Das Safe-Harbor-Urteil des EuGH und die Folgen

Fragen und Antworten

www.bitkom.org

bitkom

FAQs zu den Folgen des Safe Harbor Urteils des EuGH

Einleitung

Nach europäischem Datenschutzrecht darf eine Übermittlung personenbezogener Daten in ein Land außerhalb der Europäischen Union/des Europäischen Wirtschaftsraums (»Drittland«) nur erfolgen, wenn sichergestellt ist, dass dort ein angemessenes Datenschutzniveau herrscht. Diese Feststellung kann durch einen Angemessenheitsbeschluss der EU-Kommission erfolgen. Hinsichtlich der USA gibt es keinen solchen Beschluss. Im Jahr 2000 verständigte sich die EU-Kommission mit der US Federal Trade Commission (FTC) auf ein Verfahren, in welchem sich US-Unternehmen der Einhaltung bestimmter Datenschutzgrundsätze unterwerfen. Damit soll ein angemessenes Datenschutzniveau in den Unternehmen hergestellt werden. Dieses Verfahren wird » Safe Harbor« genannt und untersteht in den USA der Aufsicht der FTC. Safe Harbor stand schon seit längerem in der Kritik: Es wurde u. a. bemängelt, dass die FTC die Einhaltung der Selbstverpflichtungen nicht ausreichend überwache. Seit den Snowden-Veröffentlichungen wird auch der unangemessene und intransparente Zugriff durch Sicherheitsbehörden in den USA als Kritikpunkt genannt. Die EU-Kommission verhandelt daher schon seit längerem mit der US-Seite über eine Verbesserung des Verfahrens. Neben Safe Harbor gibt es für Unternehmen und andere Organisationen weitere rechtliche Möglichkeiten, den Datentransfer in die USA zu ermöglichen: Zum Beispiel die Verwendung von Standardvertragsklauseln der EU-Kommission, von der Datenschutzaufsicht genehmigte »verbindliche Unternehmensregeln« (BCR) oder die Einwilligung der betroffenen Personen.

Was hat der ↗EuGH konkret entschieden?

1. Auch wenn die EU-Kommission entschieden hat, dass in einem Land ein angemessenes Datenschutzniveau gegeben ist,[1] darf und muss ggf. eine nationale Aufsichtsbehörde eigene Ermittlungen anstellen, falls bei ihr eine Beschwerde diesbezüglich eingeht. Kommt die Aufsichtsbehörde zu dem Ergebnis, dass in dem Drittland kein angemessenes Datenschutzniveau vorhanden ist, kann sie den Angemessenheitsbeschluss der Kommission vor einem nationalen Gericht anfechten. Das nationale Gericht hat dann die Möglichkeit, eine Auslegungsfrage an den Europäischen Gerichtshof (EuGH) zu richten. Nur letzterer kann einen EU-Rechtsakt (z. B. die Safe-Harbor-Entscheidung oder Standardvertragsklauseln der Kommission) für ungültig erklären.

2. Die ↗Entscheidung 2000/520 der EU-Kommission aus dem Jahr 2000, mit der das durch Safe Harbor hergestellte Datenschutzniveau als angemessen anerkannt wurde, ist ungültig. Die Kommission hätte vor Inkrafttreten von Safe Harbor ausführlich untersuchen müssen, ob das US-amerikanische Recht ein angemessenes Datenschutzniveau tatsächlich zulässt.

1 ↗In folgenden Ländern wurde bisher ein angemessener Datenschutz festgestellt: Andorra, Argentinien, Kanada, Färöer-Inseln, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, Schweiz, Uruguay.

Dazu hätte sie laut EuGH folgende in der Datenschutzrichtlinie festgelegte Kriterien heranziehen müssen:

- Feststellung, ob es in den Vereinigten Staaten Vorschriften gibt (Rechtslage und Rechtspraxis), die dazu dienen, etwaige Eingriffe in die Grundrechte der Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt werden, zu begrenzen.

- Wirksamkeit eines gerichtlichen Rechtschutzes gegen derartige Eingriffe.

