DATENTRANSFER IN DAS VEREINIGTE KÖNIGREICH NACH DEM BREXIT

Jan Hospes / Štefan Ziman / Walter Hötzendorfer / Christof Tschohl

Researcher, Research Institute AG & Co KG
Amundsenstraße 9, 1170 Wien, AT
jan.hospes@researchinstitute.at; https://www.researchinstitute.at

Student, Universität Wien
Universitätsring 1, 1010 Wien, AT
ziman.stefan@protonmail.ch

Senior Researcher, Research Institute AG & Co KG
walter.hoetzendorfer@researchinstitute.at; https://www.researchinstitute.at

Wissenschaftlicher Leiter, Research Institute AG & Co KG
christof.tschohl@researchinstitute.at; https://www.researchinstitute.at

Schlagworte: ***DSGVO, Drittlandtransfer, Angemessenheitsbeschluss, Standarddatenschutzklauseln, interne Datenschutzvorschriften, Brexit***

Abstract: *Mit dem Austritt aus der EU wurde das Vereinigte Königreich zu einem Drittland. Somit müssen alle datenschutzrechtlichen Beziehungen neugestaltet werden, wobei der Datentransfer weiterhin den unionsrechtlichen Standards entsprechen muss. Insbesondere aufgrund der engen Zusammenarbeit des Vereinigten Königreichs mit den Vereinigten Staaten im Bereich der internationalen Überwachungsaktivitäten ist es fraglich, ob geeignete Rahmenbedingungen für Übermittlungen von Daten aus der EU in das Vereinigte Königreich geschaffen werden können.*

1. Einleitung

Mit dem Austritt des Vereinigten Königreichs aus der Europäischen Union wurde dieses auch aus datenschutzrechtlicher Sicht zu einem Drittland.[1] Dies ändert maßgeblich die Rahmenbedingungen für den Datentransfer zu den Mitgliedsstaaten der EU. Die DSGVO erkennt grundsätzlich die Notwendigkeit des Datentransfers für die internationale Wirtschaft an. Dabei wird jedoch auch festgehalten, dass der Transfer von personenbezogenen Daten in ein Drittland nur unter der strikten Einhaltung der DSGVO möglich ist.[2]

Daten dürfen an ein Drittland nur nach Maßgabe des Art. 44 ff. DSGVO übermittelt werden. Allgemein sind Übermittlungen in ein Drittland nur unter folgenden Voraussetzungen möglich:

– Vorhandensein eines Angemessenheitsbeschlusses (Art. 45 DSGVO)
– Setzung geeigneter Garantien (Art. 46 DSGVO)

Des Weiteren normiert Art. 49 DSGVO Ausnahmen für bestimmte Fälle:

– ausdrückliche Einwilligung der betroffenen Person
– Daten Übermittlung ist notwendig für die Vertragserfüllung
– wichtige Gründe des öffentlichen Interesses

[1] Anzumerken ist, dass dieser Beitrag von einem „harten" Brexit ausgeht, also einem Vollaustritt des Vereinigten Königreichs aus EU/EWR, ohne dass Abkommen über die Rechtsverbindlichkeit von Rechtsakten der EU bzw. die Unterwerfung des Vereinigten Königreichs unter die Rechtsprechung des EuGH unterzeichnet werden.

[2] Vgl. ErwGr. 101, 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 (Datenschutz-Grundverordnung).

– zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
– erforderlich zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen

Aus den aufgelisteten Zulässigkeitsnormen für Übermittlungen in das Vereinigte Königreich erscheinen zunächst der Angemessenheitsbeschluss nach Art. 45 DSGVO und die Übermittlung aufgrund von Standarddatenschutzklauseln nach Art. 46 Abs. 2 lit. c DSGVO von besonderer Relevanz, da sie einen großflächigen Datenaustausch ermöglichen und einen geringeren Prüfaufwand für die übermittelnden Stellen mit sich bringen. Daher wird sich dieser Beitrag auf diese Kernpunkte fokussieren. Daneben sind aus dem Katalog der geeigneten Garantien des Art. 46 DSGVO interne Datenschutzvorschriften von besonderem Interesse, da sie von großen Unternehmensgruppen herangezogen werden können und so das Potenzial haben eine beträchtliche Anzahl an Betroffenen zu erfassen. Sie sollen deshalb auch behandelt werden.

