Datenschutzrechtliche Auswirkungen eines „harten“ Brexits

Inhalt

Bei Rückfragen können Sie sich gerne an uns wenden:

UIMC DR. VOSSBEIN GMBH & CO KG
Otto-Hausmann-Ring 113
42115 Wuppertal

Tel.: + 49 202 946 7726 200
E-Mail: consultants@uimc.de
Internet: www.UIMC.de

1 Einleitung

Am 29. März 2019 entfaltet der Brexit Rechtskraft (es sei denn der Europäische Rat verlängert die Übergangsfrist). Das Vereinigte Königreich ist dann nicht mehr Mitglied der EU. Allerdings hat die EU dem Vereinigten Königreich angeboten, die Übergangsfrist bis Ende 2020 zu verlängern, so dass das Vereinigte Königreich bis dahin noch am Binnenmarkt und der Zollunion teilhaben könnte.

Im „Extremfall" kann es zu einem „harten Brexit" kommen, was Auswirkungen auf den grenzüberschreitenden Datenverkehr und somit auf den Datenschutz hat. Nach dem Austritt des Vereinigten Königreichs aus der EU gilt die DSGVO nicht mehr unmittelbar innerhalb des Vereinigten Königreichs (UK; hierzu gehören England, Wales, Schottland, Nordirland, Kanalinseln).[1] Die DSGVO wird jedoch weiterhin Auswirkungen auf den Datenverkehr zwischen UK und der EU haben.

Von der veränderten Lage sind Unternehmen u. a. in folgenden Situationen betroffen:

A. Unternehmen mit Sitz in der EU

- Auftragsverarbeitung / Dienstleistung
  (Controller to Processor / C2P)
  - Nutzung von Shared Services (wie IT- oder Personal-Services) bei einer Mutter- oder Tochtergesellschaft mit Sitz in UK
  - Externe Dienstleister mit Sitz in UK
  - Sub-Dienstleister eines Dienstleisters mit Sitz in UK
- Datenübermittlung an eine andere Konzerngesellschaft
  (Controller to Controller / C2C)
  [bitte beachten Sie: Es existiert kein Konzernprivileg.]
  - Unternehmensübergreifende Organisationsstrukturen (Matrix-Organisation, Divisionsstrukturen mit unterschiedlichen fachlichen und disziplinarischen Vorgesetzten und Berichts-/Reporting-Wegen in verschiedenen Konzern-Gesellschaften)
- Datenübermittlung an eine andere Gesellschaft
  (Controller to Controller / C2C)
  - Im Rahmen von Versicherungsleistungen werden personenbezogene Daten an ein Unternehmen in UK übermittelt.

B. Unternehmen mit Sitz in UK

- Personenbezogene Datenverarbeitung von in der EU befindlichen Betroffenen
- Auftragsverarbeitung für Auftraggeber innerhalb der EU

[1] Denn EU-Verordnungen gelten (im Gegensatz zu Richtlinien) als unmittelbares Recht in den EU-Mitgliedsstaaten, ohne dass es eines Umsetzungsaktes bedarf.

Um den Übergang bzw. Austritt möglichst fließend zu gestalten und den grenzüberschreitenden Datenfluss von und zu britischen Unternehmen innerhalb Europas sowie um den Handel nicht über Gebühr zu beeinträchtigen, wurde in UK der Data Protection Act 2018 beschlossen.

Ferner liegt dem britischen Parlament seit dem 14. November 2018 ein Entwurf des Austrittsabkommens vor. Teil VII dieses 585 Seiten umfassenden Entwurfes betrifft den Datenschutz. Näheres können Sie der Anlage (Punkt 8.1: „Entwurf des Austrittsabkommens zwischen der EU und UK “) entnehmen. Da das Abkommen noch nicht angenommen wurde und es noch immer zum harten Brexit kommen kann, ist Folgendes bei einem harten Brexit zu bedenken:

2 Besonderheiten des „Drittland-Transfers“

UK wird mit dem Austritt zum sog. Drittland (Land außerhalb der EU/EWR). Dies bedeutet für Unternehmen, die Daten nach UK übermitteln oder mit dort ansässigen Dienstleistern zusammenarbeiten (Auftragsverarbeitung), dass neben der Rechtmäßigkeit der Übermittlung bzw. Ordnungsmäßigkeit der Auftragserteilung zusätzlich Folgendes zu prüfen ist:

