10.OKTOBER 2018
#BREXIT
#DATAFLOWS
#NODEAL

JACQUES DELORS INSTITUTE
BERLIN
Centre for European Affairs at the Hertie School of Governance

ANGEMESSEN ODER NICHT, DAS IST HIER DIE FRAGE

BREXIT UND DATENFLÜSSE – EIN LEITFADEN

PAUL-JASPER DITTRICH
Policy Fellow am Jacques Delors Institut, Berlin

Zusammenfassung

Als die Briten am 23. Juni 2016 ihre Stimme abgaben, standen personenbezogene Daten und Datenübermittlungen bei den meisten wohl nicht im Vordergrund. Während Themen wie die irische Grenze oder das Schicksal der in der EU lebenden britischen Staatsangehörigen die Schlagzeilen beherrschen, wird das künftige Verhältnis in Bezug auf Datenübermittlung und Datenschutz langfristig ebenfalls von nicht unerheblicher Tragweite für Großbritannien und die EU27 sein.

Der Grund dafür ist einfach: Am 29. März 2019 verlässt Großbritannien die Europäische Union und wird ein Drittland. Personenbezogene Daten können dann nicht mehr automatisch zwischen Großbritannien und dem Binnenmarkt übermittelt werden. Die im Mai 2018 in Kraft getretene Datenschutzgrundverordnung (DSGVO) stellt hohe Anforderungen an die Übermittlung von Daten aus der EU in Drittländer. Mit der Angemessenheitsprüfung bietet sie gleichzeitig einen Rahmen dafür, wie die Datenschutzregelung eines Landes als den EU-Normen gleichwertig erklärt werden kann, was wiederum Unternehmen die Übermittlung personenbezogener Daten in dieses Land ermöglicht.

Es ist jedoch keineswegs sicher, dass Großbritannien rechtzeitig oder überhaupt einen positiven Entscheid in der Angemessenheitsprüfung erhalten wird. Darüber hinaus müssen Großbritannien und die EU über den Umfang ihrer künftigen institutionellen Zusammenarbeit beim Datenschutz verhandeln. Unternehmen, die regelmäßig Daten zwischen den beiden Seiten austauschen, müssen wahrscheinlich zusätzliche Vorkehrungen treffen, um sich – insbesondere im Falle eines „No Deal"-Szenarios – vor potenziellem wirtschaftlichem Schaden zu schützen.

Diese Herausforderungen werden in diesem Beitrag näher beleuchtet. Zunächst wird überblicksartig die Rolle von Daten und Datenaustausch in modernen Volkswirtschaften dargestellt. Im Anschluss werden verschiedene Szenarien für die Übermittlung personenbezogener Daten nach dem Brexit beschrieben und die Angemessenheitsprüfung wird erläutert. Im letzten Abschnitt werden weitere Möglichkeiten der Zusammenarbeit im Bereich des Datenschutzes nach dem Brexit untersucht.

INHALT

1 . DATENVERKEHR ZWISCHEN GROSSBRITANNIEN UND DER EU: WAS STEHT AUF DEM SPIEL?

1.1 Die Bedeutung des Datenverkehrs für den Handel

Mit dem Brexit ist für Unternehmen der reibungslose und ungehinderte Austausch personenbezogener Daten bedroht: Als Drittland wird das britische Datenschutzniveau nicht mehr automatisch als dem europäischen Schutzniveau angemessen angesehen. Personenbezogene Daten von europäischen Bürgern können in der Folge nicht mehr automatisch und ohne zusätzliche Vorkehrungen aus dem Binnenmarkt nach Großbritannien übermittelt und dort verarbeitet werden. Ohne neue Regelungen und ohne entsprechende Vorbereitung sind Unternehmen mit Rechtsunsicherheit und sogar mit vorübergehenden Leistungsunterbrechungen konfrontiert.

> “
> HANDELSINTEGRATION ERFOLGT ZUNEHMEND DURCH DIGITALE GRENZÜBERSCHREITENDE LIEFERKETTEN

Die Berichterstattung zu diesem speziellen Thema im Zusammenhang mit dem Brexit ist gering. Dennoch könnte sich dieses Problem im Falle eines „No Deal"-Brexit als viel größer erweisen, als von den meisten Politikern und Regierungsvertretern derzeit angenommen. Handelsintegration erfolgt zunehmend durch digitale grenzüberschreitende Lieferketten, die auf die reibungslose Übermittlung personenbezogener Daten von Mitarbeitern oder Kunden angewiesen sind. Von multinationalen Konzernen mit Back-End-Rechenzentren im gesamten Binnenmarkt bis hin zu medizinischen Start-ups, die Röntgenbilder aus ganz Europa auswerten, ist die grenzüberschreitende Geschäftstätigkeit eng an den ununterbrochenen Fluss personenbezogener Daten über die Grenzen hinweg gekoppelt. Für den Export von Dienstleistungen besonders auf Daten angewiesene Branchen sind Telekommunikation, Finanzwesen und die Unterhaltungsindustrie. Infolge höherer Konnektivität, besserer Computerleistung, des Wachstums der Datenwirtschaft und des zunehmenden datengestützten Dienstleistungsverkehrs hat sich der globale grenzüberschreitende Datenverkehr (gemessen anhand der Bandbreitenauslastung) zwischen 2005 und 2014 um das 45fache erhöht und wird bis 2021 voraussichtlich noch einmal um das Neunfache zunehmen. Schätzungen zufolge sind bis zu 3,8 Prozent des globalen BIP auf einen grenzüberschreitenden Datenverkehr angewiesen.[1]