Dieser Prüfmaßstab mit strengen inhaltlichen Anforderungen muss auch für zukünftige Angemessenheitsbeschlüsse der Kommission herangezogen werden.

Die Safe Harbor Entscheidung ist also aus formalen Gründen wohl rückwirkend ungültig.[2] Die Unternehmen, die sich die letzten 15 Jahre auf Safe Harbor gestützt haben, genießen jedoch einen Vertrauensschutz und müssen für den bisherigen Datentransfer in die USA keine Maßnahmen seitens der Aufsichtsbehörden befürchten. Eine zukünftige Datenübermittlung auf Basis dieser Rechtsgrundlage ist jedoch nicht mehr zulässig.

Was hat der EuGH noch festgestellt?

- Die EU-Charta der Grundrechte muss bei der Interpretation für ein angemessenes Datenschutzniveau immer herangezogen werden. In diesem Fall waren Artikel 7, 8 und 47 der ↗Charta betroffen.

- Für eine Adäquanzentscheidung muss die Kommission begründet feststellen, dass das betreffende Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein Schutzniveau der Grundrechte gewährleistet, das dem in der Rechtsordnung der Union garantierten Niveau der Sache nach gleichwertig ist. (Ziff. 96 des Urteils)

- Der massenhafte Zugriff auf personenbezogene Daten ohne irgendeine Differenzierung, Einschränkung oder Ausnahme verstößt gegen den Grundsatz der Verhältnismäßigkeit. (Ziff. 93 des Urteils)

- Das Grundrecht auf gerichtlichen Rechtsschutz der Charta (Art. 47) verlangt, dass Bürger die Möglichkeit haben müssen, Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken. (Ziff. 95 des Urteils)

2 So zumindest laut Giovanni Buttarelli, Europäischer Datenschutzbeauftragter, in einem ↗Briefing

Ab wann ist die Entscheidung wirksam?

Ab sofort. Daher ist es aus Compliance Gründen angezeigt, sich möglichst schnell mit Alternativen für Safe Harbor zu befassen. Allerdings sind momentan die Aufsichtsbehörden noch dabei, sich abzustimmen und werden wohl nicht gegen einzelne Unternehmen vorgehen, ohne diesen die Chance zu geben, ihre Prozesse umzustellen.

Die nationalen EU-Datenschutzbehörden (Artikel 29 Gruppe) gewähren den Unternehmen eine **Umstellungsfrist bis Ende Januar 2016**. Zwar besteht damit die Hoffnung auf einen koordinierten europäischen Ansatz. Allerdings ist diese Umstellungsfrist nicht bindend für die Aufsichtsbehörden in den EU-Mitgliedstaaten, da diese unabhängig und daher nicht weisungsgebunden sind. Deutsche Aufsichtsbehörden können daher schon jetzt auf Basis von Beschwerden Untersuchungen anstellen und gegebenenfalls einen Datentransfer in die USA untersagen.

Wie haben Politik und Datenschutzbehörden reagiert?

- **7. Oktober 2015: ↗Statement der zuständigen EU-Kommissarin Vera Jourová**
  Die Kommission betont, sie werde weiter mit den USA verhandeln, um eine Überarbeitung des Safe Harbor Abkommens zu erreichen. Gleichzeitig werde sie eng mit den europäischen Aufsichtsbehörden zusammenarbeiten, um eine Fragmentierung des Binnenmarktes zu verhindern. Für die weitere transatlantische Übermittlung personenbezogener Daten weist sie auf andere Transfermechanismen hin.

- **13. Oktober 2015: ↗Statement des zuständigen Ausschusses[3] im Europäischen Parlament**
  Das Europäische Parlament weist auf seinen ↗Entschließungsantrag vom 12. März 2014 hin und kritisiert die EU-Kommission, dass seit den Snowden-Enthüllungen zu wenig passiert sei. Das Parlament begrüßt daher die Safe Harbor Entscheidung des EuGH und fordert die Kommission auf, den in der Resolution gemachten Forderungen bis Ende 2015 nachzukommen. Sollte dies nicht geschehen, würde es sich das Recht vorbehalten, gegen die Kommission mit einer Untätigkeitsklage und Budgeteinschränkungen vorzugehen.

