Brexit Quick Brief

Datenschutz und -übermittlung

Kernpunkte

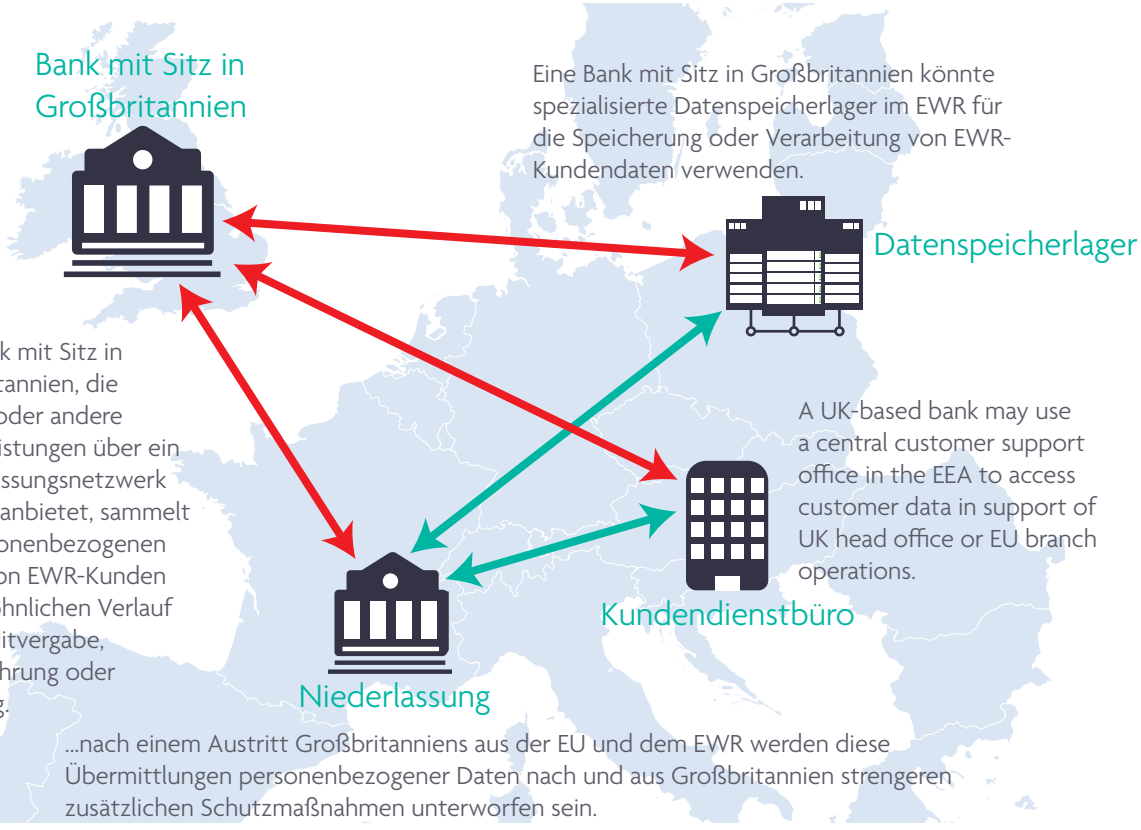
- Die Übermittlung personenbezogener Daten über verschiedene Standorte hinweg ist ein integraler Bestandteil moderner Bankgeschäfte. Finanzdienstleistungsunternehmen speichern und verarbeiten Daten digital als Teil ihrer Geschäftstätigkeiten. Hierunter fallen unter anderem die Privat- und Geschäftskontoführung, die Kreditvergabe, der Wertpapierhandel, die Investitionen, die Verhinderung von Finanzkriminalität und das Personalmanagement.
- Innerhalb der EU und des EWR unterliegt die Verarbeitung personenbezogener Daten der EU-Datenschutzregelung, die dem Schutz der individuellen Privatsphäre und anderer Informationsrechte dient. Diese Regulierung genehmigt die Übermittlung personenbezogener Daten innerhalb des EWR. Viele Banken und andere Unternehmen in der EU haben sich diesen Rahmen zunutze gemacht, um ihre Datenverarbeitung oder ihren Kundendienst und Back-Office-Funktionen durch ihre Zusammenlegung an wenigen zentralen Standorten innerhalb der EU bzw. des EWR zu rationalisieren.
- Nach der Entscheidung Großbritanniens aus der EU auszutreten haben sowohl Großbritannien als auch die EU ein gemeinsames Interesse an der Sicherung der effizienten Datenübermittlung in einer zunehmend digitalen Welt, in der der freie Datenverkehr Teil alltäglicher Geschäftstätigkeiten ist.
- Die EU hat substantielle Schutzmaßnahmen für die Übermittlung personenbezogener Daten außerhalb der EU eingerichtet, deren Anwendung komplex und ressourcenintensiv sein kann und auch eine juristische Herausforderung darstellen kann. Die EU ersetzt derartige Einschränkungen mit einer allgemeinen Genehmigung des freien Datenverkehrs, wenn sie die Datenschutzstandards eines anderen Landes als „angemessen“ anerkennt.
- Eine Einigung Großbritanniens mit der EU über ein „angemessenes Niveau“ der jeweiligen Datenschutzregulierungen könnte sich nach dem Austritt Großbritanniens aus der EU als schwierig erweisen. Die Erfahrung des Einigungsprozesses der EU mit den USA auf einen Rahmen zur Feststellung eines angemessenen Datenschutzniveaus weist auf einige potentielle Streitfragen bei künftigen Verhandlungen hin.
- Selbst wenn eine Entscheidung über die Angemessenheit getroffen werden kann, wird dieser Prozess einige Zeit dauern. Daher müssen eventuell Übergangsvereinbarungen getroffen werden.
- Ohne eine Vereinbarung zum angemessenen Datenschutzniveau bzw. im Vorfeld einer Vereinbarung müssten Unternehmen bei Fehlen einer Übergangsvereinbarung