Für diese sich verändernde Handelslandschaft ist die Struktur der britischen Wirtschaft exemplarisch innerhalb Europas. Das Land ist stark auf Dienstleistungen (insbesondere Finanzdienstleistungen) fokussiert. 43 Prozent der Gesamtexporte sind dienstleistungsbezogen. Auch ist das Land bei der Entwicklung digitaler Anwendungen Vorreiter in Europa. Das britische Geschäftssegment der Digitaltechnologie trägt rund zehn Prozent zur Gesamtheit britischer Dienstleistungen bei, was unter den G20 den höchsten Anteil darstellt. Etwa ein Drittel aller europäischen Start-ups im Bereich der künstlichen Intelligenz befinden sich in Großbritannien, und London gilt als die europäische Hauptstadt für Fintech-Unternehmen.[2] Das größte Rechenzentrum Europas (weltweit das drittgrößte) befindet sich ebenfalls in Großbritannien.[3]

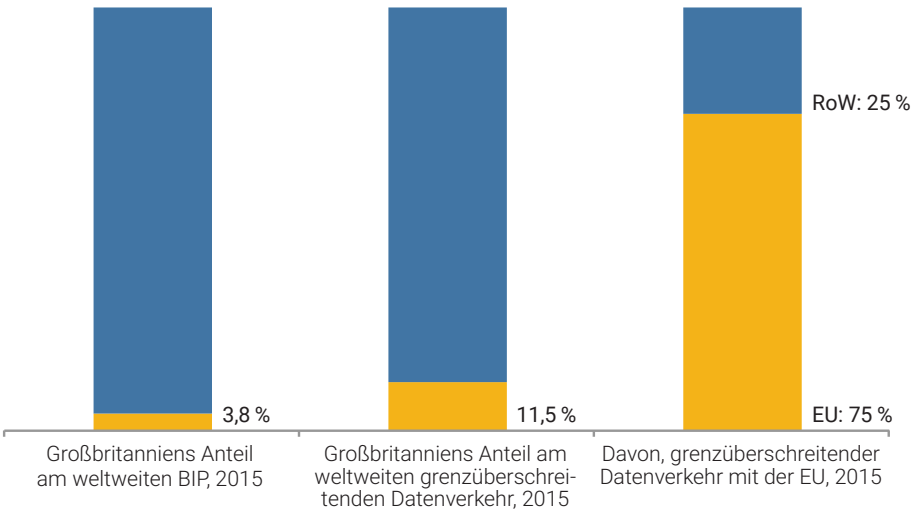
Ein wachsendes Handelsvolumen zwischen Großbritannien und der EU basiert auf Digitaltechnologie. Private Käufer im Internet sowie große Unternehmen, die auf physische und di-

1. McKinsey Global Institute, "Digital Globalization: The new Era of Global Flows", 03.2016.
2. Roland Berger, "Artificial Intelligence – A Strategy for European Startups", 2018.
3. Aditya Kishore, "Should UK data centres fear Brexit?, DatacenterDynamics", 26.04.2016.

gitale Lieferketten angewiesen sind, übermitteln regelmäßig personenbezogene Daten über den Ärmelkanal. Großbritannien hat in Bezug auf das BIP nicht nur einen sehr hohen Anteil am globalen Datenverkehr, der über britisches Territorium führt (siehe Grafik auf der folgenden Seite), sondern ein Großteil dieser Daten werden zwischen Großbritannien und der EU übermittelt: Schätzungsweise drei Viertel des gesamten britischen Datenverkehrs entfällt auf die EU.[4] Dies betrifft Datenverkehr im Zusammenhang mit der Bereitstellung von Informationen, mit Kommunikation, Suchanfragen, Audio- und Videodaten, Finanztransaktionen oder mit dem Datenaustausch zwischen bzw. innerhalb von Unternehmen. Inwieweit dieser Datenverkehr personenbezogene Daten von Betroffenen in Europa überträgt, ist nicht zu ermitteln. Ebenso schwierig ist es, die genauen wirtschaftlichen Auswirkungen auf die EU festzumachen, die eine Unterbrechung dieses Datenverkehrs haben würde. Der Großteil des Dienstleistungshandels ist jedoch unbestritten auf grenzüberschreitenden Datenverkehr angewiesen.

Die wirtschaftlichen Auswirkungen dieser Rechtsunsicherheit wären für Großbritannien wahrscheinlich schlimmer als für die EU, da die britische Wirtschaft viel stärker von Dienstleistungen und Dienstleistungsexporten abhängig ist als die meisten anderen europäischen Volkswirtschaften. Im Falle eines Brexit ohne vereinbartes Regelwerk für die Zukunft („no deal") werden allerdings auch europäische Unternehmen mit Unsicherheiten und bürokratischem Mehraufwand konfrontiert sein. Aufgrund der Unsicherheit in Bezug auf die Regeln für die Übermittlung personenbezogener Daten aus der EU nach Großbritannien könnten Investitionsentscheidungen verzögert oder gar nicht erst getroffen werden. Erste Anzeichen für datenbedingte Nicht-Investitionsentscheidungen in Großbritannien wird bereits in den Medien berichtet. berichtet.[5]

FIGUR 1 ▪ Großbritannien ist stark in globale und europäische Datenflüsse integriert.



Quelle: Frontier Economics and Eurostat.

4. UK House of Lords, "Brexit: The EU data protection package", 3rd Report of Session 2017–19, 18.07.2017.
5. Aliya Ram, Nicolas Megaw, Mehreen Khan, "Companies review arrangements for data transfer after Brexit", Financial Times, 11.08.2018.

