeln weiter, zB die Information der Betroffenen nach Art. 13 Abs. 1 lit. f DS-GVO – jetzt halt zum Datentransferaustausch. Wie bisher ist zu prüfen, ob das empfangende Unternehmen auf der DPF-Liste als „aktiv" eingetragen ist und ob die Datenkategorien, die übermittelt werden, davon abgedeckt werden. Und wie Frau Schmitz gesagt hat: US-Unternehmen, die schon jetzt zB nach Art. 3 Abs. 2 DS-GVO (Marktortprinzip) unter die DS-GVO-Regeln fallen, müssen alle bestehenden Regeln einhalten.

ZD: Herr Dr. Spies, von europäischer Seite ist häufig die Kritik zu hören, dass es in den USA grundsätzlich an einem Datenschutzverständnis fehle. Dabei existiert inzwischen eine Vielzahl von Datenschutzgesetzen in den einzelnen Bundesstaaten, wie zB der California Consumer Protection Act (CCPA), und im Juni 2022 wurde in den USA überraschend ein Entwurf für ein nationales

Datenschutzgesetz vorgelegt, der sog. American Data Privacy and Protection Act (ADPPA). Wie schätzen Sie die datenschutzrechtliche Situation in den USA ein?

Spies: Das EU-US DPF ist sozusagen der Ersatzreifen für das weiter nicht existierende, umfassende US-Bundesdatenschutzgesetz, da das DPF vermutlich ein Marktstandard für alle US-Unternehmen wird. Klar, eine Executive Order könnte jederzeit aufgehoben werden, aber dann fiele wohl auch das DPF in sich zusammen. Viele US-Unternehmen richten sich jetzt schon nach dem strengen Standard des kalifornischen Datenschutzgesetzes CCPA in seiner neuesten Fassung. Und der CCPA enthält bereits schon viele Elemente der DS-GVO. Die Lücke ist nicht so groß.

ZD: Wird das neue Abkommen halten? Was müsste passieren, damit es nicht mehr als Rechtsgrundlage für den Datentransfer dienen kann?

Spies: Schwer zu sagen, aber hier in Washington ist man optimistisch, dass es hält. Der genannte Ombudsmann hatte zur Zeit des Privacy Shield meines Wissens nicht einmal tätig werden müssen. Das könnte sich jetzt ändern.

Schmitz: Auf europäischer Ebene ist man sehr zuversichtlich, dass das Abkommen Bestand haben wird, schon allein deshalb, weil sich die EU-Kommission an den rechtlichen Vorgaben des EuGH, insbesondere in den Punkten Notwendigkeit, Verhältnismäßigkeit und Rechtsschutzsystem, orientiert hat. Man ist aber auch realistisch und nimmt die Aussagen und Ankündigungen von Max Schrems zur Kenntnis. Formal wird es aber kein Schrems III geben. Aus Datenschutzgründen wird der EuGH für alle ab 1.7.2018 anhängig gemachten Vorabentscheidungsersuchen nur mehr fiktive Fallnamen und nicht mehr die Namen der Verfahrensbeteiligten verwenden.

ZD: Es bleibt also sowohl interessant als auch spannend. Wir werden die Entwicklungen bei Behörden und Unternehmen diesseits und jenseits des Atlantiks verfolgen und aktuell darüber berichten. Vielen Dank für das Gespräch.

Barbara Schmitz, Rechtsanwältin bei BAY GmbH Wirtschaftsprüfungs-/Rechtsanwaltsgesellschaft in München sowie Mitglied des ZD-Wissenschaftsbeirats, und Dr. Axel Spies, Rechtsanwalt in der Kanzlei Morgan, Lewis & Bockius in Washington DC sowie ZD-Mitherausgeber, im Gespräch mit Anke Zimmer-Helfrich, Chefredakteurin der ZD.