- **16. Oktober 2015: ↗Statement der »Artikel 29 Gruppe«[4]**
  - Die Artikel-29-Gruppe untersucht derzeit, ob andere Transfermechanismen wie Standardvertragsklauseln und BCRs auch von der Safe Harbor Entscheidung betroffen sind. Bis zu einem endgültigen Beschluss können und sollten diese Rechtsgrundlagen vorerst genutzt werden.

3 ↗Der Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) befasst sich mit Datenschutzthemen.

4 Die ↗Artikel-29-Datenschutzgruppe ist das unabhängige Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes. Die Gruppe besteht aus je einem Vertreter der jeweiligen nationalen Datenschutzbehörden, dem Europäischen Datenschutzbeauftragten und einem – nicht stimmberechtigten – Vertreter der Europäischen Kommission.

- Die Übergangs- und Umsetzungsfrist für Unternehmen und politische Akteure läuft bis Ende Januar 2016. Die Artikel-29-Gruppe wird bis dahin mit Blick auf das EuGH-Urteil eine Analyse der Transfermechanismen durchführen. Die Verhandlungspartner EU-Kommission und USA werden gebeten, bis dahin eine politische Lösung zu finden. Die Unternehmen sollen bis dahin vorläufig auf andere Rechtsinstrumente umsteigen. Ab Februar 2016 haben Aufsichtsbehörden vor, alle geeigneten und angemessenen Mittel zur Durchsetzung der Safe-Harbour Entscheidung anzuwenden.

- **20. Oktober 2015**: Die irische Aufsichtsbehörde erklärt, sie werde den vorgelegten Einzelfall Schrems untersuchen. ↗Statement der irischen Aufsichtsbehörde.

- **23. Oktober 2015**: Das Europäische Parlament veröffentlicht eine überarbeitete Version seines Entschließungsantrags von 2014 und fordert die Kommission und Mitgliedsstaaten erneut zum Handeln auf. Zudem kritisiert es nationale Gesetze zur Vorratsdatenspeicherung, die in der letzten Zeit z. B. von Frankreich und Großbritannien erlassen wurden. ↗Entschließungsantrag des Parlaments.

- **26. Oktober 2015**: Die für Safe Harbor zuständige Kommissarin Jourová gab ein ↗Update zu »Safe Harbor 2« im LIBE-Ausschuss des Europäischen Parlaments.

- **06. November 2015**: Die EU-Kommission veröffentlicht eine ↗Kommunikation (KOM (2015) 566 final), in der sie insbesondere andere Rechtsinstrumente für die Übermittlung von personenbezogenen Daten erläutert.

Wie haben sich die deutschen Aufsichtsbehörden positioniert?

Für Unternehmen können je nach Sitz und Tätigkeit unterschiedliche deutsche Aufsichtsbehörden in den einzelnen Bundesländern zuständig sein. Daher haben unterschiedliche Bewertungen der Datenschutzinstitutionen große praktische Bedeutung.

- **26. Oktober** ↗Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

- **26. Oktober 2015**: ↗Gemeinsames Positionspapier der deutschen Aufsichtsbehörden: Für die weitere Anwendung von Standardvertragsklauseln und BCRs ist die Datenschutzkonferenz (DSK) deutlich kritischer als die Artikel-29-Gruppe. Sie lehnt für die Zukunft die Anwendbarkeit von diesen Instrumenten zwar nicht generell ab, kündigt aber an, zunächst keine **neuen** Genehmigungen für Datenexporte in die USA auf Grundlage von BCRs oder Datenexportverträgen mehr zu erteilen. Darüber hinaus sollen Datenübermittlungen auf Basis von EU-Standardvertragsklauseln und BCRs zukünftig stärker daran gemessen werden, ob eine willkürliche Überwachung der Daten durch US-Behörden verhindert wird und ob eine Rechtsschutzmöglichkeit der Betroffenen in den USA existiert (vgl. Ziff 94 und 95 des Urteils).