2 . DATENVERKEHR NACH DEM 29. MÄRZ

> UM EINE UNGEHINDERTE ÜBERMITTLUNG PERSONENBEZOGENER DATEN ZU ERMÖGLICHEN, MUSS DER BRITISCHE DATENSCHUTZ ALS ANGEMESSEN FÜR DAS EU-DATENSCHUTZNIVEAU ERACHTET WERDEN

Wie genau sieht die Bedrohung aus, die der Brexit für den Datenverkehr darstellt? Kurz zusammengefasst ist das Grundproblem Folgendes: Als Mitglied der EU und des Binnenmarkts gilt das britische Datenschutzniveau als angemessen (übereinstimmend), und Unternehmen können personenbezogene Daten ohne weitere Schutzvorkehrungen weiterleiten und verarbeiten (speichern, auswerten, kombinieren usw.), solange sie sich insgesamt an die DSGVO halten. Nach dem Brexit wird dies nicht mehr automatisch der Fall sein. Stattdessen wird Großbritannien aller Voraussicht nach aus regulatorischer Perspektive ein Drittland werden, und das britische Datenschutzniveau wird für die automatische Übermittlung personenbezogener Daten europäischer Bürger nach Großbritannien und deren Speicherung in Großbritannien nicht mehr als sicher angesehen.[6] Um wieder eine ungehinderte Übermittlung personenbezogener Daten zu ermöglichen, muss der britische Datenschutz als angemessen für das EU-Datenschutzniveau erachtet werden.

Das zukünftige Verhältnis hinsichtlich des Datenverkehrs wird davon abhängen, wie der Brexit letztlich vollzogen wird, d. h. vom Grad der zukünftigen politischen, rechtlichen, institutionellen und wirtschaftlichen Anbindung Großbritanniens an den Binnenmarkt. Die Optionen reichen von der Fortführung der derzeitigen Praktiken des Datentransfers (wenn Großbritannien dem Europäischen Wirtschaftsraum, EWR, beitritt) bis hin zu einer vorübergehenden Unterbrechung des Verkehrs in Falle eines „No Deal"-Szenarios. Als am Wahrscheinlichsten gilt jedoch, dass die EU den Datenschutzrahmen Großbritanniens während der Übergangsphase überprüfen und schließlich für angemessen erklären wird.

2.1 EWR-Mitgliedschaft: Ein unwahrscheinliches Szenario

Wenn Großbritannien nach dem Brexit im Binnenmarkt verbleibt (z. B. im EWR, ähnlich Norwegen) und damit im Zuständigkeitsbereich des Europäischen Gerichtshofs (EuGH) bleibt, können personenbezogene Daten ohne weitere Einschränkungen grenzüberschreitend ausgetauscht werden.[7] Die derzeitigen Bestimmungen über den Datenaustausch (in Bezug auf den freien Datenverkehr und die Zusammenarbeit im Bereich Sicherheit) bleiben in Kraft. Als EWR-Mitglied würde für Großbritannien uneingeschränkt die Datenschutzgrundverordnung gelten, so dass das Land möglicherweise auch Teil des Europäischen Datenschutzausschusses (EDSA) sein kann. Der EDSA besteht aus Mitgliedern der nationalen Datenschutzbehörden der Mitgliedstaaten und dem Europäischen Datenschutzbeauftragten (EDSB). Eine der Hauptaufgaben ist die Beratung bei grenzüberschreitenden Datenschutzkonflikten im Binnenmarkt. Während die Vollmitgliedschaft den Mitgliedstaaten vorbehalten ist, könnte Großbritannien wie Norwegen ein Beobachterstaat werden. Ein Szenario im EWR-Stil erscheint zu diesem Zeitpunkt jedoch höchst unwahrscheinlich, da dafür eine Trendwende innerhalb Großbritanniens notwendig wäre, denn die beiden Parteiführungen lehnen derzeit alles ab, was einer vollständigen Teilnahme am Binnenmarkt unter der Gerichtsbarkeit des EuGH gleichkommt.

6. European Commission, "Notice to Stakeholders, Withdrawal of the United Kingdom from the Union and EU Rules in the Field of Data Protection", 09 January 2018.

7. Apart from a small, but considerable number of national data localization measures, which in some member states for example force companies to store tax and other accounting data in the country they were generated. For more information see ECIPE, "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", Policy Brief No. 03/2016.

2.2 Wie kann man als Drittland den freien Datenverkehr sicherstellen?

Wenn die EWR-Mitgliedschaft die unwahrscheinlichste Option für das zukünftige Verhältnis zwischen Großbritannien und der EU ist, wird Großbritannien mit ziemlicher Sicherheit zu einem Drittland werden. Der Prozess sieht wie folgt aus: Wenn das Europäische Parlament und das Unterhaus dem Austrittsabkommen zustimmen, beginnt die so genannte Übergangszeit nach dem Brexit-Datum am 29. März. Die europäischen Regeln des Acquis Communautaire und somit die Regeln für den Schutz und Austausch von Daten gelten bis Dezember 2020. Danach wird Großbritannien als Drittland betrachtet, und das künftige Verhältnis wird den Regelungen der Verordnung (EU) 2016/679 (Datenschutzgrundverordnung, DSGVO) über die Übermittlung von Daten in Drittländer und die Verarbeitung personenbezogener Daten europäischer Herkunft in Drittländern unterliegen. Die jeweiligen Regeln, die zumeist bereits mit der Datenschutzrichtlinie von 1995 (95/46/EG) eingeführt wurden, wurden im Rahmen der DSGVO überarbeitet, präzisiert und erweitert.