UK Finance Quick Briefs sind eine Reihe kurzer Beiträge, die den Leser über wichtige wirtschaftliche, regulatorische und politische Fragen rund um den Brexit informieren sollen. Obwohl der Schwerpunkt auf den Bankwesen liegt, haben viele der diskutierten Themen allgemeine Relevanz. BQB können einzeln oder in Verbindung mit anderen Beiträgen der BQB-Reihe gelesen werden. Es ist geplant, die Reihe um Themen zu erweitern, die in Zukunft an Bedeutung gewinnen. Weitere Informationen finden Sie unter www.ukfinance.org.uk/quickbriefs

neue überbrückende Systeme für die Zwischenzeit herstellen, welche die Einhaltung von Einschränkungen beim personenbezogenen Datenverkehr zwischen Großbritannien und der EU gewährleisten. Es wird für Unternehmen in allen Branchen wichtig sein zu überprüfen, inwieweit sie selbst und Drittunternehmen innerhalb ihrer Versorgungskette diese Vorgaben erfüllen, da es kein einheitliches Konformitätsmodell geben wird. Das könnte sich als komplexe Aufgabe erweisen und könnte die Umsiedlung einiger Geschäftsbereiche erfordern.

- Diese Problematiken haben wesentliche Auswirkungen weit über den Banken- und Finanzdienstleistungssektor hinaus – alle Unternehmen, die auf die Übermittlung personenbezogener Daten zwischen der EU und Großbritannien angewiesen sind, könnten potentiell betroffen sein.
- Es muss daher auch ein Rahmen geschaffen werden, durch den gewährleistet wird, dass Datenübermittlungen zwischen Großbritannien und Nicht-EU-Ländern sicher und effizient fortlaufen können.