Die DSK hebt hervor, dass der EuGH die völlige Unabhängigkeit der zuständigen Aufsichtsbehörden bei der Prüfung von Datenübermittlungen bestätigt hat. Es kommt also im Einzelfall auf die Bewertung der jeweiligen Landesdatenschutzbeauftragten an, die sich recht unterschiedlich geäußert haben:

- **14. Oktober 2015**: Das ULD veröffentlicht schon einen Tag vor dem offiziellen ersten Treffen der Artikel-29-Gruppe seine rechtliche Analyse der Safe Harbor Entscheidung. Es legt einen sehr strengen Maßstab an und kommt zu dem Ergebnis, dass auch andere Transfermechanismen wie Standardvertragsklauseln, BCRs und Einwilligung in Zukunft wohl nicht mehr genutzt werden können. Nur der Abschluss eines völkerrechtlichen Datenschutzabkommens oder eine umfassende Änderung des US-amerikanischen Rechts würden etwas an der Situation ändern. ↗Positionspapier - Schleswig-Holstein

- **26. Oktober 2015**: Der Hamburgische Datenschutzbeauftragte hat klargestellt, dass er vorerst nicht gegen Datenübermittlungen auf Grundlage von EU-Standardvertragsklauseln oder BCRs vorgehen wird. ↗Statement - Hamburg

- **27. Oktober 2015**: Der LfDI RLP hält sich weitestgehend an das Positionspapier der deutschen Aufsichtsbehörden. Zudem betont er, er stehe den verantwortlichen Stellen beratend zur Seite. Interessant ist die Aussage, er werde »soweit möglich die verantwortlichen Stellen auf Alternativen zu Datenverarbeitungen in den USA hinweisen, also auf Dienstleister, die Datenverarbeitungen ausschließlich innerhalb der EU oder in Staaten mit angemessenem Datenschutzniveau vornehmen. ↗Positionspapier - Rheinland-Pfalz

- **27. Oktober 2015**: Der LDI NRW informiert, er werde in Übereinstimmung mit dem Statement der Artikel-29-Gruppe eine Übergangsfrist bis zum 31. Januar 2016 einräumen. Bis dahin werde er aus eigener Initiative keine Maßnahmen gegen Datenübermittlungen in die USA aufgrund der EU-Standardvertragsklauseln sowie bereits genehmigter BCRs oder Datenexportverträge ergreifen. Allerdings seien anlassbezogene Maßnahmen im Einzelfall zum Schutz der Grundrechte betroffener Personen jederzeit möglich. ↗Statement - NRW

- **5. November 2015**: Der hamburgische Datenschutzbeauftragte erläutert in seinem Statement das weitere Vorgehen seiner Behörde: Zunächst werden Unternehmen in seinem Zuständigkeitsbereich identifiziert, die mit hoher Wahrscheinlichkeit Daten in die USA übermitteln. Diese erhielten dann Informationen zum EuGH-Urteil, zum Stand der rechtlichen Entwicklungen und zu den weiteren geplanten Umsetzungsschritten. Diese Unternehmen werden dann im zweiten Schritt bis Ende Januar 2016 um Auskunft gebeten. Erst ab Februar 2016 werde er rechtliche Maßnahmen zur Durchsetzung des Urteils ergreifen. ↗Positionspapier - Hamburg

Wie haben sich europäische Aufsichtsbehörden positioniert?

Für Unternehmen können je nach Sitz und Tätigkeit verschiedene europäische Aufsichtsbehörden zuständig sein. Daher haben unterschiedliche Bewertungen der Datenschutzinstitutionen große praktische Bedeutung.

- ↗Übersicht der unterschiedlichen Reaktionen einzelner europäischen Datenschutzaufsichtsbehörden.

- **27. Oktober 2015**: ↗Blogpost von David Smith, UK Deputy Commissioner and Director of Data Protection. »Don't panic, don't rush and wait for further guidance« sind die zentralen Botschaften der britischen Aufsichtsbehörde. Es wird empfohlen, eine Bestandsaufnahme der bestehenden Datenschutzprozesse im eigenen Unternehmen zu machen, zu überlegen, welche alternativen Rechtsgrundlagen in Frage kommen und zu beobachten, wie es auf rechtlich-politischer Ebene weitergeht.