2. Rahmenbedingungen für einen Datenverkehr zwischen der EU und dem Vereinigten Königreich als Drittland

Rechtswidrige Datenübermittlungen in Drittländer können unmittelbar aus EU- bzw. EWR-Staaten stammen, sie können ihren Weg aber auch mittelbar über ein Drittland, zugunsten dessen ein Angemessenheitsbeschluss besteht, nehmen. Art. 44 S. 1 DSGVO trägt diesem Umstand Rechnung, indem er solche Weiterübermittlungen beschreibt und den Zulässigkeitskriterien unterwirft. Nach Art. 44 S. 2 DSGVO sind alle Regelungen zur Drittlandübermittlung (Art. 44 bis 50 DSGVO) so auszulegen, dass das Schutzniveau der DSGVO nicht untergraben wird.

In seiner Entscheidung in der Rechtssache Schrems II[3] hat der EuGH den Durchführungsbeschluss (EU) 2016/1250 (Privacy Shield), welcher die maßgebliche Grundlage für den Datenaustausch zwischen der EU und den USA war, für ungültig erklärt. Ausschlaggebend für diese Beurteilung waren insbesondere die umfangreichen sicherheitsbehördlichen und geheimdienstlichen Befugnisse der USA und der für diese Vorgänge mangelhafte Rechtsschutz für Unionsbürger (wie für alle nicht US-Bürger). In diesem Rahmen stellte der EuGH fest, dass die auf Section 702 FISA[4] gestützten Überwachungsprogramme der USA keine geeigneten Einschränkungen erkennen ließen.[5] Auch in Verbindung mit der PPD-28[6] würde die Rechtslage nicht den im Unionsrecht nach dem Grundsatz der Verhältnismäßigkeit bestehenden Mindestanforderungen genügen.[7] Zudem eröffne der im Durchführungsbeschluss (EU) 2016/1250 angeführte Ombudsmechanismus den betroffenen Personen keinen Rechtsweg zu einem Organ, das geeignete Garantien böte, welche den nach Art. 47 der GRC[8] erforderlichen Garantien für einen effektiven Rechtsschutz der Sache nach gleichwertig wären.[9] Die Bindungswirkung einer Entscheidung im gegenständlichen Vorabentscheidungsverfahren erstreckt sich grundsätzlich auf alle im Ausgangsverfahren zuständigen nationalen Gerichte.[10] Aus dem Zweck des Vorabentscheidungsverfahrens, die einheitliche Anwendung des Unionsrechts in den Mitgliedstaaten sicherzustellen, wird vertreten, dass Vorabentscheidungen auch über den konkreten Fall hinaus Bedeutung zukommen sollte. Die genaue Qualität und der Inhalt einer solchen allgemeinen Bindungswirkung sind zwar strittig[11], eine ganz allgemeine einheitliche Auslegungsmaxime des Unionsrechts reicht hier jedoch aus, um hinsichtlich der Zulässigkeitsnormen für die Übermittlung in Drittländer relevant zu sein. Somit ist davon auszuge-

3 EuGH 16.07.2018, C311/18.
4 Foreign Intelligence Surveillance Act.
5 EuGH 16.07.2018, C311/18, Rz. 180.
6 Presidential Policy Directive 28 vom 17. Jänner 2014.
7 EuGH 16.07.2018, C311/18, Rz. 184.
8 Charta der Grundrechte der Europäischen Union (2012/C 326/02).
9 EuGH 16.07.2018, C311/18, Rz. 197.
10 Schima in: Mayer/Stöger (Hrsg.), EUV/AEUV, Art 267 AEUV, Rz. 198.
11 Schima in: Mayer/Stöger (Hrsg.), EUV/AEUV, Art 267 AEUV, Rz. 200.

hen, dass das Urteil grundsätzlich auch in allfälligen Verfahren bezüglich Übermittlungen aus der EU in das Vereinigte Königreich als wesentlicher Maßstab herangezogen wird.