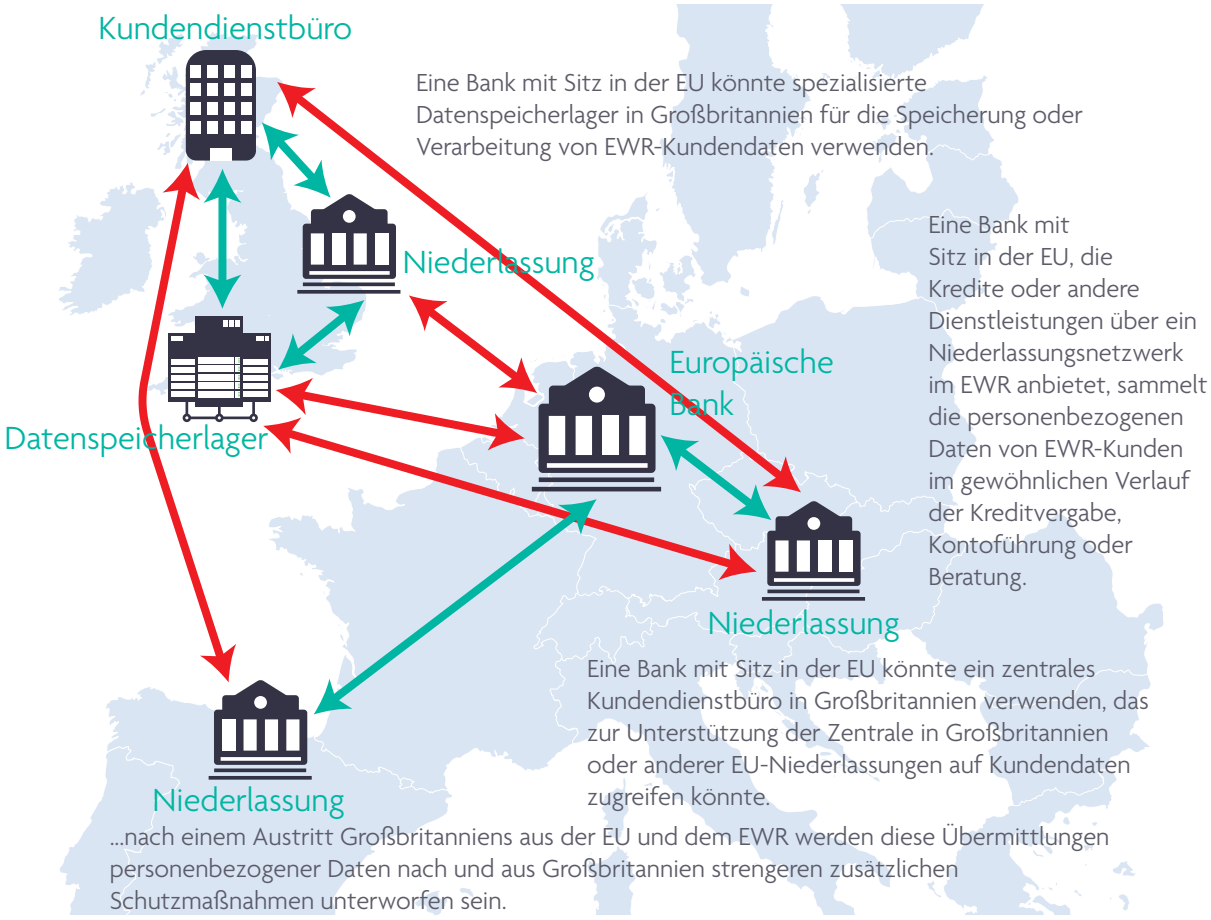
Datenübermittlung innerhalb und außerhalb des EU-Binnenmarkts



Unbeschränkte Datenübermittlung.

Datenübermittlung, die potentiell zusätzlichen strikten Schutzmaßnahmen unterworfen ist.

Bank mit Sitz in der EU



Datenverkehr im EU-Binnenmarkt

Viele Banken und andere Unternehmen in der EU haben ihre Datenlagerung oder -verarbeitung oder ihren Kundendienst oder Back-Office-Funktionen durch die Zusammenlegung an zentralen Standorten innerhalb der EU rationalisiert.

Die Übermittlung personenbezogener Daten über verschiedene Standorte hinweg ist ein integraler Bestandteil moderner Bankdienstleistungen. Banken und andere Finanzdienstleistungsunternehmen speichern und verarbeiten personenbezogene Daten digital als Teil ihrer allgemeinen Geschäftstätigkeiten. Hierunter fallen unter anderem die Kreditvergabe, der Wertpapierhandel, die Investitionen, die Privat- und Geschäftskontoführung sowie die Einhaltung der Sorgfaltspflichten und gesetzlichen Bestimmungen, z. B. zur Verhinderung von Geldwäsche und der Finanzierung von Terroristen. Die verschiedenen Standorte eines Unternehmens tauschen untereinander Daten aus, zum Beispiel zur Verarbeitung in spezialisierten Einrichtungen. Hierunter fallen unter anderem individuelle Kundendaten, Mitarbeiterdaten oder Geschäftskundendaten soweit sie zum Beispiel den Vorstand oder die Mitarbeiter des jeweiligen Geschäftskunden betreffen. In einer zunehmend digitalen Wirtschaftswelt ist die grenzüberschreitende Übermittlung von Daten innerhalb von und zwischen Unternehmen ein Teil der alltäglichen Geschäftstätigkeiten in einer riesigen Bandbreite von Branchen weit über den Banken- und Finanzdienstleistungssektor hinaus.

