Centrum für Europäische Politik
FREIBURG | BERLIN

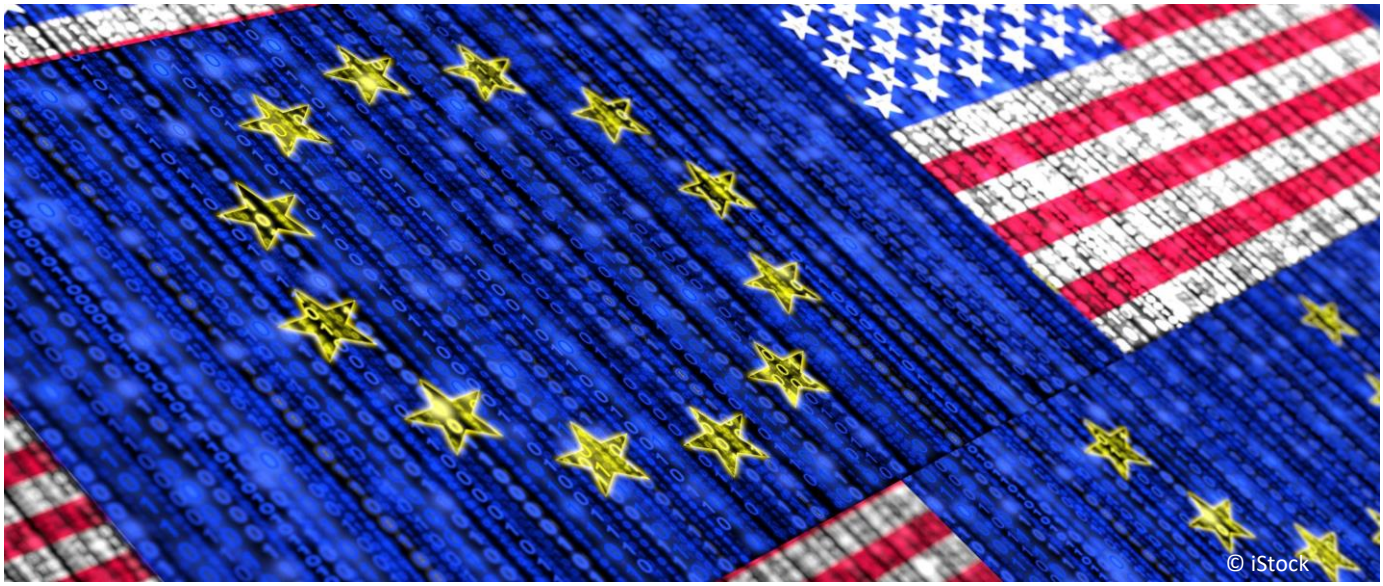
cepStudie

26. Januar 2021

Unzulässigkeit der Datenübermittlung in die USA

Das EuGH-Urteil „Schrems II“ und seine Folgen

Anja Hoffmann



Nach dem „Schrems II“-Urteil des EuGH dürfen Transfers personenbezogener Daten in die USA nicht mehr auf den „Privacy-Shield“-Beschluss gestützt werden, weil die USA keinen ausreichenden Datenschutz bieten. Derzeit werden Datentransfers daher meist auf Standardvertragsklauseln gestützt, deren Nutzung grundsätzlich zulässig bleibt.

Kernthesen

- Auch auf Standardvertragsklauseln und unternehmensinterne Datenschutzregelungen dürfen Datentransfers in die USA nicht gestützt werden, wenn die dortigen Datenempfänger den US-Überwachungsgesetzen unterliegen und Zugriff auf die Dateninhalte im Klartext haben.
- In diesen Fällen können auch ergänzende Datenschutzmaßnahmen Zugriffe der US-Behörden nicht wirksam verhindern.
- Insbesondere Transfers an Cloud-Dienste und Transfers innerhalb von Unternehmensgruppen in die USA sind daher in diesen Fällen rechtswidrig. Der Datenexporteur – oder die Aufsichtsbehörde – muss den Datentransfer stoppen.
- Weder ein reformierter „Privacy Shield“ noch die von der EU-Kommission im November 2020 vorgeschlagenen geänderten Standardvertragsklauseln ändern etwas hieran, solange die USA ihre Überwachungsgesetze nicht auf das nach EU-Recht zulässige Maß begrenzen und EU-Bürgern keine wirksamen Rechtsbehelfe gewähren.
- Das Gleiche gilt für Datentransfers in andere Drittländer, soweit deren Überwachungsgesetze mit dem Datenschutz der EU kollidieren. Dies muss in jedem Einzelfall geprüft werden.

Kernpunkte

Zum „Schrems II“-Urteil des EuGH

- Transfers personenbezogener Daten aus der EU in die USA dürfen nicht länger auf den „Privacy-Shield“-Beschluss der EU-Kommission gestützt werden. Der Europäische Gerichtshof (EuGH) hat diesen Beschluss im „Schrems II“-Urteil zu Recht für ungültig erklärt, weil der „Privacy Shield“ keinen im Vergleich zur EU gleichwertigen Datenschutz bietet.
- Datentransfers in ein Drittland auf der Basis von Standardvertragsklauseln (SDPC) – das sind von der EU-Kommission freigegebene Datenschutz-Musterklauseln, die zwischen Datenexporteur und Datenempfänger vereinbart werden – sind weiterhin grundsätzlich zulässig. Datenexporteur und -empfänger müssen aber prüfen, ob das Recht des Drittlands und die SDPC insgesamt einen dem EU-Niveau im Wesentlichen gleichwertigen Schutz für die Daten gewährleisten, und die Betroffenen, deren Daten übermittelt werden, durchsetzbare Rechte und wirksame Rechtsbehelfe haben.

Zur Umsetzung des „Schrems II“-Urteils

- Der Europäische Datenschutzausschuss (EDSA) hat nach dem Urteil zwei Empfehlungsentwürfe veröffentlicht. Danach sind bei der Prüfung des Schutzniveaus im Drittland alle Umstände des spezifischen Datentransfers – u.a. Kategorien und Format der übermittelten Daten – zu berücksichtigen, nicht aber die subjektive Einschätzung der Wahrscheinlichkeit behördlicher Zugriffe.
- Darüber hinaus müssen sich Datenexporteur und Datenempfänger nach den SDPC vergewissern, ob das Recht im Drittland es dem Datenempfänger erlaubt, die SDPC auch einzuhalten. Problematisch sind insbesondere Datentransfers an Empfänger, denen das Recht des Drittlands Verpflichtungen auferlegt, die den SDPC widersprechen und deren Garantie untergraben.
- Die Pflicht des Datenempfängers, Behörden im Drittland Daten offenzulegen oder Zugriff auf diese zu gewähren, steht laut dem EDSA der Einhaltung der SDPC nicht entgegen, wenn das Drittland bei seinen Überwachungsmaßnahmen die „wesentlichen europäischen Garantien“ einhält.
- Überwachungsmaßnahmen erfüllen die „wesentlichen europäischen Garantien“ des EDSA, wenn sie auf klaren Regeln für die Datenverarbeitung beruhen, die Eingriffe erforderlich und angemessen sind und im Drittland eine unabhängige Aufsicht und wirksame Rechtsbehelfe existieren.
- Halten die Überwachungsmaßnahmen die Garantien nicht ein – was bei den US-Überwachungsgesetzen der Fall ist –, fehlt es an einem im Wesentlichen gleichwertigen Schutzniveau. Die SDPC allein reichen dann nicht aus; vielmehr muss der Datenexporteur zusätzlich ergänzende Datenschutzmaßnahmen vorsehen.
- Es besteht Rechtsunsicherheit, welche zusätzlichen Maßnahmen der Datenexporteur ergreifen muss, um die Schutzlücken zu schließen. Die Aufsichtsbehörden schlagen hierzu technische Maßnahmen wie die Anonymisierung, Verschlüsselung, Pseudonymisierung oder Aufspaltung der Daten, ergänzende Vertragsklauseln und organisatorische Maßnahmen vor.
- Verschärfte Vertragspflichten, z.B. über Datenzugriffe zu informieren oder diese rechtlich anzugreifen, und organisatorische Maßnahmen wie interne Richtlinien erhöhen den Schutz, reichen aber allein nicht aus und müssen durch technische Maßnahmen ergänzt werden. Denn auch verschärfte Vertragspflichten können weder die Behörden im Drittland binden noch effektive Rechtsbehelfe für EU-Bürger schaffen.
- Technische Maßnahmen können unverhältnismäßige behördliche Zugriffe nach Ansicht des EDSA allenfalls dann wirksam verhindern, wenn selbst der Datenempfänger nicht fähig ist, die Daten zu entschlüsseln, zu de-pseudonymisieren oder zu rekonstruieren. Dies kommt nur in wenigen Fällen in Betracht, etwa wenn Daten allein zu Sicherungszwecken im Drittland gespeichert werden.

- Hat oder benötigt der Datenempfänger zur Verarbeitung Zugriff auf den Klartext der Daten, schützen auch technische Maßnahmen nicht effektiv vor behördlicher Überwachung. Ist der Empfänger im Besitz des Schlüssels, könnte er verpflichtet sein, diesen an die Behörden herauszugeben. Auch aktuell diskutierte „Hintertüren“ in Verschlüsselungssoftware würden den Schutz vereiteln.
- Kann der Datenexporteur durch zusätzliche Maßnahmen keinen dem EU-Niveau gleichwertigen Datenschutz gewährleisten, muss er – oder in zweiter Linie die Aufsichtsbehörde – die Datenübermittlung stoppen. Bei Transfers in die USA sind aber gar keine Maßnahmen ersichtlich, die behördliche Zugriffe auf Basis der dortigen Überwachungsgesetze wirksam verhindern könnten, soweit dem Datenempfänger der Zugriff auf die Daten nicht versperrt ist.
- Auch die von der Kommission im November 2020 vorgeschlagenen geänderten SDPC können aus den genannten Gründen nur zusammen mit technischen Maßnahmen einen gleichwertigen Datenschutz bieten. Um zusätzliche Unklarheiten zu vermeiden, sollten die neuen SDPC genauer mit den Empfehlungen des EDSA abgestimmt werden.

Schlussfolgerungen für Transfers personenbezogener Daten in die USA

- Alle Datentransfers in die USA an Empfänger, die den US-Überwachungsgesetzen unterliegen und die Zugriff auf die Dateninhalte im Klartext haben, sind daher derzeit unzulässig. Betroffen sind u.a. Transfers an Anbieter von Cloud-Diensten und Transfers innerhalb von Unternehmensgruppen zur Erbringung von Personaldienstleistungen.
- Die EU-Datenschutzaufsichtsbehörden sollten Hilfestellung bei der Auslegung geben, welche Datenempfänger unter die US-Überwachungsgesetze fallen und welche Transfers daher kritisch sind.
- Solange die USA ihre Überwachungsgesetze nicht auf das nötige Maß begrenzen und EU-Bürgern keine wirksamen Rechtsbehelfe gewähren, helfen weder ergänzte SDPC noch ein neuer, „verbesserter“ „Privacy Shield“.

Konsequenzen für andere Transferinstrumente und Datentransfers in andere Drittländer

- Die Ausführungen des EuGH zu den SDPC sind auf andere Transferinstrumente wie verbindliche unternehmensinterne Datenschutzregelungen (BCR) übertragbar. Deren Nutzung birgt daher bei Datentransfers in die USA vergleichbare Risiken, wenn die Empfänger dortigen Überwachungsgesetzen unterliegen.
- Überwachungsgesetze, die mit den SDPC kollidieren, können auch in anderen Drittländern bestehen. Datenexporteure müssen daher auch bei Datentransfers in andere Länder, für die kein Angemessenheitsbeschluss besteht, das Schutzniveau prüfen und die SDPC ggf. ergänzen. Datentransfers in das Vereinigte Königreich bleiben zumindest vorläufig zulässig.
- Die EU-Kommission muss bestehende Angemessenheitsbeschlüsse für andere Drittländer kritisch daraufhin überprüfen, ob sie die vom EuGH aufgestellten Anforderungen (noch) erfüllen.

Fazit

- Die rechtssicherste Lösung ist, von den beschriebenen Datentransfers in Drittländer abzusehen, die Daten so in der EU zu speichern, dass US-Unternehmen oder ihre Tochtergesellschaften keine Kontrolle darüber haben, und ausschließlich entsprechende europäische Provider zu nutzen.
- Die hohen Anforderungen an den Datenschutz in der EU und die derzeitige Transferpraxis fallen auseinander. Datenexporteure, die rechtswidrige Datentransfers nicht einstellen, riskieren hohe Bußgelder. Auch die Entwürfe der Empfehlungen des EDSA und der geänderten SDPC der EU-Kommission versprechen allenfalls für eine begrenzte Zahl der Fälle eine rechtssichere und zugleich praxistaugliche Lösung des Dilemmas.
- Das „Schrems II“-Urteil bietet die Chance, hochwertige und sichere Dienste (z.B. Clouds) in der EU zu stärken. Nur dann ist der Wechsel zu EU-Dienstleistern langfristig eine Alternative. Die Schaffung von Gaia-X als erster europäischer Cloud kann ein richtiger Schritt in diese Richtung werden.

Inhaltsverzeichnis

Einleitung

Die Übermittlung personenbezogener Daten aus der EU an in den USA niedergelassene Unternehmen gehört für viele europäische Unternehmen zum Geschäftsalltag. Die EU-Datenschutzgrundverordnung[1] (DSGVO) erlaubt derartige Übermittlungen in Drittländer allerdings nur unter bestimmten Voraussetzungen. Der Europäische Gerichtshof (EuGH) hat in seinem „Schrems II"-Urteil[2] im Juli 2020 erneut schonungslos aufgezeigt, dass die Hürden für rechtmäßige Datentransfers in Drittländer hoch gesetzt sind. Nach einer kurzen Einführung in die allgemeinen Voraussetzungen für die internationale Datenübermittlung in Kapitel 1 analysiert die vorliegende cep**Studie** in Kapitel 2 dieses Urteil und dessen Auswirkungen. Im Anschluss hieran widmet sich ein separates Kapitel 3 der Frage, wie die Anforderungen des Schrems II-Urteil umzusetzen sind, und beleuchtet dabei auch die Entwurfsfassungen der Empfehlungen des Europäischen Datenschutzausschusses und der neuen Standarddatenschutzklauseln der EU-Kommission (nachfolgend: Kommission). In Kapitel 4 werden sodann weitere aktuelle Entwicklungen nach Erlass des Urteils dargestellt und gewürdigt, ein Fazit gezogen und ein kurzer Ausblick vorgenommen. Kapitel 5 fasst schließlich die wesentlichen Ergebnisse zusammen.

1 Welche Voraussetzungen gelten für Datenübermittlungen in Drittländer?

Wer personenbezogene Daten (nachfolgend: „Daten")[3] für wirtschaftliche Zwecke in ein Drittland außerhalb der EU oder an eine internationale Organisation[4] übermittelt (nachfolgend als „Datenexporteur" bezeichnet), muss – zusätzlich zu den Regeln, die für Datenverarbeitungen innerhalb der EU gelten – die in der DSGVO geregelten Bestimmungen über die Datenübermittlung in Drittländer einhalten.[5] Unter einem Drittland ist dabei jedes Land außerhalb des Europäischen Wirtschaftsraum zu verstehen.[6] Der Empfänger der Daten im Drittland wird nachfolgend als „Datenempfänger" bezeichnet. Sowohl Datenexporteure als auch Datenempfänger können dabei entweder Stellen sein, die nach der DSGVO für die Verarbeitung der Daten verantwortlich sind (Verantwortliche)[7] oder Stellen, die Daten in deren Auftrag verarbeiten (Auftragsverarbeiter)[8].

Datenübermittlungen in Drittländer sind nach der DSGVO grundsätzlich verboten, sofern sie nicht durch eine Rechtsgrundlage im EU-Recht erlaubt werden. Die DSGVO selbst sieht dafür verschiedene Rechtsgrundlagen vor, darunter Angemessenheitsbeschlüsse (Kapitel 1.1), „geeignete Garantien", die insbesondere in Standarddatenschutzklauseln bestehen können (Kapitel 1.2), und Ausnahmeregeln für bestimmte Fälle von Datentransfers (Kapitel 1.3).

---

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

2 EuGH, Rs. C-311/18 (Data Protection Officer/Facebook Ireland Ltd und Maximilian Schrems, Urteil vom 16. Juli 2020, ECLI:EU:C:2020:559, nachfolgend abgekürzt als „Schrems II"-Urteil bezeichnet.

3 Nachfolgend wird statt „personenbezogene Daten" vereinfacht der Begriff „Daten" verwendet. Wenn nachfolgend von „Daten" gesprochen wird, sind damit personenbezogene Daten i.S.v. Art. 4 Nr. 1 DSGVO gemeint.

4 Nachfolgend wird statt „Drittland oder internationale Organisation" vereinfacht der Begriff „Drittland" verwendet. Wenn von „Drittland" gesprochen wird, ist damit zugleich auch die Übermittlung an eine internationale Organisation gemeint.

5 Art. 44 – 50 DSGVO. Hierdurch soll sichergestellt werden, dass das Schutzniveau der DSGVO auch dann nicht unterschritten wird, wenn Daten aus der EU heraus in Drittländer übermittelt werden.

6 Der EWR umfasst neben allen EU-Mitgliedsstaaten auch die Staaten Island, Liechtenstein und Norwegen der Europäischen Freihandelsassoziation (EFTA). Die DSGVO gilt aufgrund des Abkommens über den EWR (vgl. u.a. Annex XI und Protokoll 37) auch für diese drei Staaten. Siehe dazu auch Europäischer Datenschutzausschuss, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data vom 10.November 2020, S. 20.

7 Art. 4 Nr. 7 DSGVO.

8 Art. 4 Nr. 8 DSGVO.

1.1 Angemessenheitsbeschlüsse und „Privacy Shield“

Ohne besondere Genehmigung dürfen Daten u.a. dann in ein Drittland übermittelt werden, wenn die EU-Kommission (nachfolgend: „Kommission“) im Wege eines Angemessenheitsbeschlusses festgestellt hat, dass das Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen ein „angemessenes Datenschutzniveau“ zum Schutz der Privatsphäre sowie der Freiheiten und Grundrechte von Personen garantiert.[9] Vergleichsmaßstab ist das Schutzniveau der DSGVO, die wiederum im Lichte der in der Charta der Grundrechte der EU (nachfolgend „GRCh“) verbürgten Grundrechte auszulegen ist. Um „angemessen“ zu sein, muss das Schutzniveau im Drittland mit dem in der EU garantierten Niveau zwar nicht identisch, ihm aber „der Sache nach gleichwertig“ sein.[10] Bei der Prüfung, ob ein Drittland ein angemessenes Schutzniveau bietet, muss die Kommission vor allem berücksichtigen, ob das Drittland nach seinen innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen

- Rechtsstaatlichkeit gewährleistet und Menschenrechte und Grundfreiheiten achtet,
- Betroffenen durchsetzbare Rechte und wirksame Rechtsbehelfe gewährt und
- mittels unabhängiger Aufsichtsbehörden die Einhaltung der Datenschutzvorschriften sichert.[11]

Die Kommission hat bislang Angemessenheitsbeschlüsse für zahlreiche Länder erlassen.[12] Für die USA hatte sie mit dem „Privacy-Shield“-Beschluss[13] – ebenso wie bei dessen Vorgänger, der „Safe Harbour“-Entscheidung[14] – einen „besonderen“, weil auf bestimmte Empfänger begrenzten Angemessenheitsbeschluss gefasst. Dieser Beschluss regelte Datenschutzbestimmungen für Datentransfers aus der EU in die USA, die zuvor zwischen der EU und den USA ausgehandelt worden waren und wie ein Schutzschild („Privacy Shield“) fungieren sollten. In dem Beschluss hatte die Kommission festgestellt, dass die USA insoweit ein angemessenes Datenschutzniveau gewährleisteten, als die Daten an bestimmte dort niedergelassene Unternehmen und sonstige Stellen[15] übermittelt wurden, die zuvor in einem Selbstzertifizierungsverfahren erklärt hatten, die Grundsätze des „Privacy Shield“[16] zu beachten. Daten durften damit unter den Voraussetzungen dieses Beschlusses an derart selbstzertifizierte Unternehmen – zuletzt mehr als 5.200 US-Unternehmen[17] – übermittelt werden. Zahlreiche EU-Unternehmen stützten ihre Datentransfers an US-Unternehmen auf diese Rechtsgrundlage.

1.2 Standarddatenschutzklauseln und andere „geeignete Garantien“

In ein Drittland, für das kein gültiger Angemessenheitsbeschluss der Kommission besteht, der diesem Land ein angemessenes Datenschutzniveau bescheinigt, dürfen Daten u.a. dann übermittelt werden,

---

9 Art. 45 Abs. 1 DSGVO.

10 EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 94.

11 Art. 45 Abs. 2 DSGVO.

12 Eine Übersicht der bislang erlassenen Angemessenheitsentscheidungen der Kommission findet sich unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

13 Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46 über die Angemessenheit des vom EU-US Datenschutzschild gebotenen Schutzes (ABl. L 207 vom 01.08.2016, S. 1ff.). „Privacy Shield“ ist der englische Name für den in diesem Beschluss geregelten EU-US Datenschutzschild.

14 Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „Sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA), ABl. L 215 vom 25.08.2000, S. 7-47.

15 Nachfolgend wird vereinfacht nur von „Unternehmen“ gesprochen.

16 Im Fall der „Safe Harbour“-Entscheidung waren entsprechend die sog. „Safe Harbour-Grundsätze“ zu beachten.

17 Eine Liste der zuletzt unter dem „Privacy Shield“ registrierten US-Unternehmen ist abrufbar unter https://www.privacyshield.gov/list.

wenn der EU-Datenexporteur selbst „geeignete Garantien“ vorsieht, die das möglicherweise unzulängliche Schutzniveau in dem Drittstaat kompensieren.[18] Solche Garantien können sich unter anderem aus vertraglichen Vereinbarungen zwischen Datenexporteur und Datenimporteur – z.B. sogenannten Standarddatenschutzklauseln („Standard Data Protection Clauses“, auch als Standardvertragsklauseln bezeichnet, nachfolgend „SDPC“) – ergeben.[19] SDPC sind harmonisierte Musterverträge, die von der Kommission erlassen[20] oder genehmigt[21] und EU-weit zur Nutzung freigegeben werden. In ihnen werden sowohl dem EU-Datenexporteur als auch dem Datenimporteur im Drittland entsprechende Datenschutzpflichten auferlegt. Beide Parteien verpflichten sich damit vertraglich, auch im Drittland für die Einhaltung des EU-Schutzniveaus bezüglich der übermittelten Daten zu sorgen. Die Nutzung von SDPC ist nicht auf bestimmte Drittländer beschränkt. Die Kommission hat bislang in zwei Entscheidungen[22] und einem Beschluss (nachfolgend: „SDPC-Beschluss“)[23] insgesamt drei verschiedene Versionen von SDPC anerkannt. Zwei davon betreffen Übermittlungen durch einen für die Datenverarbeitung Verantwortlichen an einen anderen Verantwortlichen im Drittland. Hierfür stehen mit den „Standardverträgen I und II“ zwei alternative Klauselsätze zur Verfügung, zwischen denen die Vertragspartner wählen können.[24] Der dritte Klauselsatz betrifft Übermittlungen durch einen Verantwortlichen an einen Auftragsverarbeiter im Drittland (nachfolgend: „Standardvertrag Auftragsverarbeiter“).[25] Nach Art. 1 der jeweiligen Kommissionsentscheidung gelten die SDPC als angemessene Garantien für die Datenübermittlung.[26] Wird der jeweilige Klauselsatz unverändert in einen Vertrag zwischen EU-Datenexporteur und Datenimporteur im Drittland integriert, bedürfen Datentransfers auf Basis dieses Vertrags keiner weiteren Genehmigung.

SDPC werden in der Praxis von einer großen Anzahl von Unternehmen verwendet, um ihre Datenübermittlungen in Drittländer zu legitimieren. Auch für Datentransfers in die USA gehörten sie schon bislang – neben dem „Privacy Shield“ – zu den wichtigsten Transferinstrumenten. Laut einer repräsentativen Umfrage im Auftrag des Digitalverbands Bitcom setzten 2017 79% der Unternehmen, die Daten mit den USA austauschen, auf Standardvertragsklauseln als Rechtsgrundlage, 13% nutzten den „Privacy Shield“.[27]

---

18 Art. 46 Abs. 1 DSGVO.

19 Art. 46 Abs. 2 lit. c) und d) DSGVO. Die hier als „Standarddatenschutzklauseln“ (SDPC) bezeichneten Klauseln waren bislang auch unter dem Namen „Standardvertragsklauseln bzw. „Standard Contractual Clauses“ (SCC) bekannt. Der hier verwendete Begriff knüpft an die Terminologie in der DSGVO an.

20 Art. 46 Abs. 2 lit. c) DSGVO.

21 Art. 46 Abs. 2 lit. d) DSGVO.

22 Vgl. Entscheidung 2001/497/EG der Kommission vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG (ABl. L 181 vom 04.07.2001, S. 19ff.) geändert durch die Entscheidung 2004/915/EG der Kommission vom 27.12.2004 (ABl. L 385 vom 29.12.2004, S. 74ff). Diese Entscheidung wurden durch den Durchführungsbeschluss (EU) 2016/2297 der Kommission vom 16. September 2016 (ABl. L 344 vom 17.12.2016, S. 100 ff.) erneut geändert. Vgl. auch https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

23 Beschluss 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (ABl. L 39 vom 12.02.2010, S. 5 ff.), ebenfalls geändert durch den Durchführungsbeschluss (EU) 2016/2297 der Kommission vom 16. September 2016 (ABl. L 344 vom 17.12.2016, S. 100 ff.).

24 „Standardvertrag I“ ist im Anhang zu Entscheidung 2001/497/EG enthalten. „Standardvertrag II“ findet sich im Anhang zur Entscheidung 2004/915/EG. Er wurde durch diese Änderungsentscheidung eingeführt und als alternativer Klauselsatz in die Entscheidung 2001/497/EG aufgenommen. Details s. Fn. 22).

25 Anhang zu Beschluss 2010/87/EU, a.a.O. (Fn. 22).

26 Gemäß Art. 46 Abs. 5 S. 2 i.V.m. Art. 94 Abs. 2 DSGVO bleiben die unter der früheren Datenschutzrichtlinie 95/46/EU anerkannten SDPC auch unter der DSGVO weiterhin gültig, bis sie von der Kommission ersetzt oder aufgehoben werden.

27 https://www.bitkom.org/Presse/Presseinformation/Neue-Rechtsunsicherheit-fuer-internationalen-Datenaustausch.html

Alternativ zu SDPC können nach der DSGVO u.a. auch verbindliche unternehmensinterne Datenschutzregelungen [„Binding Corporate Rules“ (BCR)[28]], genehmigte Verhaltensregeln[29] oder Zertifizierungen[30] oder einzeln ausgehandelte und von einer Aufsichtsbehörde genehmigte Vertragsklauseln[31] „geeignete Garantien“ bieten.

1.3 Zulässige Datenübermittlungen in bestimmten „Ausnahmefällen“

Auch wenn keine geeigneten Garantien vorliegen, sind gemäß Art. 49 DSGVO Datenübermittlungen unter bestimmten Voraussetzungen durch einen Ausnahmetatbestand gerechtfertigt und damit ohne gesonderte Genehmigung zulässig. Dies ist beispielsweise der Fall, wenn und soweit der Betroffene in die Datenübermittlung ausdrücklich eingewilligt hat[32] oder wenn die Übermittlung für die Erfüllung eines Vertrags zwischen dem Verantwortlichen und dem Betroffenen[33] oder zwischen dem Verantwortlichen und einem Dritten im Interesse des Betroffenen[34] erforderlich ist. Hiernach können beispielsweise Datentransfers zur Buchung eines Fluges oder Hotelzimmers in den USA oder zur Ausführung von Überweisungen gerechtfertigt sein. Zulässig sind auch Datenübermittlungen, die zur Wahrung wichtiger Interessen oder zur gerichtlichen Geltendmachung von Ansprüchen erforderlich sind.[35] Die Ausnahmen vermögen jedoch nur die Übermittlung spezifischer Informationen zu rechtfertigen oder sind – wie Übermittlungen aufgrund eines Vertrags – auf „gelegentliche“ Übermittlungen beschränkt.[36] Solche Übermittlungen sind auch nicht schon deshalb erforderlich, weil ein Konzern aus geschäftlichen Gründen seine Personalabteilung in einem Drittland zentralisiert hat.[37] Auch die Anforderungen an eine wirksame Einwilligung sind hoch, zudem sind Einwilligungen jederzeit widerrufbar.[38] Die Masse der in der Praxis alltäglich erfolgenden Datentransfers – z.B. von Beschäftigtendaten oder Übermittlung von Daten zu Marketingzwecken oder beim Outsourcing von Dienstleistungen an Anbieter in den USA – lässt sich durch die Ausnahmen des Art. 49 DSGVO daher i.d.R. nicht rechtfertigen.

---

[28] Art. 46 Abs. 2 lit. b), Art. 47 DSGVO. Näher zu BCR siehe bereits Hoffmann, A. (2016), cepStudie „Privacy Shield“: Kein ausreichender Datenschutz im unsicheren Hafen USA, S. 17f.

[29] Art. 46 Abs. 2 lit. e) DSGVO.

[30] Art. 46 Abs. 2 lit. f) DSGVO.

[31] Art. 46 Abs. 3 lit. a) DSGVO.

[32] Art. 49 Abs. 1 lit. a) DSGVO. An das Vorliegen einer wirksamen ausdrücklichen Einwilligung stellt die DSGVO allerdings hohe Anforderungen (vgl. Art. 7 DSGVO).

[33] Art. 49 Abs. 1 lit. b) DSGVO („Anbahnung oder Erfüllung“ eines Vertrags zwischen Verantwortlichem und Betroffenem).

[34] Art. 49 Abs. 1 lit. c) DSGVO („Abschluss oder zur Erfüllung eines Vertrags zwischen dem Verantwortlichen und einem Dritten im Interesse des Betroffenen)“.

[35] Art. 49 Abs. 1 lit. d), e) und f) DSGVO.

[36] EDSA, Leitlinien 2/2018 vom 25. Mai 2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, S. 5, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-22018-derogations-article-49-under-regulation_de, ders., Recommendations 01/2020 (Fn. 6), Rn. 25.

[37] In diesem Fall fehlt es an einem unmittelbaren und objektiven Zusammenhang zwischen der Erfüllung des Arbeitsvertrags und der Übermittlung ins Drittland, vgl. EDSA, Leitlinien 2/2018 (Fn. 36), S. 10.

[38] Vgl. etwa EDSA, Leitinien 2/2018 (Fn. 36), S. 7, m.w.N.; näher zu diesen Anforderungen EDSA, Guidelines 05/2020 of 4 May 2020 on Consent unter Regulation 2016/679, S. 4ff., abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.

2 Datentransfers in die USA – das „Schrems II“-Urteil des EuGH

Große Bedeutung für den transatlantischen Datentransfer hat ein Rechtsstreit zwischen dem sozialen Netzwerk Facebook und dessen Nutzer Maximilian Schrems erlangt. Im Rahmen dieses Rechtsstreits hat der EuGH im Juli 2020 den „Privacy Shield“-Beschluss – wie zuvor bereits dessen Rechtsvorgänger, die „Safe Harbour“-Entscheidung[39] – für ungültig erklärt. Dagegen hat der EuGH die SDPC im selben Urteil für gültig erachtet. Das Urteil betrifft alle öffentlichen Stellen und Unternehmen[40], die Daten über den „Privacy Shield“ oder über alternative Garantien wie SDPC in die USA transferieren[41], hat aber auch Auswirkungen darüber hinaus. Nach einem kurzen Überblick über den Fall Schrems in Kapitel 2.1 wird in Kapitel 2.2 zunächst die Ungültigerklärung des „Privacy Shield“ näher erörtert. Kapitel 2.3 widmet sich dann der Frage, was der EuGH zu den SDPC entschieden hat. Abschließend werden in den Kapiteln 2.4 und 2.5 die Auswirkungen des Urteils auf BCR und andere Transferinstrumente sowie auf Datentransfers in andere Drittländer untersucht.

2.1 Der Fall Schrems gegen Facebook

Der Österreicher Maximilian Schrems wandte sich 2013 gegen die Praxis der Facebook Irland Ltd. (nachfolgend „Facebook“)[42], seine Daten in die USA zu übermitteln, um sie dort durch ihre Muttergesellschaft Facebook Inc. verarbeiten zu lassen. Er legte bei der irischen Datenschutzaufsichtsbehörde Beschwerde ein und forderte diese auf, die Übermittlung seiner personenbezogenen Daten in die USA zu stoppen, weil diese dort nicht ausreichend vor den Überwachungstätigkeiten der US-Behörden wie der National Security Agency (NSA) oder des Federal Bureau of Investigation (FBI) geschützt seien. Die Behörde lehnte ein Eingreifen mit der Begründung ab, dass die USA laut der „Safe Harbour“-Entscheidung der EU-Kommission ein angemessenes Schutzniveau gewährleisteten. Das Verfahren ging bis zum EuGH, der im Oktober 2015 im Urteil „Schrems I[43]“ die „Safe Harbour“-Entscheidung für ungültig erklärte.[44] Als Ersatz für diese Entscheidung erließ die Kommission 2016 den „Privacy-Shield“-Beschluss.[45]

Das Beschwerdeverfahren wurde fortgesetzt. Nachdem Facebook erklärt hatte, dass es die Datenübermittlung nunmehr in großen Teilen auf SDPC stütze, argumentierte Schrems, dass seine Daten in den USA auch unter den SDPC unzureichend geschützt seien, insbesondere gegen die dortige Massenüberwachung durch US-Geheimdienste. Die irische Behörde traf allerdings noch immer keine Entscheidung, sondern strengte gegen Schrems und Facebook ein Verfahren vor dem irischen High Court an, weil sie

---

[39] Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „Sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA), ABl. L 215 vom 25.08.2000, S. 7-47.

[40] Nachfolgend wird vereinfacht nur von „Unternehmen“ gesprochen.

[41] Orientierungshilfe des Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) Baden-Württemberg, Stand: 7. September 2020 (2. Auflage), S. 5f., abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/08/Orientierungshilfe-Was-jetzt-in-Sachen-internationaler-Datentransfer.pdf.

[42] Facebook Ireland Ltd. Ist die Vertragspartnerin aller in der EU wohnhaften Facebook-Nutzer.

[43] EuGH, Rs. C-362/14 (Maximilian Schrems/Data Protection Commissioner, Urteil vom 6. Oktober 2015, ECLI:EU:C:2015:650, nachfolgend abgekürzt als „Schrems I“-Urteil bezeichnet.

[44] Näher zu diesem Urteil u. der Ungültigkeit der „Safe Harbour“-Entscheidung s. cepStudie „Privacy Shield“ (Fn. 28), S. 9ff.

[45] Durchführungsbeschluss (EU) 2016/1250 der Kommission (Fn. 13). EU-Datenexporteure durften gemäß diesem Beschluss personenbezogene Daten aus der EU zu kommerziellen Zwecken an US-Unternehmen zum Zwecke der Weiterverarbeitung übermitteln, die sich im Wege der Selbstzertifizierung freiwillig an die Grundsätze des "Privacy Shield" banden. Denn die Kommission attestierte mit ihrem Beschluss in rechtlicher Hinsicht, dass diese Daten dann im Wesentlichen in den USA gleichwertig wie in der EU geschützt sind. Siehe dazu oben Kapitel 1.1.

generelle Zweifel an der Gültigkeit der SDPC hegte. Der High Court legte die Sache erneut dem EuGH zur Vorabentscheidung vor, um die Gültigkeit der SDPC überprüfen zu lassen.[46]

Obwohl Facebook seine Datenübermittlung nicht auf den „Privacy-Shield"-Beschluss gestützt hatte[47], stand indirekt auch dessen Gültigkeit auf dem Prüfstand. Denn zwei der gestellten Vorlagefragen zielten darauf ab, ob die Behörden und Gerichte an die Feststellung eines angemessenen Schutzniveaus in diesem Beschluss gebunden seien und ob der für den „Privacy Shield" geschaffene Ombudsperson-Rechtsbehelf[48] EU-Bürgern hinreichenden Rechtsschutz ermögliche.[49]

2.2 Rechtswidrigkeit des „Privacy Shield"-Beschlusses

Der EuGH hat nach der „Safe Harbour"-Entscheidung auch den „Privacy Shield"-Beschluss für mit dem EU-Datenschutzrecht unvereinbar und damit für ungültig erklärt.[50] Im Folgenden wird die Begründung des EuGH für die Ungültigkeit dargestellt (Kapitel 2.2.1) und bewertet (Kapitel 2.2.2).

