AXEL SPIES

EU-US-Privacy-Shield – eine schwierige Reparatur

Probleme bei den Verhandlungen und Schwierigkeiten mit der Risikoanalyse des EDSA

Schrems II
Standardvertragsklauseln
SCC
Gefährdungspotenzial
Datenübermittlung in Drittstaaten

■ Nach dem Schrems-II-Urteil steht Datenexporteuren das EU-US-Privacy-Shield für Datenübermittlungen in die USA nicht mehr zur Verfügung. Das Ausweichen der Parteien auf Standardvertragsklauseln (SCC) ist jedoch schwierig. Die vom EDSA in seinen neuesten Empfehlungen v. 18.7.2021 geforderte Risikoanalyse ist praktisch nicht umsetzbar. Es bedarf deshalb dringend einer Lösung auf politischer Ebene.
Lesedauer: 16 Minuten

■ Following the Schrems-II ruling, the EU-US-Privacy-Shield is no longer available to data exporters for the transfer of data into the USA. However, it is difficult for the parties to switch to standard contractual clauses (SCC). The risk analysis demanded by the EDPB in its latest recommendations dated July 18, 2021 is practically impossible to implement. Thus, a solution on a political level is urgently needed.

I. Ausgangslage

Wer in diesen Tagen von Brüssel oder Luxemburg aus auf die Webseite „privacyshield.gov" klickt, reibt sich verwundert die Augen. Als sei nichts geschehen, wird der Besucher dort willkommen geheißen und zur Selbstzertifizierung eingeladen. Allerdings ist die Liste selbst dort nicht mehr zugänglich. Das Privacy Shield hat von 2016 bis 2020 als Mechanismus für die Datenimporteure praktisch gut funktioniert.[1]

Die Liste der registrierten US-Unternehmen war offen einsehbar. Mit über 5.000 registrierten US-Datenimporteuren[2] gab es bis zum Paukenschlag durch das Schrems-II-Urteil eine kritische Masse. Deren Datenschutzerklärungen waren auf der Privacy-Shield-Webseite leicht auffindbar zusammengestellt. Mit der *Federal Trade Commission (FTC)* als Verbraucherschützerin war eine schlagkräftige Behörde[3] mit der Durchsetzung der Privacy-Shield-Verpflichtungen beauftragt. Die Unternehmen mussten ihre Dokumente vorab vom *US-Handelsministerium* prüfen lassen – oft in Abstimmung mit der Rechtsabteilung der *FTC*. Erst dann wurde das Unternehmen zum Privacy Shield zugelassen.

Ohne hier in die Einzelheiten der Registrierung gehen zu können[4] – der Compliance-Aufwand für die Registrierung der US-Empfänger nach dem Privacy Shield und ihre Aufrechterhaltung war erheblich, aber durchaus verkraftbar. Da deren Privacy Policies und Kontaktdaten öffentlich zugänglich und per Mausklick vergleichbar waren, bestand ein erheblicher Druck auf diese Datenimporteure, Zeit, Geld und Energie in die Privacy-Shield-Dokumente zu investieren. Trotz dieser Vorteile: Auch ein Jahr nach dem Schrems-II-Urteil haben sich die Parteien noch nicht auf eine Reparatur geeinigt.

II. Schrems-II-Entscheidung: Fokus auf Überwachungsmaßnahmen

Der *EuGH* hat im Schrems-II-Urteil zur Problematik der Überwachung und des Datenzugangs der US-Behörden in den USA klar Stellung bezogen. Das Diktum des *EuGH* im Schrems-II-Urteil zu den – aus Sicht des *EuGH* – falsch getroffenen Feststellungen der *EU-Kommission* verhindert bis heute, dass die *EU-Kommission* sich an eine Neuauflage des Privacy Shield herantraut.

