ZEITSCHRIFT FÜR DATENSCHUTZ
INTERVIEW
ZD
9/2021

Internationaler Datentransfer – Neue SCC – Marktortprinzip – Neue Angemessenheit – was geht?

ZD-Interview mit Barbara Schmitz und Axel Spies

■ Seit dem Urteil des EuGH zu „Schrems II" (Privacy Shield) herrscht bei Unternehmen und Behörden große Unsicherheit darüber, wie Dienstleistungen genutzt werden können, für die ein Datenaustausch in die USA Grundlage der Datenverarbeitung ist. Bei diesen Dienstleistungen handelt es sich größtenteils um Anbieter, die aus den Geschäftsprozessen nicht mehr wegzudenken sind. Wegen der möglicherweise drohenden und teilweise schon angekündigten Bußgelder auf Grund eines Datenschutzverstoßes wird auf allen Ebenen versucht, einen Lösungsweg zu finden. Die Spanne der Lösungen reicht dabei von Nichtnutzung über Anpassung vorhandener Werkzeuge bis hin zu komplett neuen Ansätzen. In dem folgenden Interview möchten wir die Möglichkeiten für internationale Datentransfers besprechen.

■ Since the ECJ ruling on "Schrems II" (Privacy Shield), there has been great uncertainty among companies and public authorities regarding how to use services for which a data exchange to the USA is the basis of data processing. For the most part, these services are providers that have become an indispensable part of business processes. Attempts are being made at all levels to find solutions due to the possibly impending and in part already announced administrative fines based on data protection violations. The scope of solutions reaches from non-usage to adjustment of existing tools to completely new approaches. We would like to discuss the possibilities of international data transfers in the following interview.

Lesedauer: 13 Minuten

ZD: *Frau Schmitz, Herr Dr. Spies, wie würden Sie die Stimmung in den Unternehmen beschreiben, wenn es um die Frage der Nutzung von Dienstleistungen mit Datenverarbeitung in den USA geht?*

Schmitz: Von hilflos bis rebellisch. Unmittelbar nach dem Schrems-II-Urteil im vergangenen Juli wurde – meiner Erfahrung nach – in den Unternehmen panisch versucht, die offensichtlichen Dienste mit US-Bezug aus den Geschäftsprozessen herauszunehmen. Es stellte sich dann aber schnell heraus, dass es sich bei diesen Diensten mehrheitlich um für den Betrieb relevante Dienste handelte, für die nur mit hohem zeitlichen und finanziellen Aufwand ein Ersatz zu implementieren war. Die Empfehlungen der regionalen und europäischen Datenschutzaufsichten zur Dienstleisterprüfung und die Ankündigung der EU-Kommission von neuen SCC gaben dann den Unternehmen konkrete Anhaltspunkte für Verhandlungen mit den Dienstleistern an die Hand. In der Folge entwickelten sich Diskussionen in den Expertenrunden um ergänzende Anwendungen, wie die zusätzlichen technischen und organisatorischen Maßnahmen, und auch um die Frage: Sind wirklich alle Datenübermittlungen in die USA betroffen, oder kann hier sinnvoll differenziert werden? Die hieraus entstandenen Ergebnisse sind durchaus lösungsorientiert und haben dankenswerterweise den anfänglichen Hype wieder auf ein sachliches Maß reduzieren können.

Spies: Aus Sicht der Dienstleister: Bei den meisten international tätigen Unternehmen hier in den USA ist „Schrems II" als Thema angekommen. Fast unisono wünschen sie sich eine tragfähige Einigung zwischen der US-Regierung und der EU-Kommission. Angeblich soll es bis Jahrsende dazu kommen, aber ich bin pessimistisch. Was die SCC betrifft: Die vom EuGH u.a. so eindringlich geforderte Risikoanalyse ist auch für kleinere und mittelgroße Unternehmen (auch in den USA) ohne teure Expertenhilfe von außen kaum zu bewerkstelligen. Die meisten US-Unternehmen bleiben unter dem Privacy Shield, das das U.S. Department of Commerce ja weiter verwaltet – fast so, als wäre nichts geschehen – und warten ab. Andere setzen auf Einwilligungslösungen nach Art. 49 Abs. 1 lit. a, 6 Abs. 1 lit. a DS-GVO.

