www.jusletter-it.eu

Bernd Schmidt / Claudia Bischof

Datenschutzrechtliche Folgen des Brexit

Ist Großbritannien bald ein unsicheres Drittland?

First there was a shock – then nothing happened for a long time. On 23 June 2016, the citizens of Great Britain have voted to leave the European Union and EU representatives now demand to start exit negotiations swiftly. Amongst other things, the unsettled state of Great Britain as a secure or unsecure third county – in terms of data protection – will be directly affected. The consequences for companies with business relationships to Great Britain might be substantial. The authors discuss data protection-related consequences of a Brexit, possibilities for legal reaction to the upcoming Great Britain EU exit and concerned companies' opportunities for reacting to the expected events. (ah)

Category: Articles
Region: Germany
Field of law: Data Protection

Citation: Bernd Schmidt / Claudia Bischof, Datenschutzrechtliche Folgen des Brexit, in: Jusletter IT 22 September 2016

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Inhaltsübersicht

1. Internationale Datenübermittlungen

[Rz 1] Die europäische Wirtschaft ist heute stärker vernetzt denn je – Zusammenschlüsse von Unternehmen über Grenzen hinweg sind heute die Regel. Grenzüberschreitende Datenübermittlungen sind damit eine Notwendigkeit. Die Rechtfertigung internationaler Datenübermittlungen kann jedoch praktisch mit erheblichen Herausforderungen verbunden sein.

[Rz 2] Sowohl nach europäischem Recht als auch nach Schweizer Recht, setzt eine grenzüberschreitende Datenübermittlung voraus, dass in dem Drittstaat ein angemessenes Datenschutzniveau besteht (siehe Art. 6 Abs. 1 Schweizer Bundesgesetz über den Datenschutz [DSG] und Art. 25 Abs. 1 Europäische Datenschutzrichtlinie [Richtlinie 95/46/EG; EU-DSRL]). Für die Datenübermittlung durch verantwortliche Stellen in der Schweiz führt der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte eine Liste, aus der sich der Status von Drittstaaten ergibt.[1]

[Rz 3] Für Mitgliedsstaaten der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (EWR) gilt, dass sie mit der Umsetzung der EU-DSRL ein angemessenes Datenschutzniveau gewährleisten. Verantwortliche Stellen in einem EU bzw. EWR Mitgliedstaat dürfen daher Daten in einen anderen Mitgliedsstaat übermitteln, ohne dass sich dadurch zusätzliche Anforderungen an die datenschutzrechtliche Rechtfertigung ergeben. Die EU Kommission hat zudem für Andorra, Argentinien, Kanada, Färöer-Inseln, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, Schweiz und Uruguay gemäß Art. 25 Abs. 5 EU-DSRL festgestellt, dass diese ein angemessenes Datenschutzniveau haben,[2] so dass in diese Länder personenbezogene Daten ohne zusätzliche Rechtfertigungsanforderungen übermittelt werden dürfen.

[Rz 4] Dieses System internationaler Datenübermittlungen wird für die EU bzw. den EWR mit der Europäischen Datenschutzgrundverordnung (Verordnung [EU] 2016/679; EU-DSGVO) in seinen wesentlichen Elementen fortgeschrieben.

2. Aktueller Status Großbritanniens

[Rz 5] Bisher erfordert die Datenübermittlung von verantwortlichen Stellen in der EU bzw. dem EWR zu verantwortlichen Stellen in Großbritannien keine zusätzliche datenschutzrechtliche Rechtfertigung. Für Großbritannien als EU Mitgliedsstaat gilt die Vermutung, dass mit der Um-

1 https://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=de&download=NHzLpZeg7t, lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdXt3fmym162epYbg2c_JjKbNoKSn6A-- (alle Websites zuletzt besucht am 29. August 2016).

2 http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

setzung der EU-DSRL dort ein «angemessenes Datenschutzniveau» herrscht,[3] auch wenn das britische Datenschutzniveau im EU-Vergleich teilweise als gering bewertet wird.[4] Diese Vermutung wird mit einem Austritt Großbritanniens aus der EU wegfallen und es müsste geprüft und festgestellt werden, ob auch zukünftig ein «angemessenes Schutzniveau» in Großbritannien besteht.