Die Grundlage dieser Feststellungen scheint aber nicht besonders gefestigt zu sein, denn der *EuGH* formuliert in Rn. 168: „das vorlegende Gericht ... hegt Zweifel daran, ob das Recht der USA ... im Lichte der Art. 7, 8 u 47 GRCH ... das erforderliche Schutzniveau gewährleistet."[5] Die Formulierung „hegt Zweifel" ist vage und vorsichtig für eine so bedeutende Aussage. Zudem legt der *EuGH* einen Prüfungsstandard an, der zwingende Erfordernisse des für den Datenimporteur (!) geltenden innerstaatlichen Rechts, „zur Gewährleistung der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit, der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten", ja sogar von „Verstöße[n] gegen die berufsständischen Regeln bei reglementierten Berufen, eines wichtigen wirtschaftlichen oder finanziellen Interesses eines Mitgliedstaats, des Schutzes der betroffenen Person und der Rechte und Freiheiten anderer Personen" anerkennt (Fußn. 2 zu Klausel 5 der vom *EuGH* gebilligten Standardvertragsklauseln von 2010).[6]

Der *EuGH* sagt nichts zum Schutzniveau des US-Datenschutzrechts allgemein. Er hat auch kein Urteil abgegeben, wie „angemessen" die Rechtslage in den USA im Jahre 2021 ist. Seit den *Snowden*-Enthüllungen zur US-Überwachungspraxis (2006) hat sich in den USA viel getan. Die von dem Schrems-II-Urteil aufgeworfenen Streitpunkte zwischen den USA und der EU sind gleichwohl erheblich.

So führt der *EuGH* z.B. zum Zugang der „Unionsbürger" (ein Begriff, der in der DS-GVO nirgendwo verwendet wird) in Rn. 187 aus: „Nach ständiger Rechtsprechung ist es dem Wesen eines Rechtsstaats inhärent, dass eine wirksame, zur Gewährleistung der Einhaltung des Unionsrechts dienende gerichtliche Kontrolle vorhanden sein muss. Daher verletzt eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz." Diese Forderung lässt sich kaum ohne eine Änderung des US-Rechts umsetzen, für die es im *Kongress* derzeit kaum eine Chance gibt.

Deshalb blieb der *Biden*-Administration bei dem kürzlichen Besuch des *Präsidenten* und der hochrangigen US-Delegation in

1 S. im Einzelnen *Spies,* Kap. 4 „Privacy Shield Principles" in: von dem Bussche/Voigt, Konzerndatenschutz, 2. Aufl. 2019, S. 298 ff., und *Kipker*, ZD 2021, 397.
2 Vgl. https://fortune.com/2020/07/16/privacy-shield-eu-us-companies-business/.
3 Genau genommen setzen die *FTC* und das *Department of Transportation (DOT)* die Privacy Principles um, *Spies* (o. Fußn. 1), Rn. 7-9. Am 25.6.2021 wurde *Lina Khan* zur neuen FTC-Chefin ernannt, von der sich alle Seiten eine gute Zusammenarbeit mit den europäischen Kartellbehörden versprechen.
4 *Spies* (o. Fußn. 1), Rn. 28-36.
5 *EuGH* ZD 2020, 511 m. Anm. *Moos/Rothkegel*.
6 Abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32010D0087&from=DE#ntr2-L_2010039DE.01001001-E0002.

Brüssel kaum etwas anderes übrig, als die Gesprächsfäden weiter aufzugreifen und auf einen allgemeinen Fahrplan (Roadmap) für die Verhandlung zum Datenfluss mit den Europäer*innen zu setzen. Im Kommuniqué[7] des *Weißen Hauses* zum G7-Gipfel v. 13.6.2021 heißt es dementsprechend: „Wir werden die Zusammenarbeit in bestimmten Bereichen in Bezug auf die Entwicklung der zukünftigen Grenzen unterstützen. Auf der Grundlage der Arbeit unserer Minister für Digitales und Technologie sind wir uns einig, dass der Schwerpunkt unserer Zusammenarbeit in diesem Jahr auf einem strukturierten Dialog zu bestimmten Bereichen liegen wird: ... – Förderung des freien Datenflusses mit Vertrauen, um das Potenzial wertvoller datengesteuerter Technologien besser zu nutzen und gleichzeitig die Herausforderungen im Zusammenhang mit dem Datenschutz weiter anzugehen. Zu diesem Zweck unterstützen wir unseren Fahrplan der Digitalminister für die Zusammenarbeit beim freien Datenfluss ...".