ZD: *Was halten Sie von den neuen SCC? In Artikel 1 Abs. 1 des Durchführungsbeschlusses ist es ja bei der Formulierung geblieben, dass die SCC für Verarbeitungen gelten, wenn der Datenimporteur nicht der DS-GVO unterliegt. In Erwägungsgrund 7 S. 3 des Durchführungsbeschlusses könnte dies jedoch nicht für Importeure unter dem Marktortprinzip gelten. Was halten Sie beide davon?*

Spies: Die in der DS-GVO neu geschaffene Regelung zum sog. Marktortprinzip eröffnet grundsätzlich diese Möglichkeit. Grundlage hierfür ist, dass Satz 2 von Erwägungsgrund 7 neu in die endgültige Fassung eingefügt wurde und somit den vorherigen Satz 2 (jetzt Satz 3) ergänzt. Überraschend ist das nicht, denn der EDSA hatte das bereits in einer gemeinsamen Stellungnahme mit dem EDSB vorgeschlagen (s. Stellungnahme 2/2021, abrufbar unter: edpb_edps_jointopinion_202102_art46sccs_de.pdf, Rn. 27) und schon in der Leitlinie 3/2018 (abrufbar unter: edpb_guidelines_3_2018_territorial_scope_after_consulta-

tion_de.pdf (europa.eu)) zum räumlichen Anwendungsbereich der DS-GVO in diese Richtung argumentiert. Die Schlüsselfaktoren – europäisches Datenschutzniveau und territorialer Anwendungsbereich – bilden dabei die Maßstäbe. Immer, wenn für ein Produkt oder eine Dienstleistung Daten europäischer Bürger*innen erhoben und verarbeitet werden, muss ein entsprechendes Datenschutzniveau der DS-GVO gewährleistet werden, und zwar unabhängig davon, wo diese Daten lokal verarbeitet werden. Der Ansatz, den räumlichen Anwendungsbereich der DS-GVO als Grundlage für die Sicherstellung eines angemessenen Datenschutzniveaus festzustellen, schafft zum einen die Verpflichtung der Vertragsparteien, das Datenschutzniveau der DS-GVO zu gewährleisten, und zum anderen unternehmerische Freiheiten bei der Auswahl des Dienstleisters. So könnte auch ein Unternehmen in den USA gewählt werden, wenn es z.B. seinen Sitz in einem Bundesstaat mit entsprechenden Datenschutzgesetzen hat und praktische Erfahrungen mit (sicherheits-)behördlichen Auskunftsersuchen hinsichtlich der Art der zu übermittelnden Daten.

Schmitz: Dieser Annahme wird ja hier und da der Wortlaut des Art. 44 DS-GVO entgegengehalten. Nach meinem Verständnis geht dieser Einwand aber fehl. Zum einen durch den strukturellen Aufbau der DS-GVO, wonach Art. 3 als allgemeingültige Regelung vor die Klammer gezogen wird. Zum anderen verweist Art. 44 DS-GVO in Satz 1 auf die Möglichkeit von „sonstigen Bestimmungen dieser Verordnung", sodass die DS-GVO in jedem Fall anwendbar bleibt – auch ohne SCC.

ZD: *Wie sind die Chancen, dass sich die US-Regierung und die EU auf einen Nachfolgemechanismus zum Privacy Shield einigen?*