In dem Drittland muss ein angemessenes Datenschutzniveau bestehen. Zu den Ländern, die als sichere Drittländer seitens der EU-Kommission anerkannt wurden, zählen u. a. die Isle of Man, Guernsey und Jersey, die zu UK gehören. Obschon UK eine Anerkennung anstrebt und im Zuge der Brexit-Vorbereitungen bereits den Data Protection Act 2018 erlassen hat, so ist dennoch damit zu rechnen, dass UK bis zum 29. März 2019 noch nicht als sicheres Drittland anerkannt wird (falls dies überhaupt geschieht). Näheres kann der Anlage (Punkt 8.2: „Verhandlungen über den Angemessenheitsbeschluss “) entnommen werden; aktuell liegt kein Anerkennungsbeschluss vor.

3 Möglichkeiten zur Gewährleistung eines angemessenen Datenschutzniveaus

Bis zur Anerkennung eines angemessenen Datenschutzniveaus in UK muss die Einhaltung eines angemessenen Datenschutzniveaus beim Datenexport auf andere Weise sichergestellt werden. **Andernfalls müssten zum Stichtag (29. März 2019) alle Datentransfers nach UK beendet werden.**

Ein angemessenes Datenschutzniveau kann durch folgende geeignete Garantien, die in Art. 46 DSGVO genannt sind, gewährleistet werden:

- Standarddatenschutzklauseln der EU-Kommission [EU-Standardvertragsklauseln / Standard Contractual Clauses / SCC]
  (Art. 46 Abs. 2 lit. c, 93 Abs. 2 DSGVO)
- Standarddatenschutzklauseln der Aufsichtsbehörden
  (Art. 46 Abs. 2 lit. d, 93 Abs. 2 DSGVO)
- Verbindliche interne Datenschutzvorschriften [Binding Corporate Rules / BCR]
  (Art. 46 Abs. 2 lit. b, Art. 47 DSGVO)

» Ebenfalls möglich, aktuell aber weniger geläufig.

- Genehmigte Verhaltensregeln zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder Auftragsverarbeiters im Drittland (Art. 46 Abs. 2 lit. e, 40 DSGVO)
- Abschluss eines genehmigten Zertifizierungsmechanismus zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder Auftragsverarbeiters im Drittland (Art. 46 Abs. 2 lit. f, 42 DSGVO)
- Rechtlich bindende und durchsetzbare Dokumente zwischen öffentlichen Stellen (Art. 46 Abs. 2 lit. a DSGVO)

4 Anwendungsfälle für Unternehmen mit Sitz in der EU

Die folgende Auflistung an Anwendungsfällen deckt lediglich die Hauptbereiche ab. Bei Rückfragen oder weiteren Anwendungsfällen können Sie sich gerne an uns wenden.

4.1 Auftragsverarbeitung (AV): C2P

Grundsätzlich ist mit dem Dienstleister im Rahmen der Auftragsverarbeitung ein Vertrag abzuschließen. Dies gilt unabhängig davon, ob der Dienstleister innerhalb oder außerhalb der EU ansässig ist. Ein Muster finden Sie im Online-Formular-Center der UIMC. Nachfolgendes gilt zusätzlich für Dienstleister mit Sitz außerhalb der EU. **Hierbei ist es unerheblich, ob die (Unter-)Auftragsverarbeitung durch eine weitere Konzern-Gesellschaft oder durch einen externen Dienstleister durchgeführt wird.**

Bestehen konzernintern bereits AV-Verträge [bspw. mit einem britischen Mutterkonzern oder einem britischen externen Dienstleister (unabhängig davon, ob die Verarbeitung der Daten innerhalb oder außerhalb der EU erfolgt)], so müssen bei einem harten Brexit zusätzlich mindestens eine der in Punkt 3 genannten Maßnahmen ergriffen werden. Typischerweise handelt es sich hierbei um EU-Standardvertragsklauseln (SSC); im Rahmen einer konzern-internen Auftragsverarbeitung sind auch Binding Corporate Rules (BCR) möglich.

Falls noch nicht im Vertrag enthalten, sollten die Verträge zur Auftragsverarbeitung insofern überarbeitet werden, dass Passagen bzgl. des Datentransfers in ein Drittland (UK) eingefügt werden sollten. Für alle zukünftig abzuschließenden AV-Verträge mit Konzerngesellschaften oder Dritten in UK gilt das oben Gesagte ebenfalls, d. h. es bedarf einer Passage bzgl. Drittlandstransfer sowie zusätzlich SCC oder BCR o. ä.