Wie werden personenbezogene Daten innerhalb des EU-Binnenmarkts übermittelt?

Innerhalb der EU und des EWR unterliegt die Verarbeitung personenbezogener Daten der EU-Datenschutzregelung, die Datenübermittlungen innerhalb des EWR erlaubt. Zentral dabei ist die europäische Datenschutzrichtlinie, die Mindeststandards für den Zugriff auf personenbezogene Daten von EU/EWR-Einzelpersonen sowie deren Speicherung, Verarbeitung und Übermittlung setzt, um ihre Rechte und Interessen, insbesondere in Bezug auf ihre Privatsphäre, zu schützen. Soweit Unternehmen diese Datenschutzvorgaben einhalten, dürfen sie die personenbezogenen Daten von Kunden und Mitarbeitern innerhalb der EU frei übermitteln. Das bildet die Grundlage für ein breites Spektrum an alltäglichen Aktivitäten, und viele Banken und andere Unternehmen in der EU haben sich diesen Rahmen zunutze gemacht, um effektiver und effizienter zu arbeiten durch die Rationalisierung ihrer Datenlagerung bzw. -verarbeitung oder um Kundendienstleistungen oder Back-Office-Funktionen von zentralen Standorten innerhalb der EU aus anzubieten.

Der EU-Datenschutzrahmen wird derzeit überarbeitet. Die Datenschutzrichtlinie wird durch die 2018 in Kraft tretende EU-Datenschutz-Grundverordnung (DSGVO) ersetzt. Die DSGVO führt strengere Auflagen für Unternehmen in vielen Bereichen ein und fasst mehrere Aspekte des EU-Datenschutzes auf der EU-Ebene zusammen, unter anderem auch die Verantwortlichkeit für die Feststellung eines angemessenen Datenschutzniveaus für Nicht-EU-Länder. Die DSGVO führt auch ein zentralisierteres Aufsichtssystem sowie eine Schlichtungsregelung bei Differenzen zwischen nationalen Datenschutzbehörden ein. Jedoch bietet sie weiterhin einen hohen Grad an Freiheit für die freie Übermittlung personenbezogener Daten zwischen Unternehmen oder anderen Organisationen in der EU und dem EWR – die aber strengen Datenschutzbestimmungen für personenbezogenen Daten unterliegt mit besonders strengen Schutzklauseln für „vertrauliche personenbezogene Daten“, die zum Beispiel die Gesundheit, Strafregistereinträge oder ethnische Herkunft von Einzelpersonen betreffen.

How is personal data moved out of the EU?

Durch den Austritt aus der EU und dem EWR würde Großbritannien den EU-Datenschutzrahmen verlassen. Sowohl die Datenschutzrichtlinie als auch die DSGVO erlauben die Übermittlung der Daten von EU/EWR-Einzelpersonen in Länder außerhalb der EWR, wenn jene ein angemessenes Datenschutzniveau bieten. Die EU bietet dazu zwei Möglichkeiten:

- Durch eine Reihe zusätzlicher Schutzmaßnahmen, die Unternehmen für die Übermittlung personenbezogener Daten in Länder außerhalb des EWR befolgen müssen. Diese erfordern je nachdem eine Bandbreite an potentiell komplexen Verpflichtungen zusätzlich zur Standarddatenschutzpraxis, unter anderem Auflagen zur Einholung der Zustimmung von Kunden zur grenzüberschreitenden Übermittlung ihrer Daten in Nicht-EWR-Länder oder die Verwendung von speziellen Musterverträgen, um grenzüberschreitende Datenübermittlungen zu genehmigen (siehe Tabelle 1: Datenübermittlungsmöglichkeiten im Vergleich); oder
- Durch eine Bewertung der Datenschutzbestimmungen des Landes, in das die Daten übermittelt werden, in der das dortige Datenschutzniveau als für EU-Standards „angemessen“ eingestuft wird im Hinblick auf Gesetzgebung, Praxis und Aufsicht. Dabei handelt es sich im Wesentlichen um eine Variation der „Gleichwertigkeitsbewertungen“ (siehe BQB Nr. 4: „Was ist Gleichwertigkeit und wie funktioniert sie?“), die häufig bei EU-Bestimmungen in anderen Bereichen Anwendung findet. Diese Bewertung wird derzeit durch die EU-Kommission mithilfe von Informationen der nationalen Datenschutzbehörden in der EU durchgeführt wird – ein Modell, welches weitestgehend in den neuen Regulierungen beibehalten wurde. Für einige Nicht-EU-Ländern, unter anderem die Schweiz, Argentinien, Israel und Kanada, wurde eine Angemessenheit des Datenschutzniveaus auf diese Weise festgestellt. Das Datenschutzniveau in die EU selbst wurde von mehreren Ländern für angemessen erklärt, in denen ansonsten grenzüberschreitende Datenübermittlungen einschränkt werden.

Folgen – Alternativen und die „Klippe“

Übergangsregelungen sind nötig, um einen „Klippen“-Effekt bei der Übermittlung von Daten zwischen der EU und Großbritannien zu verhindern.

Beim Austritt aus der EU müssen in Großbritannien ausreichende Datenschutzmaßnahmen für die Daten von EU/EWR-Einzelpersonen und umgekehrt geschaffen werden sowie eine effiziente Möglichkeit zur Übermittlung personenbezogener Daten zwischen den Ländern. Sowohl Großbritannien als auch die EU haben ein gemeinsames Interesse an der fortwährenden Sicherung der effizienten Datenübermittlung in einer zunehmend digitalen Welt, in der der freie Datenverkehr Teil des alltäglichen Geschäfts ist.

Theoretisch wäre es denkbar, dass das Recht auf freie Datenübermittlung zwischen den beiden Marktwirtschaften über Nacht erlischt, sobald Großbritannien aus der EU austritt, mit ernst zu nehmendem Risiko einer Störung der Geschäftstätigkeit von Unternehmen – inklusive ihrer Kunden und Mitarbeiter – wenn sie für ihre Dienstleistungen auf diese Freiheit angewiesen sind. Die einzige Möglichkeit, die Unsicherheit in diesem Bereich auszuräumen, ist durch Übergangsregelungen oder eine gegenseitige Feststellung eines angemessenen Datenschutzniveaus durch Großbritannien und die EU.

Ohne diese Art von Sicherheit im Vorfeld des Austritts Großbritanniens müssen Unternehmen aus Großbritannien und der EU 27 die Konformität mit EU-Bestimmungen durch alternative Schutzmaßnahmen für Datenübermittlungen gewährleisten. Diese haben jedoch alle Nachteile (siehe Tabelle 1: Datenübermittlungsmöglichkeiten im Vergleich). In der Folge und um sicherzustellen, dass sie die notwendige Datenverarbeitung weiterhin durchführen können, müssen Unternehmen eventuell ihre grenzüberschreitende Datenverarbeitung umsiedeln, einen Umzug ihrer Datenzentren ins Auge fassen und/oder weitere Verfahren anwenden, um problematische grenzüberschreitende Übermittlungen personenbezogener Daten zu verhindern.

Eine „Angemessen-heitsfeststellung“ durch die EU

Eine Feststellung eines angemessenen Datenschutzniveaus durch die EU zu erhalten könnte sich als schwierig erweisen.

Um eine Angemessenheitsfeststellung durch die EU zu erhalten, muss Großbritannien einen Datenschutzrahmen beibehalten, der in ausreichendem Maße mit dem der EU übereinstimmt, damit diese als vergleichbar gewertet werden kann. Das erfordert eine Bewertung, die über die reinen Datenschutzgesetze hinausgeht, und könnte sich als schwierig erweisen (siehe Kasten 1: Die USA, Großbritannien und Angemessenheit des Datenschutzniveaus aus Sicht der EU).