[Rz 6] Dieser Nachweis dürfte mit gewissen Herausforderungen verbunden sein. Die ab 2018 geltende EU-DSGVO führt im Vergleich zur EU-DSRL zahlreiche Neuregelungen ein, die in Großbritannien bislang nicht umgesetzt sind, zum Beispiel die Verzeichnisse von Verarbeitungstätigkeiten gemäß Art. 30 EU-DSGVO, die Bestellung eines Datenschutzbeauftragten gemäß Art. 37 EU-DSGVO oder die Verträge zur Auftragsdatenverarbeitung gemäß Art. 28 EU-DSGVO.[5]

3. Gestaltung des datenschutzrechtlichen Status von Großbritannien

[Rz 7] Wie Großbritannien sein Datenschutzrecht nach einem EU Austritt gestaltet ist offen. Sicher ist jedoch, dass der EU Austritt das datenschutzrechtliche Rechtfertigungssystem für Datenübermittlungen aus der EU bzw. dem EWR nach Großbritannien erschüttern wird. Auch andere Staaten, wie die Schweiz müssen dann die Frage nach der Angemessenheit des Datenschutzniveaus in Großbritannien neu bewerten. Unternehmen innerhalb der EU bzw. des EWR müssen Datenübermittlungen nach Großbritannien künftig auf alternative Rechtfertigungen stützen. Auch für verantwortliche Stellen in der Schweiz wird sich nach einem Brexit die Frage stellen, ob Großbritannien noch ein «angemessenes Datenschutzniveau» gewährleistet.

[Rz 8] Aktuell ist Großbritannien noch Mitglied der EU. Das kann sich gemäß Art. 50 Abs. 2 Vertrag über die Europäische Union (EU-Vertrag) auch erst ändern, wenn Großbritannien dies verbindlich beschließt und dem Europäischen Rat mitteilt, also einen entsprechenden Antrag stellt. Dann kommt es zu Austrittsverhandlungen und zum Abschluss eines Abkommens in dem die gegenseitigen Beziehungen für die Zukunft geregelt werden.[6] Es ist nicht zwingend, aber natürlich sinnvoll, auch den datenschutzrechtlichen Status Großbritanniens in einem solchen Abkommen zu regeln. Welchen Inhalt ein Austrittsabkommen zwischen der EU und Großbritannien in dieser Hinsicht haben wird, ist aktuell nicht sicher vorherzusagen. Wahrscheinlich sind jedoch die im Folgenden aufgezeigten Szenarien.

3.1. Beitritt zum EWR – das Norwegen Modell

[Rz 9] Das Szenario mit der geringsten Auswirkung auf die Gestaltung von Datenübermittlungen zwischen EU bzw. EWR und Großbritannien wäre ein Beitritt Großbritanniens zum EWR. Diesen Weg haben zuvor schon Island, Liechtenstein und Norwegen gewählt, indem sie mit der EU ein

---

3 Tim Wybitul, Handbuch Datenschutz im Unternehmen, Verlag Recht und Wirtschaft, Frankfurt 2011, Rn. 272 f.

4 Barbara Mayer/Gerhard Manz, Der Brexit und seine Folgen auf den Rechtsverkehr zwischen der EU und dem Vereinigten Königreich, in: Betriebs-Berater 2016, Heft 30 (59), S. 1731–1740.

5 Sibylle Gierschmann, Brexit – Was passiert, wenn Großbritannien «Drittland» wird?, in: MultiMedia und Recht 2016, Heft 8, S. 501–502.

6 Zur Geschichte dieser erst mit dem Vertrag von Lissabon geschaffenen Regelung und ihren Anforderungen im Detail siehe Alexander Thiele, Der Austritt aus der EU – Hintergründe und rechtliche Rahmenbedingungen eines «Brexit», in: Europarecht 2016, Heft 3, S. 281.

Abkommen über den gemeinsamen Binnenmarkt geschlossen haben. Dieser Weg ist auch unter dem Stichwort «Norwegen Modell» bekannt.

[Rz 10] Der EWR besteht aus EU Mitgliedsstaaten und den Staaten der European Free Trade Association (EFTA) mit Ausnahme der Schweiz. Für diese EFTA Staaten ist ein Prozess vorgesehen, in dem die EFTA relevanten europäischen Rechtsakte in die Anlagen zum EFTA Vertrag aufgenommen werden. Diese Rechtsakte gelten dann unmittelbar für diese EFTA Staaten und schaffen eine Rechtslage wie für EU Mitgliedsstaaten.

[Rz 11] Die EU-DSRL ist in diesem Verfahren geltendes Recht in Island, Liechtenstein und Norwegen geworden und hat zur Umsetzung entsprechender nationaler Datenschutzgesetze geführt, die ein angemessenes Datenschutzniveau sicherstellen.