- **06. November 2015**: Die italienische Aufsichtsbehörde äußert sich zu der ↗Legalität der alternativen Transfermechanismen (BCRs und Standardvertragsklauseln).

Wie geht es auf der rechtlich-politischen Ebene weiter?

- **Koordination der Aufsichtsbehörden**: Die Aufsichtsbehörden in Europa werden sich in der Artikel 29 Gruppe weiter abstimmen und bald eine einheitliche Position beziehen. Dies soll verhindern, dass die EuGH-Entscheidung in einzelnen EU-Mitgliedsstaaten unterschiedlich ausgelegt wird. Insbesondere muss untersucht werden, ob auch Standardvertragsklauseln und BCRs von der Entscheidung betroffen sind. Diese müssen ggf. an die im EuGH-Urteil gemachten Vorgaben angepasst werden. Zudem muss generell näher untersucht werden, welche Kriterien für ein der EU gleichwertiges Datenschutzniveau zukünftig herangezogen werden müssen.

- **Erklärende Mitteilung der Kommission**: Kommissarin Jourová verkündete am 26. Oktober im LIBE-Ausschuss, dass auch die Kommission bald eine erklärende Kommunikation zum Thema Safe Harbor veröffentliche.

- **Bilaterale Verhandlungen mit den USA**: Um eine dauerhafte Lösung für den Datentransfer zwischen den USA und Europa zu garantieren, muss die Kommission mit den USA Verhandlungen aufnehmen und ein bilaterales Abkommen aushandeln. Die deutschen Datenschutzbehörden fordern auch die Bundesregierung auf, in direkte Verhandlungen mit der US-Regierung zu treten. Ein überarbeitetes Safe Harbor Abkommen (»Safe Harbor 2«) könnte Teil der

Lösung sein. Sowohl das Europäische Parlament als auch die Mitgliedsstaaten (Ausschuss nach Artikel 31)[5] werden neben der Kommission dabei eine zentrale politische Rolle spielen.

- **Gesetzgebung in den USA**: Wie Kommissarin Jourová in ihrer Rede im Europäischen Parlament am 26. Oktober 2015 betonte, gab es in der letzten Zeit schon einige datenschutzrechtliche Entwicklungen in den USA. Es muss geprüft werden, inwiefern die bisher verabschiedeten Gesetze den Vorgaben des EuGH gerecht werden und wo ggf. nachgebessert werden muss.

- **Irischer Supreme Court**: Der oberste irische Gerichtshof muss noch in der Sache selbst entscheiden (Max Schrems gegen Facebook). Derzeit analysiert die irische Aufsichtsbehörde den Einzelfall.

Relevante Entwicklungen:

- **↗US Freedom Act**: Der US-Kongress hat die von Präsident Obama versprochene Geheimdienstreform am 2. Juni 2015 angenommen. Der Senat stimmte am 2. Juni mit 67 zu 32 Stimmen für den sogenannten USA Freedom Act. Kurz darauf setzte Obama das Gesetz mit seiner Unterschrift in Kraft.

- **↗Presidential Policy Directive Number PPD - 28**: Diese Richtlinie schafft Grundsätze und Verfahren für Mitarbeiter von Geheimdiensten (»Office and Intelligence and Analysis employees«) bei der Ausübung ihrer nachrichtendienstlichen Tätigkeiten (» Signals Intelligence Activties«).

- **↗Judicial Redress Act**: EU-Bürger sollen bei Datenschutzverletzungen gegen US-Behörden klagen können. Der Judicial Redress Act wurde schon im US-amerikanischen Repräsentantenhaus, einer der zwei Kammern des Kongresses, verabschiedet. Er muss jetzt noch in der anderen Kammer, dem Senat, vorgelegt und verabschiedet werden.

Im Oktober 2015 wurde die ↗Studie »A comparison between US and EU Data Protection Legislation for Law Enforcement Purposes« veröffentlicht, die auf Anfrage des LIBE-Ausschusses von Prof. Dr. Franziska Böhm von der Universität Münster erarbeitet wurde. Die Studie untersucht auch den »USA Freedom Act«, den »Draft Judicial Redress Act« und weitere Entwicklungen im amerikanischen Datenschutzrecht.