2.2.1 Inhaltliche Begründung der Ungültigerklärung

Der EuGH begründet die Ungültigerklärung des „Privacy Shield"-Beschlusses damit, dass das Schutzniveau, das die USA im Rahmen des „Privacy Shield" für die übermittelten Daten gewährleisten, entgegen der Feststellung der Kommission nicht dem Niveau „der Sache nach" gleichwertig sei, das die DSGVO im Lichte der GRCh garantiere.[51] Die deutsche Übersetzung der vom EuGH in den beiden Schrems-Urteilen verwendeten Formulierung „der Sache nach gleichwertig" ist unglücklich gewählt. Im Hinblick auf die englischen[52] und französischen[53] Urteilsfassungen erscheint es passender, diese Formulierung mit „im Wesentlichen gleichwertig" zu übersetzen. Der EuGH will damit ausdrücken, dass ein „angemessenes" Schutzniveau im Drittland – dessen Feststellung notwendige Voraussetzung für den Erlass eines Angemessenheitsbeschlusses ist – zwar keinen identischen Schutz voraussetzt, der Schutz im Drittland dem in der EU gewährleisteten Schutz aber im Kern entsprechen muss. Nachfolgend wird daher statt „der Sache nach gleichwertig" die Formulierung „im Wesentlichen gleichwertig" verwendet.

Der EuGH hält die DSGVO für anwendbar, da es sich um Datentransfers zwischen privaten Wirtschaftsteilnehmern handle. Dass Behörden des Drittlandes ggf. zu Zwecken der nationalen oder öffentlichen Sicherheit auf die Daten zugreifen könnten, führe nicht dazu, dass Datentransfers dem Anwendungsbereich der DSGVO entzogen wären.[54] Inhaltlich stützt sich der EuGH im Kern auf die beiden folgenden Argumente:

---

46 Näher zum Sachverhalt EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 50-67.

47 Generalanwalt Saugmandsgaard Øe, Rs. C-311/18 (Data Protection Officer/Facebook Ireland Ltd und Maximilian Schrems), Schlussanträge vom 19. Dezember 2019, ECLI:EU:C:2019:1145, Rn. 185.

48 Die Ombudsperson sollte Anfragen und Beschwerden von EU-Bürgern wegen möglicher Datenzugriffe durch US-Nachrichtendienste prüfen und beantworten, die über eine zentrale EU-Stelle bei der Ombudsperson eingereicht wurden. In ihrer Antwort sollte die Ombudsperson dann entweder erklären, dass das US-Recht eingehalten wurde oder – falls dies nicht der Fall war – die Nichteinhaltung abgestellt wurde, vgl. dazu Anhang III Anlage A Ziffer 3 des „Privacy Shield"-Beschlusses (Fn. 13).

49 Zu den Vorlagefragen im Einzelnen siehe EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 68 sowie cepAktuell vom 17.04.2018. Zur mündlichen Verhandlung siehe cepAktuell vom 10.07.2019.

50 EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 201.

51 EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 185, 197, 198.

52 Englische Formulierung: „essentially equivalent level of protection".

53 Französische Formulierung: un niveau adéquat de protection essentiellement équivalent".

54 EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 80-89. Der EuGH stellt damit klar, dass Datentransfers zwischen privaten Wirtschaftsteilnehmern zu gewerblichen Zwecken in den Anwendungsbereich der DSGVO fallen. Es handle sich nicht um spezifische Tätigkeiten des Staates. Daran ändere es auch nichts, dass die Behörden des Drittlandes u.a. zu Zwecken der

- Die Zugriffsmöglichkeiten durch die US-Behörden greifen in unverhältnismäßiger Weise in die Grundrechte der Betroffenen nach Art. 7 und 8 GRCh ein, deren personenbezogene Daten in die USA übermittelt werden.[55]
- EU-Bürger haben bei Überwachungsmaßnahmen in den USA keinen hinreichenden Rechtsschutz, um Zugang zu ihren Daten oder deren Berichtigung oder Löschung zu erwirken.[56]

2.2.1.1 Unvereinbarkeit der Zugriffsrechte der US-Behörden mit der EU-Grundrechtecharta

Der EuGH führte aus: Bei der Beurteilung des Schutzniveaus in einem Drittland müsse die Kommission insbesondere prüfen, ob für Betroffene, deren Daten übermittelt werden, im Drittland die Rechte auf Achtung des Privatlebens nach Art. 7 GRCh sowie auf Datenschutz nach Art. 8 GRCh gewährleistet seien.[57] Die Speicherung und der Zugang zu personenbezogenen Daten durch eine Behörde stellten Eingriffe in die in Art. 7 und 8 GRCh verankerten Grundrechte auf Achtung des Privatlebens und auf Datenschutz dar.[58] Zwar enthalte der „Privacy Shield"-Beschluss umfangreiche Datenschutzgrundsätze und US-amerikanische Zusicherungen. Diese würden aber schon im Beschluss selbst wieder beschränkt, weil die Datenempfänger aufgrund von Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen ggf. verpflichtet seien, die Grundsätze nicht anzuwenden.[59] Vielmehr müssten sie den US-Behörden im Rahmen der US-Überwachungsprogramme Zugriff auf die übermittelten personenbezogenen Daten gewähren. Dies könne etwa auf Basis der auf Section 702 des Foreign Intelligence Surveillance Act (FISA)[60] gestützten Überwachungsprogramme PRISM[61] und UPSTREAM[62] oder auf der Grundlage der Executive Order 12333[63] (nachfolgend „E.O. 12333") geschehen. Zwar seien auch im EU-Recht unter den in Art. 51 Abs. 1 GRCh[64] geregelten Voraussetzungen Grundrechtseinschränkungen möglich. Die fraglichen US-Überwachungsprogramme

nationalen oder öffentlichen Sicherheit auf die Daten zugreifen könnten. Die Ausnahmen vom Anwendungsbereich der DSGVO (hier: Art. 2 Abs. 2 lit, a, b und d) seien eng auszulegen. Zudem ergebe sich aus Art. 45 Abs. 2 lit. a DSGVO, dass die Kommission beim Erlass eines Angemessenheitsbeschlusses auch die Rechtsvorschriften des Drittlands in Bezug auf die öffentliche und nationale Sicherheit und den behördlichen Datenzugriff prüfen müsse. Datentransfers könnten daher nicht schon wegen der Existenz solcher Zugriffsmöglichkeiten dem Anwendungsbereich der DSGVO entzogen sein.

55 EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 169-185. Näher dazu unten Kapitel 2.2.1.1.

56 EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 139. Näher dazu unten Kapitel 2.2.1.2.

57 EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 169.

58 EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 171 m.w.N.

59 EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 164.

60 US-Gesetz zur Überwachung in der Auslandsaufklärung. Nach den Feststellungen des vorlegenden Gerichts können US-Behörden nach Section 702 FISA die Überwachung nichtamerikanischer Staatsbürger genehmigen, die sich außerhalb der USA aufhalten („Nicht-US-Person"). Die Vorschrift diene als Grundlage für die US-Überwachungsprogramme PRISM und UPSTREAM, vgl. EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 61.

61 Im Rahmen des PRISM-Programms sind Anbieter von Internetdiensten laut den Feststellungen des vorlegenden Gerichts verpflichtet, der NSA die gesamte Kommunikation vorzulegen, die von einem „Selektor" versandt oder empfangen wurde, diese werde von der NSA z.T. an andere Behörden weitergeleitet, vgl. EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 61.

62 Im Rahmen des UPSTREAM-Programms müssen die Telekommunikationsunternehmen der NSA gestatten, die Internetverkehrsflüsse zu kopieren und zu filtern, um Zugang zu der Kommunikation (Metadaten und Inhalte) zu erlangen, die von einer von einem „Selektor" erfassten Nicht-US-Person versandt oder von ihr empfangen wurde oder sie betreffe.

63 Der US-Präsident kann die Aktivitäten der US-Nachrichtendienste innerhalb bestimmter Grenzen lenken, u.a. durch Executive Orders, vgl. Erwägungsgrund 68 des „Privacy Shield"-Beschlusses (Fn. 13). E.O. 12333 erlaubt der NSA nach den Feststellungen des vorlegenden Gerichts Zugang zu Daten, die sich auf dem Weg in die USA befinden, mittels Zugriff auf die am Grund des Atlantiks verlegten Seekabel, sowie die Sammlung und Speicherung dieser Daten, bevor sie in den Vereinigten Staaten ankommen und dort den Bestimmungen des FISA unterliegen. Die auf die E.O. 12333 gestützten Tätigkeiten sind nicht gesetzlich geregelt, vgl. EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 63, 183.

64 Nach Art. 52 Abs. 1 S. 1 GRCh müssen Eingriffe in Grundrechte gesetzlich geregelt sein und den Wesensgehalt der Grundrechte achten. Zudem müssen Einschränkungen nach Art. 52 Abs. 1 S. 2 GrCh erforderlich, d.h. verhältnismäßig sein und den dort genannten in der EU anerkannten Einschränkungen – dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer – tatsächlich entsprechen.

erfüllten diese Voraussetzungen jedoch nicht[65]: sie seien trotz der Einschränkungen in der Presidential Policy Directive 28 (nachfolgend „PPD-28“)[66] nicht auf das zwingend erforderliche Maß beschränkt und daher unverhältnismäßig.[67] Die damit verbundenen Eingriffe seien folglich nicht gerechtfertigt.

2.2.1.2 Fehlender gleichwertiger gerichtlicher Rechtsschutz für Betroffene

Ferner müsse die Kommission, so der EuGH, bei der Prüfung der Angemessenheit berücksichtigen, ob die Betroffenen, deren Daten in ein Drittland übermittelt werden, dort wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe i.S.v. Art. 47 GRCh einlegen können.[68] Die Kommission habe jedoch im „Privacy Shield“-Beschluss selbst festgestellt, dass das US-Recht nicht gegen alle rechtswidrigen Zugriffe durch US-Überwachungsbehörden Rechtsbehelfe für betroffene EU-Bürger vorsehe, zumindest nicht, wenn die Zugriffe auf bestimmten Rechtsgrundlagen basierten.[69] Auch die Einschränkungen[70] und Betroffenenrechte im Rahmen der übrigen Überwachungsprogramme[71] seien gegenüber den US-Behörden nicht gerichtlich durchsetzbar.[72] Der zum Schließen dieser Rechtslücken von Kommission und USA ins Leben gerufene Ombudsperson-Rechtsbehelf könne die bestehenden Mängel des gerichtlichen Rechtsschutzes vor einem unabhängigen Gericht nicht ausgleichen. Zum einen sei zweifelhaft, ob die Ombudsperson, die unmittelbar dem US-Außenministerium unterstehe, von der Exekutive unabhängig sei. Zum anderen könne die Ombudsperson gegenüber den US-Überwachungsbehörden keine verbindlichen Entscheidungen treffen.[73] EU-Bürger hätten folglich keinen hinreichenden Rechtsschutz, um Zugang zu ihren Daten zu erlangen oder deren Berichtigung oder Löschung zu verlangen. Der gerichtliche Rechtsschutz in den USA entspreche daher nicht dem in der EU durch Art. 47 GRCh garantierten Niveau.[74]

2.2.2 Bewertung

2.2.2.1 Ausdehnung der Entscheidung auf den „Privacy Shield“-Beschluss

Der EuGH hat die Gelegenheit genutzt, auch über den „Privacy Shield“ zu entscheiden, obwohl es in dem Verfahren hauptsächlich um Datentransfers auf der Basis von SDPC[75] ging. Demgegenüber hatte der zuständige Generalanwalt – dessen Anträgen der Gerichtshof oft folgt – in seinen Schlussanträgen

---

65 Im Detail führte der EuGH hierzu aus, Eingriffe bedürften einer gesetzlichen Grundlage und seien auf das absolut Notwendige zu beschränken. Nach seiner Rechtsprechung seien Grundrechtseingriffe nur verhältnismäßig, wenn die gesetzliche Grundlage für diese Eingriffe den Umfang der Einschränkung selbst festlege und klare und präzise Regeln und Mindesterfordernisse für die Eingriffsmaßnahme vorsehe. Weder Section 702 FISA noch E.O. 12333 genügten diesen Anforderungen. Die Beschränkungen der Überwachung durch die PPD-28 seien nicht ausreichend, da sie Massenerhebungen von Daten auf der Basis von E.O. 12333 nicht hinreichend klar und präzise begrenzten und zudem für die Betroffenen nicht gerichtlich durchsetzbar seien, vgl. EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 181.

66 Presidential Policy Directive 28. Durch von US-Präsident Reagan erlassene PPD-28 wurde die ‚Signalaufklärung‘ durch den US-Nachrichtendienst einigen Einschränkungen unterworfen. Der US-Präsident kann die Aktivitäten der US-Nachrichtendienste in den vom Kongress gesetzten Grenzen lenken, insbesondere durch Executive Orders oder Presidential Directives. Zwei zentrale Rechtsvorschriften dieser Art sind die E.O. 12333 und die PPD-28 (vgl. Erwägungsgründe 68, 69 des „Privacy Shield“-Beschlusses (Fn. 13).

67 EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 169-185.

68 Art. 45 Abs. 2a DSGVO, vgl. EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 186.

69 Z.B. auf Basis der E.O. 12333, EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 191.

70 Z.B. durch die PPD-28 (Fn. 66).

71 Gemeint sind die auf Section 702 FISA gestützten Überwachungsprogramme wie PRISM oder UPSTREAM.

72 EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 192.

73 EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 195f.

74 EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 192, 197.

75 Zu dieser Frage siehe Kapitel 2.3.

zwar Zweifel an dessen Gültigkeit geäußert, eine Entscheidung über den „Privacy Shield“ aber nicht für entscheidungserheblich gehalten.[76]

Der EuGH rechtfertigte seine Entscheidung damit, das vorlegende Gericht[77] habe mitgeteilt, bei der Entscheidung des Rechtsstreits auch Rechtsänderungen wie das zwischenzeitliche Inkrafttreten des „Privacy Shield“ berücksichtigen zu müssen. Zudem sei die Frage, ob ein angemessenes Schutzniveau für die USA verbindlich festgestellt sei, für die Beurteilung der Pflichten relevant, die Datenexporteuren, Datenempfängern und Aufsichtsbehörden bei der Nutzung von SDPC oblägen. Ferner ziele eine der Vorlagefragen explizit darauf ab, ob der im „Privacy Shield“-Beschluss geregelte Ombudsperson-Rechtsbehelf einen hinreichenden gerichtlichen Rechtsschutz i.S.v. Art. 47 GRCh böte.[78]

Es erscheint plausibel, dass die Nutzung von SDPC an weniger strenge Pflichten geknüpft werden kann, wenn im Drittland ohnehin ein angemessenes Schutzniveau besteht. Fraglich ist aber, ob das auch dann gilt, wenn die Angemessenheitsfeststellung wie beim „Privacy Shield“ auf bestimmte zertifizierte Unternehmen beschränkt ist. Die Entscheidung des EuGH, auch über die Gültigkeit des „Privacy Shield“ zu entscheiden, lässt sich dennoch rechtfertigen. Zum einen ist die Beurteilung der Entscheidungserheblichkeit einer Vorlagefrage Sache des nationalen Gerichts und wird vom EuGH nicht überprüft.[79] Zum anderen war die Gültigkeit des „Privacy Shield“ tatsächlich mit den Vorlagefragen zu den SDPC verknüpft, weil der im „Privacy Shield“-Beschluss geregelte Ombudsperson-Rechtsbehelf ausdrücklich auch für Daten gelten sollte, die gemäß SDPC, BCR oder Ausnahmeregelungen in die USA übermittelt werden.[80] Dennoch ist es für das Vertrauen in die Justiz wünschenswert, dass die Frage der Entscheidungserheblichkeit vom vorlegenden Gericht stets sorgfältig geprüft und Vorlagefragen entsprechend formuliert werden, um den Eindruck einer „Selbstermächtigung“ der Gerichte zu vermeiden. Dies gilt umso mehr, als der EuGH durch seine Schrems-Rechtsprechung einen gewissen Sonderweg für Datenschutzaufsichtsbehörden geschaffen hat, transferrelevante Kommissionsentscheidungen gerichtlich überprüfen zu lassen.[81]

2.2.2.2 Ungültigerklärung des „Privacy Shield“

Durch die Ungültigerklärung des „Privacy-Shield“-Beschlusses besteht für die USA kein gültiger Angemessenheitsbeschluss mehr. Von dem Urteil betroffen sind alle EU-Unternehmen, die bislang personenbezogene Daten auf der Basis des „Privacy Shield“ in die USA transferiert haben oder Anbieter nutzen, die sich auf den „Privacy Shield“ stützten. Für diese Unternehmen ist durch das Urteil erneut die maßgebliche Rechtsgrundlage für den Transfer personenbezogener Daten an jene über 5.200 US-Unternehmen[82] weggefallen, die sich dem „Privacy Shield“ unterworfen hatten. Eine Übergangszeit

---

[76] Generalanwalt Saugmandsgaard Øe, Schlussanträge in der Rs. C-311/18 (Fn. 47), Rn. 161ff. Der Generalanwalt führte insbesondere aus, die Frage nach der Gültigkeit des „Privacy Shield“-Beschlusses sei dem EuGH weder ausdrücklich vorgelegt worden noch sonst zwingend für die Entscheidung des High Court oder der irischen Datenschutzbehörde erforderlich. Facebook habe seine Transfers auch nicht auf den „Privacy Shield“ gestützt (Rn. 190-193). Da der „Privacy Shield“-Beschluss auf die Datenübermittlung an selbstzertifizierte Unternehmen beschränkt sei, könne er die irische Behörde in Bezug auf eine Aussetzung von Transfers auf der Basis anderer Rechtsgrundlage (SDPC) nicht binden. Dennoch hat sich der Generalanwalt in einem Hilfsgutachten mit der Gültigkeit des „Privacy Shield“-Beschlusses befasst und Zweifel an dessen Vereinbarkeit mit der DSGVO im Lichte der EU-GRCh und der EMRK geäußert (Rn. 308, 342).

[77] Hier der irische High Court.

[78] Rn. 151 ff.

[79] Dies ergibt sich bereits aus dem Wortlaut des Art. 267 Abs. 2 AEUV: „hält dieses Gericht eine Entscheidung darüber […] für erforderlich“. Hintergrund ist, dass die Entscheidungserheblichkeit i.d.R. nach nationalem Recht zu beurteilen ist, zu dessen Anwendung und Auslegung der EuGH jedoch nicht befugt ist.

[80] Anhang III Anlage A des „Privacy Shield“-Beschlusses (s. Fn. 13).

[81] Zu den Pflichten der Aufsichtsbehörden vgl. auch unten Kapitel 2.3.4.

[82] Eine Liste der zuletzt unter dem „Privacy Shield“ registrierten US-Unternehmen ist abrufbar unter https://www.privacyshield.gov/list.

hat der EuGH den Unternehmen ausdrücklich nicht eingeräumt.[83] Datentransfers in die USA dürfen daher nicht länger auf den „Privacy Shield“, sondern müssen auf eine andere Rechtsgrundlage gestützt werden. Datentransfers, die nicht auf eine andere Rechtsgrundlage gestützt werden können, sind unzulässig und müssen gestoppt werden.

Sachgerecht ist, dass der EuGH – wie schon der Generalanwalt[84] – davon ausgeht, dass die fraglichen Datenübermittlungen zwischen Unternehmen nicht vom Anwendungsbereich der DSGVO ausgenommen sind. Ansonsten wären die DSGVO-Vorschriften zur Datenübermittlung in Drittländer praktisch bedeutungslos, da eine spätere Verarbeitung gewerblich übermittelter Daten zu Zwecken der nationalen Sicherheit nie ausgeschlossen werden kann.[85]

Angesichts der von vielen Seiten und auch vom cep seit Jahren geäußerten Kritik[86] am „Privacy Shield“ kam dessen Ungültigerklärung nicht überraschend. Auch unter dem „Privacy Shield“ blieben massive Datenzugriffe durch US-Behörden möglich. Solche Zugriffe greifen in das Recht auf Privatleben und auf Datenschutz[87] ein, denn sowohl Inhaltsdaten als auch Metadaten können sehr genaue Aufschlüsse über das Privatleben einer Person geben.[88] Bereits in seinem „Schrems I“-Urteil hatte der EuGH „klare und präzise Regeln für die Tragweite und die Anwendung“ staatlicher Maßnahmen und „Mindestanforderungen“ für Eingriffe gefordert, um ausreichende Garantien für die Betroffenen zu schaffen.[89] Diesen Anforderungen genügten die im „Privacy Shield“-Beschluss aufgeführten Beschränkungen und Garantien nicht.[90] Der EuGH hat zu Recht entschieden, dass der Umfang möglicher Massenerhebungen im Wege von Zugriffen auf die im Transit befindlichen Daten unter E.O. 12333 vom Umfang her nicht hinreichend klar und präzise eingegrenzt wird.[91] Inwiefern die Einschränkungen von PRISM und UPSTREAM durch die PPD-28 inhaltlich ausreichend waren, konnte der EuGH offen lassen, da die darin geregelten Anforderungen nicht gerichtlich durchsetzbar seien und schon deshalb kein im Wesentlichen gleichwertiges Schutzniveau gewährleisten könnten.[92]

Auch den Ombudsperson-Rechtsbehelf hat der EuGH zu Recht als unzureichend erachtet und damit die vom cep geäußerte Kritik[93] an diesem Rechtsbehelf bestätigt. Denn die Ombudsperson ist weder komplett unabhängig noch hat sie die Kompetenz, gegenüber den US-Überwachungsbehörden verbindliche Entscheidungen treffen oder diese zu einem Tätigwerden zu zwingen. Beschwerden an den Ombudsmann sind daher Rechtsbehelfen bei einem unabhängigen Gericht nicht gleichwertig.

---

83 EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 202.

84 Generalanwalt Saugmandsgaard Øe, Schlussanträge in der Rs. C-311/18 (Fn. 47), Rn. 100-110.

85 Generalanwalt Saugmandsgaard Øe, Schlussanträge in der Rs. C-311/18 (Fn. 47), Rn. 107.

86 Vgl. bereits Hoffmann, A., cepStudie „Privacy Shield“ (Fn. 28), S.33ff.

87 Diese Rechte schützen sowohl die Vertraulichkeit des Inhalts der Kommunikation, als auch vor einem Zugriff auf Metadaten (Verkehrsdaten und Standortdaten), vgl. Generalanwalt Saugmandsgaard Øe, Rs. C-311/18 (Fn. 47), Rn. 257.

88 EuGH, Urteil vom 8.4.2014, C-293/12 und C-594/12 – Digital Rights Ireland u.a., Rn. 27, EuGH, Urteil vom 21. 12.2016, C-203/15 und C-698/15 - Tele2 Sverige und Watson u. a., Rn. 98f; Generalanwalt Saugmandsgaard Øe, Schlussanträge in der Rs. C-311/18 (Fn. 47), Rn. 257. Für das Vorliegen eines Eingriffs kommt es aber nicht auf die Sensibilität der Daten oder mögliche Nachteile für den Betroffenen an, vgl. EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 171.

89 EuGH, Rs. C-362/14 - Schrems I (Fn. 43), Rn. 91, ebenso nunmehr Urteil in der Rs. C-311/18 - Schrems II (Fn. 2), Rn. 176.

90 Vgl. Anhang VI des „Privacy Shield“-Beschlusses. Zu den Einzelheiten siehe cepStudie „Privacy Shield“ (Fn. 28), S.40ff.

91 EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 183.

92 Zur abweichenden deutschen Übersetzung der Worte „im Wesentlichen gleichwertig“ in der deutschen Urteilsfassung vgl. oben Kapitel 2.2.1.

93 Einzelheiten siehe cepStudie „Privacy Shield“ (Fn. 28), S. 44 ff. Trotz der im „Privacy Shield“-Beschluss genannten Rechtsschutzmöglichkeiten bot dieser auch im Übrigen keinen effektiven gerichtlichen Rechtsschutz gegen staatliche Zugriffe.

Insgesamt weist das Urteil verschiedene Parallelen zum „Schrems I"-Urteil[94] auf, in der der EuGH die „Safe Harbour"-Entscheidung der Kommission für ungültig erklärt hatte.[95] Die Ungültigerklärung des „Privacy Shield"-Beschlusses hat auch Diskussionen über das ähnlich gestrickte Schweizer Datenschutzabkommen mit den USA ins Rollen gebracht.[96]

2.3 Ausführungen des EuGH zu den Standarddatenschutzklauseln (SDPC)

Neben der Entscheidung über den „Privacy Shield" hat der EuGH im „Schrems II"-Urteil vor allem verschiedene Fragen zur Nutzung von SDPC als Rechtsgrundlage für Datentransfers beantwortet. Dabei hat er zunächst festgestellt, dass der den verwendeten SDPC zugrunde liegende Beschluss[97] (nachfolgend: „SDPC-Beschluss") wirksam ist, sodass die SDPC grundsätzlich weiter verwendet werden dürfen (Kapitel 2.3.1). Ferner hat er zum erforderlichen Schutzniveau bei der Verwendung von SDPC Stellung bezogen (Kapitel 2.3.2) und die Pflichten konkretisiert, die den Datenexporteuren in der EU und den Datenempfängern im Drittland (Kapitel 2.3.3) sowie den EU-Datenschutzaufsichtsbehörden (Kapitel 2.3.4) bei der Nutzung von SDPC obliegen. Diese Ausführungen des EuGH zu den SDPC werden abschließend bewertet (Kapitel 2.3.5).

2.3.1 Der SDPC-Beschluss bleibt wirksam

Der EuGH sieht keinen Grund, den SDPC-Beschluss[98] für ungültig zu erklären, der den von Facebook genutzten SDPC zugrunde lag. SDPC beträfen nicht ein bestimmtes Drittland, sondern gälten einheitlich und könnten daher in jedem Drittland unabhängig vom dortigen Schutzniveau als vertragliche Garantien verwendet werden.[99] Je nach Rechtslage und Praxis im Drittland könne sich entweder die Situation ergeben, dass durch die SDPC ein angemessenes Schutzniveau der Daten im Drittland gewährleistet sei, oder die Situation, dass die SDPC möglicherweise kein ausreichendes Mittel darstellten, um einen angemessenen Schutz zu gewährleisten.[100] Im Ergebnis enthalte der SDPC-Beschluss aber wirksame Mechanismen, die in der Praxis gewährleisten könnten, dass das notwendige Schutzniveau im Drittland eingehalten werde oder dass andernfalls die Datenübermittlungen ausgesetzt würden, wenn gegen die Klauseln verstoßen werde oder ihre Einhaltung unmöglich sei.[101]

---

[94] Näher Hoffmann, A., cepStudie „Privacy Shield" (Fn. 28), S.11 ff.

[95] Auch dort galt: Zugriffe durch US-Behörden hatten Vorrang, Eingriffe waren nicht genug begrenzt, die Kommission hatte die Mängel selbst festgestellt und der EuGH prüfte den Beschluss scheinbar ohne zwingende Notwendigkeit.

[96] Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) kam im September 2020 in einer Stellungnahme https://www.newsd.admin.ch/newsd/message/attachments/62787.pdf zu dem Ergebnis, dass der zwischen den USA und der Schweiz vereinbarte „Privacy Shield" (PS CH) ebenfalls kein adäquates Schutzniveau biete. Der EDÖB berief sich dabei auf das „Schrems II"-Urteil, das allerdings für die Schweiz nicht bindend ist. Eine Aufhebung des PS ist damit jedoch nicht verbunden. Die Einschätzung steht unter dem Vorbehalt der Schweizer Gerichte.

[97] Beschluss 2010/87/EU, vgl. 22 sowie oben Ziffer 1.2.

[98] Facebook nutzte die SDPC-Version für Auftragsverarbeiter, welche dem Beschluss 2010/87/EU der Kommission (s. Fn. 22) als Anhang beigefügt ist. Das Urteil ist aber auf die Entscheidung 2001/497/EG und die darin verankerten Standardverträge I und II (vgl. Fn. 22 sowie oben Ziffer 1.2) übertragbar.

[99] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 130, 133.

[100] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 126.

[101] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 137 – 148. Der Datenempfänger versichere mit der Unterzeichnung der SDPC, dass er auch bei der Verarbeitung der Daten im Drittland den EU-Datenschutzstandard (vereinfachte Formulierung, der EuGH bezieht sich auf Art. 3 lit. f) SDPC-Beschluss) einhalte und keinen Gesetzen unterliege, die ihm die Einhaltung der SDPC unmöglich machten. Beim Eintritt eines Konfliktfalls oder bei einer Rechtsänderung müsse er dem Datenexporteur mitteilen, dass er die SDPC nicht einhalten könne. Dieser sei dann verpflichtet, die Datenübermittlung auszusetzen oder zu beenden. Hilfsweise müsse die zuständige EU-Aufsichtsbehörde tätig werden, die vom Datenexporteur nach den SDPC auch u.a. über die ihm vom Datenimporteur mitgeteilten Rechtsänderungen informiert werden müsse.

2.3.2 Erforderliches Schutzniveau bei der Verwendung von SDPC

Der EuGH hat klargestellt: Bei Datenübermittlungen auf der Basis von SDPC müsse ein Schutzniveau für die übermittelten Daten gewährleistet sein, das dem in der EU garantierten Niveau im Wesentlichen[102] gleichwertig ist.[103] Die Anforderungen an das Schutzniveau entsprechen daher denen bei Datenübermittlungen im Rahmen eines Angemessenheitsbeschlusses. Vergleichsmaßstab sei das Schutzniveau der DSGVO[104], die wiederum im Lichte der in der GRCh verbürgten Grundrechte auszulegen sei.[105]

Bei der Prüfung, ob das Schutzniveau gleichwertig ist, sei Folgendes zu berücksichtigen:

- „insbesondere“ die vertraglichen Regelungen zwischen dem Datenexporteur in der EU und dem Datenimporteur im Drittland[106] – hier also die SDPC;
- das Recht im Drittland einschließlich der Zugriffsbefugnisse der dortigen Behörden auf die übermittelten Daten; dabei müsse der Datenexporteur wie die Kommission bei der Prüfung eines Angemessenheitsbeschlusses vorgehen und alle in der nicht abschließenden Liste des Art. 45 Abs. 2 DSGVO aufgeführten Elemente der Rechtsordnung des Drittlands berücksichtigen[107]; und speziell
- die Existenz durchsetzbarer Rechte und wirksamer Rechtsbehelfe für betroffene Personen.[108]

Demnach kann eine Datenübermittlung auf SDPC[109] gestützt werden, wenn die SDPC, das Recht des Drittlandes sowie bestehende durchsetzbare Rechte und Rechtsbehelfe in der Gesamtschau ein Schutzniveau gewährleisten, das mit demjenigen der DSGVO und der GRCh zwar nicht identisch sein muss, ihm aber im Wesentlichen gleichwertig ist.[110]

2.3.3 Pflichten von Datenexporteur und Datenempfänger bei der Nutzung von SDPC

2.3.3.1 Pflicht zur Prüfung des Schutzniveaus

Der EuGH betont, in erster Linie sei der Datenexporteur für die Prüfung und Einhaltung des Schutzniveaus im Drittland verantwortlich. Während für den Erlass eines Angemessenheitsbeschlusses die Kommission das Schutzniveau im Drittland prüfe, müsse – wenn kein Angemessenheitsbeschluss vorliegt – der Datenexporteur diese Prüfung vornehmen.[111] Um ein im Wesentlichen gleichwertiges[112] Schutzniveau wie in der EU zu gewährleisten, müsse er nach Art. 46 Abs. 1 DSGVO „geeignete Garantien“ vorsehen, die die im Drittland bestehenden Mängel an Datenschutz ausgleichen.[113]

---

[102] Formulierung in der deutschen Urteilsfassung: „der Sache nach gleichwertig“. Zur Übersetzung dieser Formulierung vgl. oben Kapitel 2.2.1.
[103] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 96, 105.
[104] Zur Anwendbarkeit der DSGVO auf die fraglichen Datenübermittlungen siehe bereits oben Kapitel 2.2.1.
[105] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 101.
[106] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 104.
[107] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 104. Zu diesen Elementen gehören raus folgt im Prinzip, dass der Datenexporteur den gesamten Katalog des Art. 45 Abs. 2 DSGVO bei der Prüfung berücksichtigen muss.
[108] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 92, 104, 105.
[109] Gleiches muss für andere Garantien i.S.d. Art. 46 Abs. 2 DSGVO, z.B. BCR und genehmigte Vertragsklauseln, Verhaltensregeln und Zertifizierungsmechanismen gelten.
[110] Das Recht des Drittlandes plus die geeigneten Garantien müssen damit zusammen das gleiche Schutzniveau bieten, wie es die Kommission auch für den Erlass eines Angemessenheitsbeschlusses prüfen und bestätigen müsste – dort allerdings ohne Berücksichtigung zusätzlicher Garantien. Zur hiesigen Verwendung der Formulierung „Im Wesentlichen gleichwertig“ statt „der Sache nach gleichwertig“ (deutsche Urteilsfassung) vgl. oben Kapitel 2.2.1.
[111] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 129-134.
[112] Zur hiesigen Verwendung der Formulierung „Im Wesentlichen gleichwertig“ vgl. oben Kapitel 2.2.1.
[113] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 95f., 131.

Nach dem Inhalt der SDPC seien sowohl der Datenexporteur in der EU als auch der Datenempfänger im Drittland vertraglich verpflichtet, sich vor einer Datenübermittlung zu vergewissern, dass im Drittland das erforderliche Schutzniveau eingehalten wird und das Recht des Drittlands es dem Empfänger erlaubt, die SDPC einzuhalten.[114]

Es liege deshalb in der Verantwortung des Datenexporteurs, vor der Datenübermittlung in jedem Einzelfall – „gegebenenfalls" in Zusammenarbeit mit dem Datenempfänger – zu prüfen, ob

(1) das Recht des Drittlandes und die vom Datenexporteur vorgesehenen „Garantien" (hier die SDPC) in ihrer Kombination ein Schutzniveau für die übermittelten Daten gewährleisten, das dem der DSGVO und der GRCh im Wesentlichen gleichwertig[115] ist, und zwar auch hinsichtlich des Bestehens durchsetzbarer Rechte und wirksamer Rechtsbehelfe[116], und

(2) das Recht im Drittland es dem Datenempfänger erlaubt, die SDPC einzuhalten.