[Rz 12] Für die DSGVO ist das Verfahren zur Aufnahme als verbindlicher EFTA Rechtsakt noch nicht abgeschlossen. Es ist aber davon auszugehen, dass die EU-DSGVO im gesamten EWR verbindliches Recht wird. Sollten sich Großbritannien und die EU auf diesen Weg verständigen, bliebe datenschutzrechtlich fast alles beim Alten.

3.2. Der Schweizer Weg

[Rz 13] Die Schweiz ist dem EWR nicht beigetreten, so dass dort aus der EU-Perspektive zunächst nicht die Vermutung eines angemessenen Datenschutzniveaus gilt. Ergebnis der Verhandlungen um den Austritt Großbritanniens aus der EU könnte auch sein, nicht dem EWR beizutreten. Wie für die Schweiz würde sich auch für Großbritannien die Frage stellen, ob dort ein angemessenes Datenschutzniveau besteht, das es rechtfertigt, Datenübermittlungen ohne zusätzliche Voraussetzungen zuzulassen.

[Rz 14] Wie aktuell gemäß Art. 25 Abs. 6 EU-DSRL kann die EU Kommission künftig gemäß Art. 45 Abs. 1 DSGVO prüfen und feststellen, ob ein Drittland ein angemessenes Datenschutzniveau gewährleistet. Eine solche Entscheidung wäre zunächst verbindlich, könnte aber gegebenenfalls durch den Europäischen Gerichtshof (EuGH) überprüft und ggf. aufgehoben werden. Dies ist jüngst geschehen im Fall der Safe-Harbor-Entscheidung für Datenübermittlungen in die USA.[7]

[Rz 15] Für Datenübermittlungen zwischen der EU bzw. dem EWR und der Schweiz ist es mit diesem Verfahren gelungen, einen weitgehend komplikationsfreien Datenverkehr zu ermöglichen. Grundsätzlich könnte dies auch für Datenübermittlungen nach Großbritannien funktionieren. Als Folge der Safe-Harbor-Entscheidung des EuGHs sind die Aufsichtsbehörden jedoch verpflichtet, auch beim Vorliegen einer Angemessenheitsentscheidung für einzelne Datenübermittlungen zu prüfen, ob ein angemessenes Datenschutzniveau tatsächlich gewährleistet ist.

[Rz 16] Das könnte sich für Großbritannien auf längere Sicht als Problem erweisen. Bei der Prüfung berücksichtigen die Datenschutzaufsichtsbehörden nämlich auch Zugriffsbefugnisse von Behörden und Diensten auf personenbezogene Daten, was vor dem Hintergrund einer traditionell engen Zusammenarbeit Britischer Behörden mit US Behörden problematisch werden könnte. Zu berücksichtigen wäre für eine Entscheidung über die Angemessenheit des Datenschutzstandards in Großbritannien auch bereits heute geäußerte Kritik, dass in Großbritannien der Schutz

7 Urteil des EuGH C362/14 vom 6. Oktober 2015.

der Informationellen Selbstbestimmung schwächer ausgestaltet ist als in anderen EU Mitgliedsstaaten.[8]

[Rz 17] Großbritannien wäre daher gut beraten, individuell eine Regelung in einem Austrittsabkommen zu vereinbaren, die den Status eines sicheren Drittstaats festschreibt.

3.3. Datenübermittlungen nach Großbritannien als unsicheres Drittland

[Rz 18] Sollte Großbritannien im Rahmen der Austrittsverhandlungen keinen Status als sicheres Drittland erhalten oder diesen wieder verlieren, müssten Datenübermittlungen nach Großbritannien entsprechend der sogenannten Zweistufentheorie gerechtfertigt werden. Dieses Konzept internationaler Datenübermittlungen ist in seinen wesentlichen Elementen sowohl in der EU-DSRL als auch in der EU-DSGVO enthalten. Für Datenübermittlungen nach Großbritannien würden sich dann Herausforderungen und Probleme stellen, die man in der Praxis des Datenschutzrechts für Übermittlungen in Drittstaaten ohne angemessenes Datenschutzniveau kennt.

[Rz 19] Auf der ersten Stufe müssten die Voraussetzungen einer datenschutzrechtlichen Rechtfertigung wie für eine Datenübermittlung innerhalb der EU bzw. des EWR oder in ein sicheres Drittland – wie die Schweiz – geschaffen werden.