Das Vereinigte Königreich und die USA weisen ein hohes Maß an Zusammenarbeit bezüglich des Datenaustauschs im Bereich der Strafverfolgung und des Geheimdienstwesen auf.[12] Am 3. Oktober 2019 unterzeichneten das Vereinigte Königreich und die USA im Rahmen des US CLOUD Act[13] das bilaterale Abkommen CS USA No. 6 (2019)[14]. Dieses ermöglicht Vollzugsbehörden beider Länder den direkten Zugang zu elektronischen Daten, die von Unternehmen in dem jeweils anderen Land gespeichert werden. Art. 5 CS USA No. 6 (2019) normiert die Aufsicht über erfolgte Anfragen durch eine unabhängige Stelle. Dem Wortlaut nach hat diese Stelle aber bloß eine nachträgliche Kontrollfunktion. Das Erfordernis einer vorherigen richterlichen Genehmigung für den Zugang zu personenbezogenen Daten ist nicht erkennbar, wodurch die im geltenden Rechtshilfeabkommen (US-UK MLAT)[15] vorgesehenen Schutzvorkehrungen ausgedünnt würden. Art. 3 US-UK MLAT hat für derartige Anfragen bisher eine Vorabkontrolle normiert. Zudem sind die Gerichte jenes Landes für die Überprüfung zuständig, welches eine Anfrage gestellt hat. Für Anfragen von US-Behörden an UK-Stellen sind daher US-Kontrollinstanzen zuständig. Diese Verschiebung der in diesem Fall bisher gem. Art. 3 US-UK MLAT geltenden Kontrollzuständigkeit der UK Central Authority (UKCA) lässt keinen Raum für Kontrolle durch Stellen des Vereinigten Königreichs oder der EU. Art. 4 Abs. 3 CS USA No. 6 (2019) nimmt Personen, welche den Vertragsparteien zugehörig sind, vom persönlichen Anwendungsbereich des Abkommen aus, enthält aber keine weiteren Einschränkungen des Betroffenenkreises. Daten aller EU-Bürger, die im Vereinigten Königreich verarbeitet werden, können so potenziell Gegenstand einer Anfrage von US-Behörden werden.

In einer Zusammenschau der Entscheidung in der Rechtssache Schrems II einerseits und dem Abkommen CS USA No. 6 (2019) ist festzuhalten, dass Daten von EU-Bürgern, welche in das Vereinigte Königreich übermittelt werden, ohne weitere Sicherheitsmaßnahmen oder Kontrollmöglichkeiten durch EU-Stellen in ein Drittland (USA) weitergeleitet werden können oder sogar müssen, dessen Datenschutzniveau durch den EuGH bereits grundlegend als unzureichend befunden wurde. Die Subsumtion aller Zulässigkeitsnormen für Übermittlungen zwischen der EU und den dem Vereinigten Königreich ist (soweit keine Änderung der Rechtslage eintritt) stets vor diesem Hintergrund zu prüfen.

3. Datenübermittlung aufgrund eines Angemessenheitsbeschlusses

Ein Angemessenheitsbeschluss wird durch die Europäische Kommission nach Maßgabe des Art. 45 DSGVO gefasst. Dabei hat sie das Schutzniveau im Drittland, für welches ein Angemessenheitsbeschluss abgeschlossen werden soll, zu berücksichtigen. Hierbei sind die Faktoren Rechtsstaatlichkeit, Durchsetzung der Datenschutzvorschriften, Achtung von Menschenrechten, internationale Verpflichtungen und die Existenz sowie Wirksamkeit von Aufsichtsbehörden einzubeziehen.[16] Nach gesicherter Rechtsprechung des EuGH ist ein angemessenes Datenschutzniveau nur dann gegeben, wenn es jenem der EU „der Sache nach gleichwertig“[17] ist. Der EuGH stellt damit klar, dass es auf der Ebene des Schutzniveaus keine wesentlichen Einschränkungen geben darf, erkennt aber an, dass sich die Mittel, wie im Drittland ein der Sache nach gleichwertiger Datenschutz erreicht werden kann, von denen der EU unterscheiden können.[18]