2.3.3.2 Pflicht zur Ergänzung von SDPC

Der EuGH führt weiter aus: Komme der Datenexporteur hingegen bei der Prüfung zu dem Ergebnis, dass die SDPC in Anbetracht der Rechtslage und Praxis im Drittland allein nicht ausreichen, um ein angemessenes Schutzniveau für die Betroffenen zu gewährleisten, könne es sich als notwendig erweisen, die in den SDPC enthaltenen Garantien zu ergänzen.[117] Dies könne dadurch geschehen, dass der Datenexporteur den SDPC zusätzliche Klauseln oder Garantien hinzufügt bzw. zusätzliche Maßnahmen ergreift.[118]

Der EuGH hält es also nicht für erforderlich, dass alle nötigen Garantien zwingend in den SDPC enthalten sein oder schon durch die einschlägigen Rechtsvorschriften des Drittlandes gewährleistet werden müssen.[119] Er erachtet SDPC allerdings etwa „möglicherweise" dann nicht als ausreichend, wenn das Recht des Drittlands dortigen Behörden Eingriffe in die Datenschutzrechte der Betroffenen erlaubt.[120] Denn die SDPC könnten naturgemäß keine drittstaatlichen Behörden binden, die nicht Vertragspartei seien. Sie böten folglich keine Garantien, die den Behörden entgegengehalten werden könnten.[121]

2.3.3.3 Pflicht zur Aussetzung der Datentransfers

Könne der Datenexporteur aber im Einzelfall keine hinreichenden zusätzlichen Maßnahmen ergreifen, um diesen Mangel auszugleichen und den erforderlichen Schutz zu gewährleisten, sei er verpflichtet, die Übermittlung auszusetzen oder zu beenden.[122] Dies sei insbesondere dann der Fall, wenn das Recht des Drittlands dem Datenempfänger Verpflichtungen auferlege, die den SDPC widersprächen, und

---

[114] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 141, 142.
[115] Zur hiesigen Verwendung der Formulierung „Im Wesentlichen gleichwertig" vgl. oben Kapitel 2.2.1.
[116] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 134, 141f., 105, 131.
[117] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 126, 127, 132.
[118] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 132ff.
[119] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn 128ff. Die Prüfung des angemessenen Schutzniveaus bei SDPC unterscheide sich daher von der Prüfung bei einem Angemessenheitsbeschluss, den die Kommission nur erlassen dürfe, wenn das Recht des Drittlands bereits alle erforderlichen Garantien biete. Bei Erlass eines SDPC-Beschlusses sei die Kommission nicht verpflichtet, die Angemessenheit des Schutzniveaus in allen Drittländern zu prüfen, in die Daten auf der Basis der SDPC übermittelt werden könnten.
[120] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 126.
[121] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 132, 127.
[122] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 135. Auch nach den SDPC sei der Datenexporteur in diesem Fall berechtigt, vom Vertrag zurückzutreten und die Rücksendung oder Zerstörung der bereits ins Drittland übermittelten Daten und deren Kopien zu verlangen, vgl. EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 140 ff. unter Verweis auf Klausel 5 lit. a, b der SDPC (Anhang zu Beschluss 2010/87/EU).

daher geeignet seien, die durch die SDPC beabsichtigte vertragliche Garantie zu untergraben, dass die Daten angemessen vor dem Zugriff der Behörden des Drittlands geschützt seien.[123]

Wann aber „widersprechen“ rechtliche Verpflichtungen des Empfängers den SDPC und untergraben hiermit deren Garantie? Auch hierauf geht der EuGH ein: nach den im vorliegenden Fall geltenden SDPC[124] sei ein Widerspruch zu und damit ein Verstoß gegen die Klauseln nur anzunehmen, wenn die Verpflichtungen des Datenempfängers im Drittland über das hinausgingen, was in einer demokratischen Gesellschaft erforderlich sei, um u.a. die Sicherheit des Staates, die Landesverteidigung oder die öffentliche Sicherheit zu gewährleisten.[125] Hat die Kommission einen Angemessenheitsbeschluss erlassen, ist dies laut EuGH offenbar ein Indiz dafür, dass kein Widerspruch zwischen SDPC und den Verpflichtungen im Drittland besteht.[126]

2.3.4 Pflichten der Aufsichtsbehörden bei auf SDPC gestützten Datentransfers

Der EuGH verdeutlicht auch die Pflichten der Datenschutzaufsichtsbehörden bei auf SDPC gestützten Datenübermittlungen.[127] Liegt kein gültiger Angemessenheitsbeschluss vor[128], müsse die Aufsichtsbehörde eine auf SDPC gestützte Übermittlung in ein Drittland aussetzen[129] oder verbieten[130], wenn sie zu dem Ergebnis komme, dass die Daten im Drittland nicht gleichwertig wie in der EU geschützt seien. Dies könne entweder dann der Fall sein, wenn die Behörde der Auffassung sei, dass der Datenexporteur die Standardvertragsklauseln im Drittland nicht einhält[131] (z.B. aus Bequemlichkeit missachtet), oder dass er sie nicht einhalten kann (z.B. weil ihm im Drittland widersprechende Verpflichtungen auferlegt werden). Weitere Voraussetzung sei jedoch, dass der erforderliche Schutz der übermittelten Daten nicht durch andere Mittel[132] – sprich: durch weitere Klauseln oder zusätzliche Garantien – gewährleistet werden kann.

Könne der Datenexporteur im Einzelfall keine hinreichenden zusätzlichen Maßnahmen ergreifen, um diesen Mangel auszugleichen und den erforderlichen Schutz zu gewährleisten, sei er selbst verpflichtet, die Übermittlung auszusetzen oder zu beenden.[133] Stelle er die Datenübermittlung in einem solchen Fall dennoch nicht ein, sei in zweiter Linie die zuständige EU-Datenschutzaufsichtsbehörde verantwortlich, die Datenübermittlung zu beenden. Dies sei insbesondere dann der Fall, wenn das Recht des Drittlands dem Datenempfänger Verpflichtungen auferlege, die den SDPC widersprächen, und

---

[123] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 135, 141. Erforderlich und damit unschädlich sind gemäß Fußnote 1 zu Klausel 5 des Beschlusses 2018/87/EU etwa international anerkannte Sanktionen, Erfordernisse der Steuerberichterstattung oder Anforderungen zur Bekämpfung der Geldwäsche. Hat die Kommission einen Angemessenheitsbeschluss erlassen, ist dies laut EuGH offenbar ein Indiz dafür, dass kein Widerspruch zwischen SDPC und den Verpflichtungen im Drittland besteht (Rn. 141).

[124] Vorliegend die Klauseln im Anhang zu Beschluss 2010/87/EU der Kommission (s.22).

[125] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 141. Erforderlich und damit unschädlich sind gemäß Fußnote 1 zu Klausel 5 des Beschlusses 2018/87/EU etwa international anerkannte Sanktionen, Erfordernisse der Steuerberichterstattung oder Anforderungen zur Bekämpfung der Geldwäsche.

[126] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 141.

[127] Siehe dazu bereits EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 117ff.

[128] Dies umfasst sowohl den Fall, dass die Kommission keinen Anwesenheitsbeschluss für das betreffende Land erlassen hat, oder dass der EuGH diesen – wie vorliegend den „Privacy Shield“-Beschluss – für ungültig erklärt hat.

[129] Art. 58 Abs. 2 lit. j DSGVO.

[130] Art. 58 Abs. 2 lit. f DSGVO.

[131] Dies ergibt sich auch aus EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 137, 148.

[132] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 121.

[133] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 135. Auch nach den SDPC sei der Datenexporteur in diesem Fall berechtigt, vom Vertrag zurückzutreten und die Rücksendung oder Zerstörung der bereits ins Drittland übermittelten Daten und deren Kopien zu verlangen, vgl. EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 140 ff. unter Verweis auf Klausel 5 lit. a, b der SDPC (Anhang zu Beschluss 2010/87/EU).

daher geeignet seien, die durch die SDPC beabsichtigte vertragliche Garantie zu untergraben, dass die Daten angemessen vor dem Zugriff der Behörden des Drittlands geschützt seien.[134]

Anders sei die Rechtslage, wenn ein gültiger Angemessenheitsbeschluss vorliegt, der für die Aufsichtsbehörden bindend ist. Diese dürften dann nicht verbindlich feststellen, dass das Drittland kein angemessenes Schutzniveau gewährleistet, sondern müssten die Gerichte anrufen, um auf diesem Weg möglicherweise eine Vorabentscheidung vor dem EuGH zu erwirken.[135]

2.3.5 Bewertung

2.3.5.1 Pflicht zur Prüfung des Schutzniveaus

Der Gerichtshof hebt hervor, dass Daten – egal auf welcher Rechtsgrundlage der Transfer ins Drittland erfolgt – immer im Wesentlichen gleichwertig[136] wie in der EU geschützt sein müssen. Das in der EU durch DSGVO und GRCh verbürgte Schutzniveau darf also auch bei einem Transfer ins Drittland nicht unterschritten werden. Während der Datenexporteur bei einem Angemessenheitsbeschluss ohne weiteres Zutun von einem gleichwertigen Schutz ausgehen darf, liegt es bei Fehlen eines solchen Beschlusses in seiner Verantwortung, geeignete Garantien zu liefern, die einen gleichwertigen Schutz sicherstellen. Nach der DSGVO[137] können SDPC grundsätzlich solche Garantien darstellen. Gewährleisten diese im Einzelfall in der Gesamtschau mit dem Recht des Drittlands einen im Wesentlichen gleichwertigen Schutz, und wird dieser auch nicht durch entgegenstehende Verpflichtungen konterkariert, ist die Übermittlung auf Basis der SDPC grundsätzlich zulässig, sofern die Klauseln auch tatsächlich eingehalten werden. Der EuGH hat jetzt aber erstmals festgestellt, dass die SDPC in bestimmten Fällen nicht ausreichen, um das nötige Schutzniveau zu gewährleisten. Es genügt daher nicht, SDPC einfach nur zu unterzeichnen. Vielmehr muss der Datenexporteur das Schutzniveau „in jedem Einzelfall“ prüfen. Je nach Rechtslage und Praxis im Drittland kann er dabei zu dem Ergebnis kommen, dass die übermittelten Daten – auch unter Berücksichtigung der SDPC – nicht gleichwertig wie in der EU geschützt sind.

Die Prüfpflicht, ob im Einzelfall ein gleichwertiges Datenschutzniveau besteht – deren Bestehen vom EuGH nun klargestellt wurde – bürdet den EU-Datenexporteuren eine bedeutende Aufgabe auf, die viele Unternehmen vor große Schwierigkeiten stellen dürfte.[138] Nicht nur müssen sie sich einen Überblick über das Recht des Drittlandes verschaffen, sondern auch prüfen, ob der Datenempfänger unter diesem Recht die vertraglich vereinbarten Regeln zum Datenschutz auch tatsächlich einhalten kann. Hierzu kann der Datenexporteur sich zwar an den Datenempfänger wenden. An der zutreffenden Beurteilung der Rechtslage in den USA ist allerdings sogar die Kommission gescheitert, wie die

---

[134] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 135. Zur Frage, wann ein solcher Widerspruch vorliegt, vgl. bereits oben Kapitel 2.3.3.3.

[135] Liegt ein gültiger Angemessenheitsbeschluss vor, durch den die Übermittlung im Ergebnis genehmigt wird, ist dieser Beschluss für die Aufsichtsbehörden bindend. Diese dürfen deshalb nicht verbindlich feststellen, dass das Drittland kein angemessenes Schutzniveau gewährleistet. Legt ein Betroffener eine Beschwerde ein, weil er der Ansicht ist, dass die Übermittlung seiner Daten gegen die DSGVO verstößt, müssen die Aufsichtsbehörden dieser Beschwerde aber nachgehen und in voller Unabhängigkeit prüfen, ob die Anforderungen der DSGVO bei der Übermittlung gewahrt werden. Hat eine Aufsichtsbehörde nach einer solchen Prüfung Zweifel an der Gültigkeit des Angemessenheitsbeschlusses, kann sie Klage vor den nationalen Gerichten erheben, die sodann ggf. eine Vorabentscheidung vor dem EuGH erwirken können, vgl. EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 117f., 120 und EuGH, Rs. C-362/14 - Schrems I (Fn. 43), Rn. 52, 57, 65.

[136] Zur hiesigen Verwendung der Formulierung „Im Wesentlichen gleichwertig“ vgl. oben Kapitel 2.2.1.

[137] Art. 46 Abs. 2 lit. c DSGVO.

[138] Siehe dazu etwa die Kritik von Seiten der DIHK, vgl. Hoppe, T./Neuerer, D./Siebenhaar, H., EuGH kippt Rechtsgrundlage für Datentransfers in die USA, 16. Juli 2020, abrufbar unter https://www.handelsblatt.com/politik/international/privacy-shield-abkommen-eugh-kippt-rechtsgrundlage-fuer-datentransfers-in-die-usa/26009730.html und Siebenhaar, H., 5000 Firmen betroffen: EU-Unternehmen drängen auf neue rechtliche Basis zum Datentransfer mit den USA, 17. August 2020, https://www.handelsblatt.com/technik/sicherheit-im-netz/verhandlungen-ueber-privacy-shield-5000-firmen-betroffen-eu-unternehmen-draengen-auf-neue-rechtliche-basis-zum-datentransfer-mit-den-usa/26090814.html.

Ungültigerklärung der „Safe Harbour"-Entscheidung und des „Privacy Shield"-Beschlusses durch den EuGH im Schrems-Fall zeigt. Schon damit steht fest, dass für Datenexporteure mit der Nutzung von SDPC künftig ein erheblicher Aufwand verbunden sein wird, der weitaus größer sein dürfte, als ihn viele Unternehmen bislang betrieben haben. Wie die Prüfung des Schutzniveaus im Drittland im Einzelnen zu erfolgen hat, lässt der EuGH offen. Auf diese Frage soll im Rahmen eines eigenen Kapitels (Kapitel 3) näher eingegangen werden.

2.3.5.2 Pflicht zur Ergänzung von SDPC

Der EuGH zeigt für Fälle, in denen SDPC keinen ausreichenden Schutz bieten, eine mögliche Lösung auf: Datenexporteure können – und müssen – die SDPC-Klauseln ergänzen oder weitere, zusätzliche Garantien vorsehen. [139] Da es auf eine Gesamtschau von geltendem Recht und Garantien ankommt, reicht es aus, wenn der Datenexporteur neben den SDPC weitere Garantien vorsieht, die den Mangel an Datenschutz im Drittland ausgleichen.

In welchen Fällen SDPC ergänzt werden können bzw. müssen, wird im Urteil aber nicht völlig klar. Einerseits führt der EuGH aus, dass dies notwendig sein könne, weil SDPC die am Vertrag nicht beteiligten Behörden im Drittland nicht binden.[140] Andererseits lässt er erkennen, dass der Datenexporteur keine hinreichenden zusätzlichen Maßnahmen ergreifen könne, wenn das Recht des Drittlands dem Datenempfänger Verpflichtungen auferlegt, die den SDPC widersprechen und ihre Garantie untergraben.[141] Die Frage, wann und durch welche Maßnahmen SDPC künftig effektiv ergänzt werden können bzw. müssen, wird ebenfalls im nachfolgenden Kapitel 3 gesondert erörtert.

2.3.5.3 Transfers an Empfänger, die unter die US-Überwachungsgesetze fallen

Es ist naheliegend, dass der EuGH mit Verpflichtungen, die die Garantie der SDPC untergraben, etwa die bei der Prüfung des „Privacy Shield" als unverhältnismäßig befundenen[142] Datenzugriffe von US-Behörden auf Basis der US-Überwachungsprogramme meint. Datenempfänger, die vertraglich an SDPC gebunden sind, dürften in ähnlichen Konflikten stehen wie die unter dem „Privacy Shield" zertifizierten Datenempfänger, die verpflichtet waren, dessen Datenschutzgrundsätze nicht anzuwenden, soweit diese mit ihrer vorrangigen Pflicht kollidierten, Behörden im Interesse der nationalen Sicherheit Zugriff auf die Daten zu gewähren. Es ist daher davon auszugehen, dass die Verpflichtungen, die den Datenempfängern im Zusammenhang mit den streitgegenständlichen US-Überwachungsprogrammen obliegen, auch den SDPC widersprechen. Soweit die Datenempfänger gesetzlich zur Kooperation mit den Überwachungsbehörden verpflichtet sind, können sie den in den Klauseln versprochenen Schutz folglich nicht einhalten. Dadurch wird die vertragliche Garantie der SDPC untergraben und der Datenexporteur müsste die Übermittlungen stoppen. Richtigerweise dürfte das Urteil aber so zu verstehen sein, dass diese Pflicht auch in den Überwachungsfällen dann nicht greift, wenn der Datenexporteur den erforderlichen Datenschutz trotz grundsätzlich drohender Überwachungsgefahr im Einzelfall mit anderen Mitteln doch noch gewährleisten kann.[143] Umgekehrt formuliert lässt sich damit Folgendes festhalten: Fallen die Datentransfers an Empfänger in den USA in den Anwendungsbereich der US-Überwachungsgesetze, entfällt die Verpflichtung, die Übermittlungen zu stoppen, nur dann, wenn im

[139] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 126, 127, 132.
[140] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 132.
[141] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 135.
[142] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 165.
[143] Dies lässt sich daraus ableiten, dass der EuGH in der Zusammenfassung seiner Antwort auf die achte Vorlagefrage allgemein ausführt, dass Aufsichtsbehörden Datentransfers verbieten müssen, wenn SDPC aus ihrer Sicht nicht eingehalten werden können, und der erforderliche Datenschutz „nicht mit anderen Mitteln gewährleistet werden kann", vgl. EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 121.

Einzelfall durch zusätzliche Garantien doch ein im Wesentlichen gleichwertiger Schutz gewährleistet werden kann. In welchen Fällen und durch welche Maßnahmen dies in Betracht kommt, wird in Kapitel 3 näher untersucht.

2.4 Übertragbarkeit des „Schrems II"-Urteils auf andere Transferinstrumente

Die Wertungen des „Schrems II"-Urteils zu den SDPC sind auf unternehmensinterne Datenschutzregelungen („Binding Corporate Rules", BCR) und andere Transferinstrumente i.S.d. Art. 46 DSGVO übertragbar.[144] Denn laut EuGH muss ein dem DSGVO-Standard im Wesentlichen gleichwertiges[145] Schutzniveau bei jeder Datenübermittlung in ein Drittland gewährleistet werden, unabhängig davon, auf welche Rechtsgrundlage die Datenübermittlung in das Drittland gestützt wird.[146] Jeglicher Datentransfer in ein Drittland steht damit unter dem Vorbehalt eines gleichwertigen Datenschutzniveaus.

Bei BCR handelt es sich um unternehmensinterne Datenschutzregelungen, die ebenfalls keine Behörden im Drittland binden. Ebenso wie bei SDPC können auch die in BCR enthaltenen Regelungen durch das Recht des Drittlands konterkariert werden. Bezogen auf Datenübermittlungen in die USA bedeutet dies: Auch bei der Nutzung von BCR dürfte das US-Recht Vorrang haben, auch hier fehlt es an hinreichenden Rechtsbehelfen. Die gleichen Erwägungen sind auch bei Nutzung der übrigen in Art. 46 DSGVO genannten Garantien wie genehmigten Verhaltensregeln und Zertifizierungsverfahren anzustellen. Auch hier bestehen die oben angedeuteten Schwierigkeiten, durch ergänzende Maßnahmen ein im Wesentlichen gleichwertiges[147] Schutzniveau zu schaffen, auf die in Kapitel 3 noch näher eingegangen wird. Für Datenübermittlungen an US-Empfänger, die den US-Überwachungsgesetzen unterliegen, bieten damit auch diese alternativen Instrumente als solche keine rechtssichere Lösung mehr. Der Europäische Datenschutzausschuss (nachfolgend: „EDSA") diskutiert aktuell die genauen Auswirkungen des „Schrems II"-Urteils auf die Nutzung von BCR und hat weitere Informationen dazu angekündigt, ob in die BCR ggf. zusätzliche Verpflichtungen aufgenommen werden müssen. Der EDSA will hierzu ggf. die Arbeitsdokumente[148] mit den Übersichten über die Bestandteile und Grundsätze von BCR für Verantwortliche und Auftragsverarbeiter aktualisieren.

Im Ergebnis müssen Datenexporteur und -empfänger damit bei allen auf „Garantien" gestützten Datentransfers im Einzelfall prüfen, ob diese Garantien ausreichen, um in der Gesamtschau ein im Wesentlichen gleichwertiges[149] Datenschutzniveau gewährleisten zu können, oder ob die verbliebenen Mängel durch zusätzliche Garantien ausgeglichen werden können.[150] Ist dies nicht der Fall, müssen die Datentransfers gestoppt werden.

---

[144] Ebenso der Europäische Datenschutzausschuss, Recommendations 01/2020 (Fn. 6), Rn. 58 ff., ders., Recommendations 02/2020 (Fn. 166), Ziff. 1.5.; Informationsschreiben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 8. Oktober 2020 zur Auswirkung des „Schrems II-Urteils" auf den internationalen Datentransfer, S. 2.

[145] Zur hiesigen Verwendung der Formulierung „Im Wesentlichen gleichwertig" vgl. oben Kapitel 2.2.1.

[146] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 92.

[147] Zur hiesigen Verwendung der Formulierung „Im Wesentlichen gleichwertig" vgl. oben Kapitel 2.2.1.

[148] Artikel 29 Datenschutzgruppe, Arbeitsdokument WP 256/rev.01 mit einer Übersicht über die Bestandteile u. Grundsätze verbindlicher interner Datenschutzvorschriften (BCR), zul. überarbeitet u. angenommen am 6. Februar 2018, (für Verantwortliche), sowie Arbeitsdokument WP 257/rev.01 mit e. Übersicht über d. Bestandteile u. Grundsätze verbindl. interner Datenschutzvorschriften (BCR) für Auftragsverarbeiter, zul. überarbeitet u. angenommen am 6. Februar 2018.

[149] Zur hiesigen Verwendung der Formulierung „Im Wesentlichen gleichwertig" vgl. oben Kapitel 2.2.1.

[150] Ebenso Pressemitteilung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 28.07.2020, abrufbar unter https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_schrems2.pdf.; so jetzt wohl auch EDSA, Recommendations 1/2020 (Fn. 6), Rn. 60 für BCR und einzeln ausgehandelte und von einer Aufsichtsbehörde genehmigte Vertragsklauseln.

2.5 Auswirkungen auf Datentransfers in andere Drittländer

Das „Schrems II“-Urteil bezieht sich formell nur auf den Datentransfer an Empfänger in den USA, hat aber Bedeutung darüber hinaus. Entsprechende staatliche Zugriffsrechte, die mit den SDPC kollidieren, könnten auch in anderen Ländern bestehen. Wer Daten auf der Basis geeigneter Garantien – also gestützt auf SDPC, BCR oder ein anderes in Art. 46 DSGVO genanntes Transferinstrument – in Drittländer ohne Angemessenheitsbeschluss übermitteln will, muss gleichermaßen zuvor das Schutzniveau in diesen Ländern prüfen und festgestellte Mängel durch ergänzende Garantien ausgleichen.

Eine solche Prüfung wäre grundsätzlich seit dem 01.01.2021 auch bei Datenübermittlungen ins Vereinigte Königreich erforderlich. Zu diesem Zeitpunkt ist das Vereinigte Königreich aus dem Binnenmarkt ausgeschieden und damit grundsätzlich zu einem Drittland geworden. Die DSGVO, die aufgrund des Austrittsabkommens während der Brexit-Übergangsphase noch bis zum 31.12.2020 im Vereinigten Königreich weitergegolten hatte[151], gilt dort nun formal nicht mehr. Kurz vor dem Jahreswechsel haben sich die EU und das Vereinigte Königreich jedoch auf ein umfangreiches Handels- und Kooperationsabkommen[152] geeinigt, das auch neue Übergangsregelungen für die Übermittlung personenbezogener Daten enthält. In diesem Abkommen wurde u.a. festgelegt, dass die Übermittlung personenbezogener Daten aus der EU[153] an das Vereinigte Königreich unter bestimmten Voraussetzungen[154] während einer Übergangszeit nicht als Übermittlung an ein Drittland gilt. Dies hat zur Folge, dass die strengen Voraussetzungen der Art. 44 ff. DSGVO über die Datenübermittlung in Drittländer weiterhin nicht auf Übermittlungen personenbezogener Daten in das Vereinigte Königreich anwendbar sind. Datenübermittlungen nach Großbritannien müssen folglich während dieser Übergangszeit – anders als Datentransfers in andere Drittländer[155] – (noch) nicht auf Ausnahmeregeln oder Transferinstrumente wie SDPC oder BCR gestützt werden.[156] Die Übergangszeit begann am 1. Januar 2021 und beträgt vier Monate, verlängert sich aber, wenn keine der Vertragsparteien Einwände erhebt, automatisch um zwei weitere Monate. Sie endet dagegen vorzeitig, wenn die Kommission einen Angemessenheitsbeschluss für das Vereinigte Königreich erlässt oder wenn das Vereinigte Königreich entweder sein Datenschutzrecht ändert oder bestimmte näher geregelte datenschutzrechtliche Befugnisse ohne die Zustimmung der EU im neugeschaffenen Partnerschaftsrat ausübt.[157] Datentransfers in das Vereinigte Königreich sind damit vorerst weiterhin unter den bisherigen Voraussetzungen möglich, voraussichtlich bis mindestens Ende April 2021. Das Europäische Parlament muss allerdings noch seine Zustimmung zu dem

---

[151] Abkommen über den Austritt des Vereinigten Königreichs Großbritannien und Nordirland aus der Europäischen Union und der Europäischen Atomgemeinschaft, ABl. L 29 vom 31.01.2020, S. 7ff., Art. 71 Abs. 1, Art. 126, 127.

[152] Handels- und Kooperationsabkommen zwischen der Europäischen Union u. der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland anderseits, ABl. L 444 vom 31.12.2020, S. 14-1449.

[153] Gleiches gilt für Übermittlungen aus Island, Liechtenstein und Norwegen in das Vereinigte Königreich, Art. FINPROV.10a Abs. 2 Handels- und Kooperationsabkommen (Fn. 200).

[154] Voraussetzung ist etwa, dass das am 31.12.2020 im Vereinigten Königreich geltende Datenschutzrecht weitergilt und dass das Vereinigte Königreich bestimmte näher aufgeführte datenschutzrechtliche Befugnisse nicht ohne die Zustimmung der EU im mit Vertretern beider Parteien besetzten Partnerschaftsrat ausübt, vgl. Art. FINPROV.10a Abs. 1, 3 Handels- und Kooperationsabkommen (Fn. 200).

[155] In Bezug auf den mit dem Abkommen verbundenen Sonderstatus Großbritanniens im Vergleich zu anderen Drittländern wird die Frage der Vereinbarkeit mit dem völkerrechtlichen Gleichheitsgrundsatz aufgeworfen, vgl. Uhlemann, H., The UK post-Brexit: the status of sui generis?, 11. Januar 2021, abrufbar unter https://www.datenschutz-notizen.de/the-uk-post-brexit-the-status-of-sui-generis-2928489/.

[156] EDPB, Updated information note on data transfers under the GDPR to the United Kingdom after the transition period, 13. Januar 2021, S. 1, abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_informationnote_20201215_transferstoukaftertransitionperiod_updated20210113_en.pdf; vgl. bereits Pressemitteilung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 28.12.2020, abrufbar unter https://www.datenschutzkonferenz-online.de/media/pm/20201228_pm_Brexit.pdf.

[157] Art. FINPROV.10a Abs. 4, 5, Art. FINPROV.11 Abs. 2, 3 Handels- und Kooperationsabkommen (Fn. 200).

Abkommen erteilen; danach muss der Rat den Beschluss über den Abschluss des Handels- und Kooperationsabkommens noch formal annehmen.[158] Das Abkommen wird aber bereits vorläufig angewendet.[159] Die Kommission geht davon aus, dass das Abkommen mit dem Vereinigten Königreich von der EU allein abgeschlossen werden konnte und eine zusätzliche Ratifizierung des Abkommens durch die EU-Mitgliedstaaten nicht erforderlich ist.[160]

Einen Angemessenheitsbeschluss für das Vereinigte Königreich hat die Kommission bislang noch nicht erlassen. Durch die neue Übergangszeit hat sie sich zwar ein weiteres Zeitpolster hierfür verschafft. Der Erlass eines rechtssicheren Angemessenheitsbeschlusses dürfte aber angesichts der hohen Anforderungen an die Rechtmäßigkeit eines solchen Beschlusses schwierig sein, nicht zuletzt auch mit Blick auf bekannt gewordene Praktiken der britischen Sicherheits- und Nachrichtendienste für die Beschaffung und Verwendung von Massenkommunikationsdaten. Denn der EuGH hat in seinem Urteil vom 6. Oktober 2020 zur Vorratsdatenspeicherung erkannt, dass eine Regelung wie die streitgegenständliche britische Verpflichtung von Anbietern elektronischer Kommunikationsdienste, Verkehrsdaten und Standortdaten allgemein und unterschiedslos an die Sicherheits- und Nachrichtendienste weiterzugeben, die Grenzen des unbedingt Notwendigen überschreitet und nicht gerechtfertigt ist.[161] Erlässt die Kommission bis Ende Juni 2021 keinen Angemessenheitsbeschluss, müssen Datenexporteure die Grundsätze des „Schrems II"-Urteils spätestens ab Juli 2021 auch bei Datentransfers ins Vereinigte Königreich beachten und ggf. entsprechende zusätzliche Schutzmaßnahmen ergreifen.[162]

Schließlich müssen im Nachgang zu dem „Schrems II"-Urteil auch bestehende Angemessenheitsbeschlüsse für andere Drittländer daraufhin überprüft werden, ob diese Länder die vom EuGH aufgestellten Anforderungen (noch) erfüllen.[163] Ist dies nicht der Fall, muss die Kommission die Beschlüsse überarbeiten oder – so die festgestellten Mängel nicht beseitigt werden können – aufheben. Dies könnte auch durch den EuGH drohen, falls Aufsichtsbehörden oder Gerichte auch die Gültigkeit anderer Angemessenheitsbeschlüsse in Zweifel ziehen und die Gerichte sodann den EuGH um Vorabentscheidung ersuchen.

---

[158] https://www.consilium.europa.eu/de/press/press-releases/2020/12/29/eu-uk-trade-and-cooperation-agreement-council-adopts-decision-on-the-signing/.

[159] https://www.consilium.europa.eu/de/press/press-releases/2020/12/29/eu-uk-trade-and-cooperation-agreement-council-adopts-decision-on-the-signing/, Art. FINPROV.11 Abs. 2 Handels- und Kooperationsabkommen (Fn. 200).

[160] https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2532.

[161] EuGH, Urteil vom 6. Oktober 2020, C-623/17, Privacy International, Rn. 80-82.

[162] EDPB, Updated information note on data transfers under the GDPR to the United Kingdom, a.a.O. (Fn. 156), S. 2.

[163] Die Kommission hat bereits vor Jahren angekündigt, eine solche Überprüfung der Angemessenheitsbeschlüsse vornehmen zu wollen, vgl. Mitteilung COM(2017) 7 vom 10. Januar 2017: Austausch und Schutz personenbezogener Daten in einer globalisierten Welt, S. 10f. Siehe dazu bereits cep**Analyse** Nr. 25/2017, Datenübermittlung in Drittländer, S. 2ff.

3 Umsetzung des „Schrems II“-Urteils: Prüfpflicht und Ergänzung von SDPC

3.1 Einleitung

Wie in Kapitel 2.3 ausgeführt, ist der Datenexporteur nach dem „Schrems II“-Urteil bei der Nutzung von SDPC verpflichtet, das Schutzniveau im Drittland zu prüfen und erforderlichenfalls ergänzende Maßnahmen zu ergreifen. Der EuGH gibt in seinem Urteil jedoch nur wenig Hilfestellung, wie Datenexporteure diese Pflichten im Einzelnen umsetzen sollen. Insbesondere lässt er offen, welche Umstände in die Prüfung des Schutzniveaus einzubeziehen sind und wann und durch welche Maßnahmen SDPC ergänzt werden müssen, um Schutzdefizite auszugleichen und das Schutzniveau auf ein dem EU-Level gleichwertiges Niveau anzuheben. Dies hat zu großer Rechtsunsicherheit geführt.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (nachfolgend „LfDI BW“) hatte – soweit ersichtlich – als erste Behörde eine konkrete „Orientierungshilfe“ zum Urteil veröffentlicht und eine Checkliste und spezifische Ergänzungen der SDPC vorgeschlagen.[164]

Der Europäische Datenschutzausschuss („EDSA“), der sich aus Vertretern der nationalen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten zusammensetzt und eine einheitliche Anwendung der DSGVO in der EU sicherstellen soll, hat im November 2020 die Entwurfsfassungen zweier Empfehlungen veröffentlicht, in denen er auf diese Fragen eingeht. Beide Empfehlungen (1/2020[165] und 2/2020[166]) betreffen die Nutzung von Standardvertragsklauseln und vergleichbaren Transferinstrumenten. Sie sind für Datenexporteure nicht bindend, sollen ihnen aber bei der Bewältigung ihrer komplexen Aufgaben helfen, das Schutzniveau im Drittland zu beurteilen und geeignete zusätzliche Maßnahmen zu identifizieren.[167] Bereits im Juli 2020 hatte der EDSA Antworten auf häufig gestellte Fragen zum „Schrems II“-Urteil veröffentlicht[168] und darin erste Empfehlungen für die Nutzer von SDPC gegeben. Um detailliertere Empfehlungen auszuarbeiten und geeignete ergänzende Maßnahmen zu ermitteln, mit deren Hilfe das erforderliche Datenschutzniveau eingehalten werden kann, hatte der EDSA eine „Taskforce“ eingesetzt.[169] Im Rahmen einer Konsultation konnten bis zum 21. Dezember 2020 Stellungnahmen zu den Empfehlungsentwürfen eingereicht werden.

Drittens hat der Europäische Datenschutzbeauftragte (EDSB), der nach Art. 52 Abs. 3 der Verordnung (EU) 2018/1725 für die Überwachung und Durchsetzung der Datenschutzregeln bei der Datenverarbeitung durch EU-Organe oder -Einrichtungen zuständig ist, Ende Oktober 2020 eine „Strategie“ veröffentlicht, wie EU-Organe und -Einrichtungen das „Schrems II“-Urteil umsetzen können.[170]

Viertens hat die EU-Kommission im November 2020 ihren angekündigten Entwurf neuer SDPC[171] veröffentlicht. Zu diesem Entwurf konnten im Rahmen einer Konsultation bis zum 10.12.2020 Stellungnahmen eingereicht werden.

---

[164] Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41).
[165] EDSA, Recommendations 1/2020 (Fn. 6).
[166] EDSA, Recommendations 2/2020 of 10 November 2020 on the European Essential Guarantees for surveillance measures.
[167] EDSA, Recommendations 1/2020 (Fn. 6) S. 2.
[168] EDSA, Häufig gestellte Fragen zum Urteil des Gerichtshofs der EU in der Rechtssache C-311/18 — Data Protection Commissioner gegen Facebook Ireland Ltd und Maximilian Schrems vom 23.07.2020, S. 2 Fn. 2, abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_faqs_schrems_ii_202007_adopted_de.pdf.
[169] https://edpb.europa.eu/news/news/2020/european-data-protection-board-thirty-seventh-plenary-session-guidelines-controller_de.
[170] European Data Protection Supervisor, Strategy for Union Institutions, offices, bodies and agencies to comply with the “Schrems II” Ruling, 29. Oktober 2020.
[171] EU-Kommission, Entwurf eines Durchführungsbeschlusses zu Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer gemäß der Verordnung (EU) 2016/79 des Europäischen Parlaments und des Rates (englische

Das vorliegende Kapitel setzt sich im Detail mit der Prüfung des Schutzniveaus (Kapitel 3.2) und den vorgeschlagenen ergänzenden Maßnahmen zur Aufstockung des Schutzniveaus (Kapitel 3.3) auseinander und analysiert dabei auch die genannten Vorschläge von EDSA, EDSB und der Kommission.

3.2 Prüfung des Schutzniveaus im Drittland

Nach dem „Schrems II"-Urteil muss der Datenexporteur vorab – und „soweit angemessen" in Zusammenarbeit mit dem Datenempfänger – prüfen, ob die SDPC im konkreten Fall tatsächlich einen gleichwertigen Schutz bieten. In Anlehnung an die Terminologie des EDSB wird diese Prüfung des Schutzniveaus nachfolgend als Transfer-Folgenabschätzung (TFA) bezeichnet. [172]

3.2.1 Transfer-Folgenabschätzung

Der EuGH geht im „Schrems II-Urteil" nicht näher darauf ein, wie die Feststellung des Schutzniveaus im Drittland im Einzelnen zu erfolgen hat. Er hat zu dem Vorschlag des Generalanwalts[173], die Prüfung unter Berücksichtigung sämtlicher Umstände der einzelnen Übermittlung – z.B. der Art und des Zwecks der Übermittlung und der Sensibilität der Daten – vorzunehmen[174], nicht Stellung bezogen. Für eine Heranziehung der Gesamtumstände spricht jedoch, dass er eine Prüfung „in jedem Einzelfall" fordert. Der EDSA konkretisiert in seinen Empfehlungen Nr. 1/2020[175] unter anderem, wie der Datenexporteur bei der Prüfung des Schutzniveaus vorgehen muss und wie er unter Einbeziehung der Empfehlungen 2/2020 feststellen kann, ob das Schutzniveau der SDPC im Drittland beeinträchtigt ist. Seiner Ansicht nach muss der Datenexporteur prüfen, wie das Recht des Drittlands auf die geplanten Transfers anzuwenden ist und ob dieses Recht oder die Praxis im Drittland den in den SDPC verankerten Schutz für die zu übermittelnden Daten oder die Ausübung dort verankerter Rechte auf Zugang, Berichtigung oder Löschung beeinträchtigen könnte.[176] Auch der EDSA geht davon aus, dass der Datenexporteur bei dieser Prüfung die gesamten Umstände des spezifischen Datentransfers einbeziehen muss.[177] Dazu gehören nach seiner Auffassung etwa der Zweck des Transfers[178], die am Transferprozess beteiligten Akteure[179], der Sektor, in dem der Transfer erfolgt[180], die Kategorien der übermittelten Daten[181], ob die Daten im Drittland gespeichert werden oder nur ein Ferngriff auf diese erfolgt, in welchem Format die Daten übermittelt werden (im Klartext, pseudonymisiert oder verschlüsselt), und ob sie evtl. in ein anderes Drittland übermittelt werden. Laut dem EDSA erhält der Datenexporteur die entsprechenden Informationen über Recht und Praxis im Drittland im besten Fall direkt vom Datenempfänger oder durch Analyse öffentlicher Gesetzgebung[182], kann daneben aber auch andere relevante und objektive Faktoren wie frühere Präzedenzfälle berücksichtigen.[183]

Fassung). Dieser Beschlussentwurf wird nachfolgend als „Entwurf eines Durchführungsbeschlusses zu SDPC" bezeichnet; die in dessen Anhang geregelten Klauseln werden nachfolgend abgekürzt als „Neue SDPC, Entwurf v. November 2020" bezeichnet.