Ferner ist umstritten, wenn der Auftragsverarbeiter innerhalb der EU sitzt und der Verantwortliche außerhalb, ob die Anforderungen der DSGVO „für den Rücktransfer“ der Daten vom Auftragsverarbeiter an den Verantwortlichen eingehalten werden müssen.

4.2 Unterauftragnehmer im Rahmen der Auftragsverarbeitung

Im AV-Vertrag sollte geregelt sein, wie bei der Beauftragung eines Unterauftragnehmers (insbesondere in einem Drittland wie UK bei einem harten Brexit) durch einen Auftragnehmer zu verfahren ist. Wenn im AV-Vertrag diesbezüglich nichts geregelt ist, ist die Inanspruchnahme von Unterauftragsverarbeitern durch den Auftragsverarbeiter ohne vorherige schriftliche Genehmigung des Verantwortlichen ausgeschlossen (Art. 28 Abs. 2 S. 1 DSGVO). Man kann jedoch eine generelle Genehmigung erteilen, dass der Auftragsverarbeiter den Verantwortlichen (nur) über die Inanspruchnahme eines Unterauftragsverarbeiters (und in welchem Drittland sich dieser befindet) vorab informieren muss und dass der Verantwortliche das Recht hat, der Inanspruchnahme des Unterauftragsverarbeiters zu widersprechen (Art. 28 Abs. 2 S. 2 DSGVO).

Falls solche Passagen bereits im AV-Vertrag enthalten sind, weil Datentransfers in andere Drittländer bereits stattfinden oder angedacht sind, sollten zumindest bezüglich Unterauftragnehmern in dem zukünftigen Drittland UK folgende Informationen im AV-Vertrag hinzugefügt werden (Stichtag ist der 29.03.2019, falls es zum harten Brexit kommt):

» Name des Unterauftragnehmers im Drittland,
» Angabe des Drittlandes, in dem der Unterauftragnehmer sitzt bzw. in dem der Unterauftragnehmer seine Server hat und somit das Drittland, in das personenbezogene Daten transferiert werden,
» Art der Dienstleistung,
» Datum der Beauftragung mit der Datenverarbeitung,
» Festlegung der Maßnahmen, mit denen ein angemessenes Datenschutzniveau sichergestellt wird (SSC, BCR etc.).

Für neu abzuschließende Verträge mit Dienstleistern im Rahmen der Auftragsverarbeitung empfehlen wir (unabhängig davon, ob der Dienstleister selbst in UK sitzt oder bereits Sub-Dienstleister in UK bekannt sind), dass jede Verlagerung in ein Drittland der vorherigen Zustimmung des Auftraggebers bedarf. Ferner sind die Bedingungen der Verlagerung zu definieren.

4.3 Datenübermittlung: C2C

Falls noch nicht innerhalb eines Datenschutzvertrags enthalten, sollten die Datenschutzverträge insofern überarbeitet werden, dass Passagen bzgl. des Datentransfers in ein Drittland eingefügt werden.

Es muss bei einem harten Brexit zusätzlich mindestens eine der in Punkt 3 genannten Maßnahmen ergriffen werden; typischerweise handelt es sich hierbei um EU-Standardvertragsklauseln (SSC) und bei einem konzerninternen Datentransfer ggf. auch Binding Corporate Rules (BCR).

5 Anwendungsfälle für Unternehmen mit Sitz in UK

5.1 Verarbeitung von Daten als Verantwortlicher

Die DSGVO ist zudem anwendbar, wenn der Verantwortliche außerhalb der EU niedergelassen ist, aber personenbezogene Daten von Betroffenen verarbeitet, die sich in der Union befinden. Der Aufenthalt in der EU, selbst der kurzfristige Aufenthalt, genügt hierfür. Der Betroffene muss nicht zwingend EU-Bürger sein, um von der DSGVO geschützt zu werden. Die DSGVO gilt in diesen Fällen selbst dann, wenn der jeweilige Vertragspartner ebenfalls außerhalb der EU angesiedelt ist; beispielsweise ein Unternehmen aus UK sammelt Visitenkarten auf einer Messe in Deutschland, auf der auch Besucher aus den USA sind.

Voraussetzung für die Anwendbarkeit der DSGVO unter diesen Umständen ist, dass die Verarbeitung personenbezogener Daten der in der EU befindlichen betroffenen Personen

» im Zusammenhang mit dem Anbieten von Waren / Dienstleistungen (gegen Entgelt oder unentgeltlich) steht oder
» zum Zwecke der Beobachtung des Verhaltens der betroffenen Personen in der EU (Internetaktivitäten, Profiling) erfolgt.