Es ist begrüßenswert, dass der Dialog zum freien Datenfluss transatlantisch so hoch aufgehängt ist, aber in der Sache haben sich Handelsministerin *Raimondi* und die Vertreter der *EU-Kommission* (EU-Justizkommissar *Reynders* und EU-Kommissarin *Vestager*) bei ihrem Treffen „zur Etablierung eines umfassenden Nachfolgers des Privacy-Shield-Rahmenwerks"[8] kaum angenähert.

Da kein Ende der Verhandlungen in Sicht ist und eine eventuelle Einigung mit ziemlicher Sicherheit wieder vor Gericht angefochten werden wird, weichen viele Unternehmen auf Standardvertragsklauseln (SCC) aus. Deren Umsetzung ist nirgendwo öffentlich einsehbar und wird von keiner Behörde vorab im Einzelfall geprüft – im Unterschied zum Privacy Shield. Manche Unternehmen setzen auch oder statt der SCC auf die „Ausnahmen für bestimmte Fälle" in Art. 49 DS-GVO, um den Datenfluss in die USA rechtlich zu sichern,[9] aber die SCC sind und bleiben praktisch extrem wichtig.

Zur „Unterstützung der Industrie" hat die *EU-Kommission* nach längerer Diskussion am 4.7.2021 neue SCC veröffentlicht.[10] Die Umsetzungsfrist für den EU-Beschluss beträgt 3 plus 15 Monate. Auf dem Papier ist das ein erheblicher Zeitraum, aber wenn man sich vor Augen hält, dass alle Verträge mit den Verantwortlichen und Auftragnehmern in Drittstaaten auf die neuen SCC umgestellt werden müssen, bleibt nicht sehr viel Zeit. Organisationen mit bestehenden SCC müssen bis zum 27.12.2022 die neuen SCC implementieren, aber schon dann, wenn die den SCC zu Grunde liegende Vereinbarung zwischen den Parteien neu verhandelt oder der Umfang der Datenverarbeitung während der Übergangszeit geändert wird, müssen die neuen SCC berücksichtigt werden.

Die neuen SCC wurden von einigen begrüßt, von anderen als viel zu bürokratisch abgelehnt. Die in den SCC zahlreich auftauchenden Zusagen dürften international versierten Anwält*innen, die Garantien (engl. „warranties") juristisch vorsichtig wie rohe Eier behandeln, einige Probleme bereiten. Sehr bürokratisch ist auch die Auflistung der Unterauftragsnehmer in Anhang III der SCC mit Namen, Anschrift, Kontaktperson usw., wenn Daten an Auftragsverarbeiter im Drittstaat (Modul 2 oder 3) übermittelt werden. Ohne einer tieferen Analyse der neuen SCC vorgreifen zu wollen,[11] scheinen die Datenexporteure und -importeure mit den neuen SCC nicht gerade ein Glückslos gezogen zu haben.

III. EDSA: Empfehlungen für die Risikoanalyse

Das wäre alles nicht so schlimm, wenn die Behörden nicht die Risikoanalyse („data transfer impact assessment"), die an sich schon äußerst komplex ist, mit den SCC verbunden hätten. Der *EDSA* nennt sein bis dato leider nur in Englisch vorliegendes 48-seitiges Papier v. 18.7.2021 „Empfehlungen" („Recommendations")[12], aber de facto sind es die geltenden Leitlinien. Die nachfolgenden Beobachtungen zeigen, dass sie aber kaum praktisch umsetzbar sind.