[172] Englisch: Transfer Impact Assessment (TIA), vgl. EDSB (Fn. 218), S. 8.

[173] Generalanwalt Saugmandsgaard Øe, Schlussanträge in der Rs. C-311/18 (Fn. 47), Rn. 109.

[174] Für diesen „pragmatischeren" Ansatz plädiert etwa die Kanzlei Norton Rose Fulbright, Schrems II landmark ruling: A detailed analysis, Juli 2020, vgl. https://www.nortonrosefulbright.com/en/knowledge/publications/ad5f304c/schrems-ii-landmark-ruling-a-detailed-analysis.

[175] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6).

[176] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 30, 32, 34.

[177] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 28-33.

[178] Z.B. Marketing, HR, Speicherung, IT Support, oder Erstellung klinischer Studien.

[179] Z.B. öffentliche oder private Stellen, Verantwortliche oder Auftragsverarbeiter.

[180] Z.B. Online-Marketing, Telekommunikation, Finanzen.

[181] Z.B. Daten von Kindern.

[182] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 30, 42.

[183] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 42f.

Wie der EDSA ausdrücklich ausführt, darf der Datenexporteur sich allerdings bei seiner Bewertung nicht auf subjektive Erwägungen stützen, z.B. auf die (fehlende) Wahrscheinlichkeit ungerechtfertigter behördlicher Zugriffe.[184]

EU-Institutionen, die Daten in die USA transferieren, sind ebenfalls nach der Strategie des für sie „zuständigen" EDSB aufgefordert, zusammen mit den Datenempfängern TFAs vorzunehmen und ergänzende Schutzmaßnahmen zu etablieren, um Datentransfers in die USA fortsetzen zu können. Spätestens im Laufe des Frühlings 2021 sollen sie dem EDSB über alle fortgesetzten Transfers in Drittländer ohne angemessenes Schutzniveau, alle aus diesem Grund gestoppten Transfers und Kategorien von Transfers berichten. Einzelheiten zur Prüfung des Schutzniveaus nennt der EDSB nicht. Er will aber eruieren, ob solche Prüfungen auch gemeinsam von verschiedenen Behörden und Datenexporteuren durchgeführt werden könnten, und insgesamt eng mit dem EDSA kooperieren.[185]

3.2.2 Feststellung einer Beeinträchtigung der Garantien der SDPC anhand der „wesentlichen europäischen Garantien"

Besonderes Augenmerk muss der Datenexporteur bei der Prüfung nach Ansicht des EDSA auf Vorschriften legen, die Datenempfänger verpflichten, den Behörden des Drittlands Daten offenzulegen oder ihnen Zugriff darauf zu gewähren (z.B. für Strafverfolgungszwecke, nationale Sicherheitszwecke oder regulatorische Aufsicht).[186] Derartige Eingriffe können die Garantien der SDPC beeinträchtigen. Unterliegt der Empfänger im Drittland solchen Vorschriften, muss der Datenexporteur weiter prüfen, ob diese Eingriffe gerechtfertigt sind. Dies ist laut EDSA dann der Fall, wenn sich die Befugnisse der nationalen Behörden und die korrespondierenden Pflichten der Datenempfänger im Rahmen dessen halten, was in einer demokratischen Gesellschaft zur Gewährleistung u.a. der Sicherheit des Staates, der Landesverteidigung und der öffentlichen Sicherheit erforderlich ist.[187] Denn das Grundrecht auf Datenschutz werde nicht schrankenlos gewährt, sondern müsse im Einklang mit dem Verhältnismäßigkeitsprinzip gegen andere Grundrechte abgewogen werden.[188] Ob ein Eingriff, der einem derartigen Ziel von allgemeinem Interesse dient, als gerechtfertigt anzusehen sei, sei anhand der Art. 47 und 52 GRCh zu beurteilen.[189] Um dem Datenexporteur diese Beurteilung zu erleichtern, hat der EDSA zusätzlich die ergänzenden Empfehlungen 2/2020 über die „wesentlichen europäischen Garantien" für Überwachungsmaßnahmen[190] veröffentlicht. In dem Dokument, das bereits nach dem „Schrems I"-Urteil von der früheren Art. 29-Datenschutzgruppe[191] verfasst und nun vom EDSA aktualisiert wurde, werden – auf Basis der Rechtsprechung des EuGH und des EGMR – vier wesentliche europäische Garantien aufgelistet, an denen Überwachungsmaßnahmen im Drittland zu messen sind:[192]

1. Eingriffe sollte auf klaren, präzisen und zugänglichen Vorschriften beruhen.
2. Erforderlichkeit und Angemessenheit im Hinblick auf die verfolgten legitimen Ziele sind nachzuweisen.
3. Es sollte ein unabhängiger Aufsichtsmechanismus bestehen.

---

[184] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 42.
[185] Strategie des EDSB, a.a.O. (Fn. 170), S. 8f.
[186] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 36.
[187] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 36.
[188] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 1.
[189] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 37.
[190] EDSA, Recommendations 2/2020, a.a.O. (Fn. 166).
[191] Die Art. 29-Datenschutzgruppe war ein durch die frühere EU-Datenschutzrichtlinie 95/46/EG geschaffenes unabhängiges Gremium insbesondere der nationalen Datenschutzaufsichtsbehörden und als solches die Vorgängerin des EDSA.
[192] EDSA, Empfehlungen 2/2020, a.a.O. (Fn. 166), S. 8.

4. Dem Bürger müssen wirksame Rechtsbehelfe zur Verfügung stehen.

Diese vier Garantien sind Kernelemente im Rahmen der Prüfung, ob Überwachungsmaßnahmen in Drittländern die SDPC konterkarieren.[193] Werden diese Garantien eingehalten, spricht dies dafür, dass die mit Überwachungsmaßnahmen verbundenen Eingriffe in die Grundrechte auf Datenschutz und Privatsphäre – etwa Zugriffe auf die Daten, deren Speicherung oder weitere Nutzung – nicht über das hinausgehen, was in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, und damit als gerechtfertigt angesehen werden können.[194] Die in den SDPC verankerten Garantien werden dann durch diese Eingriffe nicht beeinträchtigt[195] und die SDPC können somit grundsätzlich ein gleichwertiges Schutzniveau bieten.[196] Überschreiten die Eingriffe hingegen diesen Rahmen, sind die Eingriffe in der Regel nicht gerechtfertigt. Die Garantien der SDPC werden dann durch sie beeinträchtigt und der Datenempfänger kann die SDPC nicht einhalten. In diesem Fall fehlt es an einem im Wesentlichen gleichwertigen Schutzniveau.[197]

Die vier Garantien sind – worauf der EDSA ausdrücklich hinweist – bis zu einem gewissen Grad interpretationsbedürftig.[198] Die Anforderungen an eine Erfüllung aller vier Garantien sind jedoch hoch. Es stellt sich daher die Frage, ob die Garantien hinsichtlich der Überwachungs- bzw. Offenlegungspflichten von Behörden überhaupt von einer nennenswerten Zahl von Drittländern erfüllt werden können.[199] Die USA beispielsweise erfüllen die wesentlichen europäischen Garantien[200] nicht: zum einen gehen die Zugriffsbefugnisse der US-Behörden unter den US-Überwachungsgesetzen laut dem EuGH über das Erforderliche hinaus; zum anderen fehlt es an effektiven Rechtsbehelfen für Betroffene. Auch wenn der EDSA nur Section 702 FISA erwähnt, ist mit dem EuGH davon auszugehen, dass auch Zugriffe im Rahmen von E.O. 12333 während des Transits unverhältnismäßig und ungerechtfertigt sind.[201] Die US-Überwachungsgesetze beeinträchtigen folglich die Garantien der SDPC.

3.3 Zusätzliche Maßnahmen zur Ergänzung der SDPC

Welche zusätzlichen Maßnahmen kann der Datenexporteur nun aber in welchen Fällen ergreifen, um mögliche Lücken im Schutz der transferierten Daten zu schließen? Und wann versprechen ggf. auch diese Maßnahmen keinen wirksamen Schutz? Da von der Kommission erlassene SDPC-Sätze unverändert übernommen werden müssen, kommen nur separate, zusätzliche Klauseln oder sonstige

[193] EDSA, Recommendations 2/2020, a.a.O. (Fn. 166), Rn. 48. Der EDSA weist ausdrücklich darauf hin, dass die wesentlichen europäischen Garantien nur Teil der Prüfung des Schutzniveaus sind. Weder zielen sie darauf ab, alle für die Feststellung eines angemessenen Schutzniveaus erforderlichen Elemente zu definieren, noch darauf, alle Elemente aufzulisten, die bei der Beurteilung zu berücksichtigen sind, ob das Recht des Drittlands Datenexporteur und -Empfänger daran hindert, angemessene Schutzmaßnahmen zu gewährleisten, vgl. Rn. 8.

[194] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 39.

[195] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 39.

[196] EDSA, Recommendations 2/2020, a.a.O. (Fn. 6), Rn. 44.

[197] EDSA, Recommendations 2/2020, a.a.O. (Fn. 166), Rn. 51.

[198] EDSA, Recommendations 2/2020, a.a.O. (Fn. 166), Rn. 49.

[199] Dies kann zu Problemen führen, wenn neue Angemessenheitsbeschlüsse erlassen oder bestehende Beschlüsse überprüft werden müssen. Denn der EDSA geht wie selbstverständlich davon aus, dass die Kommission einen Angemessenheitsbeschluss nur für Drittländer erlassen kann, die die wesentlichen europäischen Garantien einhalten, vgl. Recommendations 2/2020, a.a.O. (Fn. 166), Rn. 52. Gleiches muss dann für die Überprüfung eines Angemessenheitsbeschlusses gelten.

[200] Dies wird verneint von Christakis, T., "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1), abrufbar unter https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/.

[201] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 184. Auch nach dem vom EDSA genannten Transit-Beispielsfall wäre allenfalls ein bloßer Transit durch die USA zulässig, vorausgesetzt, dass niemand in den USA Zugriff auf den Schlüssel hat und keine Hintertüren (backdoors) in Hard- oder Software existieren. Zugriffe während des Transits an Empfänger in den USA, die die Daten entschlüsseln können und müssen, werden von diesem Beispielsfall nicht erfasst.

Garantien in Betracht. Der EDSA listet in Anhang 2 seiner Empfehlungen Nr. 1/2020 einige konkrete Beispiele für technische, vertragliche und organisatorische Maßnahmen auf, die Datenexporteure zusätzlich zu den SDPC und anderen Transferinstrumenten des Art. 46 DSGVO ergreifen können, um das Schutzniveau für die übermittelten Daten im Drittland auf ein dem EU-Schutzniveau gleichwertiges Niveau anzuheben. Vor Veröffentlichung der Empfehlungen des EDSA hatte bereits der LfDI BW verschiedene technische und vertragliche Ergänzungsmaßnahmen vorgeschlagen.[202]

3.3.1 Technische Maßnahmen

3.3.1.1 Vorschläge des EDSA und des LfDI BW

Als technische Zusatzmaßnahmen schlägt der EDSA beispielhaft eine „starke Verschlüsselung“ und eine Pseudonymisierung der übermittelten Daten vor. Auch der LfDI BW hat eine Verschlüsselung oder eine Anonymisierung der Daten als mögliche Lösung vorgeschlagen.[203] Während eine Anonymisierung den Personenbezug der Daten und damit die Anwendbarkeit der DSGVO auf diese Daten generell entfallen lässt, zielen Verschlüsselung und Pseudonymisierung im Kern darauf ab, potenziell rechtswidrige Zugriffe auf die übermittelten Daten zu unterbinden, die entweder während des Transits oder später im Bereich des Empfängers erfolgen können.[204] Sind die Daten im Bereich des Empfängers, gilt es zu verhindern, dass Behörden entweder durch direkten Zugriff auf die Datenverarbeitungssysteme des Empfängers oder dadurch Zugang zu den Daten erlangen, dass sie den Empfänger auffordern, bestimmte Daten zu extrahieren und der Behörde zu übergeben.[205] Im Einzelnen sollen die Maßnahmen technisch verhindern, dass Behörden betroffene Personen identifizieren, Informationen über sie ableiten, diese in einen anderen Kontext setzen oder die Daten mit anderen bereits in ihrem Besitz befindlichen Datensätzen kombinieren können.

A. „Starke“ Verschlüsselung

Der EDSA geht davon aus, dass in bestimmten Anwendungsfällen durch eine „starke“ Verschlüsselung ein im Wesentlichen gleichwertiges Schutzniveau sichergestellt werden kann, und zwar auch dann, wenn im Drittland ungerechtfertigte behördliche Eingriffe drohen. Unklar ist, was der EDSA mit „starker Verschlüsselung“ meint. Vermutlich sind darunter folgende Anforderungen an die Verschlüsselung gemeint, die der EDSA detailliert auflistet: der Verschlüsselungsalgorithmus und seine Parametrisierung (z.B. die Schlüssellänge und Betriebsart) müssten dem Stand der Technik entsprechen und als robust gegenüber Kryptoanalysen anzusehen sein, die von den Behörden des Drittlands unter Berücksichtigung der ihnen zur Verfügung stehenden Ressourcen und technischen Möglichkeiten (z.B. Rechenleistung für Brute-Force-Angriffe) durchgeführt werden. Zudem hängt die erforderliche Stärke der Verschlüsselung laut dem EDSA auch davon ab, wie lange die Vertraulichkeit der Daten gewahrt werden muss. Schließlich müsse der Verschlüsselungsalgorithmus fehlerfrei durch ordnungsgemäß gewartete konforme Software implementiert werden. Die Schlüssel müssten zuverlässig verwaltet werden, und der Datenexporteur oder eine von ihm betraute Stelle in einem sicheren Gebiet (das innerhalb des EEA liegt oder für das ein Angemessenheitsbeschluss gilt) müsse die alleinige Kontrolle über die Schlüssel haben. Nachfolgend werden die Anwendungsfälle und die Voraussetzungen aufgelistet, unter denen der EDSA eine solche Verschlüsselung für wirksam erachtet.

---

[202] Zu den folgenden Vorschlägen vgl. Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41), S. 7, 10, 11 (technische Maßnahmen), 11f (vertragliche Maßnahmen).
[203] Zu den folgenden Vorschlägen vgl. Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41), S. 7, 10, 11.
[204] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 74.
[205] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 75.

1. Speicherung verschlüsselter Daten im Drittland zu Sicherungszwecken (Backup):[206]

(1) Die Daten werden im Drittland durch den Empfänger (Host Provider) lediglich gespeichert – insbesondere zu Sicherheitszwecken – und nicht anderweitig verarbeitet;

(2) der Datenempfänger benötigt keinen Zugriff auf die Daten im Klartext;

(3) die Daten sind nach neustem Stand der Technik „stark" verschlüsselt, und

(4) der Datenempfänger hat keinen Zugriff auf den Schlüssel.

2. Reiner Transit verschlüsselter Daten durch ein Drittland:[207]

(1) Die Daten werden (über das Internet) auf dem Weg zu einem sicheren Drittland (für das ein Angemessenheitsbeschluss gilt) geographisch durch ein unsicheres Drittland geleitet;

(2) die Daten werden nach dem Stand der Technik robust transportverschlüsselt und erforderlichenfalls zusätzlich auf Anwendungsebene Ende-zu-Ende verschlüsselt;

(3) es wird eine vertrauenswürdige Public-Key-Zertifizierungsstelle oder Infrastruktur genutzt und die Daten werden nach Stand der Technik gegen Angriffe geschützt, und

(4) die Daten können im Transitland nicht entschlüsselt werden (das Transitland hat keinen Zugriff auf den Schlüssel),

(5) die Existenz von Hintertüren (backdoors) in Hard- oder Software wurde ausgeschlossen.

3. Übermittlung verschlüsselter Daten an Berufsgeheimnisträger:

Einen weiteren Anwendungsfall der Verschlüsselung sieht der EDSA in der Übermittlung verschlüsselter Daten an Berufsgeheimnisträger wie Ärzte oder Rechtsanwälte, etwa zur gemeinsamen medizinischen Behandlung eines Patienten oder zur Erbringung von Rechtsdienstleistungen, unter den folgenden Voraussetzungen[208]:

(1) Die Daten werden an Berufsgeheimnisträger übermittelt, die nach dem Recht des Drittlands von potenziell rechtswidrigen Zugriffsgewährungspflichten auf Daten und Schlüssel freigestellt sind;

(2) die Daten werden nach dem Stand der Technik Ende-zu-Ende verschlüsselt übermittelt;

(3) der Empfänger leitet die Daten nicht an unsichere Dritte (z.B. Auftragsverarbeiter) weiter;

(4) der Empfänger schützt den Schlüssel durch technische und organisatorische Maßnahmen gegen unautorisierte Nutzung und Offenlegung, und

(5) der Datenexporteur hat belegt, dass sein Schlüssel mit dem des Empfängers korrespondiert.

B. Pseudonymisierung oder Aufspaltung der Daten

Ferner kann nach Ansicht des EDSA auch eine Pseudonymisierung oder Aufspaltung der Daten in bestimmten Fällen geeignet sein, potenziell ungerechtfertigte Datenzugriffe im Drittland zu verhindern. Dabei muss der Verantwortliche laut dem EDSA berücksichtigen, dass die Behörden im Drittland möglicherweise bereits andere Informationen über die Betroffenen haben. Er muss analysieren, ob die Behörden die Daten auch dann nicht dann nicht einer natürlichen Person zuordnen können, wenn sie alle verfügbaren Informationen verknüpfen. So könnten die Behörden etwa bereits anderweitig über bestimmte Daten über die Nutzung von Informationsdiensten (z.B. Zugriffszeit, aufgerufene Funktionen,

[206] Die Voraussetzungen sind hier der besseren Lesbarkeit halber stark verkürzt dargestellt. Entsprechende Details s. EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 79ff.

[207] Die Voraussetzungen sind hier verkürzt dargestellt. Details s. EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 84ff.

[208] Die Voraussetzungen sind hier verkürzt dargestellt. Details s. EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 85f.

Geräteeigenschaften) durch bestimmte Betroffene verfügen. Denn die Betreiber dieser Dienste könnten ebenfalls zur Gewährung von Zugriff auf diese Daten verpflichtet sein.[209] Nachfolgend werden die Anwendungsfälle und die Voraussetzungen aufgelistet, in denen der EDSA eine Pseudonymisierung oder Aufspaltung der Daten für wirksam erachtet.

1. Übermittlung pseudonymisierter Daten zu Analysezwecken, z.B. Forschungszwecken:[210]

(1) Die Daten werden pseudonymisiert (Art. 4 Nr. 5 DSGVO) zu Analysezwecken übermittelt;
(2) nur der Datenexporteur kann die Daten de-pseudonymisieren;
(3) die zur De-pseudonymisierung nötigen Informationen werden technisch und organisatorisch gesichert und ausschließlich in der EU oder in einem sicherem Drittland separat aufbewahrt[211], und
(4) die Behörden im Drittland können die Daten auch unter Heranziehung bereits in ihrem Besitz befindlicher Informationen über bestimmte Betroffene nicht natürlichen Personen zuordnen.

2. Gemeinsame Datenverarbeitung aufgespaltener Daten durch zwei oder mehr unabhängige Auftragsverarbeiter ohne Offenlegung der Inhalte

Daneben hält der EDSA auch eine gemeinsame Verarbeitung von Daten durch unabhängige Empfänger in verschiedenen Ländern für eine mögliche Lösung. Durch die richtige Aufspaltung von Daten könne verhindert werden, dass die Empfänger von den Daten Kenntnis nehmen könnten oder ihr Inhalt durch einseitige Zugriffe offengelegt werde[212], und zwar unter folgenden Voraussetzungen:[213]

(1) Der Datenexporteur spaltet die Daten in mehrere Teile auf, von denen jeder für sich ohne zusätzliche Informationen nicht ausreicht, um die Daten zu rekonstruieren;
(2) jeder Teil wird an einen Auftragsverarbeiter in einem anderen Land übermittelt;
(3) die Auftragsverarbeiter können die Daten gemeinsam verarbeiten, ohne dass einer von ihnen dadurch zusätzliche Informationen erlangt;
(4) der für die gemeinsame Verarbeitung verwendete Algorithmus ist sicher vor „aktiven Gegnern“;
(5) die Behörden in den Drittländern haben keinen Zugriff auf die Daten und es gibt auch keine Anhaltspunkte für eine Kooperation zu dem Zweck, die Daten zu rekonstruieren, und
(6) der Datenexporteur erhält die Verarbeitungsergebnisse von jedem Auftragsverarbeiter getrennt und fügt die erhaltenen Teile zusammen, um das Endergebnis zu erhalten.

3.3.1.2 Grenzen technischer Maßnahmen

Der EDSA betont allerdings, dass die genannten technischen Maßnahmen nach derzeitigem Stand der Technik nicht effektiv sind und bestehende Schutzlücken daher nicht schließen können, wenn

(1) die Zugriffsbefugnisse der Behörden im Drittland über das hinausgehen, was in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist[214], und

[209] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 81-83.
[210] Die Voraussetzungen sind hier verkürzt dargestellt. Details s. EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 80ff.
[211] In einem in einem Mitgliedstaat oder einem von einem Angemessenheitsbeschluss erfassten Drittland.
[212] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 132.
[213] Die Voraussetzungen sind hier der besseren Lesbarkeit halber verkürzt dargestellt. Entsprechende Details finden sich in den Empfehlungen des EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 86.
[214] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 88.

(2) der Datenempfänger Zugriff auf die Daten im Klartext hat bzw. diese im Klartext verarbeiten muss, d.h. es technisch erforderlich ist, dass die Daten im unverschlüsselten bzw. entschlüsselten Zustand verarbeitet werden.

Ist der Datenempfänger im Besitz des Schlüssels, reicht es in diesen Fällen auch nicht aus, wenn die Daten verschlüsselt übermittelt werden. Auch eine Kombination aus Transportverschlüsselung und Verschlüsselung während der Speicherung bietet dann nach Ansicht des EDSA keinen hinreichenden Schutz.[215] Ebenso hatte zuvor schon der LfDI BW mitgeteilt, dass eine Verschlüsselung nur dann als Lösung in Frage komme, wenn nur der Datenexporteur den Schlüssel habe und die Verschlüsselung auch von den Behörden nicht gebrochen werden könne.[216]

Der EDSA listet beispielhaft folgende Anwendungsfälle auf, in denen auch technische Maßnahmen nicht weiterhelfen:

- Datenübermittlung an Anbieter von Cloud-Diensten oder an andere Auftragsverarbeiter, die Zugang zu den Daten im Klartext benötigen, um die Daten auftragsgemäß zu verarbeiten,[217]
- Übermittlung an einen Datenempfänger im Drittland, der zur selben Unternehmensgruppe oder zu einer Unternehmensgruppe gehört, mit der eine gemeinsame wirtschaftliche Tätigkeit ausgeübt wird, und der die Daten im Klartext für eigene Geschäftszwecke benötigt, z.B. um per Telefon oder E-Mail mit den Kunden des Datenexporteurs zu kommunizieren oder für diesen Personaldienstleistungen zu erbringen.[218] Ein typisches Beispiel hierfür dürfte die zentralisierte Verarbeitung von HR Daten im US-Mutterunternehmen sein. Dies gilt unabhängig davon, ob die Daten über einen Kommunikationsdienst (z.B. E-Mail, Fax) direkt übermittelt werden, oder ob eine direkte Fernzugriffsmöglichkeit des Empfängers über ein allgemein verwendetes Informationssystem besteht (gemeint sein dürften Internet oder Firmen-Intranet). [219]

Zudem weist der EDSA darauf hin, dass technische Maßnahmen wie Verschlüsselung oder Pseudonymisierung auch dann nicht weiterhelfen, wenn das Recht des Drittlands derartige technische Maßnahmen verbietet oder diese von den Behörden umgangen werden können.[220] Selbst in den wenigen Anwendungsfällen, in denen diese Maßnahmen Schutzlücken grundsätzlich schließen könnten – nämlich insbesondere dann, wenn der Empfänger die Daten nicht im Klartext benötigt – bieten sie dann keinen hinreichenden ergänzenden Schutz. Zusammengefasst bietet nach Ansicht des EDSA beispielsweise

(1) eine Verschlüsselung keinen zusätzlichen Schutz, wenn

- das Drittland die Verschlüsselung oder den Import verschlüsselter Daten verbietet, was laut dem EDSA in einigen Drittstaaten der Fall ist[221], oder wenn
- der Datenempfänger bzw. eine Stelle im Transitland Zugriff auf die Klardaten oder auf den Schlüssel hat und verpflichtet ist, diesen den dortigen Behörden zu übergeben, was bei Empfängern möglich sein könnte, die Section FISA 702 unterliegen[222];

[215] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 89.
[216] Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41), S. 7, 11.
[217] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 88.
[218] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 90.
[219] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 90.
[220] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 52.
[221] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 33 Fn. 40.
[222] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 76.

(2) eine Pseudonymisierung keinen zusätzlichen Schutz, wenn der Empfänger Zugriff auf die Klardaten hat oder die Behörden im Drittland über Informationen verfügen, durch deren Kombination mit den Daten sie die Daten de-pseudonymisieren können[223];

(3) eine Aufspaltung von Daten keinen zusätzlichen Schutz, wenn Anhaltspunkte dafür bestehen, dass die Behörden im Drittland durch Kooperation Zugriff auf andere Datenteile erlangen oder die Daten durch Verknüpfung mit bestehenden Daten Betroffenen zuordnen können.[224]

3.3.1.3 Bewertung

Die Zulässigkeit der Transfers hängt nach dem oben Gesagten erstens maßgeblich davon ab, ob sich die Zugriffsbefugnisse der Behörden im Drittland im Rahmen dessen halten, was in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, und deshalb gemäß Art. 47, 52 GRCh als gerechtfertigt anzusehen sind. Ist dies nicht der Fall, kommt es aus der Sicht des EDSA zweitens entscheidend darauf an, in welchem Format der Datenempfänger die Daten verarbeitet. Grob zusammengefasst kristallisiert sich aus der Bewertung des EDSA Folgendes heraus:

(1) In den Fällen, in denen die behördlichen Zugriffsbefugnisse im Drittland sich im Rahmen dessen halten, was in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, sind Datentransfers auf Basis der SDPC grundsätzlich zulässig, weil der Datenempfänger in der Lage ist, die SDPC einzuhalten.[225] Das Schutzniveau ist dann insoweit i.d.R. im Wesentlichen gleichwertig.

(2) In den Fällen, in denen die Zugriffsbefugnisse der Behörden im Drittland über das hinausgehen, was in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, sind aus der Sicht des EDSA im Wesentlichen nur Datentransfers zulässig, bei denen weder der Datenempfänger noch sonst jemand im Drittland auf die Klardaten zugreifen kann.

Datentransfers in die USA gehören zur zweiten Fallgruppe, weil die Zugriffsbefugnisse der US-Behörden laut dem EuGH über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist, und es zudem an effektiven Rechtsbehelfen für Betroffene fehlt. Datentransfers an Empfänger, die den genannten US-Überwachungsgesetzen unterliegen, sind aus der Sicht des EDSA nur dann noch zulässig, wenn jeglicher Zugriff auf die Klardaten durch technische Maßnahmen tatsächlich unmöglich oder ineffektiv gemacht wird.[226]

Dies ist laut der Empfehlungen des EDSA nur dann der Fall, wenn die Daten so gut geschützt sind, dass selbst der Datenempfänger sie nicht entschlüsseln, nicht de-pseudonymisieren oder aufgespaltene Daten nicht einseitig rekonstruieren kann. Eine Ausnahme stellt die Übermittlung verschlüsselter Daten an Berufsgeheimnisträger dar, die von den unverhältnismäßigen Zugriffsgewährungspflichten im Drittland auf Daten und Schlüssel freigestellt sind.

In der Praxis dürfte der Datenempfänger aber in der Mehrzahl der Fälle Zugriff auf die Daten im Klartext benötigen, diese also diese nicht verschlüsselt, anonymisiert oder pseudonymisiert verarbeiten können. Unterliegt der Empfänger den US-Überwachungsgesetzen, sind in diesen Fällen aus der Sicht des EDSA nach derzeitigem Stand der Technik keine effektiven technischen Maßnahmen ersichtlich, durch die ein behördlicher Zugriff und damit ein Eingriff in die Rechte der Betroffenen verhindert werden kann.

---

[223] EDSA, Recommendations 1/2020, Rn. 80ff.
[224] EDSA, Recommendations 1/2020, Rn. 86.
[225] EDSA, Recommendations 1/2020, Rn. 44.
[226] EDSA, Recommendations 1/2020, Rn. 44.

Diese strenge Beurteilung des EDSA erscheint nachvollziehbar. Die vorgeschlagenen Maßnahmen versprechen in der Mehrzahl der Fälle keinen wirksamen Schutz oder sind in der Praxis zumindest schwierig umzusetzen:

Eine **Anonymisierung** von Daten lässt den Personenbezug der Daten und damit die Anwendbarkeit der DSGVO zwar entfallen. Sie scheidet aber gerade aus, wenn der Datenempfänger in den USA die Daten im Klartext verarbeiten können muss, sie also gerade nicht in anonymisierter Form verarbeiten kann. Diese Methode dürfte damit in der Mehrzahl der Fälle, in denen die Daten zur Verarbeitung in die USA übersandt werden, keine Lösung darstellen. Zudem bestehen noch Unklarheiten darüber, wann Datensätze ausreichend anonymisiert sind.

Daneben ist es in der Tat fraglich, inwieweit sich die Datenzugriffe durch US-Behörden durch **Verschlüsselung** tatsächlich verhindern lassen. Eine Ende-zu-Ende-Verschlüsselung könnte allenfalls den Zugriff auf Daten während des Transits durch Anzapfen der Kabel am Meeresboden verhindern, sofern die Verschlüsselung nicht ohnehin durch die US-Behörden dekodiert werden kann. Der EDSA geht offenbar davon aus, dass US-Unternehmen, die Section 702 FISA unterliegen, verpflichtet sein könnten, den Behörden Schlüssel zur Entschlüsselung der Daten zur Verfügung zu stellen; möglicherweise können sie auch verpflichtet werden, Hintertüren in verschlüsselte Kommunikationssoftware einzubauen. Nur wenn beides nicht der Fall wäre, dürften behördliche Zugriffe wirklich ausgeschlossen sein. Allerdings hat der internationale Geheimdienstverbund „Five Eyes“, zu dem u.a. die Geheimdienste aus den USA und Großbritannien gehören, Technologieunternehmen zuletzt im Oktober 2020 in einer „Internationalen Erklärung“[227] aufgefordert, in ihre Ende-zu-Ende-verschlüsselte Kommunikationssoftware Hintertüren einzubauen.[228] Auch auf EU-Ebene gibt es politische Bestrebungen, Möglichkeiten des Zugangs zu verschlüsselten Daten zu Sicherheits- und Strafverfolgungszwecken zu etablieren. So hat der Rat der EU im Dezember 2020 trotz erheblicher Kritik u.a. von Seiten der deutschen Datenschutzkonferenz[229] eine Entschließung[230] zur Verschlüsselung mit dem bedeutungsvollen Titel „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ angenommen.[231] In dieser vom deutschen Bundesregierung ausgearbeiteten[232] Entschließung fordert der Rat die Entwicklung von Möglichkeiten, um die Verschlüsselung durch Messaging- und andere Kommunikationsdienste zu brechen.[233] Zwar wird betont, dass die EU weiterhin eine starke Verschlüsselung als “Stützpfeiler des Vertrauens in die

---

[227] Internationale Erklärung: Ende-zu-Ende-Verschlüsselung und öffentliche Sicherheit, englische Fassung abrufbar unter https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety.

[228] Pettinger, B., Verschlüsselte Daten – ein Dorn im Auge der Five Eyes, 14. Oktober 2020, abrufbar unter https://www.dr-datenschutz.de/verschluesselte-daten-ein-dorn-im-auge-der-five-eyes/ und Monroy, M., Bundesinnenministerium plant EU-Erklärung gegen Verschlüsselung, 23. September 2020, abrufbar unter https://netzpolitik.org/2020/bundesinnenministerium-plant-eu-erklaerung-gegen-verschluesselung/.

[229] Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 25.11.2020, Für den Schutz vertraulicher Kommunikation durch eine sichere Ende-zu-Ende-Verschlüsselung – Vorschläge des Rates der EU stoppen, abrufbar unter https://www.datenschutzkonferenz-online.de/media/en/TOP_29_Entschlie%C3%9Fung_Verschl%C3%BCsselung.pdf. Zur weiteren Kritik vgl. etwa Ebelt, F., Error: Regierungen planen Angriff auf Verschlüsselung, 11.11.2020, https://digitalcourage.de/blog/2020/crypto-wars-regierungen-angriff-verschluesselung, m.w.N. Auch inhaltlich gibt es Kritik, vgl. Kurzgutachten des wissenschaftlichen Dienstes des Deutschen Bundestags, https://www.andrej-hunko.de/start/download/dokumente/1547-wd-kurzinformation-zum-brechen-oder-umgehen-von-ende-zu-ende-verschluesselungen/file, vgl. dazu auch https://netzpolitik.org/2020/wissenschaftliche-dienste-eu-vorschlag-zur-umgehung-von-verschluesselung-unbrauchbar/.

[230] Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung vom 14. Dezember 2020, Ratsdok. Nr. 13084/1/20 REV 1, abrufbar unter https://www.zeit.de/digital/datenschutz/2020-11/verschluesselung.pdf.

[231] Vgl. Pressemitteilung des Rats vom 14.Dezember 2020.

[232] https://netzpolitik.org/2020/bundesinnenministerium-plant-eu-erklaerung-gegen-verschluesselung/.

[233] Krempl., S., Crypto Wars: EU-Staaten beschließen Resolution zu Entschlüsselung, 14.12.2020, abrufbar unter https://www.heise.de/news/Crypto-Wars-EU-Staaten-beschliessen-Resolution-zu-Entschluesselung-4988717.html.