5 Der Ausschuss nach Artikel 31 wurde gemäß Artikel 31 der Datenschutzrichtlinie 95/46/EG eingesetzt. Er umfasst Vertreter der Mitgliedstaaten, die gemeinsam Entscheidungen treffen, wenn die Zustimmung der Mitgliedstaaten gemäß der Richtlinie erforderlich ist. Beispielsweise ist der Ausschuss am Verfahren für die Annahme von ↗Angemessenheitsentscheidungen beteiligt.

Was ist von den Verhandlungen zu »Safe Harbor 2« zu erwarten?

Die Kommission hat im Jahr 2013 in ihrer Kommunikation das Safe Harbor Abkommen untersucht (↗Kommunikation v (COM (2013) 847 final) und einen ↗Missstand beim Datenschutz festgestellt, insbesondere wegen des massenhaften und undifferenzierten Zugriffs auf personenbezogene Daten. Auf diese Kommunikation bezieht sich auch der EuGH in seinem Urteil. Als Maßnahme hat die Kommission 13 Empfehlungen aufgestellt, wie Safe Harbor verbessert werden muss. Seitdem laufen die Verhandlungen mit den USA zu ↗»Safe Harbor 2«, die laut Kommission vor der EuGH-Entscheidung ↗fast abgeschlossen waren. Insbesondere die 12. und 13. Empfehlung bezüglich des Zugriffs der Geheimdienste hat schon vor der EuGH-Entscheidung zu Einigungsproblemen geführt. Jetzt muss überprüft werden, ob der bisher ausgehandelte Text, den Voraussetzungen, die der EuGH in seiner Entscheidung vorgibt (siehe Feststellungen in Part I), standhält. Falls nicht, muss nachverhandelt werden.

Wer ist von der Entscheidung des EuGH betroffen?

Betroffen sind all jene Unternehmen, die personenbezogene Daten an Unternehmen in den USA übermitteln oder Dienstleister nutzen, die das tun. Direkt betroffen sind jene Unternehmen, bei denen die Datenübermittlungen auf Grundlage einer Safe Harbor Zertifizierung erfolgen und keine zusätzlichen Vereinbarungen wie Standardvertragsklauseln oder Einwilligungen genutzt werden. Indirekt könnte die Urteilsbegründung des EuGH auch die Rechtmäßigkeit der Nutzung der Standardvertragsklauseln oder Binding Corporate Rules in Frage stellen. Aber formal hat diese bislang niemand beanstandet.

Was sollen Anbieter tun, die Safe Harbor nutzen?

Die Datenübermittlung in den USA auf Grundlage einer Safe Harbor-Zertifizierung ist seit 6. Oktober 2015 unzulässig. Unternehmen, deren Dienstleistungen auch die Verarbeitung von personenbezogenen Daten in den USA umfasst und die bisher auf der Grundlage von Safe Harbor Daten verarbeitet haben, sollten nun alternative Rechtsgrundlagen für die Übermittlung prüfen. Darauf ausgerichtete Datenschutzerklärungen, Werbematerialien und Texte auf Webseiten müssen ebenfalls angepasst werden.

1. Im ersten Schritt sollte im Unternehmen eine Bestandsaufnahme gemacht werden, welche bisherigen Datenströme auf die Rechtsgrundlage von Safe Harbor gestützt wurden. Das sollte sich in der Regel aus den entsprechenden Verträgen zur Datenverarbeitung ergeben.

2. Im zweiten Schritt sollte überlegt werden, auf welche alternativen Rechtsgrundlagen ein Datentransfer gestützt werden kann.

Grundsätzlich gibt es mehrere zulässige Rechtsgrundlagen für die Datenübermittlung in ein Drittland:

Zur Vertragserfüllung notwendige Datenübermittlung: Eine Datenübermittlung ist zulässig, wenn zwischen dem Betroffenen und der verantwortlichen Stelle ein Vertrag abgeschlossen worden ist für dessen Erfüllung die Datenübermittlung erforderlich ist (Beispiel: Kunde K möchte, dass sein Reisebüro für ihn in Sydney ein Hotelzimmer reserviert.). Ein Vertrag kann auch ein Arbeitsvertrag sein, so dass die Übermittlung von Arbeitnehmerdaten in ein Drittland auf Grund eines Arbeitsvertrages zulässig sein kann.