Art. 44-50 der DSGVO befassen sich mit den Regeln und Bestimmungen, nach denen personenbezogene Daten in Drittländer außerhalb der EU bzw. außerhalb des EWR übermittelt und verarbeitet werden dürfen. Die DSGVO sieht für die Übermittlung personenbezogener Daten in Drittländer mehrere Möglichkeiten vor. Das umfassendste Instrument zur Gewährleistung des freien Verkehrs personenbezogener Daten zwischen der EU und einem bestimmten Drittland ist der so genannte Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO).[8] Sobald die Kommission erklärt hat, dass das vorgegebene Datenschutzniveau den EU-Normen voll und ganz entspricht, dürfen Unternehmen und Behörden personenbezogene Daten aus der EU ohne Einschränkungen übermitteln und verarbeiten. Dies kann sich auf das gesamte Drittland, ein bestimmtes Gebiet oder einen Sektor erstrecken und wird von der Kommission laufend überprüft.

Die Möglichkeit, von der Kommission einen positiven Angemessenheitsbeschluss zu erhalten, bestand bereits im Rahmen der Datenschutzrichtlinie von 1995 und soll sowohl den Schutz personenbezogener Daten europäischer Bürger außerhalb des EU-Gebiets als auch einen reibungslosen grenzüberschreitenden Datenverkehr gewährleisten. Das reguläre Verfahren (auf der Grundlage von Art. 45 DSGVO) zur Erlangung des Angemessenheitsstatus stellt sich wie folgt dar: Nachdem das Drittland sich mit einem Angemessenheitsantrag an die Kommission gewandt hat, überprüft die Kommission den Datenschutzrahmen, die Aufsichtsbehörden und die Übereinstimmung der Datenschutzbestimmungen des Drittlandes mit dem EU-Äquivalent – der am 25. Mai 2018 in Kraft getretenen DSGVO. Nach der Erteilung des Angemessenheitsstatus unterliegt das jeweilige Land weiterhin der laufenden Überwachung durch die Kommission, um die dauerhafte Angemessenheit der Datenschutzbestimmungen des Landes entsprechend denen der EU zu gewährleisten. Das Europäische Parlament und der Rat können Änderungen des Status des Angemessenheitsbeschlusses beantragen (ändern, zurückziehen).

> BISHER SIND NUR ZWÖLF DATENSCHUTZSYSTEME ANDERER LÄNDER ALS DEN EUROPÄISCHEN NORMEN ANGEMESSEN ANERKANNT

Bisher sind nur zwölf Datenschutzsysteme anderer Länder (darunter einige Territorien der britischen Krone wie Jersey) als den europäischen Normen angemessen anerkannt, d. h., dort wurden ähnliche Datenschutzbestimmungen wie die der EU eingeführt.[9] Den USA (mit dem Privacy Shield Framework, das den Angemessenheitsbeschluss für Safe Harbour ersetzt hat) und Kanada (hinsichtlich kommerzieller Organisationen) wurde eine teilweise

8. European Commission, "Adequacy of the protection of personal data in non-EU countries", Official Homepage.
9. The European Commission lists the following countries and Crown dependencies on its website: Andorra, Argentina, Canada (limited to commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the United States (within the Privacy Shield Framework)

Angemessenheit zugesprochen. Das letzte Land, das den Angemessenheitsstatus erhalten soll, ist Japan nach dem Abschluss des Freihandelsabkommens zwischen der EU und Japan.[10] Beide Seiten erkennen gegenseitig ihre Datenschutzsysteme als angemessen an. Das Verfahren für diese Länder dauerte durchschnittlich jeweils 28 Monate[11] und war im Falle der USA wiederholt Gegenstand von Rechtsstreitigkeiten über die Rechtmäßigkeit der Datenübermittlung. Die Mindestdauer für die Überprüfung, Verhandlung und schließlich den Angemessenheitsbeschluss wird auf zwei Jahre geschätzt.

2.3 „Privacy Shield" zwischen Großbritannien und der EU?

Wie wahrscheinlich ist ein rascher und positiver Angemessenheitsbeschluss der Kommission für Großbritannien? Der Fall ist bisher einzigartig, da das Land Teil des europäischen Rechtsrahmens und damit des Datenschutzsystems des Binnenmarkts war. Die Chancen für einen schnellen Prozess sind daher prinzipiell hoch. Einige Beobachter sind der Ansicht, dass die Verhandlungen zwischen Großbritannien und der EU viel schneller abgeschlossen werden könnten und aufgrund der Nähe der beiden Datenschutzsysteme möglicherweise nur zwölf bis 18 Monate dauern werden.

> "DIE MEISTEN BEOBACHTER SIND DER ANSICHT, DASS GROSSBRITANNIEN IM PRINZIP RASCH EINEN ANGEMESSENHEITS-BESCHLUSS ERHALTEN KÖNNTE

Hauptgrund für diesen Optimismus ist die fortgesetzte Anwendung der DSGVO-Normen für den Datenschutz nach dem Brexit und des neuen britischen Datenschutzgesetzes, das am 23. Mai 2018 die Königliche Zustimmung erhielt.[12] Mit dem Gesetz wird die DSGVO weder vor noch nach dem Austritt des Landes aus der EU in britisches Recht umgesetzt. Als Verordnung trat die DSGVO in Großbritannien wie in jedem anderen Mitgliedstaat am 25. Mai 2018 in Kraft. Die Umsetzung nach dem Brexit wird mit dem britischen Gesetzentwurf über den Austritt aus der Europäischen Union (European Union Withrawal Bill) erreicht. Der Gesetzentwurf unterstützt und ergänzt jedoch die Einführung der DSGVO und betrifft Bereiche, in denen die Verordnung Raum für nationale Ermessensspielräume gelassen hat.[13] Außerdem verfügt das Land über eine angesehene und erfahrene Datenschutzbehörde (Information Commissioner's Office). Die meisten Beobachter sind daher der Ansicht, dass Großbritannien im Prinzip rasch einen Angemessenheitsbeschluss erhalten könnte.[14]

Auf der anderen Seite sprechen einige Faktoren gegen ein einfaches und schnelles Verfahren. Seit der EuGH-Entscheidung von 2015 über Safe Harbour[15] und der Einführung der DSGVO erfordert jeder Angemessenheitsbeschluss als Voraussetzung für Drittländer den Schutz der Grundrechte (zu denen der Datenschutz gehört). Großbritannien wird ein Schutzniveau nachweisen müssen, das dem Status eines Grundrechts angemessen ist. Dieses Verfahren beinhaltet die Überprüfung aller britischen Rechtsvorschriften und Praktiken im Zusammenhang mit den Aktivitäten der nationalen Sicherheitsbehörden und Nachrichtendienste.