Digitalisierung und in den Schutz der Grundrechte“ unterstütze.[234] Weil die Ende-zu-Ende-Verschlüsselung aber auch den eigentlich legalen behördlichen Zugang zu Daten Krimineller verhindere, müssten gleichzeitig für die zuständigen Behörden im Bereich Sicherheit und Strafjustiz innovative „technische und operative“ Möglichkeiten geschaffen werden, rechtmäßig für legitime, klar definierte Zwecke der Bekämpfung von Terrorismus oder schwerer oder organisierter Kriminalität auf relevante Daten im Klartext zuzugreifen. Derartige Lösungen sollen "in enger Abstimmung mit den Diensteanbietern“ entwickelt werden. Dabei sollen die Grundrechte und das EU-Datenschutzrecht in vollem Umfang gewahrt bleiben. Zudem müssen die technischen Lösungen für den Zugang zu verschlüsselten Daten den Prinzipien der Legalität, Transparenz, Notwendigkeit und Verhältnismäßigkeit entsprechen.[235] Der Rat bekräftigt diese Forderungen in seinen Schlussfolgerungen zur inneren Sicherheit und zu einer europäischen Polizeipartnerschaft, in welchen er zugleich fordert, derartige technische und operative Lösungen in einem Rechtsrahmen zu verankern.[236] Laut einem Begleitdokument zur Entschließung[237] ist der Rat ferner zu einem engen Austausch mit den Staaten der „Five Eyes“ und insbesondere dem Vereinigten Königreich „entschlossen“. Dabei nimmt er ausdrücklich auf die „Internationale Erklärung“ gegen Ende-zu-Ende-Verschlüsselung Bezug.[238]

Derartige Bestrebungen liegen auf der Linie der Kommission, die in ihrem ebenfalls im Dezember 2020 veröffentlichten Aktionsplan gegen Terrorismus[239] angekündigt hat, gemeinsam mit den Mitgliedstaaten nach rechtlichen, betrieblichen und technischen Lösungen für den rechtmäßigen Zugriff auf verschlüsselte Inhalte zu suchen.[240] Auch in ihrer im Juli veröffentlichten Strategie für eine wirksamere Bekämpfung des Kindesmissbrauchs[241] hat die Kommission angekündigt, nach Lösungen zu suchen, wie Unternehmen sexuellen Missbrauch von Kindern in Ende-zu-Ende-verschlüsselter elektronischer Kommunikation aufdecken und melden können.

Der politische Druck auf Internetdienstleister, einen Dialog über technische Maßnahmen für den Zugang zu Ende-zu-Ende-verschlüsselter Kommunikation zu führen,[242] dürfte dadurch weiter zunehmen. Die Kommission zieht offenbar sogar entsprechende EU-Vorschriften in Erwägung, um Dienstleister früher oder später zu entsprechenden Maßnahmen zu verpflichten.[243] Sind derartige Hintertüren aber einmal etabliert, besteht allerdings die Gefahr, dass sie auch von unbefugten Dritten oder ausländischen Geheimdiensten geknackt und genutzt werden – wenn sie nicht ohnehin künftig mit diesen

---

[234] Entschließung des Rates zur Verschlüsselung (Fn. 230), Ziffer 4.

[235] Entschließung des Rates zur Verschlüsselung (Fn. 230), Ziffer 4-7.

[236] Ratsdok. Nr. 13083/1/20 vom 24.11.2020, abrufbar unter https://data.consilium.europa.eu/doc/document/ST-13083-2020-REV-1/de/pdf, Ziffer 34.

[237] Ratsdok. Nr. 12864/20 vom 16.11.2020, Recommendations for a way forward on the topic of encryption, abrufbar unter abrufbar unter https://www.statewatch.org/media/1515/eu-council-encryption-possible-ways-forward-12864-20.pdf.

[238] Monroy, M. Fünf Jahre Kampf gegen Ende-zu-Ende-Verschlüsselung, 2.12.2020, abrufbar unter https://netzpolitik.org/2020/wie-alles-anfing-fuenf-jahre-kampf-gegen-ende-zu-ende-verschluesselung/.

[239] Communication COM(2020)795 final from the Commission to the European Parliament, the European Council, the Council, The European Economic and Social Committee and the Committee of the Regions vom 09.12.2020 – A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, S. 20.

[240] Fanta, A. EU-Kommissarin: „Wir brauchen EU-Vorschrift zu Verschlüsselung“, abrufbar unter https://netzpolitik.org/2020/eu-kommissarin-wir-brauchen-eu-vorschrift-zu-verschluesselung/.

[241] Mitteilung COM(2020) 607 vom 24.07.2020 an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss u. d. Ausschuss d. Regionen, EU-Strategie für eine wirksamere Bekämpfung des sexuellen Missbrauchs v. Kindern, abrufb. unter https://ec.europa.eu/transparency/regdoc/rep/1/2020/DE/COM-2020-607-F1-DE-MAIN-PART-1.PDF, S.2.

[242] Monroy, M. Fünf Jahre Kampf gegen Ende-zu-Ende-Verschlüsselung, 2.12.2020, abrufbar unter https://netzpolitik.org/2020/wie-alles-anfing-fuenf-jahre-kampf-gegen-ende-zu-ende-verschluesselung/.

[243] Fanta, A. EU-Kommissarin: „Wir brauchen EU-Vorschrift zu Verschlüsselung“, abrufbar unter https://netzpolitik.org/2020/eu-kommissarin-wir-brauchen-eu-vorschrift-zu-verschluesselung/.

geteilt werden –, oder dass die „Nachschlüssel" von den Anbietern an Behörden im Drittländern herausgegeben werden müssen.[244] Ob Verschlüsselung unter diesen Umständen noch als zusätzliche Garantie für Datenübermittlungen in unsichere Drittländer dienen kann, ist mehr als fraglich.

Probleme bestehen auch bei der **Pseudonymisierung**. Auch hier wird man die De-pseudonymisierbarkeit durch Drittlandsbehörden faktisch nicht ausschließen können. Eine wirksame Pseudonymisierung erscheint zudem schwierig umzusetzen. Es dürfte für Datenexporteure schwer abzuschätzen sein, über welche Informationen die Behörden bereits verfügen und inwieweit sie diese nutzen können, um die Daten bestimmten natürlichen Personen zuordnen.

Können folglich auch technische Maßnahmen wie Verschlüsselung und Pseudonymisierung behördliche Zugriffe auf Klardaten nicht effektiv verhindern, muss der Datenexporteur daher konsequenter Weise die Transfers stoppen, und der Datenempfänger muss die Daten zurückgeben oder zerstören.[245]

Problematisch daran ist, dass bei dieser strengen Sichtweise die Mehrzahl der Datenübermittlungen an Empfänger, die den US-Überwachungspflichten unterliegen, derzeit konkret unzulässig wären – nämlich alle, die eine Verarbeitung der Daten im Klartext zum Ziel haben. Datenexporteuren, die sich legal verhalten wollen, bleibt demnach derzeit nur eine einzige Lösung: die Datentransfers einzustellen. Eine Alternative ist – auch nach den Empfehlungen des EDSA – nicht in Sicht.

Der EDSA schließt allerdings nicht aus, dass im Zuge der technischen Entwicklungen Maßnahmen hervorgebracht werden, mit denen die Empfänger ihre Geschäftszwecke auch ohne Zugriff auf die Daten im Klartext erreichen können.[246] Interessant daran ist, dass der EDSA nicht erwähnt – und somit offenbar nicht zu erwarten scheint – dass Transfers an solche Empfänger bei weiterer technischer Verbesserung der Verschlüsselungstechniken generell zulässig werden könnten.

Auch im Rahmen der Evaluierung der möglichen Ergänzungsmaßnahmen könnte man erwägen, die Wahrscheinlichkeit eines behördlichen Datenzugriffs im Drittland zu berücksichtigen. Denn das Risiko eines Eingriffs und damit einer Rechtsverletzung könnte in bestimmten Fällen niedriger sein als in anderen, etwa wenn wenig sensible Daten übermittelt werden oder wenn die Wahrscheinlichkeit eines behördlichen Datenzugriffs im Drittland als gering eingeschätzt wird. In diesen Fällen könnten demzufolge weniger umfangreiche Zusatzgarantien nötig sein. Der EDSA hat ausdrücklich ausgeführt, dass der Datenexporteur sich bei seiner Bewertung des Schutzniveaus nicht auf subjektive Erwägungen wie die (fehlende) Wahrscheinlichkeit ungerechtfertigter behördlicher Zugriffe berufen könne.[247] Transfers werden daher aus seiner Sicht offenbar nicht allein deshalb zulässig, weil die Wahrscheinlichkeit eines tatsächlichen Datenzugriffs durch die US-Behörden im Einzelfall gering ist. Daher dürfte es auch bei der Evaluierung der ergänzenden Schutzmaßnahmen aus Sicht des EDSA nicht auf die Wahrscheinlichkeit tatsächlicher Zugriffe ankommen. Die fehlende Möglichkeit zur Berücksichtigung des tatsächlichen Risikos von Datenzugriffen wird zum Teil kritisiert.[248] Auch die DSGVO enthalte Elemente einer Risikoabwägung und sehe etwa im Rahmen der Datenschutz-Folgeabschätzung (Art. 35 Abs. 1 DSGVO) ausdrücklich eine Risikoabschätzung vor. Dem ließe sich entgegenhalten, dass die DSGVO in den Art. 44ff.

---

[244] Kurz, C., Von jahrelangen Debatten über Hintertüren unbeeindruckt, 14.11.2020, abrufbar unter https://netzpolitik.org/2020/it-sicherheit-von-jahrelangen-debatten-ueber-hintertueren-unbeeindruckt/.

[245] EDSA, Empfehlungen 1/2020, Rn. 52. Gleiches gilt in Fällen, wo derartige technische Maßnahmen wie Verschlüsselung zwar möglich sind, vom Recht des Drittlands aber verboten oder umgangen oder „geknackt" werden und daher keinen zusätzlichen Schutz bieten.

[246] EDSA, Recommendations 1/2020, Rn. 89.

[247] EDSA, Recommendations 1/2020, Rn. 42; vgl. bereits oben Kapitel 3.2.1.

[248] Vgl. etwa Christakis, T., "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 2), abrufbar unter https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2/.

gerade keine solche Risikoabschätzung vorsieht. Zudem dient die Folgenabschätzung in Art. 35 DSGVO dem Zweck, Risiken zu identifizieren und unter Anwendung bestimmter Prozesse zu managen und zu minimieren. Darauf, ob die US-Behörden ihre Zugriffsrechte ausüben oder nicht, hat der Datenexporteur aber keinen Einfluss; das daraus resultierende Restrisiko ist somit für ihn nicht „managebar". Auch welche Interessen die US-Behörden aktuell verfolgen, ist für den Datenexporteur weder offenkundig noch beeinflussbar; diese Interessen können sich zudem ändern: Daten, die heute für die Behörden uninteressant sind, können morgen durchaus von Interesse sein. Auch der EuGH hat eher auf die Zugriffsmöglichkeit der Behörden abgestellt, ohne sich zur Wahrscheinlichkeit eines Zugriffs zu äußern. So hat er im „Schrems I"-Urteil angenommen, dass eine Regelung, die es den Behörden „gestattet", generell auf Inhalte elektronischer Kommunikation zuzugreifen, sogar den Wesensgehalt des Grundrechts auf Achtung des Privatlebens (Art. 7 GRCh) verletzt.[249] Dennoch ist fraglich, ob umfangreiche Transferverbote durch Datenschutzaufsichtsbehörden durch die EU-Datenschutzbehörden mit dem Verhältnismäßigkeitsprinzip vereinbar sind, wenn das tatsächliche Risiko eines Zugriffs der US-Behörden oder der mögliche daraus resultierende Schaden für die Betroffenen gering erscheint. Denn diese Transferverbote greifen ebenfalls in Grundrechte wie die unternehmerische Freiheit und die Berufsfreiheit der Datenexporteure ein. Der EDSA sollte deshalb klarstellen, ob und in welchen Fällen die Einstellung bzw. Untersagung der Datentransfers oder die Verhängung von Bußgeldern unverhältnismäßig sein kann, wenn ein Zugriff auf die Daten zwar theoretisch möglich ist, die Transferparteien diese aber durch technische Maßnahmen schützen und objektive Umstände glaubhaft machen, nach denen es faktisch ausgeschlossen oder extrem unwahrscheinlich ist, dass die Behörden im Drittland den Aufwand einer Entschlüsselung oder De-Pseudonymisierung betreiben werden.

3.3.1.4 Von den US-Überwachungsgesetzen „bedrohte" Datentransfers

Wie oben ausgeführt,

sind derzeit alle Datenübermittlungen an Empfänger, die den US-Überwachungsgesetzen unterliegen und die Daten im Klartext verarbeiten (müssen), konkret von der Unzulässigkeit bedroht. Dies betrifft erstens Datenübermittlungen, die für die Datenverarbeitung verantwortliche Unternehmen und Stellen in der EU eigenhändig vornehmen, z.B:

- Eine EU-Tochtergesellschaft eines US-Unternehmens übermittelt die Daten an ihre Muttergesellschaft in den USA, wo sie verarbeitet werden (Fall Facebook).
- Ein EU-Unternehmen lagert bestimmte Datenverarbeitungen, z.B. im Bereich Personalwesen, an ein Unternehmen in den USA aus.
- Ein EU-Unternehmen steht in Handelsbeziehungen mit einem Unternehmen in den USA und tauscht mit diesem personenbezogene Daten über Kunden oder Beschäftigte aus, z.B. Adressen oder Verträge.[250]

Die Möglichkeit eines behördlichen Zugriffs besteht aber zum anderen gleichermaßen, wenn Unternehmen oder Stellen in der EU sich eines Auftragsverarbeiters bedienen und dieser dann Daten in die USA übermittelt, für die die Unternehmen oder Stellen verantwortlich sind.[251] Beispiele hierfür sind:

[249] EuGH, Rs. C-362/14 - Schrems I (Fn. 43), Rn. 94.
[250] Vgl. Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41), S. 6.
[251] Vgl. Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41), S. 7.

- Ein EU-Unternehmen nutzt einen IT-Dienstleister, der personenbezogene Daten in einer Cloud speichert, die von einem Unternehmen in den USA gehostet wird.[252]
- Ein EU-Unternehmen nutzt ein Videokonferenzsystem eines US-amerikanischen Anbieters, der Daten der Teilnehmer erhebt und in die USA übermittelt.[253]

Die Möglichkeit eines behördlichen Zugriffs besteht auch dann, wenn der Datenempfänger in den USA zwar nicht selbst den US-Überwachungsgesetzen unterliegt, aber Subunternehmer, z.B. Provider, einsetzt, die ihrerseits unter diese Gesetze fallen.[254]

Unternehmen müssen daher insbesondere prüfen,

- ob sie selbst oder die von ihnen genutzten Auftragsverarbeiter Daten ihrer Kunden, Nutzer oder Beschäftigten in der EU an Empfänger übermitteln, die unter die US-Überwachungsgesetze fallen,
- ob der Empfänger in den USA die Daten ggf. an andere Empfänger weiterleitet, die ihrerseits unter die US-Überwachungsgesetze fallen, und
- ob diese Empfänger Zugriff auf die Daten im Klartext haben.

Welche konkreten Datentransfers an welche Datenempfänger unter die US-Überwachungsgesetze fallen, hängt von deren Auslegung ab. Das vom EuGH zitierte US-Recht – Section 702 FISA[255] und E.O. 12333[256] – gilt für jede Übermittlung in die USA auf elektronischem Wege, die in den Anwendungsbereich dieser Vorschriften fällt. Section 702 FISA verpflichtet alle Telekommunikationsbetreiber und alle Anbieter elektronischer Kommunikationsdienste[257] zur Kooperation mit den US-Behörden; E.O. 12333 gestattet die elektronische Überwachung einer nicht öffentlichen Kommunikation ohne die Zustimmung der betroffenen Person.[258] Kritisch sind damit vor allem Übermittlungen an US-Unternehmen aus dem weiten Bereich der elektronischen Kommunikationsdienste. Erfasst dürften aber auch Übermittlungen an US-Unternehmen sein, die zwar nicht selbst unter diese Definition fallen – z.B. Banken –, aber einen US-Anbieter elektronischer Kommunikationsdienste einsetzen.[259] Dies dürfte bei vielen US-Unternehmen der Fall sein. Es wäre hilfreich, wenn der EDSA bzw. die Datenschutzaufsichtsbehörden – z.B. durch Leitlinien – Hilfestellung geben könnten, welche Empfänger unter die jeweiligen Überwachungsgesetze fallen, welche Daten konkret gefährdet sind bzw. inwieweit auch Datentransfers an sonstige Empfänger betroffen sein können, weil diese Empfänger US-Telekommunikationsbetreiber oder US-Kommunikationsdienste nutzen. Eine solche Hilfestellung fehlt bislang völlig. Auch der EDSA geht in seinen Empfehlungen hierauf bislang nicht näher ein.

---

[252] Vgl. Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41), S. 6.
[253] Vgl. Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41), S. 6.
[254] So wohl Schrems, M. https://noyb.eu/de/faqs-zum-fall-eugh, sowie https://www.cbronline.com/opinion/cloud-quake-safe-harbor. Ebenso jetzt wohl auch EDSA, Recommendations 1/2020, Rn. 44.
[255] Vgl. Fn. 60.
[256] Vgl. Fn. 63.
[257] Die Begriffe "Telekommunikationsbetreiber" und „Anbieter elektronischer Kommunikationsdienste" werden in 50 U.S. Code § 1881 (b)(4) definiert, der wiederum auf Definitionen in weiteren Gesetzen verweist.
[258] Vgl. auch EDSA, Häufig gestellte Fragen z. Urteil des Gerichtshofs der EU i. d. Rechtssache C-311/18 (Fn. 168), S. 2 Fn. 2.
[259] So wohl Schrems, M. https://noyb.eu/de/faqs-zum-fall-eugh, 12. Juli 2020, sowie https://www.cbronline.com/opinion/cloud-quake-safe-harbor, 11. August 2020.

3.3.2 Vertragliche und organisatorische Maßnahmen

3.3.2.1 Vorschläge des EDSA und des LfDI BW

Neben den genannten technischen Maßnahmen listet der EDSA auch ergänzende vertragliche oder organisatorische Maßnahmen zur Ergänzung von SDPC auf. Zuvor hatte bereits der LfDI BW in seiner Orientierungshilfe verschiedene vertragliche Maßnahmen vorgeschlagen.

I. **Vertragliche Maßnahmen**

Zu den derzeit vorgeschlagenen vertraglichen Maßnahmen gehören

(1) die vertragliche Regelung der **Verpflichtung**, **spezifische technische Maßnahmen zu benutzen**,[260]

(2) zusätzliche **Informations- und Transparenzpflichten** wie

- die Verpflichtung des Datenempfängers, nach bestem Wissen und Kräften Informationen über das anwendbare Recht im Drittland sowie über Zugriffe, Zugriffsverlangen und ergriffene Maßnahmen zur Verhinderung von Zugriffen zur Verfügung zu stellen,[261]
- Pflichten des Datenexporteurs, die Informationen über das anwendbare Recht und damit seine Prüfung des Schutzniveaus zu dokumentieren, verbunden mit der Verpflichtung des Datenempfängers, potenzielle Änderungen im Vergleich zu den dokumentierten Aussagen mitzuteilen,[262]
- die Erklärung des Datenempfängers, weder Hintertüren (backdoors) für behördliche Zugriffe eingebaut noch Datenzugriffe sonst erleichtert zu haben und auch nicht gesetzlich hierzu oder zur Herausgabe von Schlüsseln verpflichtet zu sein, verbunden mit Vertragsstrafen und Kündigungsrechten für den Fall des Verstoßes,[263]
- das Recht des Datenexporteurs, selbst oder durch Dritte, vor Ort oder per Fernzugriff (remote) Audits oder Inspektionen beim Datenempfänger und seinen Subauftragnehmern durchzuführen, um festzustellen, ob und inwieweit Daten an Behörden weitergegeben wurden,[264]
- eine ggf. mit einer Vertragsstrafe bewehrte verschärfte Verpflichtung des Datenempfängers, den Datenexporteur sofort zu unterrichten, wenn er die SDPC nicht (mehr) einhalten kann[265], sowie Fristen und Prozeduren zur schnellen Unterbrechung der Datenflüsse und Rückgabe der Daten[266],
- die Verpflichtung des Datenempfängers, täglich eine kryptographisch unterzeichnete Nachricht zu senden, dass er bislang keine Aufforderung zur Offenlegung von Daten erhalten hat; bleibt die Info aus, kann der Datenempfänger auf den möglichen Erhalt einer Aufforderung schließen,[267]
- die Verpflichtung des Datenexporteurs, Betroffene bei jeder Datenübermittlung in „unsichere“ Drittländer zu informieren (und nicht nur bei Übermittlung sensibler Daten),[268]

---

[260] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 97f.
[261] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 99; vgl. bereits Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41) für rechtlich bindende Zugriffsverlangen einer Vollstreckungsbehörde, S. 11f.
[262] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 100.
[263] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 103, 104.
[264] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 105f.
[265] In Fällen, in denen das Schutzniveau in einem Drittstaat zunächst als gleichwertig erachtet wird.
[266] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 107ff.
[267] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 110f. Diese sogenannte „Warrant Canary“-Methode funktioniert nur, wenn das Drittland solche passive Mitteilungen nicht verbietet, den Empfänger nicht verpflichtet, falsche Mitteilungen abzusenden, und der Schlüssel sicher aufbewahrt wird, oder verschiedene Personen die Nachricht signieren und versenden.
[268] Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41), S. 11.

- die Verpflichtung des Datenempfängers, Datenexporteur und Betroffenen über die Vergabe von Unteraufträgen zu informieren;[269]

(3) **Verpflichtungen** des **Datenempfängers**, bestimmte **Maßnahmen** zu ergreifen, etwa

- die Rechtmäßigkeit von Zugriffsanforderungen zu prüfen und diese nach besten Kräften rechtlich anzugreifen, wenn das Recht des Drittlands dafür Möglichkeiten eröffnet, und die Offenlegung der Daten zurückzuhalten, bis er letztinstanzlich rechtskräftig hierzu verpflichtet wurde,[270]
- falls eine US-Behörde Daten anfordert, dieser mitzuteilen, dass die Anforderung seinen vertraglichen Verpflichtungen widerspricht, und den Datenexporteur und/oder die zuständige Aufsichtsbehörde zu informieren[271],
- bei Zugriffen auf Daten im Klartext zu Geschäftszwecken (inkl. Support) zuvor stets die Einwilligung des Datenexporteurs oder des Betroffenen einzuholen, oder den Zugriff auf die im EWR gespeicherten Daten technisch an eine Interaktion des Datenexporteurs oder des Betroffenen zu knüpfen, etwa bei technischem Support via Fernzugriff,[272]

(4) Verpflichtung des **Datenexporteurs** und des **Datenempfängers**, **Maßnahmen** zu ergreifen, etwa

- den Betroffenen sofort über Zugriffsverlangen zu informieren, damit dieser ggf. in der EU oder im Drittland Rechtsbehelfe einlegen kann; hilfsweise, wenn diese Information verboten ist, nach besten Kräften zu versuchen, eine Aufhebung des Mitteilungsverbots zu erwirken[273];
- den Betroffenen bei der Ausübung seiner Rechte im Drittland zu unterstützen[274], z.B. bei der Einlegung von „Ad hoc-Rechtsbehelfsmechanismen“ oder durch rechtliche Beratung.

(5) die **vertragliche** Vereinbarung einer unmittelbaren – nicht nur subsidiären – oder verschuldensunabhängigen **Haftung** des Datenempfängers bei Schäden oder die Aufnahme der in Anhang II der SDPC für Auftragsverarbeiter[275] genannten Entschädigungsklausel in den Vertrag.[276]

II. Organisatorische Maßnahmen

Der EDSA schlägt ferner organisatorische Maßnahmen vor, um das Risikobewusstsein und die Reaktionsfähigkeit des Datenexporteurs zu stärken.[277] Dazu gehören – insbesondere in Unternehmensgruppen – die Einführung interner Richtlinien, Methoden und Standards, die möglichst auch dem Datenempfänger auferlegt werden sollen. Darin sollen insbesondere Verantwortlichkeiten klar zugeordnet, Berichts- und Kommunikationswege geklärt und interne betriebliche Abläufe (etwa zum rechtlichen Vorgehen bei Zugriffsanforderungen) sowie „Best Practices“ festgelegt werden. Interne Zugriffs- und Vertraulichkeitsrichtlinien sollen mit Hilfe von Audits und Disziplinarmaßnahmen durchgesetzt werden. Ferner sollen spezifische Teams für Datentransfers gebildet und Mitarbeiter beim Datenempfänger regelmäßig anhand von praktischen Beispielen geschult werden, wann Datenzugriffe nach EU-Standard ungerechtfertigt sind. Dokumentationen und Transparenzberichte über Zugriffsanfragen sollen erstellt und dem Datenexporteur zur Verfügung gestellt werden. Ferner schlägt der EDSA die

[269] Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41), S. 12.
[270] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 112f., ebenso bereits Orientierungshilfe des LfDI BW, a.a.O. (Fn. 43), S. 12.
[271] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 114.
[272] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 116f.
[273] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 118f.
[274] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 120, 121.
[275] Vgl. Fn. 25.
[276] Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41), S. 12f.
[277] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 122ff.

Einführung strenger Datenschutz- und Datensicherheitsrichtlinien vor, die auf EU-Zertifizierung, Verhaltensregeln oder auf internationalen Standards (z.B. ISO-Normen) und von der EU-Cybersicherheitsagentur ENISA vorgeschlagenen „best practices“ beruhen und unter Berücksichtigung des Standes der Technik, des Risikos für die übermittelten Daten und der Wahrscheinlichkeit behördlicher Anfragen erfolgen soll.[278]

3.3.2.2 Grenzen vertraglicher und organisatorischer Maßnahmen

Der EDSA stellt allerdings ausdrücklich klar, dass auch die von ihm aufgelisteten vertraglichen und organisatorischen Maßnahmen – z.B. interne Richtlinien – die Behörden im DL nicht binden und daher grundsätzlich allein keine Lösung bieten, wenn das Recht im Drittland hinsichtlich der Überwachungs- bzw. Offenlegungspflichten nicht die wesentlichen europäischen Garantien verkörpert.[279] Denn diese Maßnahmen können ungerechtfertigte behördliche Zugriffe nicht verhindern. Der EDSA betont aber, dass ergänzende vertragliche und organisatorische Maßnahmen technische Maßnahmen flankieren und vervollständigen und behördliche Zugriffsversuche erschweren könnten.[280] Zudem könnten sie dem Datenexporteur helfen, sich der Risiken sowie neuer Entwicklungen im Drittland (besser) bewusst zu werden[281] und damit seine Verpflichtung zu erfüllen, Transfers erforderlichenfalls zu stoppen. Vertragliche und organisatorische Maßnahmen könnten somit das Schutzniveau insgesamt verbessern. Sie müssten aber durch zusätzliche technische Maßnahmen ergänzt werden, die den Zugriff auf die Daten unmöglich oder ineffektiv machten.[282]

3.3.2.3 Bewertung

Der EDSA geht zu Recht davon aus, dass in den Fällen, in denen das Recht im Drittland dem Empfänger Verpflichtungen auferlegt, die den vertraglichen Garantien widersprechen und diese untergraben, auch zusätzliche vertragliche Garantien für sich genommen nicht ausreichen:

- Auch **ergänzende Vertragsklauseln** können weder die US-Behörden binden noch einen Rechtsbehelf für EU-Bürger i.S.d. Art. 47 GRCh schaffen. Eine etwaige vertragliche Verpflichtung des Datenempfängers, Rechtsbehelfe gegen Überwachungsmaßnahmen einzulegen, erfüllt aus der Sicht des cep nicht die Anforderungen der DSGVO, wonach „den betroffenen Personen“ durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen müssen.[283] Zum einen stehen die Rechtsbehelfe allenfalls den Datenempfängern und damit gerade nicht den Betroffenen zur Verfügung. Bei Aufnahme einer zusätzlichen Drittbegünstigungsklausel in den Vertrag zwischen Datenexporteur und -empfänger hätte der Betroffene zwar einen Anspruch auf ein entsprechendes Tätigwerden des Empfängers. Fraglich ist aber, inwieweit dieser Anspruch auch durchsetzbar wäre bzw. inwieweit der Datenempfänger nach US-Recht überhaupt klagebefugt bzw. befugt ist, gegen Überwachungsmaßnahmen vorzugehen, da er durch diese möglicherweise nicht in eigenen Rechten verletzt ist. Schließlich wäre sein Vorgehen in der Sache gegen Zugriffe, die nach US-Recht verhältnismäßig und damit rechtmäßig sind, wohl wenig erfolgversprechend. Wie die Ausführungen des EuGH zum „Privacy Shield“ zeigen, sind in den USA gerade auch Eingriffe zulässig, die nicht auf das nach EU-Verständnis absolut Notwendige beschränkt sind. Die Datenempfänger dürften über die Vermeidung einer Vertragsverletzung hinaus auch kein gesteigertes Interesse an der vermutlich

[278] EDSA, Rn. 135.
[279] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 48, 93ff., 95 (für vertragliche Maßnahmen) und Rn. 48, 126
[280] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 44, 48.
[281] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 94, 102.
[282] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 44. Vgl. dazu oben Kapitel .3.3.1
[283] Art. 46 Abs. 1 DSGVO.

kostenintensiven Durchsetzung dieser Ansprüche haben. Zudem verhindert die Verpflichtung behördliche Eingriffe nicht, wenn die Rechtsbehelfe im Drittland keine aufschiebende Wirkung (Suspensiveffekt) haben, und würden dann allenfalls Schadensersatz ermöglichen. Auch der EDSA geht daher zu Recht davon aus, dass die vertragliche Verpflichtung, Zugriffsanforderungen nach besten Kräften rechtlich anzugreifen, nur wenig oder keinen zusätzlichen Schutz bietet.[284] Die vom EuGH festgestellten Mängel des effektiven Rechtsschutzes lassen sich nicht durch vertragliche Ergänzungen beheben.

- Erweiterte **Informations- und Transparenzpflichten** können dem Datenexporteur zwar helfen, das tatsächliche Risiko eines behördlichen Datenzugriffs besser einzuschätzen, lösen aber nicht das Grundproblem, dass eine solche Zugriffsmöglichkeit grundsätzlich besteht. Sie können dem Datenexporteur allenfalls helfen, zeitnah die richtigen Konsequenzen zu ziehen, etwa den Datentransfer zu stoppen. Der EDSA scheint ferner davon auszugehen, dass die vertragliche Pflicht, den Betroffenen sofort über die Zugriffsanforderung zu informieren, diesem dabei helfen kann, seine Klagebefugnis (Standing“) vor dem Gericht des Drittlands zu beweisen.[285] Welche Hilfe diese Klausel dabei bieten soll, diese Hürde zu überwinden, ist jedoch unklar. Zudem laufen diese Pflichten leer, wenn das Recht des Drittlands dem Datenempfänger verbietet, den Datenexporteur, die zuständige Datenschutzaufsichtsbehörde oder den Betroffenen über behördliche Zugriffe oder Zugriffsanforderungen zu informieren.[286] Auch die vertragliche Verpflichtung, die US-Behörde über den Konflikt zu informieren, ist nur sinnvoll, wenn damit etwa eine gerichtliche oder verwaltungsrechtliche Überprüfung der behördlichen Anordnung ausgelöst werden kann.[287]
- Die vertragliche Verpflichtung, erst nach einer Einwilligung bzw. Interaktion des Betroffenen auf die Daten zuzugreifen, ist wirkungslos, wenn der Empfänger zum Zugriff gezwungen wird oder dieser ohne Wissen des Empfängers erfolgt, oder wenn die Einwilligung des Betroffenen nicht freiwillig erfolgt.[288]
- Die vertragliche Verpflichtung, den Betroffenen bei der Ausübung seiner Rechte im Drittland zu unterstützen, ist nur wirksam, wenn im Drittland ein entsprechender und effektiver („Ad hoc“-)Rechtsbehelf existiert[289]. In den USA ist dies nicht der Fall. Diese Klausel bietet daher für Datentransfers in die USA keinen zusätzlichen Schutz.[290]
- **Erweiterte Schadensersatzpflichten** des Datenempfängers entlasten den Datenexporteur, wenn der Betroffene Schadensersatz geltend macht. Sie können helfen, die Klauseln einzuhalten, helfen allerdings nicht weiter, wenn es darum geht, eine Löschung der Daten durch die US-Behörden zu erwirken bzw. wirksam gegen die Überwachung vorzugehen. Zudem werden Datenempfänger sich solchen Pflichten auch nur unterwerfen, soweit sie die Klauseln tatsächlich einhalten können.

[284] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 112, 113.
[285] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 119.
[286] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 115.
[287] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 115.
[288] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 117.
[289] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 120, 121.
[290] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 121.

3.3.3 Der Entwurf der neuen SDPC der EU-Kommission

Die Kommission hat am 13. November 2020 wie angekündigt[291] einen modernisierten Entwurf von Standarddatenschutzklauseln (SDPC)[292] für die Übermittlung personenbezogener Daten in Drittländer veröffentlicht. Sie will dabei auch die Vorgaben aus dem Schrems II-Urteil berücksichtigt haben.[293] Die Kommission hat die SDPC nun umstrukturiert und an die DSGVO angepasst[294]. Die Modernisierung der Klauseln soll zudem der weitverbreiteten Nutzung neuer und komplexerer Verarbeitungsmethoden Rechnung tragen, in die eine Vielzahl von Datenexporteuren und Datenempfängern einbezogen und die oftmals durch lange Datenverarbeitungsketten gekennzeichnet sind.[295] Im Rahmen einer vierwöchigen Konsultation konnten Interessierte zu dem Entwurf Stellung nehmen.

Die neuen SDPC sollen alle bisher von der Kommission anerkannten SDPC-Versionen ersetzen. Die diesen zugrundeliegenden Kommissionsentscheidungen[296], die noch unter der früheren Datenschutzrichtlinie 95/46/EG erlassen worden waren, sollen aufgehoben werden.[297] Die modernisierten Klauseln bringen wichtige allgemeine Neuerungen mit sich (siehe sogleich I.), enthalten aber zudem nun erweiterte Regelungen zum Schutz vor behördlichen Datenzugriffen (unten II).

3.3.3.1 Wichtige[298] allgemeine Neuerungen

Die modernisierten Klauseln

- stellen nun eine Kombination aus allgemeinen Klauseln, die für alle Transfers gelten, und vier Klausel-Modulen für verschiedene Transferszenarien dar, zwischen denen die Parteien wählen können, um die SDPC und die in diesen enthaltenen Verpflichtungen ihrer jeweiligen Rolle und Verantwortlichkeit anzupassen;[299]
- enthalten daher nicht wie bisher nur Regeln für Datenübermittlungen zwischen zwei Verantwortlichen oder zwischen einem Verantwortlichem und einen Auftragsverarbeiter im Drittland, sondern decken künftig auch die bisher fehlenden Übermittlungsstränge vom Auftragsverarbeiter an einen im Drittland ansässigen Sub-Auftragsverarbeiter oder einen dort ansässigen Verantwortlichen ab;
- können zwischen mehreren Vertragsparteien vereinbart werden, oder weitere Verantwortliche oder Auftragsverarbeiter können den SDPC dank einer neuen „docking clause“ später beitreten[300];

---

[291] Mitteilung COM (2020) 264, S. 13

[292] EU-Kommission, Entwurf eines Durchführungsbeschlusses zu Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, a.a.O. (Fn. 219).

[293] https://ec.europa.eu/germany/news/20201113-datentransfers_de; vgl. auch „Neue SDPC, Entwurf v. November 2020“ (Fn. 171), Erwägungsgrund 18.

[294] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Erwägungsgrund 6.

[295] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Erwägungsgrund 6.

[296] Entscheidung 2001/497/EG sowie 2010/87/EU, vgl. oben Kapitel 1.2.

[297] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Art. 6.

[298] Die vorliegenden Ausführungen beschränken sich auf die für die vorliegende Thematik als wesentlich erachteten Änderungen. Weitere wichtige Änderungen sind u.a, dass die neuen SDPC auch von Datenexporteuren außerhalb der EU verwendet werden können, wenn die Verarbeitung der Daten der DSGVO unterliegt, (vgl. Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Erwägungsgrund 6), und dass die neuen SDPC zugleich die zwingenden, für die EU-interne Verarbeitung geltenden Regelungen und Pflichten enthalten, die Verantwortliche und Auftragsverarbeiter nach Art. 28 DSGVO miteinander vereinbaren müssen, so dass die Parteien künftig auf einen zusätzlichen Auftragsverarbeitungsvertrag verzichten können (vgl. Art. 1 Abs. 2 sowie Erwägungsgrund 10).

[299] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Erwägungsgrund 10.

[300] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Erwägungsgrund 10 sowie Anhang, Section I, Clause 6.