---

[12] British-U.S. Communications Intelligence Agreement and Outline - 5 March 1946, https://www.nsa.gov/news-features/declassified-documents/ukusa/ (abgerufen am 29.11.2020); auch als “Five-Eyes” Agreement bekannt.

[13] Clarifying Lawful Overseas Use of Data Act, USA H.R. 4943.

[14] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, CS USA No. 6 (2019).

[15] Mutual legal assistance Treaty Between the United States of America and the United Kingdom of Great Britain and Northern Ireland.

[16] Vgl. Art. 45 Abs. 2 DSGVO.

[17] EuGH 16.07.2018, C311/18, Rz. 162; EuGH 06.10.2015, C-362/14, Rz. 96.

[18] Schantz In: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht 1. Auflage 2019, DSGVO Art. 45, Rz. 6.

Bei der Beurteilung, ob ein Angemessenheitsbeschluss erfolgen darf, ist nach Art. 45 Abs. 1 DSGVO die Rechtslage im Drittland zu erheben. Mit erfolgtem Austritt aus der EU ist das Vereinigte Königreich nicht mehr in den räumlichen Anwendungsbereich des Art. 3 Abs. 1 DSGVO (vorbehaltlich allfälliger bei Redaktionsschluss dieses Beitrags noch nicht bekannter Abkommen) zu subsumieren. Verarbeitungsvorgänge im Vereinigten Königreich werden deshalb (weitgehend, vgl. Art. 3 Abs. 2 DSGVO) nicht mehr von der DSGVO erfasst. Das Vereinigte Königreich hat einen Entwurf für ein angepasstes Datenschutzgesetz in Form des Data Protection Act 2018 (im Folgenden DPA 2018)[19] sowie der UK General Data Protection Regulation (im Folgenden UK GDPR)[20] veröffentlicht, welche sich maßgeblich an der DSGVO orientieren und insbesondere auch Zulässigkeitsnormen für Datenübermittlungen in Drittländer[21] setzen. Nach Art. 17a DPA 2018 iVm. Art. 45 Abs. 1 UK GDPR ist etwa vorgesehen, dass der Innenminister des Vereinigten Königreichs die Angemessenheit für Datenübermittlungen aus dem Vereinigten Königreich in Drittländer beschließen kann. Diese Entscheidung ist gemäß Art. 17b DPA 2018 iVm. Art. 45 Abs. 2 UK GDPR zu begründen.

Gemäß Art. 3 Abs. 1 CS USA No. 6 (2019) verpflichten sich die Vertragsparteien sicherzustellen, dass ihre innerstaatlichen Gesetze den Rechtsadressaten erlauben, den gemäß dieses Abkommens beantragten Auskunftsersuchen nachzukommen. Diese Norm hält das Vereinigte Königreich an, zumindest partiell Datenflüsse in die USA zu ermöglichen. Sollte es zu keinem Angemessenheitsbeschluss durch das Vereinigte Königreich kommen, könnten solche Datenübermittlungen nach Art. 18 DPA 2018 iVm Art. 49 Abs. 1 lit. e UK GDPR ermöglicht werden, wonach der Innenminister des Vereinigten Königreichs die Übermittlung aus wichtigen Gründen des öffentlichen Interesses erlauben kann.