Spies: An gutem Willen fehlt es auf beiden Seiten nicht, aber sie müssen realistisch sein, was rechtlich und politisch erreicht werden kann. Wenn es darum geht, dass die US-Regierung auf dem Verordnungsweg (Executive Order des Präsidenten) einige kritisierte Punkte am Privacy Shield Framework ändert, ist vieles machbar. Z.B. könnte der Zugang zu Rechtsmitteln für Europäer*innen im Rahmen des Framework verbessert werden oder „intelligence agency privacy and civil liberties officers" (PCLOB) oder ein neues Gremium ins Verfahren mit eingebunden werden, um die Fakten zusammenzutragen. Statt eines Ombudsmanns sind andere Lösungen denkbar. Das FISA-Gericht könnte seine bestehende Prüfungskompetenz weit auslegen. Wenn aber die Europäer*innen eine grundlegende Reform der Überwachungsregeln nach FISA, EU 130222 oder PO 28 erzwingen wollen, werden sie enttäuscht werden. Dies ist mit dem gegenwärtigen US-Kongress schlicht nicht machbar.
Auf US-Seite wäre es sinnvoll, wenn die US-Regierung mehr Informationen für die Europäer*innen bereitstellen würde, wie die gegenwärtigen Überwachungsregeln funktionieren. Es gibt zu viel Geheimniskrämerei, wie ja auch bei den Geheimdiensten in Europa. Meines Wissens gibt es z.B. kaum Datenanforderungen der strafrechtlich tätigen Behörden nach dem US CLOUD Act, der in der EU so viel Wirbel verursacht. Mit dem White Paper (abrufbar unter: Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II (commerce.gov)) der US-Regierung zu „Schrems II" vom September 2020 ist ein Anfang gemacht. Leider machen sich zu wenige Datenschutzbehörden die Mühe, das White Paper genau zu lesen. Schrems tat es ja umgehend als Trump-Propaganda ab. Eine solche Initiative der US-Regierung würde einem Kerndefizit des Schrems-II-Urteils entgegenwirken, nämlich, dass der EuGH nicht auf die aktuelle Situation und Fassung der Überwachungsgesetze in den USA abgestellt hat. Es ist jetzt acht Jahre her, dass Snowden nach Russland geflohen ist. Seitdem hat sich einiges getan. Aber wie dem auch sei – wenn es zu einer Einigung kommt, werden Schrems, NOYB und andere dagegen wieder klagen. Mit diesem Risiko müssen (und können) alle Parteien leben. Ein solches Hin und Her vor Gericht gibt es hier in den USA häufig, z.B. bei dem Problem der Netzneutralität.

Schmitz: In der Tat hat sich im vergangenen Jahr einiges in Sachen internationaler Datentransfer getan. „Schrems II" hat ja nicht nur den Datentransfer in die USA berührt, sondern auch die Überprüfung der Datentransfers in andere (Nicht-)EU-Länder auf den Plan gerufen. Insbesondere der Brexit hat die Diskussion um den vorhandenen oder – vielleicht besser – erwarteten europäischen Datenschutzstandard befeuert. Mit Blick auf die nachrichtendienstlichen Tätigkeiten in UK, deren Praxis von Edward Snowden mit der in den USA auf eine Stufe gestellt wurde, verwundert die Angemessenheitsentscheidung der EU-Kommission für UK schon etwas. Entscheidend für die Annahme eines angemessenen Datenschutzniveaus waren zum einen die Möglichkeit für von Überwachungsmaßnahmen Betroffene, Klage beim Investigatory Powers Tribunal einzureichen. Zum anderen – und das ist ein interessanter Aspekt auch mit Blick auf die hier im Interview gemachten Überlegungen zum Marktortprinzip – war die Auffassung entscheidend, dass UK die Grundsätze, Rechte und Pflichten der DS-GVO und der Richtlinie zum Datenschutz bei der Strafverfolgung vollumfänglich in sein heutiges, seit dem Brexit geltendes Rechtssystem übernommen hat (s. PM EU-Kommission v. 28.6.2021). So ganz stringent scheint mir das nicht zu sein. Eine vom LIBE-Ausschuss der EU mit in Auftrag gegebene Studie zum Austausch von personenbezogenen Daten nach dem Schrems-II-Urteil macht auf 122 Seiten Ausführungen zu den europäischen Anforderungen eines angemessenen Datenschutzniveaus und den politischen Hindernissen in den Drittländern. Neben verschiedenen praktischen Lösungsmöglichkeiten finde ich vor allem folgenden Ansatz hilfreich und zukunftsorientiert: „die Ausarbeitung und Ratifizierung eines ‚minilateralen' Vertrags, der nachrichtendienstliche Aktivitäten insbesondere der 30 EU/EWR-Staaten und der ‚Five Eyes'-Länder (USA, Großbritannien, Australien, Kanada und Neuseeland) abdeckt." (LIBE-Studie, abrufbar unter: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf).