- dürfen in einen komplexeren Vertrag eingebettet und durch zusätzliche Schutzmaßnahmen ergänzt werden, die den Klauseln nicht widersprechen; im Falle eines Konflikts zwischen den SDPC und irgend einem anderen Vertrag zwischen den Parteien sollen die SDPC Vorrang haben.[301]

Neu eingeführt werden soll mit dem vorgeschlagenen Durchführungsbeschluss der Kommission neben den SDPC auch eine Informationspflicht für die Datenschutzaufsichtsbehörden: wann immer die nationalen Datenschutzaufsichtsbehörden im Rahmen ihrer Kompetenzen Datenübermittlungen aussetzen oder verbieten, müssen sie die Kommission zeitnah informieren, die dann die Information dann an die anderen Mitgliedstaaten weiterleitet.[302]

Nach Einarbeitung der Ergebnisse der Konsultation und nach Zustimmung der Mitgliedstaaten im sogenannten Komitologieverfahren (Ausschussverfahren, Art. 46 Abs. 2c, 93 Abs. 2 DSGVO) will die Kommission die finale Version der Klauseln annehmen. Zuvor muss sie noch die gemeinsame Stellungnahme des EDSB und EDSA zu den neuen Klauseln abwarten.[303] Daher ist davon auszugehen, dass die neuen Klauseln frühestens im ersten Quartal 2021 in Kraft treten werden.[304]

Nach dem Inkrafttreten der neuen Klauseln haben Datenexporteure und Datenempfänger, die bereits zuvor eine bisherige Version der Standardvertragsklauseln vertraglich vereinbart haben, ein Jahr Zeit, die bisherigen SDPC durch die neuen SDPC zu ersetzen. Sie müssen aber parallel bereits die gemäß dem „Schrems II-Urteil“ nötigen Zusatzmaßnahmen ergreifen.[305]

3.3.3.2 Neue Klauseln zum Schutz vor behördlichen Datenzugriffen

In inhaltlicher Hinsicht enthalten die neuen Klauseln im Vergleich zu den Vorversionen zusätzliche Informations- und Dokumentationspflichten und legen einen besonderen Fokus auf potenzielle Zugriffe auf die Daten durch ausländische Behörden.[306] So regelt Abschnitt 2, Klausel 2 erweiterte Verpflichtungen und Zusicherungen der Parteien für den Fall, dass Gesetze im Drittland die Einhaltung der Klauseln beeinträchtigen; daneben erweitert die nachfolgende Klausel 3 den Umfang der Verpflichtungen des Datenempfängers bei behördlichen Zugriffsanforderungen. Diese Regelungen gelten für alle Module. Auch der Umfang der Drittbegünstigungsregelungen wurde ausgeweitet, so dass Betroffene die Klauseln mit einigen Ausnahmen als Drittbegünstigte einfordern und ggf. durchsetzen können.[307] Einige dieser Pflichten ähneln stark den (vertraglichen) Verpflichtungen, die auch der EDSA in seinen Empfehlungen als ergänzende Maßnahmen vorgeschlagen hat. So sehen etwa auch die neuen Klauseln eine Pflicht zur Prüfung des Schutzniveaus unter Einbeziehung aller Umstände des Einzelfalls und zur Dokumentierung des geprüften Schutzniveaus vor.[308] Zugleich gewährleisten Datenexporteur und Datenempfänger, keinen Grund zur Annahme zu haben, dass das Recht des Drittlands einschließlich

---

[301] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Erwägungsgrund 3 sowie Anhang, Section I, Clause 4.

[302] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Art. 3.

[303] Die Kommission ist nach Art. 46 Abs. 1 der Verordnung (EU) 2018/1725 verpflichtet, vor dem Erlass von Standardvertragsklauseln (Durchführungsbeschluss) die Stellungnahme des EDSB einholen; fakultativ kann sie nach Art. 46 Abs. 2 DSGVO auch die Stellungnahme des EDSA einholen. Wie Erwägungsgrund 25 des Entwurfs eines Durchführungsbeschlusses (Fn. 219) zeigt, wird sie von dieser Möglichkeit Gebrauch machen.

[304] Ursprünglich hatte die Kommission im September angekündigt, die neuen Klauseln bis Ende 2020 zu verabschieden, vgl. Stolton, S., Don’t expect new EU-US data transfer deal anytime soon, Reynders says, 4. September 2020, abrufbar unter https://www.euractiv.com/section/data-protection/news/dont-expect-new-eu-us-data-transfer-deal-anytime-soon-reynders-says/?utm_source=EURACTIV&utm_campaign=f5a0b57faf-digital_brief_COPY_01&utm_medium=email&utm_term=0_c59e2fd7a9-f5a0b57faf-116255475. Vgl. bereits Fanta, A., EU-Kommission bereitet Scheitern von Privacy Shield vor, 29. Mai 2020, abrufbar unter https://netzpolitik.org/2020/eu-kommission-bereitet-scheitern-von-privacy-shield-vor/.

[305] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Art. 6 Abs. 3 und Erwägungsgrund 24.

[306] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Erwägungsgrund 18ff.

[307] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Erwägungsgrund 12.

[308] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Anhang, Section I, Clause 2, lit (b).

etwaiger Pflichten, Behörden Zugriff auf Daten zu gewähren, den SDPC nicht widerspricht.[309] Dabei scheinen die neuen SDPC den Datenempfänger allerdings deutlicher mit in die Pflicht zu nehmen als der EDSA.

Diese Verpflichtungen zu einer derart umfassenden Prüfung unter Einbeziehung vom Empfänger zu liefernder Informationen sind deutlich detaillierter als die bisherige Zusicherung des Datenempfängers, keinen den SDPC entgegenstehenden Gesetzen zu unterliegen[310] – galten die SDPC laut ihrem Art. 1 bislang doch als ausreichende Garantien hinsichtlich des Datenschutzes.[311] In den neuen Klauseln findet sich auch die bislang nicht in den SDPC enthaltene Pflicht des Datenempfängers wieder, Zugriffsverlangen im Drittland rechtlich anzugreifen, soweit dies nach genauer Prüfung möglich erscheint, und die Daten erst freizugeben, wenn er prozessrechtlich final dazu verpflichtet ist.[312] Die bereits unter den bisherigen SDPC bestehende Pflicht des Datenempfängers, Datenexporteur und Betroffene über behördliche Zugriffe und Zugriffsverlangen zu informieren[313], wird ebenso wie vom EDSA vorgeschlagen um die Verpflichtung ergänzt, im Verbotsfall zu versuchen, eine Aufhebung des Mitteilungsverbots zu erwirken.[314] Auch die Verpflichtung, nachträgliche Änderungen der Rechtslage mitzuteilen, wird verschärft. Zudem verpflichten die neuen SDPC den Datenexporteur, bei Erhalt einer Mitteilung sofort zusätzliche (technische oder organisatorische) Maßnahmen zu ergreifen.[315]

Darüber hinaus bleiben die SDPC der Kommission teils aber auch hinter den detaillierteren Vorschlägen des EDSA zurück. So übernehmen sie weder die Pflicht des Datenexporteurs und des Datenempfängers, den Betroffenen bei der Ausübung seiner Rechte im Drittland zu unterstützen, noch die teils vom EDSA vorgeschlagene Absicherung der Verpflichtungen durch Vertragsstrafen. Auch Fristen und Prozeduren zur schnellen Unterbrechung der Datenflüsse und Rückgabe der Daten[316] werden von der Kommission nicht vorgeschlagen. Die Erklärung des Datenempfängers, behördliche Zugriffe nicht z.B. durch Hintertüren (backdoors) erleichtert zu haben und auch nicht dazu oder zur Herausgabe von Schlüsseln verpflichtet zu sein[317], findet sich in den SDPC ebensowenig wieder wie die Pflicht des Datenempfängers, regelmäßig zu bestätigen, dass er keine Aufforderung zur Offenlegung von Daten erhalten hat.[318] Die Tabelle in *Anhang 2* zeigt anhand ausgewählter Vertragspflichten die Unterschiede zwischen den Vorschlägen des EDSA, den neuen SDPC und den bisherigen SDPC auf.

3.3.3.3 Bewertung

Dass die neuen SDPC in weiten Teilen von den Vorschlägen des EDSA für ergänzende vertragliche Maßnahmen abweichen, führt in der für Datenexporteure und Datenempfänger ohnehin unsicheren Situation zu zusätzlichen Unklarheiten. Zum einen ist schwierig zu überblicken, in welchen Details sich die Vorschläge tatsächlich unterscheiden. Zum anderen ist unklar, ob und inwieweit Datenexporteure

[309] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Erwägungsgrund 19 und Anhang, Section I, Clause 2, lit (b).
[310] Standardvertrag II (Fn. 24), Klausel II c).
[311] Art. 1 der jeweiligen Kommissionsentscheidungen zu den bisherigen SDPC (Fn. 22 und 23).
[312] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Anhang, Section II Clause 3.2 (alle Module).
[313] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Erwägungsgrund 22 sowie Anhang, Section II, Clause 3.1 (a) – alle Module.
[314] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Anhang, Section II, Clause 3.1 (b) – alle Module.
[315] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Anhang, Section II, Clause 2, lit (f).
[316] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 107ff.
[317] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 103, 104.
[318] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 110f. Diese sogenannte „Warrant Canary"-Methode funktioniert nur, wenn das Drittland solche passive Mitteilungen nicht verbietet, den Empfänger nicht verpflichtet, falsche Mitteilungen abzusenden, und der Schlüssel sicher aufbewahrt wird, oder verschiedene Personen die Nachricht signieren und versenden.

zusätzlich zu den neuen SDPC noch weitere vom EDSA vorgeschlagene vertragliche Regelungen in ihre Verträge aufnehmen sollten. Die neuen SDPC sollten daher genauer mit den Empfehlungen des EDSA abgestimmt werden. Grundsätzlich sollten sich alle vom EDSA empfohlenen und praxistauglichen Zusatzverpflichtungen auch in den SDPC wiederfinden. Andernfalls sollte klargestellt werden, wie die Datenexporteure widerspruchsfrei zusätzliche vertragliche Regelungen ergänzen können. Zwar ermutigt die Kommission die Datenexporteure dazu, die neuen SDPC durch weitere Klauseln zu ergänzen.[319] Diese ergänzenden Klauseln dürfen jedoch den SDPC nicht widersprechen.

Zu Recht geht der EDSA allerdings davon aus, dass auch die modernisierten SDPC ohne zusätzliche technische Maßnahmen keinen hinreichenden Schutz vor ungerechtfertigten Massenzugriffen bieten. Zur Begründung kann auf die obigen Ausführungen zum begrenzten Nutzen der vom EDSA vorgeschlagenen vertraglichen Maßnahmen verwiesen werden.[320] Diese nur eingeschränkte Nutzbarkeit der SDPC macht die Kommission aber nicht deutlich. Die Kommission sollte im SDPC-Beschluss ausdrücklich klarstellen, dass SDPC nach dem „Schrems II"-Urteil und der Interpretation des EDSA bei fehlendem gleichwertigen Schutzniveau im Drittland grundsätzlich nur noch in Kombination mit zusätzlichen technischen Maßnahmen als Transferinstrument verwendet werden können, durch welche die Schutzlücken effektiv geschlossen werden können. Gleichermaßen sollte sie klarstellen, dass die SDPC in Fällen, in denen auch die flankierenden technischen Maßnahmen versagen, keine taugliche Transfergrundlage sind. Nach dem Wortlaut ist schon fraglich, ob Datenempfänger, die den US-Überwachungsgesetzen unterliegen, die SDPC überhaupt unterzeichnen dürfen, da sie damit zugleich zusichern würden, keinen Rechtspflichten zu unterliegen, die die Einhaltung der SDPC beeinträchtigen könnten. Andererseits müssen die Parteien bei der Prüfung des Schutzniveaus auch die zusätzlich ergriffenen technischen und organisatorischen Schutzmaßnahmen einbeziehen.[321] Es ließe sich daher argumentieren, dass den SDPC eigentlich gegenläufige Rechtspflichten ihre Einhaltung ausnahmsweise nicht beeinträchtigen, wenn ausreichende technische Maßnahmen ergriffen werden. Dennoch sollte klargestellt werden, dass auch Empfänger, die unverhältnismäßigen Überwachungsgesetzen unterliegen, die neuen SDPC unterzeichnen dürfen, wenn sie zugleich effektive technische Maßnahmen vorsehen und dadurch die verbleibenden Schutzlücken schließen. Klargestellt werden sollte in Abstimmung mit dem EDSA auch, inwiefern subjektive Erwägungen eine Rolle bei der Bewertung des Schutzniveaus spielen dürfen.

Schließlich dürften einige Klauseln, wie die Verpflichtung des Datenempfängers, rechtlich gegen Zugriffsverlangen oder Mitteilungsverbote vorzugehen, entweder wirkungslos sein – etwa wenn diese Verlangen oder Verbote nach dem Recht des Drittlands rechtmäßig sind – oder für den Datenempfänger einen hohen Aufwand bedeuten. Zudem ist unklar, mit welcher Begründung der Datenempfänger hiergegen vorgehen soll, insbesondere wenn ihm keine Details der zugrundeliegenden Untersuchung bekannt werden.[322] Es ist daher fraglich, ob – und ggf. zu welchem Preis – Datenempfänger in Drittländern bereit sein werden, die neuen SDPC überhaupt zu unterzeichnen und die zusätzlichen Pflichten zu akzeptieren. In jedem Fall kann die Vereinbarung der neuen SDPC für den Datenexporteur einen erheblichen Aufwand bedeuten. Unternehmen müssen ihre Verträge mit Datenempfängern im

[319] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Erwägungsgrund 3.
[320] Vgl. oben Kapitel 3.3.2.3.
[321] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Erwägungsgrund 20 und Anhang, Section II Clause 2 (b) (iii).
[322] Vgl. hierzu den Blog der Latham & Watkins LLP (mehrere Autoren), The Commission's Draft Updated Standard Contractual Clauses — A Close Look, abrufbar unter https://www.globalprivacyblog.com/legislative-regulatory-developments/the-commissions-draft-updated-standard-contractual-clauses-a-close-look/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+GlobalPrivacyAndSecurityComplianceLawBlog+%28Global+Privacy+and+Security+Compliance+Law+Blog%29#page=1.

Drittland anpassen und entsprechende Verhandlungen führen, um die neuen SDPC in die Verträge zu integrieren.[323] Zudem müssen diese „en bloc“ akzeptiert werden. Einzelne Klauseln der SDPC sind nicht verhandelbar, da die SDPC unverändert übernommen werden müssen und ihr Schutzumfang allenfalls ergänzt werden darf.

3.3.4 Fazit

Die hohen Anforderungen, die der EuGH im „Schrems-Urteil“ stellt, und die – nachvollziehbar – strenge Sichtweise der Datenschutzaufsichtsbehörden stellen viele EU-Datenexporteure sowohl in der Wirtschaft als auch im öffentlichen Sektor vor erhebliche Probleme. Nicht nur die umfassende Prüfung der Rechtslage im Drittland und die Einholung der hierfür notwendigen Informationen bedeutet für sie einen immensen Aufwand. Auch richtig einzuschätzen, wann welche Zusatzmaßnahmen notwendig und wirksam sind, ist eine äußerst schwierige Aufgabe. Ein Überblick über die Prüfpflichten bei der Verwendung von SDPC findet sich in *Anhang 1*. Die Entwürfe der Empfehlungen des EDSA und der neuen SDPC beseitigen die bestehenden Unsicherheiten nur teilweise. Selbst wenn ein Datenexporteur zusätzliche Maßnahmen ergreift und dafür erhebliche Anstrengungen unternimmt, z.B. um seine internen Abläufe anzupassen, schließt dies nicht aus, dass eine Aufsichtsbehörde bzw. ein Gericht diese für nicht ausreichend erachtet und der Datenexporteur so gegen die DSGVO verstößt und hierfür eine Strafe erhalten kann. Abweichungen zwischen den Empfehlungen des EDSA und den neuen SDPC führen zudem zu zusätzlichen Unklarheiten. Alle vom EDSA empfohlenen und praxistauglichen Zusatzverpflichtungen sollten sich auch in den neuen SDPC wiederfinden, um das Schutzniveau so weit wie möglich aufzuwerten.

Klar zu sein scheint lediglich, dass Datentransfers an Unternehmen, die der US-Massenüberwachung unterliegen, gar nicht mehr[324] oder nur noch in einer eng begrenzten Zahl von Fallkonstellationen[325] auf SDPC gestützt werden können, in denen die verbliebenen Schutzlücken im konkreten Fall ausnahmsweise durch Anonymisierung oder Verschlüsselung geschlossen werden können. Potentiell unverhältnismäßige und damit ungerechtfertigte behördliche Zugriffe – wie sie in den USA drohen – können aber nach Ansicht des EDSA derzeit auch bei Einsatz technischer Maßnahmen nicht ausgeschlossen werden, wenn der Datenempfänger auf die Daten im Klartext zugreifen kann. Dies dürfte bei der Mehrzahl der Datenübermittlungen an von US-Überwachungsgesetzen erfasste Empfänger der Fall sein. Alle Übermittlungen zum Zweck der Verarbeitung von Klardaten an derartige Empfänger sind damit konkret von der Unzulässigkeit bedroht. Datenexporteure – und hilfsweise die Aufsichtsbehörden – müssten in diesen Fällen zu dem Ergebnis kommen, dass der Datenexporteur auch durch Zusatzmaßnahmen keinen gleichwertigen Schutz gewährleisten kann. Konsequenter Weise muss der Datenexporteur in diesen Fällen die Transfers stoppen und den Datenempfänger zur Rückgabe oder Vernichtung der Daten auffordern. Eine echte Alternative ist – auch nach den Empfehlungen des EDSA und nach den neuen SDPC der Kommission – nicht in Sicht. Auch die Empfehlungen des EDSA sehen in diesen Fällen für die betroffenen Unternehmen, die sich Hilfen und Klarstellung durch die Aufsichtsbehörden erhofft hatten, keine „wirtschaftsfreundlichere“ Lösung vor. Die neuen SDPC haben in diesen Fällen trotz deutlich erweiterten Pflichtenkatalogs ebenfalls nur einen begrenzten Nutzen, da sie als rein vertragliche Regelungen die Behörden im Drittland nicht binden können. Eine Wunderlösung durch EDSA oder Kommission war und ist allerdings auch nicht zu erwarten: angesichts der hohen

[323] Latham & Watkins LLP, a.a.O. (Fn. 370).
[324] So etwa Schrems, M. unter https://noyb.eu/de/node/189.
[325] So der EDSA und der LfDI BW, vgl. o. (Kapitel 3.3.1.2 und 3.3.1.3).

Anforderungen, die der EuGH stellt, sind insoweit auch die Spielräume der Behörden zur Schaffung rechtssicherer Lösungen klar begrenzt.

Für viele Datenexporteure dürfte unklar sein, wie sie diese missliche Situation lösen sollen. Der deutsche Industrie- und Handelskammertag und weitere Verbände haben daher eine „maßvolle Umsetzung" des „Schrems II"-Urteils gefordert.[326] Offen ist, ob und wie lange die Datenschutzaufsichtsbehörden es ggf. ausreichen lassen werden, dass ein Datenexporteur wenigstens – wie es der LfDI BW fordert[327] – „guten Willen" zum rechtskonformen Handeln zeigt und ergänzende Schutzmaßnahmen vorsieht, auch wenn diese Maßnahmen nach Auffassung der Datenschutzaufsichtsbehörden nicht genügen. Insbesondere sollte klargestellt werden, ab wann und in welchen Fallkonstellationen es zu Bußgeldverfahren kommen wird, wenn die von den Unternehmen etablierten Maßnahmen zur Ergänzung der SDPC nicht ausreichen, und ob „mildernde Umstände" in Betracht kommen, wenn es im Einzelfall an zumutbaren Alternativlösungen fehlt oder eine Umstellung auf solche Lösungen Zeit braucht. Denn die DSGVO[328] sieht für Verstöße gegen die Regeln über die internationale Datenübermittlung grundsätzlich Bußgelder bis zu 20 Millionen Euro oder bis zu 4% des weltweiten Vorjahresumsatzes vor.

Die rechtssicherste Möglichkeit, das Problem zu umgehen, ist, von kritischen Datenübermittlungen in Drittländer abzusehen und die Daten innerhalb der EU zu speichern sowie ausschließlich europäische Provider zu nutzen, die dies entsprechend tun. Dies dürfte allerdings zumindest kurzfristig nicht allen EU-Unternehmen ohne weiteres möglich sein.[329] Transfers an Empfänger, die den US-Überwachungsgesetzen unterliegen, könnten hingegen zulässig werden, wenn die USA ihre Überwachung auf das „zwingend erforderliche Maß" beschränken und Betroffenen aus der EU einen wirksamen Rechtsbehelf gegen die übermäßige Überwachung ermöglichen. Von beidem ist allerdings kurzfristig nicht auszugehen.

Die Lage wird zusätzlich dadurch verkompliziert, dass US-Strafverfolgungsbehörden Anbieter elektronischer Kommunikations- und Cloud-Dienste nach dem 2018 in Kraft getretenen US CLOUD Act[330] unter bestimmten Bedingungen auch zur Offenlegung von Kommunikationsdaten zwingen können, die außerhalb der Vereinigten Staaten gespeichert werden.[331] Entsprechende Anbieter, die der US-Gerichtsbarkeit unterliegen, sind nach diesem Gesetz zur Kooperation verpflichtet, vorausgesetzt, die Daten befinden sich in ihrem Besitz oder unter ihrer Kontrolle. Inwieweit US-Mutter- oder Tochtergesellschaften auch „Kontrolle" über Daten haben, die von einer mit ihnen verbundenen EU-Gesellschaft innerhalb der EU gespeichert werden, ist nicht abschließend geklärt; dies wurde allerdings in der Vergangenheit offenbar teilweise von US-amerikanischen Gerichten angenommen.[332] Datenverarbeitern in der EU, die auch derartige Zugriffsrisiken umgehen wollen, bleiben möglicherweise nur noch protektionistischere Lösungen: ausschließlich europäische Dienstleister ohne US-Bezug zu nutzen oder sicherzustellen, dass die EU-Töchter von US-Unternehmen keine eigene Kontrolle über die

[326] Gemeinsames Papier des Deutschen Industrie- und Handelskammertags und weiterer Verbände vom 29. September 2020, vgl. https://www.dihk.de/resource/blob/30918/d6be1759e37e7729d53cc28e97563cdf/verbaendepapier-privacy-shield-data.pdf S. 1ff; siehe auch https://www.dihk.de/de/aktuelles-und-presse/aktuelle-informationen/datenverarbeitung-der-wirtschaft-erheblich-blockiert--30922.

[327] Vgl. Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41), S. 11.

[328] Art. 83 Abs. 5 lit.c) DSGVO.

[329] Ebenso https://www.dr-datenschutz.de/bfdi-infoschreiben-zum-internationalen-datentransfer-nach-schrems-ii/.

[330] Gesetz über die Klarstellung der Nutzung von Daten im Ausland (US Clarifying Lawful Overseas Use of Data Act), H.R. 4943, https://www.congress.gov/bill/115th-congress/house-bill/4943/text.

[331] Siehe auch Erwägungsgrund Q und Rn. 27 der Resolution P8_TA(2018)0315 vom 5. Juli 2018 zur Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes des über dieses Gesetz „sehr besorgten" Europäischen Parlaments.

[332] Maxwell, W. / Brennan, M. / Sura, A., Demystifying the U.S. CLOUD Act: Assessing the law's compatibility with international norms and the GDPR, Hogan Lovells, Januar 2019, S. 13, abrufbar unter https://www.hoganlovells.com/en/publications/demystifying-the-us-cloud-act.

gespeicherten Daten haben. Die in den letzten Jahren erprobten, laut Medienberichten aber nicht erfolgreichen[333] Treuhand-Lösungen, bei denen europäische Töchter von US-Unternehmen ihre Rechenzentren von einem Treuhänder betreiben lassen und selbst keinen Zugang zu den Daten haben, könnten nach dem „Schrems II"-Urteil wieder interessanter werden.[334]

Einige Fortschritte gibt es aber dennoch. Nach Medienberichten haben die kalifornischen Staatsbürger im November 2020 im Zuge der US-Präsidentschaftswahlen in einem Volksbegehren dem California Privacy Rights Act 2020 (nachfolgend: „CPRA")[335] zugestimmt.[336] Der CPRA enthält verbraucherschützende Datenschutzvorschriften[337] und ergänzt den am 1.1.2020 in Kraft getretenen California Consumer Privacy Act (CCPA)[338]. Der CPRA schützt in erster Linie die Datenschutzrechte aller kalifornischen Bürger[339] und wird als sehr komplexes und restriktives Datenschutzgesetz bezeichnet.[340] Er gilt für Unternehmen, die in Kalifornien geschäftlich tätig sind und dort Daten erheben. Der CPRA hat damit weltweite Wirkung und muss auch von Unternehmen aus der EU beachtet werden.[341] Anwendbar ist er aber erst auf Unternehmen mit einem Jahresumsatz ab 25 Millionen Dollar oder Unternehmen, die 50 Prozent oder mehr ihres Umsatzes mit der Monetarisierung persönlicher Daten erzielen oder die persönliche Daten von 100.000 oder mehr Verbrauchern oder Haushalten pro Jahr verarbeiten.[342] Der CPRA erweitert die Rechte der Betroffenen und führt erstmalig in den USA eine eigenständige Datenschutzbehörde ein. Mit dem CPRA nähert sich das kalifornische Recht damit der DSGVO an. Nach Einschätzung von Experten bleibt der CPRA aber in vielen Bereichen hinter der DSGVO zurück.[343] Zudem gelten ungeachtet des CPRA die US-Überwachungsgesetze als Bundesgesetze auch in Kalifornien weiter.[344] Daher dürfte es trotz der enormen Verbesserungen im kalifornischen Datenschutz für die Kommission schwierig bleiben, einen Angemessenheitsbeschluss zu erlassen, den die Kommission theoretisch auch auf ein bestimmtes Gebiet beschränken könnte.[345] Ob die Kommission in Zukunft tatsächlich einen Angemessenheitsbeschluss für Kalifornien in Erwägung ziehen wird, bleibt abzuwarten. Insgesamt könnte der CPRA den auch in anderen US-Bundesstaaten zunehmenden Bestrebungen, den Datenschutz zu stärken[346], aber weiteren Aufwind geben.

---

[333] Microsoft stellt "Deutsche Cloud" ein, 3. September 2018, vgl. https://www.spiegel.de/netzwelt/web/deutsche-cloud-microsoft-stellt-vertrieb-seines-datendienstes-ein-a-1226307.html.

[334] Becker, M. 17. August 2020, Digitaler Stacheldraht, abrufbar unter https://www.spiegel.de/netzwelt/netzpolitik/privacy-shield-ende-digitaler-stacheldraht-a-fc64a20a-b428-4fbf-9b74-21c6c3e4469e.

[335] Volltext abrufbar unter https://iapp.org/media/pdf/resource_center/ca_privacy_rights_act_2020_ballot_initiative.pdf.

[336] Dr. Datenschutz, CCPA 2.0 – Das neue kalifornische Datenschutzgesetz, 8. Dezember 2020, abrufbar unter https://www.dr-datenschutz.de/ccpa-2-0-das-neue-kalifornische-datenschutzgesetz/; Determann, L. Datenschutz für das Silikon Valley, 24. November 2020, abrufbar unter https://www.faz.net/aktuell/wirtschaft/california-privacy-rights-act-datenschutz-fuer-das-silicon-valley-17068996.html.

[337] Vgl. im Einzelnen Kohne, M./Reed, N./Kurzweil, R., Akin Gump Strauss Hauer & Feld LLP, Calif. Privacy Law Resembles, Transcends EU Data Regulation, abrufbar unter https://www.lexology.com/library/detail.aspx?g=87c280cf-09f1-406f-81c8-a9bee06c0e82.

[338] Stoll, L. CCPA: Das strengste Datenschutzgesetz der USA, 9. Januar 2020, abrufbar unter https://www.dr-datenschutz.de/ccpa-das-strengste-datenschutzgesetz-der-usa/.

[339] Dr. Datenschutz, CCPA 2.0 – Das neue kalifornische Datenschutzgesetz (Fn. 336).

[340] Determann, L., a.a.O., (Fn. 384).

[341] Determann, L., a.a.O., (Fn. 384).

[342] Dr. Datenschutz, CCPA 2.0 – Das neue kalifornische Datenschutzgesetz (Fn. 336).

[343] Dr. Datenschutz, CCPA 2.0 – Das neue kalifornische Datenschutzgesetz (Fn. 336).

[344] Kohne, M./Reed, N./Kurzweil, R., a.a.O. (Fn. 385).

[345] Art. 45 Abs. 1 DSGVO „ein Gebiet".

[346] Bereits der Erlass des CCPA hat diese Entwicklung beflügelt, vgl. Bracy, J., With the CCPA now in effect, will other states follow?, 2. Januar 2020, abrufbar unter https://iapp.org/news/a/with-the-ccpa-now-in-effect-will-other-states-follow/.

Auf Bundesebene hat der US-Senatsausschuss für Handel, Wissenschaft und Verkehr im Dezember 2020 eine Anhörung[347] über die Zukunft des transatlantischen Datenverkehrs gehalten. Im Rahmen dieser Anhörung soll auch ein umfassendes Bundesdatenschutzgesetz in Erwägung gezogen worden sein. Nicht zuletzt im Hinblick auf den kalifornischen CPRA sollen sich Sprecher optimistisch gezeigt haben, dass im neuen Kongress signifikante Vorschläge in Sachen Datenschutz erzielt werden könnten. Allgemeiner Konsens soll dahingehend geherrscht haben, dass die USA auf ein langfristiges Ziel hinarbeiten müssen, um die zugrundeliegenden nachrichtendienstlichen Probleme anzugehen.[348] Ob es langfristig auch auf US-Bundesebene tatsächlich Fortschritte geben wird, die den Datentransfer in die USA erleichtern werden, bleibt abzuwarten.

4 Sonstige aktuelle Entwicklungen und Ausblick

Wie die vorstehenden Ausführungen zeigen, hat das „Schrems II"-Urteils angesichts seiner großen Bedeutung für den internationale Datentransfer verschiedene Gremien veranlasst, „Hilfestellungen" zu veröffentlichen, wie die vom EuGH aufgestellten Anforderungen umzusetzen und welche ergänzenden Klauseln oder Garantien ggf. denkbar und nötig sind, um ein gleichwertiges Schutzniveau zu schaffen. Auf folgende wichtige Hilfestellungen wurde in Kapitel 3 bereits eingegangen:

- die Orientierungshilfe des LfDI BW[349],
- die Empfehlungen 1/2020[350] und 2/2020[351] des EDSA,
- die Strategie des EDSB zur Umsetzung der Vorgaben des „Schrems II"-Urteils[352], und
- den Entwurf der neuen SDPC durch die Kommission[353].

Auch darüber hinaus hat das Urteil zu zahlreichen Reaktionen geführt. Das vorliegende Kapitel gibt – ohne Anspruch auf Vollständigkeit zu erheben – einen Überblick über die Reaktionen verschiedener deutscher Datenschutzaufsichtsbehörden und über andere wichtige Entwicklungen nach Erlass des Urteils, zieht ein Fazit und unternimmt einen Ausblick auf die Zukunft.

4.1 Reaktionen weiterer deutscher Datenschutzaufsichtsbehörden

Zum „Schrems 2"-Urteil hatten sich neben dem LfDI BW und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)[354] bereits vor den Stellungnahmen des EDSA auch andere deutsche Landesdatenschutzbehörden geäußert, die in Deutschland grundsätzlich für die Datenschutzaufsicht über die Wirtschaft örtlich zuständig sind. Eine Übersicht über die Stellungnahmen ist im

[347] https://www.commerce.senate.gov/2020/12/committee-to-hold-hearing-on-eu-us-privacy-shield-and-the-future-of-transatlantic-data-flows.

[348] Zu den Inhalten des Hearings vgl. Kohne, N./Reed, M./Daly, T. Akin Gump Strauss Hauer & Feld LLP, Senate Commerce Committee Hears Testimony on EU-US Privacy Shield, 10.Dezember 2020, abrufbar unter https://www.akingump.com/en/experience/practices/cybersecurity-privacy-and-data-protection/ag-data-dive/senate-commerce-committee-hears-testimony-on-eu-us-privacy-shield.html#page=1.

[349] Vgl. oben Kapitel 3.1, 3.3.1.1. und 3.3.2.1 (Quelle: Fn. 41).

[350] Vgl. insbesondere oben Kapitel 3.1., 3.2, 3.3 (Quelle: Fn. 6).

[351] Vgl. insbesondere oben Kapitel 3.1 und 3.2.2. (Quelle: Fn. 166).

[352] Vgl. oben Kapitel 3.1., 3.2 (Quelle: Fn. 170).

[353] Vgl. oben Kapitel 3.3.3 (Quelle: Fn. 219).

[354] Dr. Kelber, U., Pressemitteilung des BfDI zum „Schrems II"-Urteil des EuGH vom 16.07.2020, abrufbar unter https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/17_Schrems-II-Urteil.html. Der BfDI hat sich darüber hinaus am 8. Oktober 2020 in einem Informationsschreiben zur Auswirkung des „Schrems II-Urteils" auf den internationalen Datentransfer an die seiner Aufsicht unterliegenden öffentlichen Stellen des Bundes und Telekommunikationsunternehmen gewandt, sich darin jedoch nicht dazu geäußert, welche konkreten Zusatzmaßnahmen in Betracht kommen.

Internet verfügbar.[355] Auch die deutsche Datenschutzkonferenz (nachfolgend: „DSK"), die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, hatte bereits im Juli 2020[356] angekündigt, ihr Vorgehen mit ihren Kollegen im EDSA abzustimmen und zukünftig auch zu spezifischeren Fragestellungen zu beraten. Ebenso haben die Landesdatenschutzbehörden weitere Stellungnahmen angekündigt. Einige von ihnen hatten sich bereits anfänglich sehr kritisch im Hinblick auf fortgesetzte Transfers in unsichere Drittländer geäußert. So sieht der LfDI BW es als die zentrale Frage an, ob es für EU-Unternehmen bei der Auswahl ihrer Dienstleister und sonstigen Vertragspartner „zumutbare" Alternativangebote „ohne Transferproblematik" gäbe. Könne das Unternehmen nicht überzeugend darlegen, dass ein von ihm genutzter „Dienstleister mit Transferproblematik" nicht kurz- und mittelfristig durch einen „zumutbaren Dienstleister ohne Transferproblematik" ersetzt werden kann, werde man den Datentransfer untersagen. Der LfDI BW werde sein Vorgehen aber am Grundsatz der Verhältnismäßigkeit ausrichten.[357] Auch laut der Berliner Beauftragten für den Datenschutz und die Informationsfreiheit sind die Zeiten, in denen personenbezogene Daten „aus Bequemlichkeit oder wegen Kostenersparnissen" in die USA übermittelt werden konnten, nach dem Urteil des EuGH vorbei.[358] Beim Transfer von Daten in andere Staaten wie etwa China oder Russland werde zu prüfen sein, ob dort nicht ähnliche oder gar größere Probleme bestehen. Ähnlich äußert sich der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit. Für den internationalen Datenverkehr zögen schwere Zeiten auf. Die Aufsichtsbehörden stünden nun vor der Entscheidung, insgesamt die Datenübermittlung über SDPC kritisch zu hinterfragen, und zwar auch für andere Drittländer.[359]

Die Reaktionen ausländischer Datenschutzaufsichtsbehörden zum „Schrems II"-Urteil werden aus Platzgründen im Rahmen dieser Studie nicht dargestellt. Eine Übersicht über diese Reaktionen ist im Internet verfügbar.[360]

4.2 Deutsche Datenschutzkonferenz berät über Microsoft-Produkte

Die deutsche Datenschutzkonferenz (DSK) hat sich im November 2020 mit der Frage befasst, inwieweit das Betriebssystem Windows 10 und Microsoft 365 – eine cloudbasierte Programmsuite, die Produkte wie Word, Excel, PowerPoint, die Kommunikationsanwendung Teams sowie den Cloud-Speicher OneDrive umfasst – nach dem „Schrems II"-Urteil überhaupt noch datenschutzkonform nutzbar sind.[361] Problematisch sind dabei u.a. die automatische Übermittlung umfangreicher personenbezogener „Telemetrie-Daten" an Microsoft sowie die Zugriffsmöglichkeit von Microsoft auf in der Cloud gespeicherte Daten.[362] Ein Arbeitskreis der DSK war im Juli 2020 zu dem Ergebnis gekommen, dass ein

---

[355] Eine Übersicht der Stellungnahmen verschiedener Aufsichtsbehörden und internationaler Organisationen zum „Schrems II"-Urteil bietet u.a. die Gesellschaft für Datenschutz und Datensicherheit e.V. unter https://www.gdd.de/eu-us-privacy-shield-schrems-ii-urteil/ansichten-der-aufsichtsbehoerden-eu-us-privacy-shield.