Die britischen Nachrichtendienste verfügen über weitreichende Berechtigungen für den Zugriff auf E-Mail-Daten, das Abhören von Telefongesprächen oder den Zugriff auf Social-Media-

10. European Commission, "The European Union and Japan agreed to create the world's largest area of safe data flows", Press release, 17.07.2018.
11. Pieter Lamens and Evelyn Caesar, "GDPR & Brexit: Is there a need for an adequacy decision?", Deloitte.
12. HM Government, "Data Protection Act 2018", Official Homepage.
13. Information Commissioner's Office, "An introduction to the Data Protection Bill", May 2018.
14. House of Commons, "The Progress of the UK's negotiations on EU withdrawal: Data", Seventh Report of Session 2017-19, 26.06.2018.
15. Judgement of the Court (Grand Chamber) of 6 October 2015, "Maximilian Schrems v Data Protection Commissioner".

> WÄHREND DES ÜBERPRÜFUNGS-VERFAHRENS FÜR DEN ANGEMESSENHEITS-BESCHLUSS UNTERSUCHT DIE KOMMISSION DIE NATIONALEN SICHER-HEITSVORSCHRIFTEN GROSSBRITANNIENS

Konten, insbesondere nach der Einführung des Investigatory Powers Act 2016[16]. Darüber hinaus ist Großbritannien Teil des „Five Eyes"-Programms und könnte daher letztlich nachrichtendienstliche Daten über europäische Bürger mit seinen vier angloamerikanischen Partnern austauschen. Während des Überprüfungsverfahrens für den Angemessenheitsbeschluss untersucht die Kommission die nationalen Sicherheitsvorschriften Großbritanniens. Als Vollmitgliedsstaat könnte sich das Land bei jeder Überprüfung seiner Datenüberwachungsprogramme durch den EuGH auf nationale Sicherheitsausnahmen stützen, die sowohl in den europäischen Datenschutzgesetzen als auch in den Verträgen verankert sind.[17] In Artikel 4 Absatz 2 EUV heißt es: „Insbesondere die nationale Sicherheit fällt weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten".[18] Der materielle und territoriale Geltungsbereich der DSGVO schließt eine Datenverarbeitung außerhalb des EU-Rechts und damit die nationale Sicherheit ausdrücklich aus.[19]

Diese Ausnahmen gelten jedoch nicht für Drittländer. Daher könnte für Großbritannien der Erhalt des Angemessenheitsstatus schwierig werden. Selbst wenn die Kommission dem Beschluss zustimmt, könnte Großbritannien ähnlich wie die USA bald wieder verhandeln müssen. Deren Safe-Harbour-Beschluss der Kommission aus dem Jahr 2000 wurde im Jahr 2015 vom EuGH gekippt (Fall Schrems).[20] Großbritannien und die EU müssen dann möglicherweise eine Vereinbarung ähnlich dem Privacy Shield oder ein bilaterales Abkommen über Daten aushandeln. Das europäisch-amerikanische Regelwerk ersetzt den 2015 vom EuGH für ungültig erklärten Safe-Harbour-Angemessenheitsbeschluss. Bei diesem Regelwerk handelt es sich im Wesentlichen um informelle Garantien der amerikanischen Regierung und den Durchführungsbeschluss (EU) 2016/1250 der Kommission. Das Regelwerk zielt darauf ab, den Zugang der Regierung zu personenbezogenen Daten einzuschränken (zumindest formell vereinbart) und ein System für jährliche Überprüfungen sowie Möglichkeiten zur Abhilfe bei Verstößen einzurichten. In diesem Zusammenhang ist es auch wichtig festzustellen, dass Großbritannien durch den Austritt aus der EU auch nicht mehr Teil des Privacy Shield zwischen der EU und den USA sein wird und ein Abkommen über den Datenaustausch mit den USA neu aushandeln muss. Jede neue Vereinbarung wird jedoch auch von der Kommission genauestens geprüft und könnte einen Angemessenheitsbeschluss gefährden.

2.4 Was Unternehmen im „No Deal"-Fall tun müssen

Aus der Sicht von britischen und EU-Unternehmen sowie anderen privaten Firmen, die personenbezogene Daten nach Großbritannien übermitteln, gibt es ein Worst-Case-Szenario: Wenn bis zum 29. März keine Einigung über die Parameter des künftigen Verhältnisses (und der Austrittsvereinbarung) zwischen dem Unterhaus und dem Europäischen Parlament zustande kommt, würde Großbritannien aus dem Binnenmarkt ausscheiden. Daher gäbe es keine Übergangszeit, während der der Acquis noch gilt. Großbritannien würde ohne weitere Schutzvorkehrungen unverzüglich zu einem Drittland werden. Ein solches Ergebnis würde nach dem Brexit zu Störungen beim Datenaustausch führen.