ZD: *Frau Schmitz, können europäische Unternehmen auf ein Moratorium der Datenschutzbeauftragten bei den Strafen hoffen, bis sich die USA und die EU auf einen Nachfolger des Privacy Shield diplomatisch geeinigt haben? Und wann wird eine solche Einigung kommen?*

Schmitz: Die nationalen und europäischen Aufsichtsbehörden haben in den letzten Monaten hilfreiche Materialien und Orientierungshilfen für den Umgang mit den Auswirkungen des Schrems-II-Urteils erstellt und herausgegeben. Die Unternehmen konnten damit erste Schritte zur Umsetzung der Anforderungen des EuGH unternehmen. Erfreulicherweise ist der Grundtenor der Aufsichtsbehörde der, dass die Bemühungen der Unternehmen, wie Dienstleisterprüfung, Umstellung auf SCC und Anpassung derselben mit zusätzlichen Maßnahmen sowie Dokumentation der Prüfungstätigkeiten, gesehen werden und dass bei den Maßnahmen unterstützt wird. Die Unternehmen nehmen aber auch wahr, dass die Aufsichtsbehörden vermehrt konkrete Prüfungen durchführen und auch Bußgelder androhen. Hier wird das Dilemma sichtbar, in dem sich Aufsichtsbehörden und Unternehmen derzeit befinden. Umso wichtiger wird es, dass zeitnah auf europäischer Ebene realistische Werkzeuge für den Datentransfer in die USA zur Verfügung gestellt werden.
Realistisch deshalb, weil ein Schwerpunkt des Schrems-II-Urteils – nämlich die Kritik des EuGH an den in den USA vorhandenen Überwachungsprogrammen – zumindest in absehbarer Zeit

nicht ausgeräumt werden wird. An dieser Stelle sei es erlaubt, den vom EuGH angewendeten Prüfungsmaßstab, die Datenzugriffsbefugnisse von Sicherheitsbehörden und die Privilegierung des einheitlichen Datenschutzniveaus innerhalb des EWR, zu hinterfragen. Die hier vom EuGH zu Grunde gelegten Annahmen erschweren meines Erachtens die Aufnahme von Verhandlungen für einen neuen Angemessenheitsbeschluss für die USA. In einer Videokonferenz im Rahmen einer Veranstaltung der IAPP hat sich Dr. Ralf Sauer, stellvertretender Referatsleiter der Abteilung „Internationale Datenströme und Datenschutz" der GD Justiz und Verbraucherschutz der Europäischen Kommission, in diesem Sinne geäußert. Für ein absehbares Privacy Shield III sieht er derzeit keine nachhaltige Grundlage.

ZD: *Ist bei der Beurteilung des angemessenen Schutzniveaus die Überlegung zulässig, wonach in der Vergangenheit US-Behörden auf Unternehmensdaten noch nicht zugegriffen hätten und folglich auch künftig ein solcher Zugriff „höchst unwahrscheinlich" sei?*

Spies: Das genannte White Paper der US-Regierung führt sinngemäß an, dass die meisten Daten, die von US-Unternehmen verarbeitet werden, für die US-Sicherheitsbehörden uninteressant sind. So argumentieren viele Datenexporteure auch in ihren Risikoanalysen. Dieses Argument alleine wird für die Risikoanalyse nicht ausreichen, da der EuGH in seinem Schrems-II-Urteil die Überwachungsprogramme der USA auf der Grundlage von 702 FISA und der EO 12333 als unvereinbar mit dem von der EU im Lichte der Artikel 7 und 8 GRCh geschaffenen Datenschutzniveau ansieht. Aber das Risiko dürfte für die meisten Datensätze gering sein.

Schmitz: Ihre Frage behandelt darüber hinaus den Hintergrund, wann ein „Schrems-relevanter" Datentransfer überhaupt anzunehmen ist. Wenn z.B. ein US-amerikanisches Tochterunternehmen mit Sitz im EWR die Datenverarbeitung vornimmt und ein physischer Datentransfer in die USA nicht erfolgt. Johannes Caspar, der mittlerweile ausgeschiedene Hamburgische Datenschutzbeauftragte, hat sich in einer Veranstaltung der IHK Hamburg am 31.3.2021 dahingehend geäußert, dass dann keine Datenübermittlung in die USA anzunehmen ist, wenn die Server in der EU/dem EWR stehen. Aber ist die Speicherung der Daten im EWR wirklich die bessere Alternative? Die US-Geheimdienste kommen an Daten im Ausland häufig besser ran als im Inland, wo sie einem ganzen Bündel von gesetzlichen Restriktionen unterliegen. Eine Unterbindung des Datenflusses in die USA ist mangels Alternativen bei den Dienstleistern jedenfalls keine realistische Lösung, verursacht in Europa bei den Unternehmen und Behörden enorme Schäden und führt in die Sackgasse, wie hier in der ZD kürzlich Schwartmann/Burkhardt treffend aus verwaltungsrechtlicher Sicht beschrieben haben (ZD 2021, 235).