[356] Pressemitteilung der DSK vom 28.07.2020, (Fn. 150), S. 2.

[357] Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41), S. 14.

[358] Pressemitteilung der Berliner Beauftragten für den Datenschutz vom 17. Juli 2020, S. 2, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf.

[359] Pressemitteilung vom 16.07.2020, abrufbar unter https://datenschutz-hamburg.de/pressemitteilungen/2020/07/2020-07-16-eugh-schrems.

[360] Matthiesen, R./Heinzke, P., CMS Deutschland, Schrems II: Reaktionen auf das Urteil und Empfehlungen der Aufsichtsbehörden – Update #16, 14. Dezember 2020, abrufbar unter https://www.cmshs-bloggt.de/tmc/datenschutzrecht/schrems-ii-aufsichtsbehoerde-standardvertragsklausel-scc/.

[361] Pressemitteilung der DSK vom 26.11.2020, abrufbar unter https://www.datenschutzkonferenz-online.de/media/pm/20202711_pm_100_dsk.pdf.

[362] Vgl. dazu etwa Krempl, S, 1.12.2020, Datenschützer: Windows-10-Nutzer bei Telemetrie nicht aus dem Schneider, abrufbar unter https://www.heise.de/news/Datenschuetzer-Windows-10-Nutzer-bei-Telemetrie-nicht-aus-dem-Schneider-4976556.html; Heidrich, J., Datenschutzbehörden erklären den Einsatz von Microsoft 365 für rechtswidrig 23. Oktober

datenschutzgerechter Einsatz von Microsoft 365 nicht möglich sei. Die Ergebnisse der Analyse hat die DSK allerdings noch nicht veröffentlicht.[363] Einige der Behörden bestätigten nun zwar, dass bei Microsoft Office 365 erhebliche datenschutzrechtliche Verbesserungspotenziale bestünden. Die Gesamtbewertung des Arbeitskreises wurde jedoch noch nicht für entscheidungsreif erachtet, da sie zu undifferenziert sei. Die DSK hat zunächst eine Arbeitsgruppe eingesetzt, die einen konstruktiven Dialog mit Microsoft führen soll.[364] Eine gemeinsame Bewertung der Microsoft-Produkte soll aber noch folgen.[365]

4.3 Microsoft stellt „neue Maßnahmen“ zum Datenschutz vor

Als Reaktion auf die Empfehlungen des EDSA hat Microsoft im November 2020 angekündigt, alle Anfragen staatlicher Stellen nach Daten seiner Kunden anzufechten und betroffene Kunden darüber zu informieren – vorausgesetzt, es gibt dafür eine rechtliche Grundlage.[366] Falls die Behörde dennoch auf die Daten europäischer Microsoft-Nutzer zugreift und dies gegen die DSGVO verstößt, will Microsoft die betroffenen Kunden finanziell entschädigen. Dies gilt allerdings nur für Unternehmenskunden und Kunden aus dem öffentlichen Sektor; Privatkunden sind von diesem Schutz ausgenommen. Microsoft behauptet, mit diesen „neuen Maßnahmen“ zum Datenschutz sogar über die gesetzlichen Vorgaben und die Empfehlungen des EDSA hinauszugehen.[367] Dem ist nicht zuzustimmen. Insbesondere ist gerade fraglich, ob im Drittland stets ein rechtlicher Grund zur Anfechtung besteht und diese nach dem anwendbaren Recht tatsächlich Aussicht auf Erfolg hat. Auch nach einer gemeinsamen Bewertung verschiedener deutscher Datenschutzaufsichtsbehörden reichen diese Maßnahmen nicht aus, da eine Ergänzung der Standarddatenschutzklauseln den unverhältnismäßigen Zugriff der US-Behörden auf die Daten nicht unterbinde. Dass Microsoft als einer der größten internationalen Konzerne sich nun in die richtige Richtung bewege, sei aber ein wichtiger und vorbildlicher Schritt.[368]

4.4 Französischer Conseil d’Etat fordert zusätzliche Garantien

In Frankreich hat der französische Conseil d’Etat am 14.10.2020 zusätzliche Garantien im Sinne des „Schrems II“-Urteils für den Weiterbetrieb der im April 2020 ins Leben gerufenen französischen Plattform für Gesundheitsdaten („Health Data Hub“) gefordert, die derzeit von Microsoft gehostet wird. Microsoft müsse zwar wegen des EuGH-Urteils davon absehen, die Daten in die USA zu übertragen. Das Risiko, dass dennoch Daten den US-Behörden auf Anfrage zur Verfügung gestellt werden könnten, könne aber nicht ausgeschlossen werden. Dies rechtfertige angesichts der aktuellen Gesundheitslage zwar nicht die sofortige Schließung der Plattform. Langfristiges Ziel sollte aber die Übertragung der Plattform auf Server in Frankreich oder der EU sein. In der Zwischenzeit sollte der Vertrag mit Microsoft ergänzt und weitere Maßnahmen ergriffen werden, um die Daten besser zu schützen.[369] Die französische Aufsichtsbehörde CNIL solle die Behörden zu entsprechenden Garantien beraten und bei

2020, abrufbar unter https://www.heise.de/news/Datenschutzbehoerden-erklaeren-den-Einsatz-von-Microsoft-365-fuer-rechtswidrig-4931745.html.

[363] Krempl. S., Datenschützer sehen Microsoft 365 in Behörden als nicht rechtskonform an, 14.09.2020, abrufbar unter https://www.heise.de/news/Datenschuetzer-sehen-Microsoft-365-in-Behoerden-als-nicht-rechtskonform-an-4893604.html.

[364] Pressemitteilung verschiedener deutscher Datenschutzaufsichtsbehörden vom 02. Oktober 2020, abrufbar unter https://www.lda.bayern.de/media/pm/20201002_office365.pdf.

[365] Krempl. S., a.a.O. (Fn. 363).

[366] https://news.microsoft.com/de-de/neue-massnahmen-zum-schutz-von-daten/, Weiß, E., Microsoft macht DSGVO-Zugeständnisse, 20.11.2020, s. https://www.heise.de/news/Microsoft-macht-DSGVO-Zugestaendnisse-4966623.html.

[367] Weiß, E., Microsoft macht DSGVO-Zugeständnisse, a.a.O. (Fn. 366).

[368] Pressemitteilung des LfDI BW vom 20. November 2020, #DSGVOwirkt: Microsoft passt sich europäischem Datenschutz S. 3f., abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/11/20201120_PM_MS_Standardvertragsklauseln_Versand.pdf.

[369] https://www.cnil.fr/fr/le-conseil-detat-demande-au-health-data-hub-des-garanties-supplementaires.

Anträgen auf Genehmigung von Forschungsprojekten sicherstellen, dass die Nutzung der Plattform technisch notwendig sei.

4.5 White Paper der US-Regierung

Die US-Regierung hat im September 2020 ein „White Paper“[370] veröffentlicht, das aus ihrer Sicht relevante Informationen zu Recht und Praxis in Bezug auf behördliche Datenzugriffe in den USA auflistet, die für Unternehmen bei der nunmehr vorzunehmenden Analyse des Schutzniveaus von Interesse sein könnten. Eine rechtliche Orientierungshilfe sei damit, so die US-Regierung, allerdings nicht verbunden. In dem Papier kritisiert sie die Einschätzung des Schutzniveaus durch den EuGH. Sie führt u.a. aus, die US-Geheimdienste hätten schlicht kein Interesse an der Mehrheit der Daten, die zwischen Unternehmen übermittelt würden.[371] Zudem profitierten die EU-Mitgliedstaaten davon, dass die USA Daten u.a. zur Terrorismusbekämpfung erhöben und mit ihnen teilten.[372] Ferner gebe es im US-Recht seit 2016 zahlreiche Schutzvorkehrungen und Rechtsbehelfe gegen behördliche Datenzugriffe, die der EuGH nicht berücksichtigt habe. Die Gefahr eines geheimen Zugriffs auf die Daten durch Geheimdienste oder rechtswidrig handelnde private Stellen bestehe weltweit und auch in Europa.[373] Das Schutzniveau sei mit dem in Europa gleichwertig, da es in den EU-Mitgliedstaaten ähnliche oder sogar umfangreichere Überwachungsprogramme gebe.[374]

Es ist fraglich, ob Datenexporteure auf der Basis des White Papers zu einer positiveren Einschätzung des Schutzniveaus in den USA gelangen könnten. Ohne weitere rechtliche Beratung erscheint es aber kaum nachvollziehbar, inwieweit die aufgeführten Rechtsbehelfe und Schutzvorkehrungen im konkreten Fall tatsächlich greifen, ob sie im Verfahren tatsächlich nicht berücksichtigt wurden und ob der durch sie geschaffene Schutzstandard demjenigen in der EU tatsächlich gleichwertig ist. Insoweit wäre eine Unterstützung durch die EU-Aufsichtsbehörden bei der Einschätzung der aktuellen Rechtslage wünschenswert. Gegen das Argument, dass die Gefahr eines behördlichen Datenzugriffs eher theoretisch sei, lassen sich die oben genannten Argumente vorbringen.[375] Auch der EuGH hat die bloße Möglichkeit eines Zugriffs ausreichen lassen, um einen ungerechtfertigten Eingriff anzunehmen.[376] Zudem weicht die Beurteilung, welche Eingriffe verhältnismäßig sind, im US-Recht von derjenigen nach EU-Recht ab. Schließlich hat der EuGH auch die Massenüberwachung in der EU massiv beschränkt.[377] Dennoch sind hier die weiteren Entwicklungen abzuwarten.

4.6 Fortgang des Schrems-Verfahrens

Der Fortgang des irischen Schrems-Verfahrens beeinflusst möglicherweise das weitere Vorgehen der EU-Datenschutzbehörden. Untersagt die irische Datenschutzbehörde aufgrund des „Schrems II“-Urteils die Datentransfers – und wird dies als von den Gerichten als rechtmäßig erachtet –, könnten Datenschutzbehörden in anderen Mitgliedstaaten nachziehen und in gleich gelagerten Verfahren ähnlich entscheiden. Dies hätte große Konsequenzen für die betroffenen Unternehmen, da deren Datentransfers dadurch ggf. massiv eingeschränkt würden. Das Beschwerdeverfahren dauert bereits seit sieben Jahren an. Laut Medienberichten hat die irische Behörde Facebook Ende August 2020 über ihre

[370] https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.
[371] White Paper der US-Regierung (Fn. 370), S. 1f.
[372] Dies diene wichtigen öffentlichen Interessen der EU-Mitgliedstaaten und schütze Regierungen und Menschen in der EU.
[373] White Paper der US-Regierung (Fn. 370), S. 3, 17f.
[374] White Paper der US-Regierung (Fn. 370), S. 15.
[375] Vgl. oben Kapitel 3.3.1.3 a.E.
[376] EuGH, Rs. C-311/18 - Schrems II (Fn. 2), Rn. 183.
[377] Siehe das Urteil in der Rechtssache C-623/17 (Privacy International, Fußnote 161). Näher dazu oben Kapitel 2.5.

Vorentscheidung informiert, Facebooks Datentransfers in die USA stoppen zu wollen, und dem Unternehmen Gelegenheit zur Stellungnahme gegeben.[378] Facebook hat die gerichtliche Überprüfung dieser Vorentscheidung beantragt; zudem wird das Verfahren derzeit durch ein Parallelverfahren weiter verkompliziert. Die irische Datenschutzbehörde hat offenbar aus eigenem Antrieb neben dem eigentlichen Verfahren eine separate – über das Schrems-Verfahren hinausgehende – Untersuchung von Facebooks Datentransfers eingeleitet, gegen die sich aus unterschiedlichen Gründen sowohl Facebook als auch Schrems[379] wendeten. Schrems bezweckte damit einen zügigen Abschluss des eigentlichen Verfahrens zu erreichen.[380] Die irische Behörde hat laut Medienberichten Mitte Januar 2021 vor dem Commercial Court zugestimmt, nunmehr eine rasche Entscheidung über Schrems' Beschwerde treffen und die geplante zweite Untersuchung getrennt von Schrems' Verfahren durchführen zu wollen; im Gegenzug lässt Schrems seinen Rechtsbehelf gegen Behörde wegen der Untersuchung fallen.[381] Die Rechtsmittelverfahren von Facebook gegen die Vorentscheidung und die Einleitung der separaten Untersuchung dauern an. Die irische Behörde kann die Entscheidung des High Court abwarten, bevor sie endgültig über Schrems' Beschwerde entscheidet.[382] Es könnte daher noch immer etwas dauern, bis der „Präzedenzfall" Schrems gegen Facebook abgeschlossen ist.

4.7 Unternehmen drohen Beschwerden durch Datenschutz-Aktivisten

Unternehmen müssen nach dem „Schrems II"-Urteil auch vermehrt mit Beschwerden gegen ihre Datenübermittlungspraktiken rechnen. Laut Medienberichten[383] hat der Datenschutz-Aktivist und Verfahrensbeteiligte Maximilian Schrems über die von ihm gegründete Datenschutzorganisation „noyb" nach dem „Schrems II"-Urteil identische Beschwerden gegen eine Vielzahl europäischer Unternehmen bei nationalen Datenschutzbehörden eingelegt. Die Beschwerden richten sich dagegen, dass die Unternehmen gegen das Urteil verstoßen, indem sie auf ihren Webseiten weiterhin – aus Sicht der Organisation nicht notwendige – Tracking-Verfahren verwenden, durch welche Nutzerdaten ohne hinreichende Rechtsgrundlage in die USA übertragen würden. Die Datenschutzbehörden müssen nun über diese Beschwerden entscheiden. Der EDSA hat auch hierzu eine „Taskforce" eingesetzt, die sich mit den Beschwerden befassen und deren schnelle und europaweit einheitliche Bearbeitung gewährleisten soll.[384]

---

[378] Schechner, S./Glazer, E., Ireland to Order Facebook to Stop Sending User Data to U.S., 9. September 2020, abrufbar unter https://www.wsj.com/articles/ireland-to-order-facebook-to-stop-sending-user-data-to-u-s-11599671980?mtc=j.

[379] Schrems geht über die von ihm ins Leben gerufene Datenschutzorganisation „noyb" gegen diese Untersuchung vor.

[380] Laut Medienberichten hatte Facebook gegen die Ankündigung der irischen Datenschutzbehörde in ihrer „preliminary draft decision", die Datentransfers in die USA stoppen zu wollen, einen „judicial review" durch den High Court beantragt. Zu alldem vgl. Irish Times https://www.irishtimes.com/business/technology/facebook-to-challenge-dpc-decision-on-data-transfers-1.4354833, https://www.irishtimes.com/business/technology/inquiry-into-facebook-s-transfer-of-data-challenged-by-max-schrems-1.4378996, Reuters https://uk.reuters.com/article/uk-facebook-privacy/irish-high-court-freezes-probe-into-facebooks-eu-u-s-data-flows-idUKKBN2652FA und noyb, https://noyb.eu/de/irischer-high-court-gerichtliche-ueberpruefung-gegen-dpc-zugelassen sowie die Pressemitteilung der irischen Datenschutzbeauftragten vom 3. Dezember 2020, abrufbar unter https://www.dataprotection.ie/en/news-media/press-releases/eu-us-data-transfers-judicial-review-proceedings.

[381] Burke-Kennedy, E., DPC welcomes Schrems decision to drop legal case, 14. Januar 2021, abrufbar unter https://www.irishtimes.com/business/technology/dpc-welcomes-schrems-decision-to-drop-legal-case-1.4458656; Scally, D., Schrems criticizes Irish data regulator after Facebook case breakthrough, 13. Januar 2021, abrufbar unter https://www.irishtimes.com/business/technology/schrems-criticises-irish-data-regulator-after-facebook-case-breakthrough-1.4457728, sowie https://noyb.eu/de/irische-behoerde-gibt-klage-nach-und-will-nun-zuegig-zu-facebooks-eu-us-datenuebermittlungen.

[382] https://noyb.eu/de/irische-behoerde-gibt-klage-nach-und-will-nun-zuegig-zu-facebooks-eu-us-datenuebermittlungen.

[383] https://www.heise.de/news/Privacy-Shield-Schrems-reicht-101-Beschwerden-wegen-Datentransfers-ein-4873333.html.

[384] https://edpb.europa.eu/news/news/2020/european-data-protection-board-thirty-seventh-plenary-session-guidelines-controller_de sowie https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/22_Neue-Task-Force-EDSA.html.

4.8 „Privacy Shield 2.0“?

Die EU-Kommission und das US-Handelsministerium führen derzeit Gespräche, um das Potenzial für einen „verbesserten“ – nach „Safe Harbour“ und „Privacy Shield“ dann dritten – Angemessenheitsbeschluss „Privacy Shield 2.0“ auszuloten[385], der von Wirtschaftsverbänden gefordert wird.[386] Solange die USA ihre Überwachungspraktiken nicht auf das erforderliche Maß reduzieren und EU-Bürgern durchsetzbare Rechte und wirksame Rechtsbehelfe gewähren, wird dieses Vorgehen allerdings langfristig nicht von Erfolg gekrönt sein. Es ist nicht ersichtlich, wie die Kommission unter den vom EuGH aufgestellten Voraussetzungen ohne Anpassungen des US-Rechts zu einer Angemessenheitsfeststellung gelangen könnte. Die Kommission sollte davon absehen, erneut einen wackligen Angemessenheitsbeschluss zu fassen, nur um den von transnationalen Datenübermittlungen abhängigen Handel vorübergehend – bis zur nächsten Aufhebung durch den EuGH – zu beruhigen. Entsprechend hat EU-Justizkommissar Reynders einen „quick fix“ auch bereits ausdrücklich ausgeschlossen. Erforderlich sei eine nachhaltige, rechtssichere Lösung, die mit dem Urteil des EuGH voll im Einklang stehe. [387]

Der US-Senatsausschuss für Handel, Wissenschaft und Verkehr hat im Dezember 2020 eine Anhörung[388] über die Zukunft des transatlantischen Datenverkehrs gehalten. Im Rahmen dieser Anhörung soll u.a. die Notwendigkeit betont worden sein, vor dem 20. Januar ein kurzfristiges – z.B. für ein Jahr geltendes – Abkommen mit der EU auszuhandeln. Angesprochen wurde offenbar auch, dass untersucht werden müsse, wie ein umfassendes Bundesdatenschutzgesetz die Entwicklung eines Nachfolge-Transferinstruments erleichtern könnte. Nicht zuletzt im Hinblick auf den kalifornischen CPRA[389] sollen sich Sprecher optimistisch gezeigt haben, dass im neuen Kongress signifikante Fortschritte in Sachen Datenschutz erzielt werden könnten. Allgemeiner Konsens habe dahingehend geherrscht, dass die USA auf ein langfristiges Ziel hinarbeiten müssen, um die relevanten nachrichtendienstlichen Probleme anzugehen.[390] Ob es tatsächlich auch auf US-Bundesebene zu Verbesserungen des Datenschutzes kommen wird, die den Abschluss eines „Privacy Shield 2.0“ erleichtern, bleibt abzuwarten.

4.9 Fazit und Ausblick

Die Rechtslage nach dem „Schrems II“-Urteil bleibt unklar. Die hohen Anforderungen an den Datenschutz in der EU und die derzeitige Lebenswirklichkeit und Transferpraxis in der Wirtschaft fallen auseinander und es ist fraglich, wie beide miteinander in Einklang gebracht werden können. Unternehmen, die Daten in Drittländer übermitteln, müssen sich auf komplizierte Einzelfallanalysen des ausländischen Rechts einlassen. Der Datentransfer an Unternehmen, die den US-Überwachungsgesetzen unterliegen, ist nach dem „Schrems II“-Urteil rechtlich nur noch sehr eingeschränkt zulässig, obwohl viele

---

[385] Gemeinsame Presseerklärung von EU-Justizkommissar Reynders und U.S. Secretary of Commerce Ross vom 10.08.2020, abrufbar unter https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=684836, vgl. auch https://www.heise.de/news/EU-Kommission-verhandelt-zu-neuem-Privacy-Shield-4876922.html.

[386] Gemeinsames Papier des Deutschen Industrie- und Handelskammertags und weiterer Verbände (Fn. 374), S. 2.

[387] https://www.euractiv.com/section/data-protection/news/dont-expect-new-eu-us-data-transfer-deal-anytime-soon-reynders-says/?utm_source=EURACTIV&utm_campaign=f5a0b57faf-digital_brief_COPY_01&utm_medium=email&utm_term=0_c59e2fd7a9-f5a0b57faf-116255475.

[388] https://www.commerce.senate.gov/2020/12/committee-to-hold-hearing-on-eu-us-privacy-shield-and-the-future-of-transatlantic-data-flows, vgl. dazu auch Hengesbaugh, B., Privacy Shield 2.0 would be a win/win, 8. Dezember 2020, abrufbar unter https://www.lexology.com/library/detail.aspx?g=fbe6e1e9-56cc-4e44-8b0d-5221cf3fc802.

[389] Hierzu vgl. oben Kapitel 3.3.4.

[390] Zu den dargestellten Inhalten des Hearings vgl. Kohne, N./Reed, M./Daly, T. Akin Gump Strauss Hauer & Feld LLP, Senate Commerce Committee Hears Testimony on EU-US Privacy Shield, 10. Dezember 2020, abrufbar unter https://www.akingump.com/en/experience/practices/cybersecurity-privacy-and-data-protection/ag-data-dive/senate-commerce-committee-hears-testimony-on-eu-us-privacy-shield.html#page=1.

US-Anbieter zentral in Datenverarbeitungen von EU-Unternehmen eingebunden sind. Eine echte Lösung dieses Dilemmas[391] ist nicht in Sicht: auch die Entwürfe der Empfehlungen des EDSA und der geänderten SDPC der Kommission bieten derzeit keine rechtssichere „Patentlösungen" oder zeigen solche auf. Auch wenn insbesondere im kalifornischen Datenschutzrecht bestimmte Fortschritte zu verzeichnen sind, ist nicht davon auszugehen, dass das Schutzniveau in den USA oder bestimmten US-Bundesstaaten in naher Zukunft als gleichwertig angesehen werden kann. Unternehmen werden daher möglicherweise versuchen, so weit wie möglich auf Ausnahmetatbestände für Datenübermittlungen auszuweichen. Diese wurden bislang allerdings als wenig geeignet erachtet, um die Masse der alltäglichen Datentransfers zu rechtfertigen. Es bleibt zu hoffen, dass die Datenexporteure nicht dazu übergehen werden, die weggefallenen bzw. unsicheren Rechtsgrundlagen für den Datentransfer großflächig durch Einwilligungslösungen zu ersetzen, indem sie die Betroffenen um Erteilung ihrer Einwilligung in die Datenübermittlungen bitten. Dies gilt umso mehr, wenn denjenigen, die den Dienst nutzen wollen, dabei faktisch keine andere Wahl gelassen wird, als einzuwilligen. Denn an eine wirksame Einwilligung sind zwar hohe Anforderungen zu stellen. Im Ergebnis dürfte diese Lösung den Betroffenen aber weniger Schutz ihrer persönlichen Daten bieten als die SDPC und der aufgehobene „Privacy Shield".

Der vollständige Verzicht auf Datentransfers in die USA dürfte zumindest kurzfristig nicht allen EU-Unternehmen ohne weiteres möglich sein. Datenexporteure, die rechtswidrige Datentransfers nicht einstellen wollen oder können, verstoßen gegen die DSGVO und riskieren damit hohe Strafen: die DSGVO[392] sieht für Verstöße gegen die Vorschriften über die internationale Datenübermittlung grundsätzlich Bußgelder bis zu 20 Millionen Euro oder bis zu 4% des weltweiten Vorjahresumsatzes vor. Wie die Datenschutzaufsichtsbehörden mit diesem Konflikt der Unternehmen umgehen und ob sie Milde walten lassen können und werden, wenn es im Einzelfall an zumutbaren Alternativlösungen fehlt oder eine Umstellung auf solche Lösungen Zeit braucht, ist noch offen.[393]

Ungeachtet der dargestellten Probleme für viele Unternehmen bietet sich aber mit dieser Krise zumindest langfristig die Chance, in der EU qualitativ hochwertige Datenverarbeitungs- und -auswertungsdienste als Ausweichlösung zu etablieren und die Schaffung sicherer Clouds voranzutreiben. Dass die Wirtschaftsminister von Deutschland und Frankreich nun mit Gaia-X eine erste europäische Cloud auf den Weg bringen[394], ist ein guter Schritt in diese Richtung.[395] Aus wirtschaftlicher Sicht wäre es zudem für die EU kein Nachteil, wenn Tochtergesellschaften von US-Unternehmen sich durch das Urteil gezwungen sähen, ihre Daten in der EU zu speichern, anstatt sie durch ihre Muttergesellschaft in den USA verarbeiten zu lassen. Es müsste jedoch sichergestellt werden, dass die Daten in dieser Cloud tatsächlich wie geplant[396] vor ungerechtfertigten Zugriffen ausländischer Behörden geschützt sind.

---

391 Ebenso das Papier des Deutschen Industrie- und Handelskammertags und weiterer Verbände (Fn. 374), S. 2.

392 Art. 83 Abs. 5 lit.c) DSGVO.

393 Vgl. dazu bereits Kapitel 3.3.4.

394 Bauchmüller, M., Eine Cloud für Europa, 4. Juni 2020, abrufbar unter https://www.sueddeutsche.de/wirtschaft/gaia-x-eine-cloud-fuer-europa-1.4926831.

395 Ebenso https://www.dr-datenschutz.de/das-us-datenschutzniveau-als-problem-beim-cloud-computing/.

396 Dazu Voss, O., Cloud-Initiative Gaia-X: Wie das europäische Projekt die US-Dominanz bei Clouds beenden soll, 5. Juni 2020, abrufbar unter https://www.tagesspiegel.de/wirtschaft/cloud-initiative-gaia-x-wie-das-europaeische-projekt-die-us-dominanz-bei-clouds-beenden-soll/25888628.html.

5 Zusammenfassung

Das EU-Datenschutzrecht lässt den Transfer personenbezogener Daten in ein Drittland außerhalb des Europäischen Wirtschaftsraums (EWR) für wirtschaftliche Zwecke – sofern wie in der Mehrzahl der Fälle keine Einwilligung oder ein sonstiger Ausnahmefall vorliegt – nur dann zu, wenn die übermittelten Daten im Drittland im Wesentlichen gleichwertig wie in der EU geschützt sind. Die Kommission kann dies mit einem **Angemessenheitsbeschluss** wie dem „Privacy Shield" für die USA feststellen. Ohne Angemessenheitsbeschluss dürfen verantwortliche Stellen oder Auftragsverarbeiter in der EU („Datenexporteure") Daten in Drittländer übermitteln, wenn sie geeignete Garantien vorsehen – z.B. durch vertragliche Vereinbarung von **Standarddatenschutzklauseln (SDPC)** mit dem Datenempfänger im Drittland – und den Betroffenen, deren Daten übermittelt werden, durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

Der Europäische Gerichtshof (EuGH) hat im „Schrems II"-Urteil den **„Privacy Shield"-Beschluss** für **ungültig** erklärt. Er hielt das Schutzniveau für die übermittelten Daten, das die USA im Rahmen des „Privacy Shield" gewährleisteten, dem in der EU durch Datenschutzgrundverordnung (DSGVO) und Grundrechtecharta (GRCh) garantierten Niveau nicht für im Wesentlichen gleichwertig. Denn auch unter dem „Privacy Shield" blieben Massenüberwachungen durch US-Behörden möglich. Zu Recht befand der EuGH, dass die US-Überwachungsprogramme nicht auf das zwingend erforderliche Maß beschränkt seien und daher ein unverhältnismäßiger Eingriff in die Grundrechte der Betroffenen auf Privatsphäre und Datenschutz vorliege. Außerdem bestehe für EU-Bürger bei solchen Überwachungsmaßnahmen in den USA kein hinreichender Rechtsschutz, um Zugang zu ihren Daten oder deren Berichtigung oder Löschung zu erwirken. Auch den Ombudsperson-Rechtsbehelf hat der EuGH zu Recht für unzureichend erachtet, weil die Ombudsperson in den USA weder unabhängig sei noch verbindliche Entscheidungen gegenüber Behörden treffen könne. Datentransfers in die USA dürfen daher nicht länger auf den „Privacy Shield", sondern müssen auf eine andere Rechtsgrundlage gestützt oder gestoppt werden.

Gegenstand des „Schrems II-Urteils" waren zudem die von Facebook genutzten SDPC für Auftragsverarbeiter auf der Grundlage eines SDPC-Beschlusses der Kommission aus dem Jahr 2010 und damit ein weiteres Hauptinstrument für internationale Datentransfers. Zu Recht ist der EuGH von der **Gültigkeit des SDPC-Beschlusses** ausgegangen. Die SDPC können daher grundsätzlich weiterhin als Transferinstrument verwendet werden. Der EuGH hat aber klargestellt, dass es in diesem Fall in erster Linie Aufgabe und Verantwortung des Datenexporteurs ist, durch „geeignete Garantien" **ein „im Wesentlichen gleichwertiges" Schutzniveau** für die übermittelten Daten wie die DSGVO und die GRCh zu gewährleisten. Hierzu muss der Datenexporteur gemeinsam mit dem Datenempfänger prüfen, ob das Recht des Drittlandes und die SDPC in ihrer Kombination einen solchen Schutz gewährleisten, und dieser Schutz auch durchsetzbare Rechte und wirksame Rechtsbehelfe umfasst. Darüber hinaus muss der Datenexporteur sich vergewissern, ob das Recht im Drittland es dem Empfänger erlaubt, die SDPC auch einzuhalten. Es genügt daher nicht, SDPC nur zu unterzeichnen. Vielmehr muss der Datenexporteur das Schutzniveau „in jedem Einzelfall" prüfen. Für Datenexporteure dürfte mit der Nutzung von SDPC damit ein weitaus größerer Aufwand verbunden sein, als ihn viele Unternehmen bislang betrieben haben.

Wie der EuGH erstmals festgestellt hat, reichen SDPC in bestimmten Fällen nicht aus, um das nötige Schutzniveau zu gewährleisten. So bieten SDPC laut EuGH möglicherweise dann keinen effektiven Schutz, wenn das Recht des Drittlands dortigen Behörden Eingriffe in die Datenschutzrechte der Betroffenen erlaubt. Gelangt der Datenexporteur zu der Erkenntnis, dass die SDPC nicht ausreichen, muss

er die in den **SDPC** enthaltenen Garantien **durch zusätzliche Vertragsklauseln oder andere Maßnahmen ergänzen**, um einen im Wesentlichen gleichwertigen Schutz sicherzustellen. Ist ihm dies nicht möglich, muss er – oder in zweiter Linie die zuständige Aufsichtsbehörde – die Datenübermittlung stoppen. Letzteres ist laut EuGH der Fall, wenn das Recht des Drittlands dem Datenempfänger Verpflichtungen auferlegt, die den SDPC widersprechen und deren Garantie untergraben. Ein Widerspruch zu den SDPC liege aber nur vor, wenn die Verpflichtungen des Datenempfängers im Drittland über das hinausgingen, was in einer demokratischen Gesellschaft erforderlich sei, um bestimmte elementare Ziele wie die öffentliche Sicherheit zu gewährleisten. Es liegt nahe, dass dies aus Sicht des EuGH bei den Zugriffsbefugnissen der US-Behörden unter den US-Überwachungsgesetzen der Fall ist. Der Datenexporteur müsste damit Transfers an Empfänger stoppen, die den US-Überwachungsgesetzen unterliegen. Das Urteil dürfte allerdings so zu verstehen sein, dass diese Pflicht ausnahmsweise entfällt, wenn der erforderliche Datenschutz im Einzelfall mit anderen Mitteln doch noch gewährleistet werden kann.

Problematisch sind daher Transfers, bei denen ein Unternehmen oder ein von ihm genutzter Auftragsverarbeiter Daten von Kunden, Nutzern oder Beschäftigten in der EU an Empfänger übermitteln, die in den Anwendungsbereich der US-Überwachungsgesetze fallen. Die **EU-Datenschutzaufsichtsbehörden sollten Hilfestellung bei der Auslegung geben**, welche konkreten Datentransfers an welche Datenempfänger unter die **US-Überwachungsgesetze** fallen.

Die Ausführungen des EuGH zu den SDPC lassen sich **auf andere Transferinstrumente wie** verbindliche unternehmensinterne Datenschutzregeln (**BCR**) **übertragen**. Auch hier müssen Datenexporteur und -empfänger im Einzelfall das Bestehen eines gleichwertigen Schutzniveaus prüfen und verbliebene Mängel durch ergänzende Maßnahmen ausgleichen, oder die Transfers stoppen. Weil auch diese Instrumente die Behörden im Drittland nicht binden, können auch ihre Garantien durch das Drittlandsrecht konterkariert werden. Auch Transferinstrumente wie BCR bieten damit für Datentransfers an Empfänger, die den US-Überwachungsgesetzen unterliegen, keine rechtssichere Lösung mehr.

Entsprechende Überwachungsgesetze, die mit den SDPC kollidieren, können zudem auch in **anderen Drittländern** bestehen. Das „Schrems II"-Urteil strahlt daher indirekt auch auf Datentransfers in andere Drittländer aus, für die kein Angemessenheitsbeschluss besteht. Auch hier werden Datenexporteure das Schutzniveau prüfen und festgestellte Mängel durch ergänzende Garantien ausgleichen müssen. Dies wäre grundsätzlich seit dem 01.01.2021 auch bei Datenübermittlungen ins Vereinigte Königreich erforderlich. Die EU und das Vereinigte Königreich haben sich aber kurz vor dem Jahreswechsel in ihrem Handels- und Kooperationsabkommen darauf geeinigt, dass die Übermittlung personenbezogener Daten aus der EU an das Vereinigte Königreich unter bestimmten Voraussetzungen während einer Übergangszeit bis voraussichtlich mindestens Ende April 2021 – die sich ggf. um zwei weitere Monate verlängert – nicht als Übermittlung an ein Drittland gilt. Datentransfers in das Vereinigte Königreich sind damit vorerst weiterhin unter den bisherigen Voraussetzungen möglich und müssen (noch) nicht auf Ausnahmeregeln oder SDPC oder ein sonstiges Transferinstrument gestützt werden. Die Übergangszeit endet u.a. dann vorzeitig, wenn die Kommission einen Angemessenheitsbeschluss für das Vereinigte Königreich erlässt. Einen solchen Beschluss hat die Kommission für das Vereinigte Königreich bislang nicht erlassen. Angesichts der vom EuGH im vergangenen Jahr als unverhältnismäßig erachteten Pflichten dortiger Anbieter elektronischer Kommunikationsdienste, Daten an die britischen Sicherheitsdienste weiterzugeben, dürfte der Erlass eines rechtssicheren Angemessenheitsbeschlusses allerdings schwierig sein. Auch bestehende Angemessenheitsbeschlüsse für andere Drittländer müssen nun von der Kommission kritisch daraufhin überprüft werden, ob sie die vom EuGH aufgestellten Anforderungen erfüllen.

Wie die Prüfung des Schutzniveaus im Drittland im Einzelnen zu erfolgen hat und wann SDPC durch welche zusätzlichen Garantien SDPC effektiv ergänzt werden können, lässt der EuGH offen. Dies hat zu **Rechtsunsicherheit** und zu der Bitte um Hilfe durch die Datenschutzaufsichtsbehörden geführt.

Der **Europäische Datenschutzausschuss (EDSA)** hat im November 2020 die **Entwurfsfassungen zweier Empfehlungen** veröffentlicht, in denen er auf diese Fragen eingeht. Zuvor hatte bereits der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW) spezifische **Ergänzungen der SDPC vorgeschlagen**. Für Datentransfers von EU-Organen hat der Europäische Datenschutzbeauftragte (EDSB) ebenfalls eine erste Strategie entwickelt.