Auch ist die Datenübermittlung zulässig **zur Erfüllung eines Vertrags, der zwar nicht vom Betroffenen selbst mit der verantwortlichen Stelle geschlossen wurde, aber im Interesse des Betroffenen zwischen der verantwortlichen Stelle und einem Dritten** ist (Beispiel: Arbeitgeber überträgt Daten eines Arbeitnehmers, für den er eine Mitarbeiterversicherung abgeschlossen hat, an eine ausländische Versicherungsgesellschaft.).

Artikel 26 (1) der ↗Datenschutzrichtlinie zählt noch einige andere Rechtsgrundlagen auf, die auf bestimmte Ausnahmefälle zutreffen (z. B. wenn die Übermittlung der Daten für einen Rechtsstreit notwendig ist). ↗Mehr Informationen liefert ein Bitkom-Leitfaden oder die ↗Kommunikation der EU-Kommission (S. 8-11).

Fazit: Diese Zulässigkeitsvariante sollte auf jeden Fall geprüft werden. Sie könnte z. B. für US-Unternehmen Anwendung finden, die mittels eines Cookies oder einer App personenbezogene Daten nach EU-Recht erheben.

Einwilligung: Wenn das Unternehmen Dienstleistungen direkt an Einzelpersonen erbringt, deren Daten in die USA übermittelt werden, bietet sich möglicherweise die Einholung der Einwilligung an. ↗Nach Ansicht der deutschen Datenschutzaufsichtsbehörden kann eine Einwilligung jedoch nur unter engen Bedingungen eine Grundlage sein. So könne kein Massentransfer oder ein dauerhafter Datentransfer auf eine Einwilligung gestützt werden. Zudem könne die Einwilligung beim Export von Beschäftigtendaten oder wenn gleichzeitig auch Daten Dritter betroffen sind, nur in Ausnahmefällen genutzt werden.

Im Übrigen sind die üblichen Vorrausetzungen für die Einholung einer gültigen Einwilligung heranzuziehen. ↗Weitere Informationen zur Anforderung der Einwilligung liefert ein Bitkom-Leitfaden oder die ↗Kommunikation der EU-Kommission (S. 11-12). Wichtig ist, dass ein deutlicher Hinweis auf die Datenübermittlung in die USA und eine Darstellung daraus resultierender Konsequenzen, zum Beispiel über die Zugriffsrechte der US-Behörden, informiert werden. Es sollte zudem darauf hingewiesen werden, dass eine Einwilligung von dem Betroffenen jederzeit widerrufen werden kann und ein Verzicht auf die Widerrufsmöglichkeit mit Blick auf die Gewährleistung der informellen Selbstbestimmung ausgeschlossen ist. Unternehmen müssen also damit rechnen, dass die Einwilligung grundsätzlich entweder nicht erteilt oder jederzeit widerrufen werden kann.

Fazit: Die Einwilligungsvariante ist nicht ideal und sollte entweder nur »Plan B« darstellen oder in Kombination mit anderen Mechanismen gebraucht werden.

EU-Standardvertragsklauseln: Für die meisten Unternehmen wird der Abschluss von Standardvertragsklauseln die am ehesten kurzfristig umsetzbare Alternative sein. Mit der Verwendung dieser Mustervertragsklauseln kann ein angemessenes Datenschutzniveau für den Datentransfer hergestellt werden. Werden diese Klauseln unverändert übernommen, müssen sie nicht von der zuständigen Datenschutzbehörde genehmigt werden. Es gibt drei unterschiedliche Ausführungen der Standardvertragsklauseln: ↗Version I und ↗Version II der Standardvertragsklauseln von einer verantwortlichen Stelle in der EU an eine andere verantwortliche Stelle im Drittstaat oder die ↗Standardvertragsklauseln für Auftraggeber in der EU an Auftragsdatenverarbeiter im Drittstaat. Mehr Informationen zur Anforderung zu Standardvertragsklauseln liefert ein Bitkom-Leitfaden oder die ↗Kommunikation der EU-Kommission (S. 5-7).