Art. 45 Abs. 2 lit. a DSGVO verlangt, dass die Rechtsordnung eines Drittlandes, zu dessen Gunsten ein Angemessenheitsbeschluss ergehen soll, Sicherungen dafür vorsieht, die verhindern, dass das der EU angemessene Datenschutzniveau unterlaufen wird. Wie oben dargelegt verfügen die USA über kein angemessenes Schutzniveau, weshalb die nach britischem Recht zulässigen Übermittlungen durch das Vereinigte Königreich in die USA zum Ergebnis führen muss, dass kein Angemessenheitsbeschluss seitens der Europäischen Kommission bezüglich des Vereinigten Königreichs erfolgen darf. Sollte der o. g. Entwurf für ein Datenschutzgesetz des Vereinigten Königreichs so in Kraft treten, könnte man zunächst argumentieren, dass das Abkommen CS USA No. 6 (2019) gilt, jedoch formell noch keine Rechtsinstitute in Kraft sind, um Übermittlungen aus dem Vereinigten Königreich in die USA zu ermöglichen. Solange dies der Fall ist, sollte CS USA No. 6 (2019) einem Angemessenheitsbeschluss der Europäischen Kommission gegenüber dem Vereinigten Königreich nicht im Wege stehen. Die Rechtslage sollte dann aber durch die Europäische Kommission engmaschig kontrolliert werden. Sobald der Europäischen Kommission dabei die Schaffung eines Erlaubnistatbestandes für Übermittlungen aufgrund von Anfragen gemäß CS USA No. 6 (2019) durch das Vereinigte Königreich bekannt wird, muss dies dazu führen, dass ein allfälliger, durch sie erlassener, Angemessenheitsbeschluss nach Art. 45 Abs. 2 lit. a iVm. Art. 45 Abs. 5 DSGVO auszusetzen ist.

Weiters ist zu prüfen, ob Maßnahmen umsetzbar sind, welche einen Angemessenheitsbeschluss durch die EU trotz Datenübermittlungen zwischen den USA und dem Vereinigten Königreich ermöglichen. Sowohl die Safe Harbor-Entscheidung (2000/520/EG) als auch die Entscheidung zum Privacy Shield (Durchführungsbeschluss (EU) 2016/1250) bezogen sich nicht auf die USA selbst, sondern lediglich auf Unternehmen, die sich im Rahmen einer Selbstzertifizierung zur Einhaltung der Verarbeitungsgrundsätze verpflichteten und der Aufsicht einer benannten Behörde unterlagen.[22] Wie oben gezeigt, knüpft die Argumentationslinie des EuGH im Urteil zur Rechtssache Schrems II an geltende Normen der USA an, welche keine Ausnahmen für derartig zer-

[19] Department for Digital, Culture, Media and Sport, The Data Protection Act 2018 Keeling Schedule.

[20] Department for Digital, Culture, Media and Sport, General Data Protection Regulation Keeling Schedule.

[21] Vgl. Art. 44 ff UK GDPR.

[22] Federal Trade Commission (FTC) oder das Department of Transportation.Vgl. Schantz in: Simitis/ Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht 1. Auflage 2019, Art. 45 DSGVO, Rz. 4.

tifizierte Unternehmen kennen. Ebenso kennt CS USA No. 6 (2019) keine Ausnahmen oder Sicherungsmaßnahmen. Deshalb erscheinen bedingungslose Selbstzertifizierungen wenig sinnstiftend und zusätzliche Maßnahmen sind notwendig. Diese könnten sich entweder in Form eines effektiven Rechtsschutzes für EU-Bürger manifestieren, oder durch strikte Ausnahmen bestimmter verarbeitender Stellen im Vereinigten Königreich bzgl. Anfragen von US-Behörden vom Anwendungsbereich des CS USA No. 6 (2019), wenngleich dies in der Praxis schwer vorstellbar ist. Die diplomatische Dimension dieser Optionen ist nicht zu unterschätzen.