1. Potenzielle „Beeinträchtigungen"

Als Schritt 3 der Risikoanalyse müssen die Datenexporteure u.a. Folgendes tun: „Ein dritter Schritt besteht darin, zu beurteilen, ob es irgendetwas in den geltenden Gesetzen und/oder Praktiken des Drittlandes gibt, das die Wirksamkeit der angemessenen Sicherheitsvorkehrungen der Übermittlungsinstrumente, auf die Sie sich verlassen, im Zusammenhang mit Ihrer spezifischen Übermittlung beeinträchtigen könnte."[13]

Dieses „irgendetwas" („anything") kann alles oder nichts sein. Der auf das Lateinische zurückgehende[14] altenglische Begriff „impinge" für „beeinträchtigen" kann auch „eine Wirkung haben auf" bedeuten (vgl. engl. „impact"). Leider wird der *EDSA* in den Empfehlungen nicht viel konkreter. Weiter unten heißt es in dem verschachtelten Text:

„Die Risikoanalyse muss Elemente enthalten, die den Zugang zu Daten durch Behörden des Drittlandes Ihres Importeurs betreffen, wie zum Beispiel:
- Aussagen darüber, ob öffentliche Behörden des Drittlandes Ihres Importeurs versuchen können mit oder ohne Wissen des Datenimporteurs auf die Daten zuzugreifen – unter Berücksichtigung von Gesetzgebung, Praxis und berichteten Präzedenzfällen;
- Angaben darüber, ob Behörden des Drittlands Ihres Importeurs angesichts der Gesetze, der rechtlichen Befugnisse, der technischen, finanziellen und personellen Ressourcen, die ihnen zur Verfügung stehen, und der berichteten Präzedenzfälle in der Lage sein könnten, über den Datenimporteur oder über die Telekommunikationsanbieter oder Kommunikationskanäle auf die Daten zuzugreifen."[15]

Fazit: Es gibt kein Land, in dem der ansässige Datenexporteur diesen potenziellen Zugang guten Gewissens verneinen kann.

2. „Wesensgehalt der Grundrechte und -freiheiten" und Verschlüsselung

Damit ist die Arbeit aber noch lange nicht getan, denn es muss auch Folgendes geprüft werden: „Die Verpflichtungen oder Befugnisse, die sich aus solchen Gesetzen und Praktiken ergeben,

---

7 Vgl. https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/13/carbis-bay-g7-summit-communique/; die zitierte Roadmap v. 29.4.2021 ist abrufbar unter: http://www.g8.utoronto.ca/ict/2021-annex_2-roadmap.html.

8 Blogeintrag von *Raimondi* v. 23.6.2021, abrufbar unter: https://www.commerce.gov/news/blog/2021/06/us-secretary-commerce-gina-m-raimondo-joins-president-biden-us-eu-summit-and; *Kipker*, ZD 2021, 397, kritisiert zu Recht die „unausgesprochene Hilflosigkeit, in die man sich politisch und letztlich auch rechtlich mehr und mehr hineinmanövriert".

9 Ausf. *Leibold/Roth*, ZD-Aktuell 2021, 05247.

10 Durchführungsbeschluss 2021/914 der Kommission v. 4.6.2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der VO (EU) 2016/679 des Europäischen Parlaments und des Rates; vgl. hierzu auch *Conrad/Siara*, ZD 2021, 271 und das Interview *Schmitz/Spies*, ZD 2021, 455 – beide in diesem Heft.

11 Zum Diskussionsstand vor dem Beschluss *Spies*, ZD-Aktuell 2021, 05011.

12 EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0, Adopted on 18 June 2021, abrufbar unter: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

13 *EDPB* (o. Fußn. 12), S. 3 .