Da Art. 3 Abs. 2 lit. a DSGVO vom bloßen Anbieten spricht, bezieht dies die Sammlung von personenbezogenen Daten zum Newsletterversand mit ein. Das bedeutet also, erhebt bzw. verarbeitet ein Unternehmen aus einem Drittland selbst Daten von EU-Bürgern oder Nicht-EU-Bürgern, die sich in der EU aufhalten, so muss sich das Unternehmen aus dem Drittland an europäisches Datenschutzrecht halten. Das bedeutet bei einem „harten Brexit“ also, wenn z. B. das britische Unternehmen in Deutschland auf einer Messe vertreten ist, dort mit Messeteilnehmern ins Gespräch kommt, und deren personenbezogene Daten aufnimmt, so muss das britische Unternehmen den Informationspflichten nachkommen und eine Einwilligung einholen, z. B. um Newsletter zuschicken zu dürfen.

In dem Zusammenhang ist es von Vorteil, dass sich UK mit der EU dahingehend geeinigt hat, dass sich britische Gerichte für weitere 8 Jahre nach dem Brexit für eine Vorabentscheidung zwecks Interpretation von EU Recht (einschließlich DSGVO) an den Europäischen Gerichtshof wenden können.[2] Allerdings gibt die EU für die Konstellation, in der sowohl Verantwortlicher als auch Auftragnehmer außerhalb der EU niedergelassen sind, aber die Daten von in der EU befindlichen Betroffenen verarbeitet werden, keine SCC vor. Es müssten daher z. B. BCR oder Verhaltensregeln erstellen werden (s. o. unter Punkt 3 aufgeführte Möglichkeiten). Die UIMC unterstützt Sie hierbei.

5.2 Verarbeitung von Daten als Dienstleister/Auftragsverarbeiter

Die DSGVO ist zudem anwendbar, wenn der Auftragsverarbeiter außerhalb der EU niedergelassen ist, aber personenbezogene Daten von Betroffenen verarbeitet, die sich in der Union be-

[2] Michel Barnier, “Speech by Michel Barnier at the 28th Congress of the International Federation for European Law (FIDE)” (26 Mai 2018) <http://europa.eu/rapid/press-release_SPEECH-18-3962_en.htm>.

finden. Sofern der Auftraggeber in der EU ansässig ist, ist davon auszugehen, dass der Dienstleister (mit Sitz in der EU) personenbezogene Daten verarbeitet, die der DSGVO unterliegen. Daher ist die DSGVO ebenfalls soweit für den Dienstleister einschlägig, wie die Datenschutz-Grundverordnung Anforderungen an den Auftragsverarbeiter stellt.

6 Ausnahmetatbestände

Personenbezogene Daten dürfen ohne Abschluss geeigneter Garantien und ohne Angemessenheitsbeschluss übertragen werden, wenn

- die betroffene Person die ausdrückliche Einwilligung erteilt hat,
- Übermittlung der personenbezogenen Daten zur Erfüllung eines Vertrages mit dem Betroffenen erforderlich ist,
- dies zur Ausübung von Rechtsansprüchen nötig ist oder
- es wichtigen Gründen des öffentlichen Interesses dient.

7 Fazit

Bis zur Anerkennung eines angemessenen Datenschutzniveaus in UK muss die Einhaltung eines angemessenen Datenschutzniveaus beim Datenexport auf andere Weise sichergestellt werden. **Andernfalls müssten zum Stichtag (29. März 2019) alle Datentransfers nach UK beendet werden.** Daher empfehlen wir dringend, die aktuellen Datenflüsse zu analysieren und Maßnahmen bis zum 29.03.2019 zu ergreifen (sofern noch nicht geschehen):