Die DSGVO ist nur eines der Bereiche, in dem Großbritannien sich sorgsam um eine Angleichung seiner Standards an die EU im Bezug auf Datenschutz bemühen muss. Ein weiterer Bereich ist die Umsetzung von Cyber-Sicherheitsvorgaben, die in der Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) festgelegt sind. Diese schaffen Verpflichtungen für Unternehmen, unter anderem auch für Banken und Marktinfrastrukturunternehmen, sich selbst gegen Cyber-Angriffen zu schützen und geben Protokolle für den Austausch von Daten über Cyber-Angriffen zwischen der EU und den Behörden vor. Großbritannien muss eventuell Systeme für eine ähnliche Kooperation außerhalb der EU entwickeln. Darüber hinaus ist es gut möglich, dass die weitere Angleichung an die Standards der NIS-Richtlinie Teil einer künftigen Angemessenheitsfeststellung Großbritanniens durch die EU im Bereich Datenschutz wird.

Kasten 1: Die USA, Großbritannien und Angemessenheit des Daten-schutzniveaus aus Sicht der EU

Man könnte vielleicht meinen, dass Großbritannien als früherer EU-Mitgliedsstaat keine Probleme hätte, von der EU eine „Angemessenheitsfeststellung“ in Bezug auf seine Datenschutzbestimmungen zu erhalten. Aber das ist vielleicht nicht der Fall. Die britische Regierung hat einige der Vorgaben der DSGVO abgelehnt und wird wahrscheinlich viele der Bereiche ausnutzen, die in der Regulierung dem nationalen Ermessen überlassen sind. Zum Beispiel hat die britische Regierung 2016 verkündet, dass sie eine Bestimmung der DSGVO, die die Weitergabe von personenbezogenen Daten an ausländische Gerichte oder Aufsichtsbehörden einschränkt, nicht umsetzen wird. Obwohl diese Flexibilität für Großbritannien innerhalb der EU als Kompromisslösung möglich ist, solange das Land ein Mitgliedsstaat mit bekannten Vorbehalten in diesem Bereich ist, werden diese Differenzen einen Einfluss auf seine Chancen als Drittstaat auf eine Angemessenheitsfeststellung durch die EU haben.

Die jüngere Geschichte der EU-US-Datenübermittlungsbestimmungen haben klar das potentielle Risiko einer Geschäftsstörung von Unternehmen aufgezeigt.

- Die EU und die USA haben versucht, Unterschiede in der Datenschutzpraxis mit einem Sonderabkommen zu überwinden, das auf Verpflichtungen seitens der USA basierte, die Daten von EWR-Bürgern zu schützen: der „Safe Harbor"-Rahmen. Dies war aufgrund des Fehlens allgemeiner Datenschutzgesetzgebung in den USA erforderlich. Der Rahmen erlaubte US-Unternehmen, die unter der Aufsicht der Federal Trade Commission (FTC) standen, sich freiwillig dafür zu registrieren und sich den Datenschutzprinzipien dieses Rahmens zu verpflichten. Die EU-US-Vereinbarung wurde durch ein Gerichtsurteil aufgehoben, wodurch Unternehmen in der EU, die sich auf diesen Rahmen für einen gesetzeskonformen Datenaustausch mit US-Organisationen verlassen hatten, plötzlich unversehens gegen Datenschutzbestimmungen verstießen, wodurch sie im Eilverfahren ihre Verträge mit US-Unternehmen prüfen und anpassen mussten – eine Aufgabe von beachtlicher Komplexität. Einige Unternehmen haben diese Anpassung versäumt und wurden durch EU-Datenschutzbehörden zu Geldstrafen verdonnert.
- Das sehr ähnliche Nachfolgeabkommen – der EU-US „Privacy Shield" – wurde ausgearbeitet, um die Mängel der Safe Harbor-Vereinbarung auszuräumen. Jedoch wurde dieses auch juristisch angefochten mit der Begründung, dass dieses Ziel weiterhin verfehlt wurde, und Datenschutzbehörden haben ähnliche Bedenken geäußert. Die Chancen einer Aufhebung von Privacy Shield bleiben weiterhin ungewiss, aber könnten durch eventuelle Aktionen einer neuen US-Regierung steigen. Viele US-Unternehmen in der EU haben daher auch entschieden, sich aufgrund dieser ungewissen Zukunft nicht auf Privacy Shield zu verlassen. Obwohl Unternehmen, unter anderem auch im Finanzsektor, die nicht unter FCC-Aufsicht stehen, selbst Vereinbarungen und Schutzmaßnahmen treffen können, um den Austausch von Daten zu ermöglichen, wird dies dadurch schwieriger, teurer und birgt ein größeres juristisches Risiko.