14 Lat. impangere = einschlagen = engl. „impact".

15 *EDPB* (o. Fußn. 12), Rn. 31.

werden als mit den Verpflichtungen des Übermittlungsinstruments nach Artikel 46 DSGVO unvereinbar angesehen, wenn sie den Wesensgehalt der Grundrechte und -freiheiten der EU-Grundrechtecharta nicht respektieren oder über das hinausgehen, was in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, um eines der wichtigen Ziele zu schützen, die auch im Unionsrecht oder im Recht der Mitgliedsstaaten anerkannt sind, wie sie z.B. in Artikel 23 (1) DSGVO aufgeführt sind."[16]

Spätestens an dieser Stelle werden viele Datenexporteure die Empfehlungen frustriert zur Seite legen, aber es kommt leider noch mehr auf sie zu: „Behörden in Drittländern können sich bemühen, auf übermittelte Daten zuzugreifen a) Im Transit durch Zugriff auf die Kommunikationswege, die zur Übermittlung der Daten an das Empfängerland genutzt werden. Dieser Zugriff kann passiv erfolgen, indem der Inhalt der Kommunikation, möglicherweise nach einem Auswahlverfahren, einfach kopiert wird. Der Zugriff kann aber auch aktiv in dem Sinne erfolgen, dass sich die Behörden in den Kommunikationsprozess einschalten, indem sie den Inhalt nicht nur lesen, sondern auch Teile davon manipulieren oder unterdrücken."[17] Die Architektur moderner TK-Netze baut darauf auf, dass Daten mehrere Länder durchqueren und über Satelliten oder Unterseekabel übertragen werden können. Damit müsste in die Risikoanalyse mit einfließen, ob amerikanische, russische oder chinesische U-Boote Unterseekabel abhören und wie diesem Risiko begegnet werden kann. Und das ist kein Risiko, das plötzlich entsteht, wenn Daten die Außengrenzen des EWR verlassen – das unbefugte Eindringen („hacking") in Kommunikationsnetze kann genauso leicht im EWR wie außerhalb stattfinden.

Wenn die Datenexporteure auf Verschlüsselung der übermittelten Daten bauen, wie es häufig fast schon als Allheilmittel von Fachleuten vorgeschlagen wird, steht ihnen dieser Weg nach dem *EDSA* auch nur temporär offen: „Die Schutzkapazität von kryptografischen Algorithmen unterliegt im Laufe der Zeit einer Abnahme aufgrund der Entdeckung neuer kryptoanalytischer Techniken, dem Aufkommen neuer Rechenparadigmen wie Quantencomputing und der allgemeinen Zunahme der verfügbaren Rechenleistung."[18]

3. Trugschlüsse des EDSA

Ohne hier weiter auf die einzelnen Abhilfemaßnahmen eingehen zu können, verfestigt sich nach der Lektüre der 48-seitigen Empfehlungen der Eindruck, dass der *EDSA* überhaupt kein Interesse daran hat, den Datenexporteuren leicht handhabbare Werkzeuge in die Hand zu geben, um ihre Risikoanalyse zur Abwehr eines erheblichen Haftungsrisikos bei Übermittlungen in Drittstaaten erfolgreich durchzuführen.[19]

Vermutlich werden die Empfehlungen zu diversen von Anwaltskanzleien und Interessenverbänden wie *NOYB* entworfenen Fragebögen führen, mit denen die Datenexporteure den Schwarzen Peter der Risikoanalyse an die Datenimporteure weitergeben.[20] Es wäre besser gewesen, wenn der *EDSA* diese Due-Diligence-Fragebögen selbst entwickelt und über die *EU-Kommission* direkt an die Regierungen der Drittstaaten zur Beantwortung verschickt hätte.[21] So stehen die Datenexporteure mit den Empfehlungen vor dem Nichts.

Zusammenfassend ist der *EDSA* mit seinen Empfehlungen mehreren Trugschlüssen aufgesessen:

- Dass die Datenexporteure und -importeure in der Lage sind, das Risiko des Abhörens und Datenspeicherns durch die nationalen Sicherheitsbehörden im Drittland bei der Datenübermittlung selbst abzuschätzen: Das ist im Nebel der Geheimdiensttätigkeit mit ihren Gerüchten und Halbwahrheiten ein Ding der Unmöglichkeit.
- Dass die Daten von „Unionsbürgern" in der EU sicherer sind als im Ausland: Das stimmt nicht, weil die ausländischen Behörden bei der Auslandsüberwachung meist weniger rechtlichen und praktischen Restriktionen unterliegen als im Inland und bei einer Massenspeicherung auch gar nicht wissen, ob es sich um einen „Unionsbürger" handelt. Außerdem arbeiten die Sicherheitsbehörden in der EU und dem befreundeten Ausland eng zusammen.
- Dass die Risikoanalyse sich zwingend auf alle individuellen Datenübermittlungen zwischen den Parteien beziehen muss: Alle personenbezogenen Daten sind im Prinzip für die Geheimdienste relevant, aber tatsächlich wichtig für die geheimdienstliche Tätigkeit sind nur wenige Daten.

4. Fokus auf geheimdienstrelevante Datensätze

Deshalb ist der Standpunkt gut vertretbar, dass die meisten Datensätze aus der EU nach dem Schrems-II-Urteil ein sehr niedriges Risiko für Datenübermittlungen in Drittstaaten in sich tragen – verglichen mit der Datenverarbeitung innerhalb der EU.

Eine solche enge Auslegung des Schrems-II-Urteils geht in Richtung der Aussage des *EDSA* in Rn. 43.3 der Empfehlungen: „Alternativ können Sie zum Schluss kommen, mit der Übermittlung fortzufahren, ohne zusätzliche Maßnahmen zu ergreifen, wenn Sie der Ansicht sind, dass Sie keinen Grund zu der Annahme haben, dass die einschlägigen und problematischen Rechtsvorschriften in der Praxis auf Ihre übermittelten Daten und/oder den Importeur angewendet werden." So ist es. Die allermeisten US-Datenimporteure sind z.B. nicht direkt von den administrativen Anweisungen des FISA-Abschnitts 702 („national security letters") betroffen und werden nie solche Anweisungen erhalten.

Wenn man das zu Ende denkt, muss der Datenexporteur die Datensätze nach dem Gefährdungspotenzial für eine Datensammlung durch Geheimdienste und Sicherheitsbehörden kategorisieren. Anders kommt man aus dem Dilemma nicht heraus, dass den ausländischen Geheimdiensten, wie von *Schrems* u.a. propagiert, „alles" an Datensammlung zuzutrauen ist, aber der internationale Datenfluss nicht einfach abgestellt werden kann. Vereinfacht ausgedrückt könnte eine solche Einteilung so aussehen: Daten und Kommunikation von Militärs, hochrangigen Politiker*innen und führenden Personen in der Wirtschaft – „ja, geheimdienstrelevant", der Name der deutschen Oma, die ihre Enkel in Dubai besucht – „nein."

Mit dieser Methode, nicht alle Datenflüsse über einen Kamm zu scheren und sich auf die praktisch geheimdienstrelevanten Datensätze zu konzentrieren, könnten die Datenexporteure die

16 *EDPB* (o. Fußn. 12), Rn. 38.
17 *EDPB* (o. Fußn. 12), Rn. 80.
18 *EDPB* (o. Fußn. 12), Fußn. 81; hinzu kommt, dass der Datenimporteur im Drittstaat keinen Schlüssel zu den verschlüsselten Daten bekommen soll: "The keys are retained solely under the control of the data exporter, or by an entity trusted by the exporter in the EEA or under a jurisdiction offering an essentially equivalent level of protection to that guaranteed within the EEA.", Rn. 84 (6). Damit wird die Verschlüsselungstechnik für die Datenempfänger in Drittländern in den meisten Fällen unbrauchbar; s.a. die neue Orientierungshilfe der *DSK* zur E-Mail-Verschlüsselung v. 16.7.2021, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf.
19 Der neueste Gimmick in den Empfehlungen ist der „Warrant Canary" in Rn. 116: „whereby the importer commits to regularly publish (e.g. at least every 24 hours) a cryptographically signed message informing the exporter that as of a certain date and time it has received no order to disclose personal data or the like".
20 Vgl. Rn. 107: „structured questionnaires that the importer would fill in and sign and compounded by the importer's contractual obligation to declare within a set period of time any potential change to this information".
21 Einige der zu erwartenden Antworten findet man auch ohne einen solchen Fragebogen im *NTIA*-White-Paper der *US-Regierung* v. 28.9.2020, vgl. *Spies*, ZD-Aktuell 2020, 07327, zu dem der *EDSA* leider keine Stellung bezogen hat.