4. Datenübermittlung aufgrund von Standarddatenschutzklauseln

Basierend auf Art. 46 Abs. 2 lit. c DSGVO ist eine Datenübermittlung in ein Drittland auch aufgrund von Standarddatenschutzklauseln möglich. Konkret handelt es sich dabei um die Beschlüsse 2004/915/EG[23] und 2010/87/EU[24] der Europäischen Kommission, welche ihre Grundlage in der Richtlinie 95/46/EG[25] haben. Die Standarddatenschutzklauseln dürfen nicht verändert werden, jedoch dürfen sie um zusätzliche Klauseln erweitert werden, welche den Standarddatenschutzklauseln nicht entgegenlaufen oder das Datenschutzniveau, welches durch sie normiert wird, herabsetzen.[26] Der EuGH stellte in seinem Urteil zu Schrems II klar, dass eine Datenübermittlung in ein Drittland aufgrund von Standarddatenschutzklauseln nur dann möglich ist, wenn im Drittland ein Schutzniveau herrscht, welches jenem der Europäischen Union gleichwertig ist.[27]

Als Reaktion auf das Urteil zu Schrems II veröffentlichte der EDSA verbindliche Empfehlungen für den Datentransfer in Drittländer.[28] Diesen Empfehlungen entsprechend hat der Datenexporteur bei der Verwendung von Standarddatenschutzklauseln das Datenschutzniveau im Drittland zu bewerten. Dabei hat ihn der Datenimporteur zu unterstützen und Informationen bereitzustellen.[29] Der EDSA gab weiters eine Empfehlung ab, welche Quellen bei der Bewertung des Schutzniveaus einzubeziehen sind. Genannt werden die nationale Rechtsprechung betreffend Datenschutz, akademische Publikationen, Entscheidungen des Europäischen Gerichtshofes und des Europäischen Gerichtshofs für Menschenrechte sowie Resolutionen und Berichte zwischenstaatlicher Organisationen.[30] Auch ein Entwurf der Europäischen Kommission für neue Standarddatenschutzklauseln weist einen Ansatz für die Bewertung der Wirksamkeit von diesen auf. Hiernach sind die Gesetze des Drittlandes, einschließlich der Gesetze, welche die Offenlegung von Daten gegenüber öffentlichen Behörden vorschreiben, in die Bewertung einzubeziehen.[31] Falls die Bewertung ergibt, dass Maßnahmen nach Art. 46 DSGVO, also auch Standarddatenschutzklauseln, kein effektives Mittel für den Datentransfer in ein Drittland bieten, sind zusätzliche Maßnahmen zu ergreifen. Diese können grundsätzlich organisatorischer, technischer oder vertraglicher Natur sein, müssen aber jedenfalls effektiv sein.[32]

---

23 2004/915/EG: Entscheidung der Kommission vom 27. Dezember 2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer.

24 2010/87/EU: Beschluss 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.