16. UK Government, "UK-EU security cooperation after Brexit: EU data-sharing".
17. Karen Mc Cullagh, Brexit: "No 'clean break' for data protection law", University of East Anglia, International Law Blog.
18. EUR-LEX "Treaty on the Functioning of the European Union", Consolidated Version.
19. European Parliamentary Research Service, "Data protection rules applicable to the European Parliament and to MEPs Current regime and recent developments", Briefing, June 2018.
20. EUR-LEX "Judgment of the Court (Grand Chamber) of 6 October 2015. Maximillian Schrems v Data Protection Commissioner".

Es ist wahrscheinlich, dass die Kommission in einem „No Deal"-Szenario ein Angemessenheitsverfahren einleitet und schließlich das Datenschutzsystem Großbritanniens für gleichwertig erklärt. Ein solches Verfahren kostet jedoch Zeit und verlangt politische Anstrengungen, umso mehr, da ein Ausscheiden ohne Abkommen den politischen und diplomatischen guten Willen zwischen Großbritannien und der EU weiter beeinträchtigen könnte. Im „No Deal"-Fall müssten Unternehmen und andere private Einrichtungen daher, wenn sie alle personenbezogenen Daten (von Mitarbeiter- bis Kundendaten) übermitteln möchten, zusätzliche Sicherheitsvorkehrungen treffen. Nach der DSGVO ist bei einzelnen Unternehmen die Übermittlung personenbezogener Daten auch in Länder möglich, deren Datenschutzniveau für die EU nicht ausreichend ist.

Zu diesem Zweck muss der Auftragsverarbeiter rechtliche Garantien für den ausreichenden Schutz der betreffenden personenbezogenen Daten geben, indem der Empfänger Schutzvorkehrungen trifft, die die Konformität mit dem europäischen Datenschutzrecht gewährleisten. So ist es beispielsweise möglich, personenbezogene Daten zu übermitteln, wenn Personen, nachdem sie entsprechend aufgeklärt wurden, ihre Einwilligung zur Übermittlung und Verarbeitung ihrer Daten erteilt haben. Auch zur Erfüllung vertraglicher Pflichten können Unternehmen Daten übermitteln. Neben diesen Möglichkeiten gibt es für einzelne Unternehmen oder Organisationen zwei weitere Wege, ihr Recht auf Datenübermittlung aus der EU in ein Drittland zu sichern.

1. EU-Standardvertragsklauseln

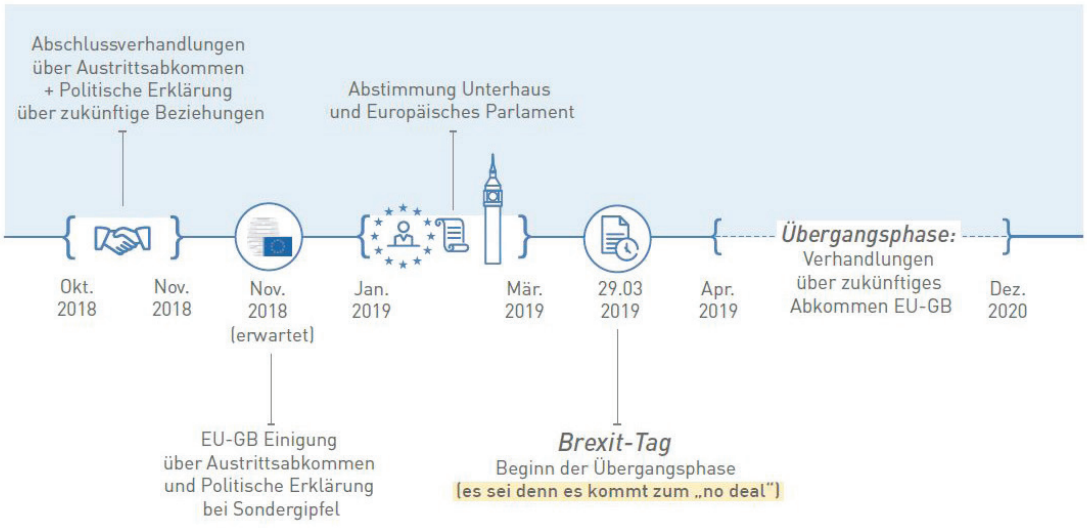
Unternehmen können die Übermittlung von Daten in Länder ohne EU-Datenschutzniveau sicherstellen, indem sie von der EU genehmigte Standardvertragsklauseln (Standard Contractual Clauses, SCCs) in ihre Dienstleistungsverträge aufnehmen und einhalten (Art. 46 DSGVO). Die entsprechenden Klauseln (Entscheidungen der Kommission 2001/497/EG, 2004/915/EG und 2010/87/EG) können auf der Website der Kommission heruntergeladen werden.[21] Ihr Vorteil ist, dass sie den Datentransfer relativ einfach ermöglichen. Andererseits unterliegen sie regelmäßigen Änderungen und werden beispielsweise mit der DSGVO aktualisiert, was zu zusätzlichen bürokratischen Verfahren führt. Das Problem mit SCCs ist, dass sie für größere integrierte Unternehmen, die routinemäßig große Datenmengen zwischen den Ländern intern übertragen müssen, nicht wirklich praktikabel sind.

2. Verbindliche interne Datenschutzvorschriften

Die zweite gängige Lösung für unternehmensinterne Datenübermittlungen in Drittländer ist die Anwendung verbindlicher interner Datenschutzvorschriften (binding corporate rules, BCR, Art. 46 DSGVO). Wie bei einem Verhaltenskodex kann ein internationales Unternehmen Vorschriften für die interne Datenübermittlung in Übereinstimmung mit den Bestimmungen der europäischen Datenschutzgesetzgebung erstellen.[22] Diese BCRs müssen von nationalen Datenschutzbehörden genehmigt werden (Art. 47 DSGVO) – ein zeitaufwändiger Prozess, der bis zu einem Jahr dauern kann. Da sie für das jeweilige Einzelunternehmen verfasst werden, sind diese Vorschriften flexibler. Das macht sie vor allem für größere Unternehmen attraktiv, aber für kleinere Unternehmen weniger praktikabel.