Safe Harbor und Privacy Shield weisen auf einige der Schwierigkeiten bei der Angemessenheitsfeststellung hin, sofern eine erforderlich ist, und zeigen Schwierigkeiten auf, die bei Verhandlungen zwischen Großbritannien und der EU bezüglich der Angemessenheit entstehen könnten. Wenn sich bei anderen EU-Staaten die Auffassung durchsetzt, dass Kernelemente des britischen Rechts- und Strafverfolgungsrahmens nicht mit relevanten EU-Prinzipien kompatibel sind, könnte dies in einer Anfechtung einer Angemessenheitsfeststellung vor dem Europäischen Gerichtshof (EuGH) oder in politischem Druck gegen die Beibehaltung der Angemessenheitsfeststellung für Großbritannien gipfeln.

Schaffung eines neuen britischen Rahmens für grenzüber-schreitende Datenüber-mittlungen

Großbritannien wird einen neuen Rahmen für jene grenzüberschreitende Datenübermittlungen schaffen müssen, die derzeit von EU-Bestimmungen erfasst werden.

Übermittlung von personenbezogenen Daten von Großbritannien in die EU/den EWR

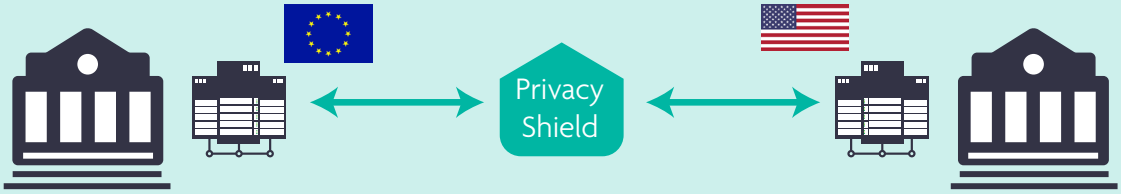
Großbritannien muss einen eigenen Rahmen zur Feststellung eines angemessen Datenschutzniveaus für die EU entwickeln, damit personenbezogene Daten von Großbritannien in die EU/den EWR übermittelt werden können. Das wird sowohl für Banken als auch für andere Unternehmen in Großbritannien wichtig sein, die personenbezogene Daten von britischen Einzelpersonen an Service-Zentren oder anderen Standorten in der EU/dem EWR zur Verarbeitung und Speicherung übermitteln wollen.

Übermittlung von personenbezogenen Daten von Großbritannien in andere Länder

Großbritannien muss auch existierende Datenübermittlungsrahmen ersetzen, die aus der Anerkennung des eines angemessenen Datenschutzniveaus in anderen Ländern hervorgegangen sind; hierunter fallen unter anderem Argentinien, Israel, Kanada, Neuseeland und die Schweiz. Es muss auch seinen Datenschutzrahmen mit den USA prüfen. Großbritannien muss eventuell dem „Privacy Shield" als Partei beitreten oder eine eigene bilaterale Vereinbarung treffen, um den nötigen

2000 EU-US Safe Harbour agreement provides a legal framework for US companies to move EU/EEA personal data to the US subject to self-regulated principles of data protection.

2015 The Safe Harbour agreement is struck down by the CJEU for inadequate guarantees of data protection. The EU assessments of the US for adequacy under the Data Protection Directive continue to identify significant variation in the protection afforded by the two regimes.



2016 The EU and the US negotiate the 'Privacy Shield' agreement containing customised data protection commitments from the US for EU/EEA personal data to allow an adequacy finding for the US regime. This agreement may still be challenged in EU courts.

Großbritannien muss auch existierende Datenübermittlungs-rahmen ersetzen, die aus der Anerkennung der Datenschutzniveaus anderer Länder hervorgegangen sind.