Der EDSA geht davon aus, dass der Datenexporteur bei der Prüfung des Schutzniveaus im Drittland die **gesamten Umstände des spezifischen Datentransfers** wie den Zweck des Transfers, die beteiligten Akteure, die Kategorien und das Format der übermittelten Daten **berücksichtigen** muss, also etwa ob die Daten im Klartext oder verschlüsselt übermittelt werden. Die hierfür nötigen Informationen soll er sich vom Datenimporteur oder aus anderen Quellen beschaffen. Auf subjektive Erwägungen, etwa eine geringe Wahrscheinlichkeit tatsächlicher ungerechtfertigter Zugriffe, soll sich der Datenexporteur hingegen – so der EDSA ausdrücklich – nicht stützen dürfen. Ist der Datenempfänger nach dem Recht des Drittlands verpflichtet, nationalen Behörden Zugriff auf Daten zu gewähren oder Daten offenzulegen, muss der Datenexporteur in einem zweiten Schritt prüfen, ob die damit verbundenen **Eingriffe** in die Datenschutzrechte der Betroffenen **gerechtfertigt** sind. Dies kann er unter Heranziehung der vom EDSA in der zweiten Empfehlung festgelegten vier „**wesentlichen Europäischen Garantien**“ feststellen. Diese sind gewahrt, wenn (1) die Überwachungsmaßnahmen im Drittland auf klaren Regeln für die Datenverarbeitung beruhen, (2) Eingriffe erforderlich und angemessen sind und (3) eine unabhängige Aufsicht und (4) wirksame Rechtsbehelfe existieren. Sind diese Garantien eingehalten, gehen die Eingriffe durch die Überwachungsmaßnahmen nicht über das in einer demokratischen Gesellschaft Notwendige und Verhältnismäßige hinaus und sind daher gerechtfertigt. SDPC können in diesen Fällen einen gleichwertigen Schutz bieten. Halten die Überwachungsmaßnahmen im Drittland diese Garantien dagegen nicht ein, werden durch die ungerechtfertigten Eingriffe die in den SDPC liegenden Garantien in der Regel konterkariert und es fehlt an einem im Wesentlichen gleichwertigen Schutzniveau. Angesichts der hohen Anforderungen ist allerdings fraglich, ob die Garantien überhaupt von einer nennenswerten Anzahl anderer Drittländer erfüllt werden können. Die USA erfüllen diese Garantien derzeit in Bezug auf ihre Überwachungsmaßnahmen nicht. Ein Überblick über die Prüfpflichten bei der Verwendung von SDPC findet sich in *Anhang 1.*

Kommt der Datenexporteur zu dem Ergebnis, dass die SDPC keinen gleichwertigen Schutz bieten, muss er prüfen, ob er das Schutzniveau durch **ergänzende Schutzmaßnahmen** weiter aufstocken kann. Hierzu schlagen EDSA und LfDI BW zusätzliche technische, vertragliche und organisatorische Maßnahmen vor. Gehen allerdings – wie in den USA – die Zugriffsbefugnisse im Drittland über das nach EU-Maßstab Notwendige und Verhältnismäßige hinaus, können aus Sicht des EDSA selbst **technische Maßnahmen** wie eine Anonymisierung, Verschlüsselung, Pseudonymisierung oder Aufspaltung der Daten die Schutzlücken **nur unter engen Voraussetzungen** schließen: die Daten müssen so gut geschützt bzw. verschlüsselt werden, dass selbst der Datenempfänger sie nicht entschlüsseln, nicht de-pseudonymisieren oder aufgespaltene Daten nicht einseitig rekonstruieren kann. Möglich ist dies nur, wenn der Datenempfänger im Drittland keinerlei Zugriff auf den Klartext der Daten hat bzw. die Daten nicht entschlüsseln oder de-pseudonymisieren muss, um sie zu verarbeiten. Nur dann können die vorgeschlagenen technischen Maßnahmen einen behördlichen Zugriff und damit verbundene Eingriffe in die Rechte der Betroffenen wirksam verhindern und damit das Schutzniveau hinreichend aufstocken.

Dies kommt jedoch aus der Sicht des EDSA **nur in wenigen Fallkonstellationen** in Betracht, etwa beim reinen Transit verschlüsselter Daten durch ein Drittland oder wenn Daten dort ausschließlich zu Sicherungszwecken gespeichert werden. Ist der Datenempfänger hingegen im Besitz des Schlüssels, bietet auch eine Verschlüsselung der Daten laut dem EDSA keinen hinreichenden Schutz, da der Empfänger zur Übergabe des Schlüssels an die Behörden verpflichtet sein könnte – es sei denn, er ist als Berufsgeheimnisträger hiervon befreit. Eine Verschlüsselung hilft auch dann nicht weiter, wenn sie durch das Drittland verboten oder durch Hintertüren in der Verschlüsselungssoftware umgangen wird. Die Schaffung derartiger Hintertüren zur Bekämpfung von Terrorismus oder schwerer Kriminalität wird derzeit von verschiedenen internationale Geheimdiensten gefordert und auch vom Rat der EU und der Kommission befürwortet. Technologieunternehmen könnten sich daher veranlasst sehen oder sogar verpflichtet werden, in verschlüsselte Kommunikationssoftware Hintertüren einzubauen. Da solche Hintertüren auch von ausländischen Geheimdiensten genutzt oder geknackt werden könnten, ist äußerst fraglich, ob Verschlüsselung künftig noch als zusätzliche Garantie für Datenübermittlungen in unsichere Drittländer dienen kann. Auch eine Pseudonymisierung, bei der ausschließlich der Datenexporteur die Daten de-pseudonymisieren kann, ist schwierig umzusetzen, zumal die Behörden im Drittland die Daten ggf. auch mit Informationen kombinieren könnten, die sich bereits in ihrem Besitz befinden.

In der Praxis benötigen Datenempfänger aber wohl in der Mehrzahl der Fälle **Zugriff auf die Daten im Klartext**, können diese also nicht verschlüsselt, anonymisiert oder pseudonymisiert verarbeiten. Problematisch sind daher u.a. Datenübermittlungen an Anbieter von Cloud-Diensten oder innerhalb einer Unternehmensgruppe zur Erbringung von Personaldienstleistungen. Da technische Lösungen insoweit **keinen effektiven Schutz** versprechen, sind nach Ansicht des EDSA folglich alle Übermittlungen an Empfänger, die den US-Überwachungsgesetzen unterliegen und die Verarbeitung von Klardaten durch den Empfänger zum Zweck haben, konkret von der **Unzulässigkeit** bedroht. Konsequenter Weise muss der Datenexporteur in diesen Fällen die Transfers stoppen.

Welche konkreten Datentransfers an welche Datenempfänger unter die **US-Überwachungsgesetze** fallen, hängt von deren Auslegung ab. Section 702 FISA gilt für Telekommunikationsbetreiber und Anbieter elektronischer Kommunikationsdienste. Erfasst sein dürften auch Übermittlungen an US-Unternehmen, die selbst nicht unter diese Definition fallen, aber einen davon erfassten Dienstleister einsetzen, was vermutlich viele US-Unternehmen tun. Der EDSA sollte Hilfestellung bei der Auslegung geben, welche Datentransfers an welche Empfänger konkret betroffen sind.

Neben technischen Maßnahmen werden von den Aufsichtsbehörden auch **vertragliche Maßnahmen** wie verschärfte vertragliche Informations-, Transparenz-, Handlungs- und Schadensersatzpflichten und **organisatorische Maßnahmen** wie die Einführung interner Richtlinien vorgeschlagen. Der EDSA geht aber zu Recht davon aus, dass in den Fällen, in denen das Recht im Drittland dem Empfänger Verpflichtungen auferlegt, die die vertraglichen Garantien untergraben, zusätzliche vertragliche und organisatorische Garantien **allein nicht ausreichend** sind. Auch ergänzende Vertragsklauseln und interne Maßnahmen können weder die US-Behörden binden noch einen effektiven Rechtsbehelf für EU-Bürger schaffen. Insbesondere schafft die vertragliche Verpflichtung des Datenempfängers, Rechtsbehelfe gegen Überwachungsmaßnahmen einzulegen, nach Ansicht des cep keinen solchen Rechtsbehelf. Erweiterte Informations- und Transparenzpflichten können dem Datenexporteur zwar helfen, bei drohendem Zugriff schneller zu reagieren, lösen aber nicht das Grundproblem, dass eine solche Zugriffsmöglichkeit besteht. Vertragliche und organisatorische Maßnahmen können bzw. müssen daher **flankierend zu technischen Maßnahmen** etabliert werden.

Die Kommission hat im November 2020 einen **neuen, verbesserten Entwurf von SDPC** für internationale Datentransfers veröffentlicht. Diese sollen die bisher von der Kommission anerkannten SDPC-Versionen ersetzen; Datenexporteure sollen ab ihrem Inkrafttreten ein Jahr Zeit haben, ihre Verträge mit den Datenempfängern anzupassen. Dies kann für die Datenexporteure einen hohen Aufwand bedeuten. Die modernisierten Klauseln enthalten Module für alle Transferszenarien und decken nunmehr auch Datenexporte durch Auftragsverarbeiter ab. Zudem erweitern nun zwei spezifische Klauseln die Pflichten und Zusicherungen der Parteien für den Fall, dass Gesetze im Drittland die Einhaltung der Klauseln beeinträchtigen, und die Pflichten des Datenempfängers bei behördlichen Zugriffsanforderungen. Einige der neuen Klauseln ähneln stark den (vertraglichen) Verpflichtungen, die auch der EDSA in seinen Empfehlungen als ergänzende Maßnahmen vorgeschlagen hat. Dazu gehören die Prüfung des Schutzniveaus unter Einbeziehung aller Umstände des Einzelfalls und die Pflicht des Datenempfängers, Zugriffsverlangen im Drittland rechtlich anzugreifen. Teilweise bleiben die neuen SDPC aber inhaltlich hinter den detaillierteren Vorschlägen des EDSA zurück und sehen zudem keine Fristen oder Vertragsstrafen vor. Die Tabelle in *Anhang 2* zeigt anhand ausgewählter Vertragspflichten die Unterschiede zwischen den Vorschlägen des EDSA, den neuen SDPC und den bisherigen SDPC auf. **Dass die SDPC von den Empfehlungen des EDSA abweichen, schafft zusätzliche Unklarheiten**. Zum einen ist schwierig zu überblicken, in welchen Details sich die Vorschläge tatsächlich unterscheiden. Zum anderen ist unklar, ob und inwieweit Datenexporteure zusätzlich zu den neuen SDPC noch weitere vom EDSA vorgeschlagene vertragliche Regelungen in ihre Verträge aufnehmen sollten. **Die neuen SDPC sollten daher genauer mit den Empfehlungen des EDSA abgestimmt werden**. Grundsätzlich sollten sich alle vom EDSA empfohlenen und praxistauglichen Zusatzverpflichtungen auch in den SDPC wiederfinden. Andernfalls sollte klargestellt werden, wie die Datenexporteure widerspruchsfrei zusätzliche vertragliche Regelungen ergänzen können. Zwar ermutigt die Kommission die Datenexporteure dazu, die neuen SDPC durch weitere Klauseln zu ergänzen.[397] Diese ergänzenden Klauseln dürfen jedoch den SDPC nicht widersprechen. Ob sich die Datenempfänger auf die verschärften Verpflichtungen einlassen werden, bleibt abzuwarten.

Auch die geänderten SDPC binden jedoch als vertragliche Regelungen die Behörden im Drittland nicht. Trotz erweiterter Pflichten können sie daher bei fehlendem gleichwertigen Schutzniveau im Drittland aus den genannten Gründen **nur in Kombination mit effektiven technischen Maßnahmen** hinreichenden Schutz vor ungerechtfertigten Massenzugriffen bieten. **Lassen sich behördliche Zugriffe auch durch technische Maßnahmen nicht effektiv unterbinden**, **scheiden auch die neuen SDPC** gänzlich **als** taugliche **Transfergrundlage aus**. Die Kommission sollte beides klarstellen.

Die hohen Anforderungen des EuGH und die – nachvollziehbar – strenge Sichtweise der Datenschutzaufsichtsbehörden stellen viele Datenexporteure in der Wirtschaft und im öffentlichen Sektor vor erhebliche Probleme und bedeuten für sie einen immensen Aufwand. Dies gilt insbesondere für die Pflicht, das Schutzniveau im Drittland umfassend zu prüfen und alle hierfür notwendigen Informationen einzuholen, sowie für die Pflicht, effektive Zusatzmaßnahmen auszuloten und zu etablieren. Selbst wenn die Datenexporteure erhebliche Anstrengungen unternehmen und Maßnahmen ergreifen, garantiert dies noch nicht, dass Aufsichtsbehörden und Gerichte diese für ausreichend erachten. Insbesondere **sollten die Aufsichtsbehörden klarstellen,** ab wann und **in welchen Fallkonstellationen es zu Bußgeldverfahren kommen wird**, falls die von den Unternehmen getroffenen Maßnahmen zur Ergänzung der SDPC nicht ausreichen. Denn die DSGVO sieht für Verstöße gegen die Vorschriften über die

[397] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Erwägungsgrund 3.

internationale Datenübermittlung grundsätzlich Bußgelder bis zu 20 Millionen Euro oder bis zu 4% des weltweiten Vorjahresumsatzes vor.

Weil der EDSA bei der Prüfung des Schutzniveaus einen risikobasierten Ansatz ablehnt, werden Datenexporteur und Datenempfänger aus seiner Sicht vermutlich auch bei der Auswahl der ergänzenden Schutzmaßnahmen nicht berücksichtigen dürfen, ob das tatsächliche Risiko eines behördlichen Datenzugriffs aus ihrer Sicht als gering einzuschätzen ist. Umfangreiche Transferverbote greifen aber ebenfalls in Grundrechte wie die unternehmerische Freiheit und die Berufsfreiheit der Datenexporteure ein. Der EDSA sollte daher klarstellen, ob und in welchen Fällen die Einstellung der Datentransfers oder die Verhängung von Bußgeldern unverhältnismäßig sein kann, z.B. weil die Wahrscheinlichkeit behördlicher Zugriffe bzw. das tatsächliche Risiko einer Rechtsverletzung gering sind und dies durch objektive Anhaltspunkte glaubhaft gemacht wird. Zudem sollte klargestellt werden, ob „mildernde Umstände" in Betracht kommen, wenn es im Einzelfall an zumutbaren Alternativlösungen fehlt oder eine Umstellung auf solche Lösungen Zeit braucht.

Die **rechtssicherste Möglichkeit, die gesamte Problematik zu umgehen, ist**, von kritischen Datenübermittlungen in Drittländer abzusehen und die **Daten innerhalb der EU zu speichern** sowie ausschließlich **europäische Provider zu nutzen**. Transfers an Empfänger, die den US-Überwachungsgesetzen unterliegen, könnten aber zulässig werden, wenn die USA ihre Überwachung auf das „zwingend erforderliche Maß" beschränken und EU-Bürgern einen wirksamen Rechtsbehelf gegen übermäßige Überwachung ermöglichen. Von beidem ist allerdings kurzfristig nicht auszugehen, auch wenn der neue California Privacy Rights Act, der das materielle Datenschutzniveau in Kalifornien deutlich verbessern wird, derzeit einige Steine ins Rollen zu bringen scheint. Zudem wird die Lage durch den US CLOUD Act weiter verkompliziert, nach dem Anbieter elektronischer Kommunikations- und Cloud-Dienste US-Strafverfolgungsbehörden ggf. auch solche Daten offenlegen müssen, die in der EU gespeichert werden, aber unter ihrer Kontrolle sind. Die zuletzt nicht sehr erfolgreichen Treuhand-Lösungen, bei denen europäische Töchter von US-Unternehmen ihre Rechenzentren von einem Treuhänder betreiben lassen, könnten daher wieder interessanter werden.

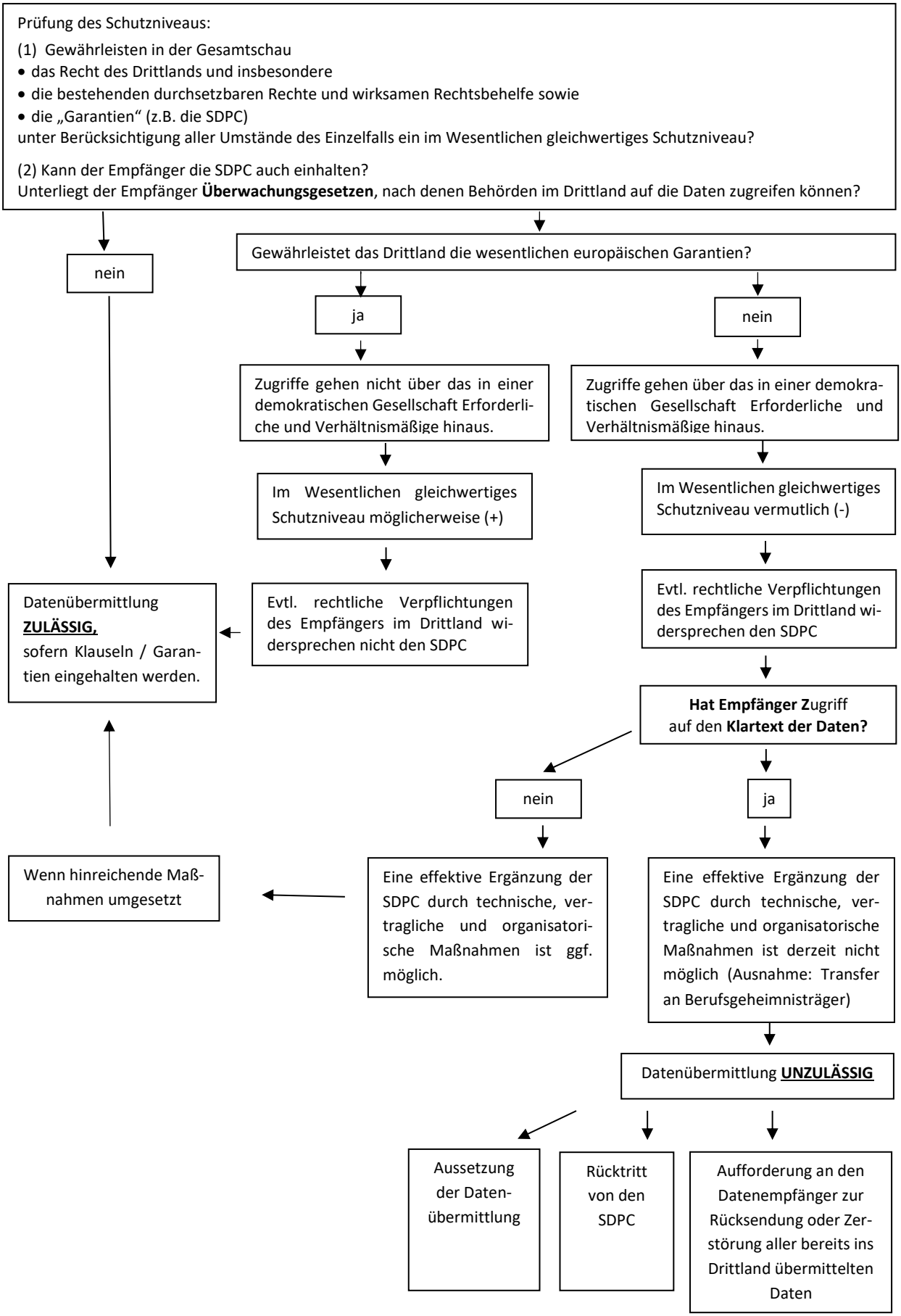
Neben EDSA, EDSB und LfDI BW haben sich zahlreiche weitere deutsche Datenschutzaufsichtsbehörden kritisch zu Datenübermittlungen auf der Basis von SDPC geäußert, die aus „Bequemlichkeit" erfolgen. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg hat Untersagungsverfügungen in Fällen angekündigt, in denen EU-Unternehmen nicht auf zumutbare Alternativangebote ohne Transferproblematik umstellen. Daneben hat die **deutsche Datenschutzkonferenz** über den rechtskonformen Einsatz von **Microsoft-Produkten** wie Windows 10 und der cloudbasierten Programmsuite Microsoft 365 beraten, die wegen der automatischen Übermittlung personenbezogener „Telemetrie-Daten" und der Zugriffsmöglichkeit von Microsoft auf in der Cloud gespeicherte Daten problematisch ist. Eine abschließende Bewertung hierzu steht noch aus. Microsoft hat zudem im November 2020 weitere Verbesserungen im Datenschutz und eine finanzielle Entschädigung von Firmenkunden angekündigt, die von einigen deutschen Datenschutzbehörden als nicht ausreichend, aber als Schritt in die richtige Richtung bewertet werden. Der **französische Conseil d'Etat** hat nach dem „Schrems II"-Urteil zusätzliche Garantien für die französische **Gesundheitsdatenplattform** und langfristig deren Migration auf europäische Server gefordert. Demgegenüber hat die **US-Regierung** im September 2020 in einem **„White Paper"** das Schutzniveau in den USA aus ihrer Sicht deutlich positiver als der EuGH dargestellt. Hierzu wäre eine Unterstützung der EU-Aufsichtsbehörden bei der Einschätzung der aktuellen Rechtslage wünschenswert. Von Interesse ist auch der Fortgang des **Beschwerdeverfahrens im Schrems-Fall**, das derzeit durch eine von der irischen Datenschutzbehörde parallel eingeleitete Untersuchung verzögert wird, gegen die weitere Rechtsbehelfe eingelegt wurden.

Untersagt die irische Behörde die Datentransfers in die USA rechtskräftig, könnte dies zum Präzedenzfall für andere Aufsichtsbehörden werden. Unternehmen müssen ferner mit **Beschwerden von Datenschutzaktivisten** rechnen. So hat die Datenschutzorganisation „noyb“ unter Berufung auf das EuGH-Urteil gegen eine Vielzahl von Unternehmen Beschwerden eingelegt. Eine „Taskforce“ des EDSA soll die schnelle und EU-weit einheitliche Bearbeitung der Beschwerden gewährleisten. Schließlich lotet die Kommission derzeit in Gesprächen mit dem US-Handelsministerium Potenzial für einen „verbesserten“ – dann dritten – Angemessenheitsbeschluss **„Privacy Shield 2.0“** aus. Solange die USA ihre Überwachungspraktiken nicht auf das erforderliche Maß reduzieren und EU-Bürgern durchsetzbare Rechte und wirksame Rechtsbehelfe gewähren, verspricht jedoch auch ein verbesserter „Privacy Shield“ keine rechtssichere Lösung. In einer Anhörung eines US-Senatsausschusses im Dezember 2020 kam die Notwendigkeit eines kurzfristigen Abkommens und von Verbesserungen des Datenschutzes auch auf US-Bundesebene zur Sprache. Hier sind die weiteren Entwicklungen zu beobachten. Änderungen im US-Recht, die einen Angemessenheitsbeschluss für die USA ermöglichen würden, sind in naher Zukunft aber nicht zu erwarten.

Eine echte Lösung des Dilemmas scheint folglich momentan nicht in Sicht. Es bleibt fraglich, wie die hohen Anforderungen an den Datenschutz mit der derzeitigen Lebenswirklichkeit und Transferpraxis in der Wirtschaft in Einklang gebracht werden können. Auch die Entwürfe der Empfehlungen des EDSA und der geänderten SDPC der Kommission ermöglichen aktuell keine rechtssichere „Patentlösungen“. Datenexporteure müssen sich auf komplizierte Einzelfallanalysen des ausländischen Rechts einlassen oder so weit wie möglich auf Ausnahmetatbestände ausweichen. **Großflächige Einwilligungslösungen sollten** aber **vermieden werden**. Denn letztlich dürften sie den Betroffenen weniger Schutz ihrer persönlichen Daten bieten als die SDPC und der aufgehobene „Privacy Shield“. Am rechtssichersten ist es, Daten ausschließlich in der EU zu speichern oder ausschließlich Auftragsverarbeiter zu nutzen, die dies tun. Um auch extraterritoriale Zugriffe auf innerhalb der EU gespeicherte Daten durch US-Behörden unter dem US CLOUD Act zu verhindern, könnte es für die europäischen Datenverarbeiter darüber hinaus sinnvoll sein sicherzustellen, dass die Kontrolle über die Daten allein in den Händen von EU-Unternehmen ohne US-Bezug verbleibt. Dies dürfte allerdings zumindest kurzfristig nicht allen EU-Unternehmen ohne weiteres möglich sein.

Im Ergebnis bietet das Urteil die **Chance**, **in der EU** zumindest langfristig bessere Datenverarbeitungs- und -auswertungsdienste als **Ausweichlösung zu etablieren** und die Schaffung sicherer Clouds voranzutreiben. Die geplante Schaffung von Gaia-X als erster europäischer Cloud ist ein richtiger Schritt in diese Richtung. Es müsste jedoch sichergestellt werden, dass die Daten in dieser Cloud tatsächlich wie geplant vor ungerechtfertigten Zugriffen ausländischer Behörden geschützt sind.

Anhang 1: Prüfpflichten des Datenexporteurs bei Verwendung von SDPC (Quelle: eigene Darstellung)



Anhang 2: Vertragliche Verpflichtungen im Vergleich (Quelle: cep)

EDSA (Empfehlungsentwürfe November 2020)[398]	**SDPC** Entwurfsfassung Kommission November 2020[399]	**Bisherige SDPC** Standardverträge I und II, Standardvertrag Auftragsverarbeiter[400]
Pflicht des **Datenexporteurs**, „ggf." zusammen mit dem Datenempfänger zu **prüfen**, ob Recht oder Praxis im Drittland den in den SDPC verankerten **Schutz beeinträchtigt**.[401]	Zusicherung des **Datenexporteurs** und des **Datenempfängers**, **keinen Grund** zur Annahme zu haben, dass das für den Datenempfänger geltende Recht und etwaige Pflichten, Behörden Zugriff auf Daten zu gewähren, den **SDPC widerspricht**.[402]	Garantie des **Datenempfängers**, **keinen** Gesetzen zu unterliegen, die die **Erfüllung** der **SDPC unmöglich** machen.[403] Pflicht des **Datenexporteurs**, sich von der Einhaltbarkeit der Verpflichtungen des Datenempfängers zu überzeugen.[404]
Pflicht des **Datenexporteurs**, bei der Prüfung des Schutzniveaus die gesamten Umstände des spezifischen Datentransfers einzubeziehen.[405]	Erklärung des **Datenexporteurs** und des **Datenempfängers**, das **Recht des Drittlands**, **alle Umstände** des konkreten Transfers und alle zusätzlichen Garantien, z.B. **ergänzende** technische **Maßnahmen** geprüft zu haben.[406]	Die Standardvertragsklauseln gelten als **ausreichende Garantien** hinsichtlich des Datenschutzes.[407]
Pflicht des **Datenempfängers**, den Datenexporteur nach besten Kräften über das Recht im Drittland zu informieren.[408]	Pflicht des **Datenempfängers**, den **Datenexporteur** nach besten Kräften mit relevanten **Informationen** zu versorgen.[409]	-
Pflicht des **Datenexporteurs**, die Prüfung des Schutzniveaus zu dokumentieren.[410]	Pflicht des **Datenexporteurs** und des **Datenempfängers**, die Prüfung des Schutzniveaus zu dokumentieren.[411]	-
Verschärfte Pflicht des **Datenempfängers**, spätere Änderungen mitzuteilen[412], und den **Datenexporteur** sofort zu unterrichten, wenn er die **SDPC nicht** (mehr) **einhalten** kann[413], sowie Fristen und Prozeduren zur schnellen Unterbrechung der Datenflüsse und **Rückgabe** der Daten.[414]	Pflicht des **Datenempfängers**, den **Datenexporteur** nachträglich über ihm bekannt gewordene Verpflichtungen zu **informieren**, die den **SDPC widersprechen**[415]**,** und des **Datenexporteurs**, sofort **zusätzliche** (technische oder organisatorische) **Maßnahmen** zu ergreifen.[416]	Pflicht des **Datenempfängers**, dem **Datenexporteur** und der zuständigen **Aufsichtsbehörde** nachträglich entgegenstehende Vorschriften und nachteilige **Gesetzesänderungen mitzuteilen**.[417]
Pflicht des **Datenexporteurs** und des **Datenempfängers**, den **Betroffenen** sofort über **Zugriffe und Zugriffsverlangen** zu informieren oder, falls dies **verboten** ist, zu versuchen, eine **Aufhebung des Mitteilungsverbots** zu erwirken. [418]	Verpflichtung des **Datenempfängers**, **Datenexporteur** und **Betroffene** über **Zugriffsverlangen** oder behördliche **Direktzugriffe** zu informieren[419], oder, falls verboten, um eine **Aufhebung des Mitteilungsverbots** zu ersuchen.[420]	Pflicht des **Datenempfängers**, den Datenexporteur über **Zugriffsverlangen** und **unberechtigte Zugriffe** zu informieren, soweit zulässig.[421]

[398] Recommendations 1/2020, a.a.O. (Fn. 6) und Recommmendations 2/2020, a.a.O. (Fn. 166).
[399] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219).
[400] Fn. 22 und 23 (25).
[401] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 30, 32, 34.
[402] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Erwägungsgrund 19 und Anhang, Section I, Clause 2, lit (b).
[403] Standardvertrag I (Fn. 26), Klausel 5 a), Standardvertrag II, Ziffer II. c).
[404] Standardvertrag II (Fn. 26), I. (c).
[405] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 28-33.
[406] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Anhang, Section I, Clause 2, lit (b).
[407] Art. 1 der jeweiligen Kommissionsentscheidungen zu den SDPC (Fn. 22 und 23).
[408] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 99.
[409] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Anhang, Section I, Clause 2, lit (c).
[410] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 99f.
[411] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219171), Anhang, Section I, Clause 2, lit (d).
[412] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 100.
[413] In Fällen, in denen das Schutzniveau in einem Drittstaat zunächst als gleichwertig erachtet wird.
[414] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 107ff.
[415] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Anhang, Section II, Clause 2, lit (e).
[416] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Anhang, Section II, Clause 2, lit (f).
[417] Standardvertrag II, Ziffer II. c); Klausel 5b Standardvertrag Auftragsverarbeiter (Fn. 26).
[418] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 99, 114, 118f; vgl. bereits Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41) für rechtlich bindende Zugriffsverlangen einer Vollstreckungsbehörde, S. 11f.
[419] Entwurf eines Durchführgsbeschl. zu SDPC (Fn. 219), Erwägungsgrd. 22 u. Anhang, Section II, Clause 3.1 (a), alle Module.
[420] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Anhang, Section II, Clause 3.1 (b), alle Module.
[421] Standardvertrag I, Klausel 5 a, Standardvertrag II, Ziffer II c); Standardvertrag Auftragsverarbeiter, Klausel 6 d (Fn. 26).

Pflicht des **Datenempfängers**, der **Behörde mitzuteilen**, dass die Anforderung seinen vertraglichen Verpflichtungen widerspricht.[422]	-	-
Pflicht des **Datenempfängers**, **Zugriffsverlangen** rechtlich zu prüfen und **anzugreifen**, soweit nach dem Recht des Drittlands möglich, und die Daten **zurückzuhalten**, bis er rechtskräftig hierzu verpflichtet wurde.[423]	Pflicht des **Datenempfängers**, **Zugriffsverlangen** rechtlich zu prüfen und **anzugreifen**, soweit nach dem Recht des Drittlands möglich, und die Daten **zurückzuhalten**, bis er rechtlich dazu verpflichtet ist.[424]	-
Vertragsstrafebewehrte Erklärung des **Datenempfängers**, behördliche Zugriffe nicht z.B. durch Hintertüren (**backdoors**) **erleichtert** zu haben oder dazu oder zur **Herausgabe von Schlüsseln verpflichtet** zu sein.[425]	-	-
Recht des **Datenexporteurs**, **Audits** oder **Inspektionen** beim Datenempfänger und seinen Subauftragnehmern durchzuführen, um festzustellen, ob und inwieweit Daten an Behörden weitergegeben wurden.[426]	Allgemeines Recht des **Datenexporteurs**, **Audits** beim Datenempfänger vornehmen **z**u lassen, insbesondere bei Anzeichen für eine Nichteinhaltung der Klauseln.[427]	Allgemeine Pflicht des Datenempfängers, nicht willkürliche **Audits** zur Feststellung der Einhaltung der Klauseln zuzulassen.[428]
Pflicht des **Datenempfängers,** regelmäßig zu bestätigen, dass er **keine Aufforderung** zur Offenlegung von Daten erhalten hat.[429]	-	-
Pflicht des **Datenexporteurs**, Betroffene bei Transfers in „**unsichere" Drittländer** zu **informieren**.[430]	-	-
Pflicht des **Datenempfängers**, **Datenexporteur** und **Betroffene** über **Unteraufträge** zu i**nformieren.**[431]	Verschiedene allgemeine Regeln zur Vergabe von **Unteraufträgen** (Modul 2 und 3)[432]	Pflicht des **Datenempfängers**, bei **Unteraufträgen** die **Einwilligung** des Datenexporteurs einzuholen.[433]
Pflicht des **Datenempfängers**, Zugriffe auf Daten technisch an eine Einwilligung oder Interaktion des Betroffenen zu knüpfen.[434]	-	-
Pflicht des **Datenexporteurs** und **Datenempfängers**, den Betroffenen bei der Rechtsausübung im Drittland **zu unterstützen**.[435]	-	-
Vertragliche Vereinbarung einer unmittelbaren – nicht nur subsidiären – oder verschuldensunabhängigen **Haftung** des Datenempfängers bei Schäden, oder einer Entschädigungsklausel.[436]	G**esamtschuldnerischen Haftung** bei **gemeinsamer Verantwortlichkeit, Entschädigung**.[437]	**Gesamtschuldnerische Haftung** beider Parteien mit Exkulpationsmöglichkeit[438] oder auf die Sorgfaltspflichten abstellende Haftung[439] oder subsidiäre Haftung des Datenempfängers (Auftragsverarbeiters)[440].

[422] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 114.
[423] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 112f., ebenso bereits Orientierungshilfe des LfDI Baden-Württemberg, a.a.O. (Fn. 41), S. 12.
[424] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Anhang, Section II Clause 3.2 (alle Module).
[425] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 103, 104.
[426] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 105f.
[427] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Anhang, Section II, Clause 1, Ziffer 1.9 (Module 2 und 3).
[428] Standardvertrag II, Ziffer II. g).
[429] EDSA, Recommendations 1/2020 (Fn. 6), Rn. 110f. Diese sogenannte „Warrant Canary"-Methode funktioniert nur, wenn das Drittland solche passive Mitteilungen nicht verbietet, den Empfänger nicht verpflichtet, falsche Mitteilungen abzusenden, und der Schlüssel sicher aufbewahrt wird, oder verschiedene Personen die Nachricht signieren und versenden.
[430] Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41), S. 11.
[431] Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41), S. 12.
[432] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Anhang, Section II Clause 4.
[433] Standardvertrag Auftragsverarbeiter, Klausel 5 h).
[434] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 116f.
[435] EDSA, Recommendations 1/2020, a.a.O. (Fn. 6), Rn. 120, 121.
[436] Orientierungshilfe des LfDI BW, a.a.O. (Fn. 41), S. 12f.
[437] Entwurf eines Durchführungsbeschlusses zu SDPC (Fn. 219), Anhang, Section II Clause 7.
[438] Standardvertrag I, Klausel 6.
[439] Standardvertrag II, Ziffer III a) (Fn. 26).
[440] Standardvertrag Auftragsverarbeiter, Klausel 6 (Fn. 26).

Centrum für Europäische Politik
FREIBURG | BERLIN

Autorin:

Dr. Anja Hoffmann, LL.M. Eur.
hoffmann@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Straße 266 | D-79098 Freiburg
Schiffbauerdamm 40 Raum 4315 | D-10117 Berlin
Tel. + 49 761 38693-0

Das **Centrum für Europäische Politik** FREIBURG | BERLIN, das **Centre de Politique Européenne** PARIS, und das **Centro Politiche Europee** ROMA bilden das **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

Das gemeinnützige Centrum für Europäische Politik analysiert und bewertet die Politik der Europäischen Union unabhängig von Partikular- und parteipolitischen Interessen in grundsätzlich integrationsfreundlicher Ausrichtung und auf Basis der ordnungspolitischen Grundsätze einer freiheitlichen und marktwirtschaftlichen Ordnung.