[Rz 20] Auf der zweiten Stufe müsste eine Rechtfertigung der Datenübermittlung in das unsichere Drittland bestehen. Dies ist nur in klar definierten Ausnahmefällen zulässig, die sich aktuell aus Art. 26 Abs. 1 EU-DSRL bzw. der Umsetzung im Recht der Mitgliedsstaaten ergeben. Diese Regelungen entsprechen im Wesentlichen Art. 6 Abs. 2 DSG, mit einer besonders relevanten Ausnahme. Eine Privilegierung von Datenübermittlungen zu konzernangehörigen Unternehmen oder Unternehmensteilen wie in Art. 6 Abs. 1 lit. g DSG gibt es im europäischen Recht nicht.

[Rz 21] Mit Inkrafttreten der EU-DSGVO ergeben sich Rechtfertigungen zur Datenübermittlung in unsichere Drittstaaten aus Art. 49 Abs. 1 EU-DSGVO und lassen diese nur (wie bereits nach der aktuellen Rechtslage) ausnahmsweise zu, zum Beispiel, wenn die betroffene Person individuell eingewilligt hat, es der Erfüllung eines Vertrages, der Geltendmachung von Rechtsansprüchen oder überwiegenden öffentlichen Interessen dient. Diese Rechtfertigungstatbestände sind in vielen Fällen, etwa der konzernweiten Nutzung von IT-Systemen oder einem konzernweiten Reporting jedoch nicht hinreichend.

[Rz 22] Hier sehen Art. 26 Abs. 4 EU-DSRL bzw. Art. 46 Abs. 2 lit. c EU-DSGVO den Abschluss von der EU Kommission genehmigter Verträge zwischen dem Datenexporteur und dem Datenimporteur im unsicheren Drittland vor. Dies sind aktuell die sogenannten EU-Standardvertragsklauseln – das derzeit wohl am meisten genutzte Instrument zur Herstellung eines angemessenen Datenschutzniveaus.[9]

[Rz 23] Alternativ können auch individuell vereinbarte Verträge geschlossen werden, sogenannte *ad hoc* Klauseln. Diese Klauseln müssen inhaltlich so gestaltet sein, dass ein wirksamer Schutz der Rechte der Betroffenen gewährleistet ist. Zudem müssen sie in dem unsicheren Drittstaat

8 Mayer/Manz (Fn. 4), S. 1731–1740.

9 Siehe hierzu grundlegend aus der Perspektive des deutschen Datenschutzrechts: Detlev Gabel, in: Jürgen Taeger/Detlev Gabel (Hrsg.), BDSG und Datenschutzvorschriften des TKG und TMG, 2. Auflage, Verlag Recht und Wirtschaft, Frankfurt 2013, § 4c Rn. 21 ff.

wirksam und durchsetzbar sein.[10] *Ad hoc* Klauseln erzeugen im Gegensatz zu den EU Standardvertragsklauseln jedoch keine Vermutung der Herstellung eines angemessenen Datenschutzniveaus beim Datenimporteur und müssen im Einzelfall von der zuständigen Aufsichtsbehörde genehmigt werden. Sie sind daher ein wenig genutztes Instrument. Dass sich hieran mit der EU-DSGVO etwas ändern wird, ist nicht zu erwarten.

[Rz 24] Eine Variante der ad *hoc* Klauseln sind sogenannte Binding Corporate Rules (BCR), mit denen die Datenübermittlung in internationalen Konzernen gerechtfertigt werden kann. Auch sie setzen einen Prozess der Kontrolle und Genehmigung durch die zuständige Aufsichtsbehörde voraus. Das in der EU-DSRL noch nicht erwähnte Instrument der BCR sowie der Prozess zu ihrer Implementierung sind nun weitgehend entsprechend der aktuellen Genehmigungspraxis der Aufsichtsbehörden ausdrücklich in Art. 47 Abs. 2 EU-DSGVO beschrieben.

[Rz 25] BCR sind insbesondere in größeren Konzernstrukturen ein geeignetes Instrument zur Rechtfertigung internationaler Datenübermittlungen. Hier steht ihr relativ hoher Implementierungsaufwand in einem angemessenen Verhältnis zu dem Ziel, flexible Lösungen für konzerninterne Datenübermittlungen zu schaffen.