21. European Commission, "Model Contracts for the transfer of personal data to third countries".
22. European Commission, "Binding Corporate Rules".

FIGUR 2 ▪ Zeitrahmen der Brexit-Verhandlungen und Übergangsfrist



Infographic: Burak Korkmaz

3 ▪ MÖGLICHES ZUKÜNFTIGES VERHÄLTNIS ÜBER DEN ANGEMESSENHEITSBESCHLUSS HINAUS

Zwei Dinge sind nach dem Brexit für das Verhältnis zwischen Großbritannien und der EU in Bezug auf Daten entscheidend: Ob und wann Großbritannien einen positiven Angemessenheitsbeschluss erhält und wie die zukünftige Zusammenarbeit über den Angemessenheitsbeschluss hinaus aussehen wird, also inwieweit Großbritannien weiterhin an der Gestaltung des europäischen Datenschutzes und an der Sicherheitszusammenarbeit mitwirken wird. Der Angemessenheitsbeschluss ist der erste und wichtigste Meilenstein auf dem Weg zu einem reibungslosen Austausch personenbezogener Daten nach dem Brexit. Er ist zudem Voraussetzung für jede andere zukünftige Regelung zum Datenschutz. Die britische Position während der Brexit-Verhandlungen ist bisher die, dass Großbritannien eine Art „Sonderverhältnis" zugestanden werden sollte, das das bisherige wirtschaftliche und politisch-regulatorische Engagement Großbritanniens in der EU berücksichtigt.

Dieses Sonderverhältnis soll aus Sicht Großbritanniens aus zwei Komponenten bestehen: Einer „Wirtschaftspartnerschaft", die über ein reines Freihandelsabkommen hinausgeht und institutionelle Zusammenarbeit in weiteren Sektoren umfasst, und einer „Sicherheitspartnerschaft", die bestehende Mechanismen und Kanäle für den Datenaustausch im Zusammenhang mit der Sicherheitszusammenarbeit aufrechterhält und weiterentwickelt.[23] Die Kommission hingegen ist nachdrücklich der Auffassung, dass Großbritannien nach dem Austritt aus der EU zu einem Drittland wird. Sie argumentiert, dass ein anderer Status als der eines Drittlandes und ein künftiges Verhältnis auf der Grundlage eines Freihandelsabkommens die Kohärenz der vier Freiheiten und die Regulierungs- und Entscheidungsautonomie der EU gefährden würde. In Bezug auf Daten und Datenverkehr gibt es zwei kritische Bereiche für die Art des zukünftigen Verhältnisses:

23. HM Government, "The Future Relationship between the United Kingdom and the European Union", 23 July 2018.

1) Der politische Prozess und die Art des Abkommens

> DIE KOMMISSION HAT WIEDERHOLT DEUTLICH GEMACHT, DASS GROSSBRITANNIEN NACH DEM AUSTRITT AUS DER UNION ZUM DRITTLAND WERDEN WIRD

Auch wenn Großbritannien höchstwahrscheinlich aus dem Regulierungssystem des Binnenmarkts ausscheiden wird, haben die britische Regierung und Theresa May den Wunsch Großbritanniens zum Ausdruck gebracht, in einem besonderen Verhältnis mit der EU zu bleiben, das über den Status eines bloßen Drittlandes hinausgeht. Im Weißbuch wird der Angemessenheitsbeschluss als ein Mechanismus genannt, der dazu dienen soll, „die Notwendigkeit anderer kostspieliger und belastender Rechtsmechanismen, wie z. B. Standardvertragsklauseln, zu vermeiden".[24] Es versteht das Angemessenheitsverfahren als Ausgangspunkt, von dem aus Großbritannien versucht, anstelle einer einseitigen Entscheidung der Kommission im Namen der Mitgliedstaaten ein rechtsverbindliches bilaterales Abkommen auszuhandeln. Die Kommission, konkret Chefunterhändler Michel Barnier,[25] hat aber wiederholt deutlich gemacht, dass Großbritannien nach dem Austritt aus der Union zum Drittland werden wird. Sie lehnt daher die Idee eines „Sonderstatus", d. h. einer weitergehenden Integration über ein Freihandelsabkommen hinaus, in verschiedenen Politikbereichen ab. Beim Datenschutz bedeutet dies, dass die Kommission bisher wenig Bereitschaft gezeigt hat, Vereinbarungen oder Verträge außerhalb der bestehenden Verfahren für Drittländer zu verhandeln. Das künftige Verhältnis in Bezug auf den Datenschutz sollte lediglich den im letzten Abschnitt beschriebenen bestehenden Angemessenheitsregeln unterliegen.[26]

2) Der Grad der Integration in die europäische Datenschutzkoordination nach dem Brexit