meisten Datenübermittlungen von ihrer Risikoanalyse ausschließen. Für geheimdienstrelevante Informationen könnten die Dienstleister ihren Kund*innen besondere Schutzmaßnahmen aus dem Katalog des *EDSA* zur Sicherung des Datenflusses anbieten – nicht aber automatisch für alle Datenströme in den Drittstaat. Die im Anhang 2 vom *EDSA* angebotenen Schutzmaßnahmen werden die Parteien ohnehin gerne von sich aus aufgreifen, weil sie keinerlei Interesse daran haben, dass staatliche und private Hacker oder illegale Datensammler Zugriff auf die übermittelten Daten haben.

Zwar fordert der *EDSA* an mehreren Stellen in den Empfehlungen, dass die Datenexporteure die „laws and practices" analysieren müssen. An anderer Stelle heißt es dann aber, dass es auf „laws and/or practices" ankomme.[22] Im Endergebnis ist die Analyse der Abhör- und Datensammlungspraxis der Behörden im Empfängerstaat für den Schutz der EU-Daten viel wichtiger als die Analyse des ausländischen Überwachungsrechts, das Änderungen unterliegt und so oder so interpretiert werden muss. Dies hat auch der *EuGH* im Schrems-II-Urteil erkannt.[23]

IV. Politischer Auftrag an alle Parteien

Die Nutzung der SCC bei der individuellen Risikoanalyse ist demnach mit vielen Problemen behaftet. I.E. sind die Empfehlungen – man muss es leider so sagen – praktisch nicht mehr als Sand, der durch die Finger rinnt, weil sie die Schwelle des erlaubten Risikos nicht präzise definieren, wie es zwingend für eine effektive Compliance erforderlich wäre. Es ist zu befürchten, dass die Datenschutzbeauftragten in Europa mit den Empfehlungen unterschiedlich umgehen, was die Rechtssicherheit untergräbt.

Was nun? Laut US-Handelsministerin *Raimondi* wollen die USA und die EU KI-Themen im neu gegründeten *Handels- und Technologierat* gemeinsam angehen, um „die Straßenverkehrsregeln" für KI gemeinsam zu schreiben. Die beiden Parteien hätten keine sehr unterschiedlichen Ansichten über Technologie und teilten das Engagement für Datenschutz, Demokratie und Gerechtigkeit.[24]

Dieses spannende Thema darf nicht von der dringend notwendigen Reparatur des Privacy Shield ablenken. Die mit den Empfehlungen bei den Datenexporteuren abgeladenen Probleme lassen sich effektiv nur durch die Politik lösen. Eine allgemeine politische Zusage, dass die US-Bundesbehörden keine EU-Daten en gros anlasslos für Geheimdienstzwecke abspeichern, dürfte *Schrems* und seine Mitstreiter*innen nicht von weiteren Klagen abhalten. Mit konkreten Zusagen könnte die *Biden*-Administration aber schon einiges in Brüssel erwirken, nämlich mit Regierungsanweisungen („Executive Orders"), so wie sie das *New America's Open Technology Institute (OTI)* vorschlägt:[25] Relativ einfach umsetzbar ist z.B. die Einrichtung eines Verfahrens zur Tatsachenermittlung in den Behörden, mittels dessen man Verschlusssachen untersuchen kann und dessen Ergebnisse dann bei einer unabhängigen Instanz angefochten werden könnten.