25 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

26 Vgl. EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Adopted on 10 November 2020, Rz. 56.

27 Vgl. EuGH 16. Juli 2020, C-311/18.

28 Vgl. EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Adopted on 10 November 2020.

29 Vgl. EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Adopted on 10 November 2020, Rz. 30.

30 Vgl. EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Adopted on 10 November 2020, Rz. 138.

31 Vgl. Annex to the Cmmission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, Section II Clause 2 lit. b ii.

32 Vgl. EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Adopted on 10 November 2020, Rz. 45 ff.

Sollen Datenübermittlungen in das Vereinigte Königreich auf Standarddatenschutzklauseln gestützt werden, ist ähnlich wie bei den obigen Ausführungen zum Angemessenheitsbeschluss darauf abzustellen, ob in Anbetracht der lokalen Gesetzeslage ein angemessenes Schutzniveau besteht bzw. ob man durch zusätzliche Maßnahmen Abhilfe schaffen muss. Grundsätzlich bestünden im Vereinigten Königreich mit dem Inkrafttreten des novellierten Data Protection Act 2018 sowie der UK General Data Protection Regulation geeignete Gesetze, um ein angemessenes Datenschutzniveau herzustellen. Sollte das Vereinigte Königreich jedoch Rechtsinstitute in Kraft treten lassen, welche Weiterübermittlungen in die USA nach CS USA No. 6 (2019) erlauben, muss eine Bewertung des Schutzniveaus auf Angemessenheit für das Vereinigte Königreich negativ ausfallen. Dies bezieht sich auf alle durch CS USA No. 6 (2019) verpflichteten Verarbeiter. Es könnten zusätzliche Maßnahmen ergriffen werden, um einen angemessen Datenschutz zu garantieren.[33] Diese Maßnahmen müssten geeignet sein, die Übermittlung personenbezogener Daten in die USA zu verhindern, oder die Daten für den aus EU-Sicht unberechtigten Empfänger unbrauchbar machen. Solche Maßnahmen wären durch die übermittelnden Stellen festzulegen und können sich etwa aus dem Format des Transfers, der Art der Daten und der Verarbeitung ergeben.[34] Beispielsweise kann eine effektive Verschlüsselung dafür sorgen, dass nur der Verantwortliche einen Personenbezug herstellen kann. Derartig verschlüsselte Daten unterliegen jedoch eingeschränkten Anwendungsmöglichkeiten und werden für viele Anwendungsfälle deshalb ungeeignet sein. Vor allem ist in der Praxis kritisch zu hinterfragen, ob tatsächlich ein solches Maß an Pseudonymisierung vorliegt, dass für den Empfänger im Drittland tatsächlich keine Art von Personenbezug herstellbar ist. Häufig zeigt eine nähere Prüfung hier in der Praxis, dass aufgrund von Kombinationsmöglichkeiten verschiedener Datenarten, insbesondere im Zusammenhang mit IP-Traffic, eben doch nicht alle Personenbezüge beseitigt wurden.

5. Datenübermittlung aufgrund interner Datenschutzvorschriften

Nach Art. 47 DSGVO ist die Übermittlung personenbezogener Daten in ein Drittland aufgrund interner Datenschutzvorschriften möglich. Hierzu ist die Genehmigung einer Aufsichtsbehörde notwendig. Zum Stichtag des 28.11.2020 finden sich auf der Webpräsenz der EDSA insgesamt sieben gelistete Unternehmen, deren interne Datenschutzvorschriften nach dem 25.05.2018 bewilligt worden sind.[35] Davor wurden rund 122 interne Datenschutzvorschriften durch Aufsichtsbehörden bewilligt.[36] 28 interne Datenschutzvorschriften wurden durch die Datenschutzbehörde des Vereinigten Königreichs (ICO[37]) bewilligt. Die DSGVO enthält keine Vorgaben für den Widerruf oder die Rücknahme einer Genehmigung durch die Aufsichtsbehörden, daher sind allfällige Widerrufe der Genehmigung nach den nationalen Rechtsordnungen zu bewerten.[38] Zum Austritt des Vereinigten Königreichs aus der EU hat der EDSA klargestellt, dass interne Datenschutzrichtlinien, welche nach dem Inkrafttreten der DSGVO erlassen worden sind, durch eine führende Datenschutzbehörde erneut zu bewerten sind. Interne Datenschutzvorschriften, welche vor dem Inkrafttreten der DSGVO und nach der Richtlinie 95/46/EG erlassen worden sind, behalten ohne neuerliche Bewertung weiterhin ihre Gültigkeit.[39]

Der EDSA merkt in seinen Empfehlungen betreffend des Drittlandtransfers an, dass für interne Datenschutzvorschriften das Urteil zu Schrems II einschlägig ist, da es sich um Abmachungen vertraglicher Natur handelt,

[33] Vgl. EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Adopted on 10 November 2020, Rz. 45.

[34] Vgl. EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Adopted on 10 November 2020, Rz. 48 ff.

[35] Vgl. https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_de (abgerufen am 29.11.2020).

[36] Vgl. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en (abgerufen am 29.11.2020).

[37] Information Commissioner's Office.

[38] Schantz in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht 1. Auflage 2019, DSGVO Art. 47, Rz. 12.