ZD: *Ergänzend zu der vorherigen Frage: Bringt die neueste Initiative von Microsoft Erleichterung bei der Umsetzung von Schrems II, dadurch, dass Microsoft auf Wunsch der Unternehmen Cloud-Daten nur in der EU speichern will?*

Schmitz: Nach meinem Verständnis geht es in dem Schrems-II-Urteil um den physischen Transfer. So heißt es in Rn. 183: „... die sich auf dem Weg in die Vereinigten Staaten befinden ...". Daten, die in der EU/dem EWR physisch liegen und nur theoretisch über die US-Muttergesellschaft von den US-Behörden angefordert werden können, unterliegen folglich nicht dem Anwendungsbereich von Art. 44 DS-GVO und sind damit nicht „Schrems-relevant". Zwar darf man den CLOUD Act auch hier nicht außer Acht lassen. Über den CLOUD Act können die amerikanischen (Sicherheits-)Behörden amerikanische Unternehmen verpflichten auch Daten aus Servern außerhalb der USA offenzulegen. Der CLOUD Act wird im Schrems-II-Urteil mit keinem Wort erwähnt. Das lässt den Schluss zu, dass der CLOUD Act nicht zur Bewertung der Angemessenheit des Datenschutzniveaus herangezogen wurde. FISA und EO 12333 sind nachrichtendienstliche Auslandsüberwachungs-Regelungen. Der CLOUD Act beinhaltet grundsätzlich keine nachrichtendienstliche Überwachung, sondern dient der Erhebung von elektronischen Beweismitteln für Strafverfahren – auch für Daten außerhalb des US-Territoriums – und das auch nur gegen einen Anbieter von „electronic communication service" oder von „remote computing service" in den USA. Für den CLOUD Act war früher ein Rechtshilfeersuchen zwischen den Strafbehörden der beteiligten Länder notwendig. Dieses langwierige Verfahren ist nach dem CLOUD Act nicht mehr erforderlich, weil die US-Strafverfolgungsbehörden die bestimmten Dokumente nunmehr direkt bei diesen Anbietern in den USA abrufen können, wenn diese auf die Dokumente Zugriff haben. Derzeit verhandeln verschiedene Länder mit den USA über ein Ersatz-Rechtsbehelfsverfahren. Ein solches Cloud-Act-Agreement besteht inzwischen zwischen UK und den USA.
Um auf die Frage zurückzukommen: Die Microsoft-Initiative zur Speicherung der Cloud-Daten auf EU-/EWR-Gebiet dürfte ein gangbarer Weg werden.

ZD: *Werden die neuen Standardverträge (SCC) der Kommission ein Erfolg, indem sie mehr Sicherheit für internationale Datentransfers bringen?*

Spies: Aus US-Sicht sind die bestehenden SCC mit jeder Menge Rechtsunsicherheiten behaftet, allein schon was die Formulierung der einzelnen Klauseln betrifft. Ich fürchte, das wird sich mit den neuen SCC und all den verschiedenen Modulen und komplizierten Anlagen nicht ändern. Aber solange die SCC nicht zu gerichtsfesten Schadensersatzansprüchen oder gar zu saftigen Strafen für die Datenimporteure führen, werden viele Datenimporteure außerhalb der EU sie weiterhin einfach abzeichnen, ungelesen abspeichern oder als Teil der AGB akzeptieren, wie das bisher schon allzu häufig der Fall ist.

Schmitz: Der modulare Ansatz bietet in jedem Fall mehr Flexibilität für Datentransfers in Drittländer. Im Ergebnis muss eine Standardisierung aber auch hier möglich sein. Denn Unternehmen können nicht für jede einzelne Datenübertragung ein eigenes Vertragskonstrukt erarbeiten. Ich hoffe, dass die von den Aufsichtsbehörden bereits erarbeiteten Prüfungsschemata zum Transfer-Impact-Assessment noch ergänzt werden, insbesondere zu den Analysen möglicher Risiken im Drittland – Stichwort: „Gepflogenheiten des Bestimmungslands".

ZD: *Es bleibt also spannend, und wir werden in der ZD die Entwicklungen verfolgen und aktuell berichten. Vielen Dank für das Gespräch.*

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



■ Vgl. hierzu auch *Conrad/Siara*, ZD 2021, 471 und *Spies*, ZD 2021, 478 – beide in diesem Heft.