In diesem Rahmen wären die US-Behörden, die Überwachungen durchführen oder bewerten, verpflichtet, Untersuchungen zur Tatsachenfeststellung in Bezug auf diese Überwachung durchzuführen – entweder durch die Datenschutzbeauftragten der Nachrichtendienste oder möglicherweise durch deren jeweiligen Generalinspektor. Diese Maßnahmen sind einfacher zu treffen als eine derzeit utopische Änderung der US-Gesetze.[26]

Im *US-Kongress* gilt derweil auch angesichts des Wahljahrs 2022, was ein Mitarbeiter in einem Interview mit Politico[27] so treffend auf den Punkt gebracht hat: „We don't win votes by giving the French more rights."

Schnell gelesen ...

- Trotz des guten Willens der Biden-Administation und der EU-Kommission kommen die Verhandlungen zu einem Nachfolge-Abkommen des EU-US-Privacy-Shield nicht vom Fleck.
- Die neuen Standardvertragsklauseln (SCC) der EU-Kommission sind nur mit Mühe und viel Aufwand von den Parteien umsetzbar.
- Die Empfehlungen des EDSA zur Risikoanalyse der Datenübermittlung in Drittstaaten sind nahezu unbrauchbar und gehen an den Anforderungen für den internationalen Datentransfer vorbei.
- Die meisten Datensätze aus der EU tragen nach dem Schrems-II-Urteil nur ein sehr niedriges Risiko für Datenübermittlungen in Drittstaaten in sich – verglichen mit der Datenverarbeitung innerhalb der EU. Die vom EuGH geforderte Risikoanalyse muss sich deshalb auf das Gefährdungspotenzial der Datensätze für eine Datensammlung durch Geheimdienste und Sicherheitsbehörden konzentrieren.

Dr. Axel Spies
ist Rechtsanwalt in der Kanzlei Morgan, Lewis & Bockius in Washington DC und Mitherausgeber der ZD.

22 *EDPB* (o. Fußn. 12), Rn. 30 und 90.

23 Vgl. die zahlreichen Bezugnahmen des *EuGH* auf die „Praxis" im Drittstaat, z.B. in Rn. 148, 158 und gleich zweimal in Rn. 126: „Demnach gibt es zwar Situationen, in denen der Empfänger einer solchen Übermittlung in Anbetracht der Rechtslage und der Praxis im betreffenden Drittland den erforderlichen Datenschutz allein auf der Grundlage der Standarddatenschutzklauseln garantieren kann, aber auch Situationen, in denen die in diesen Klauseln enthaltenen Regelungen möglicherweise kein ausreichendes Mittel darstellen, um in der Praxis den effektiven Schutz der in das betreffende Drittland übermittelten personenbezogenen Daten zu gewährleisten."

24 Comm Daily v. 26.5.2021.

25 Strengthening Surveillance Safeguards After Schrems II, A Roadmap for Reform (7.4.2021), abrufbar unter: https://www.newamerica.org/oti/reports/strengthening-surveillance-safeguards-after-schrems-ii/.

26 Der *Kongress* ist derzeit mit anderen Baustellen im Digitalbereich beschäftigt. Am 11.6.2021 wurden durch 13 Mitglieder des Repräsentantenhauses insgesamt fünf Gesetzentwürfe eingebracht, durch die der Einfluss und die Macht der Big-Tech-Konzerne begrenzt werden sollen. So sollen die der Regulierung unterliegenden Konzerne die eigenen Dienste auf ihrer Plattform nicht bevorzugt anzeigen dürfen (American Choice and Innovation Online Act). Der Platform Competition and Opportunity Act 2021 und der Ending Platform Monopolies Act sollen es Big-Tech-Konzernen verbieten, den Zugang zur Plattform und die Sichtbarkeit auf dieser von der Nutzung bestimmter eigener Zahlungs- und Logistikinfrastrukturen abhängig zu machen; näher *Heet*, MMR-Aktuell 2021, 439805.

27 Politico Digital Bridge v. 18.2.2021, abrufbar unter: https://www.politico.eu/newsletter/digital-bridge/politico-digital-bridge-privacy-shield-microchip-realpolitik-australias-rod-sims/.