[39] Vgl. EDSA, Hinweise zu verbindlichen internen Datenschutzvorschriften (BCR) für Unternehmensgruppen bzw. Gruppen von Unternehmen, für die die britische Datenschutzbehörde (ICO) die federführende Behörde für die Genehmigung ihrer BCR, 22. Juli 2020.

welche nicht dazu geeignet sind, den Gesetzesbestand im Drittland auszuhebeln. Auch bei internen Datenschutzvorschriften sollte die Angemessenheit danach beurteilt werden, in welcher Form das Vereinigte Königreich Weiterübermittlungen in die USA zulässt. Ergibt die Bewertung, dass sie keinen effektiven Schutz bieten, müssen zusätzliche Maßnahmen ergriffen werden.[40] Allerdings wurde nur eine einzige der 28 durch die Datenschutzbehörde des Vereinigten Königreichs bewilligten internen Datenschutzvorschriften nach dem Inkrafttreten der DSGVO für gültig erklärt und ist diese entsprechend den obigen Ausführungen durch eine neue führende EU Datenschutzbehörde zu bewerten, weil die Datenschutzbehörde des Vereinigten Königreichs nach dem Austritt des Vereinigten Königreichs aus der EU nicht mehr Teil des EU Systems ist. Die restlichen internen Datenschutzvorschriften unterliegen keiner Neubewertung durch eine Behörde. Der Zweck der Unterscheidung nach dem Datum der Gültigkeitserklärung ist fraglich. Unternehmen, deren interne Datenschutzvorschriften dieser Überprüfung nicht unterzogen werden, können so weiterhin vorbringen, ihre Datenübermittlungen auf formell gültige interne Datenschutzvorschriften zu stützen. Der EDSA gab im Zusammenhang mit Schrems II die Empfehlung ab, dass Übermittler ihre internen Datenschutzvorschriften prüfen sollen.[41] In diesem Sinne müssten Übermittler, welche interne Datenschutzvorschriften nutzen, diese in Frage stellen, sobald sie wirksam durch Anfragen nach CS USA No. 6 (2019) zur Weiterübermittlung in die USA verpflichtet werden könnten und ggf. alle Übermittlungen selbstständig einstellen oder weitere Maßnahmen ergreifen.

Es ist zudem denkbar, dass eine Aufsichtsbehörde interne Datenschutzrichtlinien angesichts in Kraft getretener Datenschutzgesetze im Vereinigten Königreich für gültig befindet und das Vereinigte Königreich im Nachhinein Übermittlungen in die USA freigibt. In diesem Fall wäre die Gültigkeit interner Datenschutzvorschriften durch die Behörde zu revidieren.

6. Fazit

Die zukünftige Ausgestaltung der Datenübermittlung in das Vereinigte Königreich nach dessen Austritt aus der EU ist mit zahlreichen Rechtsunsicherheiten verbunden. Bei der Bewertung des Datenschutzniveaus des Vereinigten Königreichs sollte das Augenmerk darauf gelegt werden, ob es Übermittlungen gemäß CS USA No. 6 (2019) schrankenlos zulässt. Aufgrund der langjährigen Mitgliedschaft des Vereinigten Königreichs in der EU sind Verantwortliche darauf eingestellt, keine Hürden bei Übermittlungen in die EU vorzufinden. Es ist daher absehbar, dass eine Verwehrung der Zulässigkeit von Übermittlungen aus der EU in das Vereinigte Königreich auf großen Widerstand in Wirtschaft und Politik stoßen wird. Dennoch hat insbesondere die Europäische Kommission darauf zu achten, dass die Errungenschaft des hohen datenschutzrechtlichen Niveaus und letztlich der Rechtsstaat innerhalb der EU nicht aus politischem Kalkül untergraben wird.

[40] Vgl. EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Adopted on 10 November 2020, Rz. 58 ff.

[41] Vgl. EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Adopted on 10 November 2020, Rz. 60.