<table>
<tr><th></th><th>konzern-intern</th><th>extern</th></tr>
<tr><td>Auftragsverarbeitung findet in UK statt
(Näheres in Kapitel 4.1)</td><td>1. Vertrag zur Auftragsverarbeitung (AV-Vertrag)[3]
2. plus
» BCR oder
» Standardvertragsklauseln</td><td>1. AV-Vertrag
2. plus Standardvertragsklauseln</td></tr>
<tr><td rowspan="2">Unterbeauftragung im Rahmen einer Auftragsverarbeitung findet in UK statt
(Näheres in Kapitel 4.2)</td><td colspan="2">Prüfung bestehender AV-Verträge, ob die Unterbeauftragung in Nicht-EU-Staaten geregelt ist (im UIMC-Muster enthalten):
Falls nein: nachfolgende 1. plus 2.
Falls ja: nachfolgendes 2.</td></tr>
<tr><td>1. AV-Vertrag
2. plus
» BCR (sofern Unterauftragnehmer im eigenen Konzern) oder
» Nachweis von BCR des Unterauftragnehmers oder
» Nachweis von Standardvertragsklauseln mit dem Unterauftragnehmer</td><td>1. AV-Vertrag
2. plus
» Nachweis von BCR des Unterauftragnehmers oder
» Nachweis von Standardvertragsklauseln mit dem Unterauftragnehmer</td></tr>
<tr><td>Datenübermittlung an Unternehmen mit Sitz in UK
(Näheres in Kapitel 4.3)</td><td>1. Prüfung der Rechtsgrundlage für Datenübermittlung
2. plus Vereinbarung zum Datenschutz
3. plus
» BCR oder
» Standardvertragsklauseln</td><td>1. Prüfung der Rechtsgrundlage für Datenübermittlung
2. plus Vereinbarung zum Datenschutz
3. plus Standardvertragsklauseln</td></tr>
</table>

[3] Muster im Online-Formular-Center der UIMC

8 Anlagen

8.1 Entwurf des Austrittsabkommens zwischen der EU und UK

Seit dem 14. November 2018 liegt dem britischen Parlament ein Entwurf des Austrittsabkommens vor. Teil VII dieses 585 Seiten umfassenden Entwurfes betrifft den Datenschutz.

Gemäß Art. 71 Abs. 1 des Entwurf-Austrittsabkommens findet EU-Datenschutzrecht in UK in Bezug auf die Verarbeitung personenbezogener Daten von betroffenen Personen außerhalb von UK Anwendung, sofern diese personenbezogenen Daten

a) vor Ende der Übergangszeit in UK auch schon nach Unionsrecht verarbeitet wurden oder

b) in UK nach Ablauf der Übergangszeit auf der Grundlage dieses Abkommens verarbeitet werden.

Sofern irgendwann in Zukunft ein Angemessenheitsbeschluss i. S. d. Art. 45 Abs. 3 DS-GVO durch die EU für UK getroffen würde (siehe Punkt 8.2), entfiele obige Regelung gemäß Art. 71 Abs. 2 des Entwurf-Austrittsabkommens.

Wenn dieser Angemessenheitsbeschluss wiederum zu einem späteren Zeitpunkt aufgehoben würde, so verpflichtet sich UK gemäß Art. 71 Abs. 3 des Entwurfs des Austrittsabkommens ein eigenes Datenschutzgesetz einzuführen, welches ein Datenschutzlevel sicherstellt, das dem Level des EU Datenschutzrecht entspricht.

Artikel 72 des Austrittsabkommen-Entwurfs besagt, dass unbeschadet des Artikels 71 neben dem EU Datenschutzrecht die Bestimmungen des EU-Rechts über die vertrauliche Behandlung, Nutzungsbeschränkung, Speicherdauer/-beschränkung sowie die Pflicht zur Löschung von Daten und Informationen

a) vor dem Ende der Übergangszeit oder

b) aufgrund dieser Vereinbarung

hinsichtlich solcher Daten gelten, die von Behörden oder amtlichen Stellen in UK oder von öffentlichen Auftraggebern oder öffentlichen Unternehmen in UK im Bereich der Wasser-, Energie- und Verkehrsversorgung sowie der Postdienste oder derartigen Auftraggebern, die in UK niedergelassen sind, erhoben werden.

Gemäß Artikel 73 des Entwurfs des Austrittsabkommens soll die Union die Daten, die vor Ablauf der Übergangszeit oder nach Ablauf der Übergangszeit aufgrund des Entwurf-Austrittsabkommens aus UK erhalten wurden, nicht ausschließlich aus dem Grund des Austritts von UK aus der EU anders behandeln als Daten, die von einem Mitgliedstaat erhalten werden.

8.2 Verhandlungen über den Angemessenheitsbeschluss

Ob die EU einen Angemessenheitsbeschluss zu Gunsten von UK trifft und wie lange der Prozess dauern wird, ist Zukunftsmusik.