Schutz für britische personenbezogene Daten zu gewährleisten und um Datenübermittlungen zu erleichtern. Ohne ein solches Abkommen müssten britische Firmen eigene Schutzmaßnahmen einrichten, um Datenübermittlungen zu ermöglichen. Diese wären wahrscheinlich komplex, möglicherweise weniger robust und zeitaufwändig in der Anwendung. Die Robustheit dieser britischen Regulierungen, besonders in Bezug auf die USA, könnte ein Faktor bei der Bereitschaft der EU zur Feststellung der Angemessenheit des britischen Rahmens sein.

Übermittlung von personenbezogenen Daten von anderen Ländern nach Großbritannien

Das eigene Datenschutzniveau Großbritanniens muss auch durch einige andere Länder bewertet werden, in denen die grenzüberschreitende Übermittlung personenbezogener Daten eigenen Einschränkungen unterliegt, wie z. B. Japan und Israel. Einige Länder richten sich nach der EU-Liste „angemessener" Länder bei der Erstellung einer eigenen Liste von Ländern mit Angemessenheitsschutz. Daher hätten die Ergebnisse der EU in Bezug auf Großbritannien auch einen Einfluss auf andere Länder außerhalb der EU.

Tabelle 1: Datenübermittlungsmöglichkeiten im Vergleich

Der Handlungsspielraum für die Übermittlung personenbezogener Daten...	
...Innerhalb des EWR und der EU oder aus dem EWR und der EU in Drittstaaten mit vorhandener Feststellung eines angemessenen Datenschutzniveaus.	Persönliche Daten können frei zwischen Ländern übermittelt werden, solange die Datenschutzbestimmungen in beiden Ländern eingehalten werden.
...Aus dem EWR und der EU in Drittstaaten ohne Feststellung eines angemessenen Datenschutzniveaus.	Wenn für ein Land außerhalb des EWR keine Feststellung eines angemessene Datenschutzniveaus erfolgt ist, können Firmen dennoch personenbezogene Daten an Unternehmen und Organisationen in diesem Land übermitteln, wenn sie eine aus einem Spektrum von zusätzlichen Schutzmaßnahmen umgesetzt haben. Hierunter fallen: • Modellverträge. Wenn sie legal konform miteinander Verträge abschließen können, dann können sich der Datensender und -empfänger auf einen Modellvertrag einigen, der die Datenschutzbestimmungen für die Übermittlung untereinander regelt. Aus diesem Vertragsmodell ergeben sich einige Probleme für Banken und ihre Auslandsniederlassungen, die Teil derselben Körperschaft sind. Weiterhin müssen Banken bei dieser Herangehensweise Hunderte oder sogar Tausende von Verträgen prüfen. Außerdem befassen sich die Gerichte derzeit mit der Legitimität von Modellverträgen. • Verbindliche unternehmensinterne Vorschriften (Binding Corporate Rules, BCR). Wenn ein Unternehmen den EU-Datenschutzbehörden gegenüber nachweisen kann, dass ein hoher Grad an Datenschutz konsequent und robust über alle globalen Operationen hinweg eingehalten wird, dann können diese als ausreichende Garantie des Datenschutzes bei personenbezogenen Daten anerkannt werden, sodass die grenzüberschreitende Datenübermittlung zwischen verschiedenen Unternehmensteilen möglich ist. BCRs können komplex und zeitintensiv in der Gestaltung und Absicherung sein und müssen zudem ständig überarbeitet werden. • Zusätzliche Offenlegungen und Anträge auf Genehmigung. Unternehmen können ihre Kunden um „ausdrückliche Zustimmung“ für die Übermittlung ihrer Daten ins EU-Ausland bitten. Daraus ergeben sich jedoch Herausforderungen für vielen Arten von Übermittlungen. Wenn zum Beispiel eine Übermittlung aus regulatorischen Gründen nötig ist, kann eine Bank nicht riskieren, dass ein Kunde seine Zustimmung verweigert oder sie später für wiederkehrende Übermittlungen widerruft, wodurch die Bank gegen ihre Verpflichtungen verstoßen würde.

Siehe auch:

BQB Nr. 1 Im europäischen Binnenmarkt bleiben oder austreten
BQB Nr. 2 Ein geordneter Austritt aus der EU.
BQB Nr. 3 Was ist „Passporting“ und warum ist es wichtig?
BQB Nr. 4 Was ist Gleichwertigkeit und wie funktioniert sie?
BQB Nr. 6 Zeit sich anzupassen – Sind Übergangsvereinbarungen nötig?