[Rz 26] Als neue Rechtfertigungsmechanismen gibt es mit dem Inkrafttreten der EU-DSGVO zudem genehmigte Verhaltensregeln und Zertifizierungen. Auch diese können für eine Rechtfertigung von Datenübermittlungen in unsichere Drittstaaten relevant werden. Gemäß Art. 40 EU-DSGVO können Verbände und andere Vereinigungen für ihre Mitglieder verbindliche Verhaltensregeln erlassen, die einen angemessenen Schutz der Betroffenenrechte gewährleisten und die von der zuständigen Aufsichtsbehörde genehmigt werden müssen. Auf Ebene der verantwortlichen Stelle gibt es gemäß Art. 42 EU-DSGVO zudem die Möglichkeit der Zertifizierung mit einem anerkannten Siegel oder Prüfzeichen, um eine Rechtfertigung unter anderem der Datenübermittlung in unsichere Drittstaaten zu rechtfertigen.

4. Handlungsmöglichkeiten betroffener Unternehmen

[Rz 27] Die Folgen eines Brexits sind in dieser frühen Phase noch völlig offen. Ein Antrag auf EU Austritt ist weder gestellt noch konkret angekündigt. Britische Verfassungsrechtler meinen, dass das britische Parlament – welches im Vorfeld des Referendums mehrheitlich gegen einen Brexit votiert hatte – in einem Beschluss dem Antrag auf Austritt zustimmen müsse.[11] Insoweit ist nicht absolut sicher, dass es zu einem Antrag kommen wird. Die möglichen Folgen sind aber so gravierend, dass betroffene Unternehmen sich den damit verbundenen Auswirkungen bereits jetzt annehmen sollten. Allgemeingültige Handlungsempfehlungen kann es hierfür nicht geben; gefragt sind vielmehr angepasste Reaktionen mit Augenmaß. In jedem Fall sollte aber analysiert werden, welche Datenströme im Unternehmen oder der Unternehmensgruppe nach Großbritannien fließen und ob es alternative technische Gestaltungen gibt.

[Rz 28] Soweit ein Dienstleister die Möglichkeit bietet, mit einer Gesellschaft in einem EU oder EWR Mitgliedsstaat zu kontrahieren, statt mit der britischen Schwester und dort belegene IT-Infrastruktur für den Dienst zu nutzen, sollte das jedenfalls in Erwägung gezogen werden. Auch

10 Ehmann/Helfrich, EG-Datenschutzrichtlinie, Otto Schmid Verlag, Köln 1999, Art. 26, Rn. 21.

11 Mayer/Manz (Fn. 4), S. 1731.

die Vorbereitung auf Ausstiegs-Szenarien kann im Einzelfall geboten sein. Möglich ist, in Verträgen mit Dienstleistern eine Option aufzunehmen, den Dienst im Falle eines Brexits und dem Wegfall des sicheren Drittlandstatus, zu verlagern oder den Vertrag zu beenden und den Service wieder ein- oder umzusourcen.

[Rz 29] In Konzernstrukturen können Möglichkeiten bestehen, alternative Routen und Verantwortlichkeiten zu wählen, um die Datenübermittlungen nach Großbritannien zu vermeiden. Solche Gestaltungen können im Zweifel auch als Fall Back Lösung für den Ernstfall vorgesehen werden. Soweit eine solche Gestaltung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, sollte man aber jetzt (noch) nicht in Panik verfallen. Abhängig von den Austrittsverhandlungen kann am Ende schließlich immer noch alles gut werden. Dass es zum Äußersten kommt und Großbritannien von heute auf morgen zum unsicheren Drittstaat wird, ist jedenfalls nicht besonders wahrscheinlich.

5. Fazit

[Rz 30] Nach dem der «schicksalshafte»[12] Volksentscheid über den EU Austritt Großbritanniens einen Sturm der Emotionen ausgelöst hatte, herrscht aktuell überraschende Stille. Früher oder später wird man sich aber in Großbritannien der Realität stellen und den wohl unvermeidlichen Antrag auf den Austritt stellen. Dieser wird auch das Fundament der Rechtfertigung von Datenübermittlungen nach Großbritannien erschüttern. Welche Voraussetzungen dann für Datenübermittlungen nach Großbritannien gelten ist völlig offen. Verantwortliche Stellen sollten sich dieser unsicheren Perspektive bewusst sein und diese bereits jetzt in ihre Compliance-Strategie einbeziehen.

Rechtsanwalt Dr. Bernd Schmidt, LL.M., und Rechtsanwältin Claudia Bischof sind Gründungspartner der Hamburger Kanzlei PLANIT // LEGAL. Sie beraten nationale und internationale Unternehmen im IT- und Datenschutzrecht.

12 Peter Cullen, Brexit – ein Projekt der Unvernunft, in: Europäische Zeitschrift für Wirtschaftsrecht 2016, Heft 11, S. 401.