Im Rahmen der Brexit-Verhandlungen ließ UK verlauten, dass sie einen Sitz im EDSA (EDPB = European Data Protection Board) behalten möchten. Zudem möchte UK weiterhin am One-Stop-Shop teilhaben. Michel Barnier, Brexit Verhandlungsführer auf Seiten der EU, merkte dazu jedoch an, dass die EU ihre Entscheidungsautonomie nicht mit einem Drittland teilen kann und wird, selbst nicht mit einem ehemaligen Mitgliedsstaat der EU, welcher nicht Teil des EU Rechtssystem sein möchte. Er begründete dies u. a. damit, dass nach dem Austritt von UK aus der EU die EU u. a. nicht mehr sicherstellen kann, dass UK britische Gesetze zum Datenschutz jedes Mal anpasst, wenn die EU die DSGVO updatet und auch nicht sicherstellen kann, dass die Vorschriften der DSGVO einheitlich in UK und der EU interpretiert werden.

Die EU Kommission hat am 13.11.2018 einen Notfallplan zu bestimmten Themen, u. a. dem Datenschutz veröffentlicht, für den Fall, dass das Vereinigte Königreich das Austrittsabkommen nicht unterzeichnet. Darin steht auch, dass „die Annahme eines Angemessenheitsbeschlusses nicht Teil der Krisenplanung der Kommission“ ist, d. h. ein Angemessenheitsbeschluss müsste also erst beantragt und verhandelt werden.

Was die Verhandlungen erschweren wird ist, dass UK wie ein Drittland (z. B. die USA und China) behandelt wird und die Verhandlungen diesbezüglich lange dauern können und eventuell UK nicht als Land mit angemessenem Datenschutzniveau anerkannt wird.

Diesbezüglich ist außerdem zu bedenken, dass UK den Investigatory Powers Act 2016 (aka the Snoopers‘ Charter) beschlossen hat. Dieses Überwachungsgesetz gewährt britischen Geheimdiensten weitreichende Überwachungsrechte. Man denke hier an das Safe Harbour Abkommen mit den USA, welches bereits vom EuGH gekippt wurde. Der High Court in UK hat bzgl. des Investigatory Powers Act 2016 bereits ebenfalls im April 2018 entschieden, dass dieser bzw. der Abschnitt über die Aufbewahrung von Kommunikationsdaten, nicht mit EU-Recht kompatibel ist und daher überarbeitet werden muss.

Selbst wenn die EU ein angemessenes Schutzniveau in UK feststellen würde, so nimmt der Gesamtprozess viel Zeit in Anspruch. Zunächst müssten die Modalitäten verhandelt werden. Falls es zu einem erfolgreichen Abschluss käme und beide Seiten den Datenschutz des jeweils anderen Systems als gleichwertig anerkennen (zurzeit müsste aber noch der Investigatory Powers Act 2016 geändert werden), so müssten beide Seiten den internen Prozess im jeweiligen Land einleiten. Das Kollegium der EU Kommission müsste zustimmen. Die EU müsste eine Stellungnahme des EDSA einholen. Darüber hinaus würde der Ausschuss des Europäischen Parlaments für bürgerliche Freiheiten, Justiz und Inneres informiert und dieser müsste zustimmen. Danach würde der Angemessenheitsbeschluss durch das Kollegium angenommen oder abgelehnt. Das jeweilige Drittland muss auf seiner Seite ebenfalls einen Beschluss fassen, der die Angemessenheit des Datenschutzniveaus feststellt.

Das gesamte Verfahren von der Aufnahme von Gesprächen bis hin zur Anerkennung der Angemessenheit dauert beispielsweise mit Japan voraussichtlich mindestens anderthalb Jahre.[4] Wenn man bedenkt wie die Brexit-Verhandlungen laufen, könnte man damit rechnen, dass Verhandlungen zum Datenschutzniveau sich ebenfalls lange hinziehen könnten.

Dies führt zwingend dazu, dass bei einem Brexit ohne vertragliche Übergangsregelungen zum Datenschutz die oben getätigten Ausführungen zu berücksichtigen sind.

[4] Im Januar 2017 kündigte die Kommission an, mit Japan zwecks Erreichung eines Angemessenheitsbeschlusses in einen Dialog zu treten. Mitte Juli 2018 erklärte die EU Kommission, dass die Gespräche mit Japan bezüglich eines angemessenen Datenschutzniveaus erfolgreich abgeschlossen wurden. Im Winter 2018 erwartet die Kommission das Verfahren abgeschlossen zu haben.