Großbritannien möchte über einen privilegierten Zugang zum Binnenmarkt auch im Hinblick auf den Governance-Rahmen der DSGVO verhandeln, insbesondere über die Rolle der britischen Datenschutzbehörde ICO. Großbritannien hatte zunächst gehofft, seine Mitgliedschaft in vielen europäischen Agenturen zu behalten und weiterhin in deren Gremien mitzuwirken. Das wichtigste Gremium im Bereich des Datenschutzes ist die ehemalige Artikel-29-Arbeitsgruppe, die am 25. Mai 2018 nach dem Inkrafttreten der DSGVO durch den Europäischen Datenschutzausschuss (EDSA) ersetzt wurde.[27] Großbritannien hat noch einen Sitz im EDSA, den das Land nach dem Brexit aber verlieren wird. Auch hofft Großbritannien, dass ein Abkommen – das besser als nur ein Drittlandstatus ist – dafür sorgen wird, dass die britischen Unternehmen im Rahmen des neuen „One Stop Shop"-Mechanismus der EU zur Beilegung von Datenschutzkonflikten wirksam vertreten sind. Damit ist für Unternehmen, die in mehreren Ländern des Binnenmarkts tätig sind, nur eine federführende Datenschutzbehörde zuständig, deren Entscheidung in einem Streitfall für alle Mitgliedstaaten gilt. Die Kommission lehnt die britischen Vorschläge für eine künftige institutionelle Governance im Großen und Ganzen aus den gleichen Gründen ab, aus denen sie grundsätzlich einen „Sonderstatus" für Daten ablehnt. Die Wahrung der rechtlichen Integrität des Binnenmarkts bedeutet, dass es keine Aufsichtsbehörde mit einem Drittland als Vollmitglied geben kann. Es ist von ausschlaggebender Bedeutung, dass die Entscheidungsautonomie ausschließlich bei der EU verbleibt. Großbritannien argumentiert, dass es die Entscheidungsautonomie der Union nicht beeinträchtigen wird, und akzeptiert die Zuständigkeit des EuGH für den EDSA.[28] Die EU betrachtet die Position Großbritanniens allerdings als einen Versuch, den Einfluss auf die Gerichtsbarkeit der EU nach dem Brexit beizubehalten.

24. Ibid.
25. For example, European Commission, "Speech by Michel Barnier at the 28th Congress of the International Federation for European Law (FIDE)", Lisbon 26 May 2018 and "Speech by Michel Barnier at the European Union Agency for Fundamental Rights", Vienna 19 June 2018.
26. Ibid.
27. European Data Protection Board, Homepage.
28. House of Commons, "The Progress of the UK's negotiations on EU withdrawal: Data", Seventh Report of Session 2017–19, 26.06.2018.

FAZIT: HIN ZU EINER ANGEMESSENEN UND BEHUTSAMEN ZUSAMMENARBEIT?

Der endgültige Angemessenheitsbeschluss der EU-Kommission ist, nachdem die Mitgliedstaaten grünes Licht gegeben haben, unilateral. Die jüngsten politischen Signale, beispielsweise von Kommissarin Vera Jourova, zeigten verhaltenen Optimismus, was einen positiven Angemessenheitsbeschluss betrifft.[29] Auch wenn die Kommission die britischen Datenschutzgesetze und -praktiken untersuchen muss, gibt es einen eindeutigen politischen Willen in der EU für einen positiven Beschluss. Aufgrund der Massenüberwachungspraktiken britischer Geheimdienste könnte jedoch ein positiver Angemessenheitsbeschluss letztlich beispielsweise von Datenschutzaktivisten noch angefochten werden.

Wenn Großbritannien wirklich die Vorteile der europäischen Austauschsysteme für Sicherheitsinformationen oder des Europäischen Datenschutzausschusses nutzen will, muss es viele seiner roten Linien aufgeben und die Zuständigkeit des EuGH in diesen Bereichen auch nach Ablauf der Übergangsfrist akzeptieren. Es ist sehr unwahrscheinlich, dass die EU ihre Verhandlungsposition zu diesem Kernthema ändern wird. Auch befindet sich die Kommission in einer viel besseren Verhandlungsposition. Daher sollte sie ihre Haltung nicht aufweichen, dass in Bezug auf Daten und Datenaustausch etwas anderes als der Drittländerstatus für Großbritannien die rechtliche Integrität des Binnenmarkts und die Entscheidungsautonomie der EU gefährden würde und somit nicht verhandelbar ist.

Bei einigen institutionellen Fragen könnten möglicherweise Gemeinsamkeiten gefunden werden. So könnte beispielsweise das ICO wie Norwegen beobachtendes Mitglied im EDSA werden. Auch die Zusammenarbeit zwischen dem ICO und anderen EU-Datenschutzbehörden sollte nicht mit dem Brexit enden. Der ICO hat bei der Entwicklung der EU-Datenschutzgesetze eine wichtige Rolle gespielt. Es sollte daher eine kontinuierliche Zusammenarbeit zwischen dem ICO und den EU-Datenschutzbehörden geben.

FIGUR 3 ▪ Wie wird das zukünftige Verhältnis aussehen?

Infographic: Burak Korkmaz

29. McKinsey Global Institute, "Digital Globalization: The new Era of Global Flows", 03.2016.

ON THE SAME TOPIC

- Prof. Dr. Henrik Enderlein, "Twelve Thoughts on Brexit, An interim Review", Blog Post, Jacques Delors Institut – Berlin, 29 March 2018.

- Nicole Koenig, "Towards Norway plus? EU-UK defence cooperation post-Brexit", Blog Post, Jacques Delors Institut – Berlin, 7 February 2018.

- Dr. Funda Tekin, "The Area of Freedom, Security and Justice: Brexit does not mean Brexit", Policy Paper, Jacques Delors Institut – Berlin, 13 September 2017.

- Valentin Kreilinger, Sophia Becker, Laura Wolfstädter, "Brexit: Negotiation Phases and Scenarios of a Drama in Three Acts", Policy Paper, Jacques Delors Institut – Berlin, 25 January 2017.

Managing Editor: Henrik Enderlein

Hertie School of Governance

Friedrichstraße 194, D – 10117 Berlin
info@delorsinstitut.de
www.delorsinstitut.de