Fazit: Deutsche Unternehmen sollten Standardvertragsklauseln möglichst ohne Änderungen übernehmen. Sollte dies nicht möglich sein, sollte die Rechtsansicht und Praxis der Datenschutzaufsicht in Erfahrung gebracht werden, die für sie zuständig ist. In anderen EU-Ländern muss geprüft werden, ob noch andere Voraussetzungen (z. B. Genehmigung) gelten.

Verbindliche Unternehmensreglungen (BCRs): Als angemessene Schutzgarantien für die von einer Datenübermittlung Betroffenen können auch verbindliche Unternehmensrichtlinien dienen, die die internationale Weitergabe von personenbezogenen Daten innerhalb internationaler Konzerne regeln. Durch solche »Binding Corporate Rules« werden Datenschutzgrundsätze für den Umgang mit personenbezogenen Daten, insbesondere Daten von Kunden, Aktionären und Mitarbeitern sowie Vertrags- oder Geschäftspartnern verbindlich und allgemein festgelegt. Dazu gehört unter anderem, dass die Betroffenen über den Umgang mit ihren personenbezogenen Daten in geeigneter Art und Weise leicht zugänglich informiert werden müssen, dass die Daten nur für den ursprünglichen Zweck erhoben werden dürfen und dass die Weitergabe an Dritte einer rechtlichen Grundlage bedarf. ↗Stellungnahmen Artikel 29 Gruppe zu Binding Corporate Rules. Mehr Informationen hierzu auch in der ↗Kommunikation der Kommission (S. 7-8).

Fazit: Die Prozesse von BCRs sind aufwändig zu implementieren und daher nicht kurzfristig einsetzbar. Für ihre Einführung müssen Unternehmen mit einer Dauer von 12 bis 18 Monaten rechnen. Die Datenschutzbehörden werden nach eigener Aussage derzeit keine neuen Genehmigungen für Datenübermittlungen in den USA auf Grundlage von BCRs oder Datenexportverträge erteilen.

Technisch-organisatorische Maßnahmen: Eine Überwachung durch US-Behörden in den USA kann möglicherweise noch durch technisch organisatorische Maßnahmen wie Anonymisierung oder Verschlüsselung erschwert werden. Dies stellt jedoch keine angemessene Lösung dar, wenn die Daten aktiv in den USA genutzt werden sollen.

Fazit: Die Möglichkeiten solcher technischen Maßnahmen sollte zur Risikominimierung geprüft und falls möglich genutzt werden.

Was sollen Anwender tun, die personenbezogene Daten bei US-Unternehmen verarbeiten lassen?

Unternehmen sollten Rücksprache mit den betroffenen Dienstleistern (z. B. Cloud- und Softwareanbieter) halten, um herauszufinden, was diese anbieten können um zukünftig eine rechtskonforme Nutzung zu gewährleisten. US-amerikanische Unternehmen, die bisher auf der Basis von Safe Harbor gearbeitet haben, sind derzeit dabei, angemessene Lösungen zu implementieren. Manche Anbieter haben ihren Kunden bereits die Umstellung auf Standardvertragsklauseln angeboten.

Wie können Aufsichtsbehörden gegen Unternehmen vorgehen?

Aussetzen des Datentransfers: Bevor die Aufsichtsbehörde dem Unternehmen als letzten Schritt einen Datentransfer in die USA untersagen kann, muss sie zunächst andere Maßnahmen ergreifen:

1. **Anordnung zur Abstellung eines Verstoßes:** Die Behörde muss auf das Unternehmen zugehen und dazu auffordern, den Verstoß (z. B. die Übermittlung auf Grundlage von Safe Harbor) zu unterlassen.

2. **Androhung eines Zwangsgelds und Setzung einer angemessenen Frist zur Umsetzung:** Sollte das Unternehmen nicht darauf reagieren, kann die Behörde ein Zwangsgeld verhängen, das allerdings vorher angedroht werden muss.

3. **Untersagungsverfügung nach Ablauf der Frist:** Wenn das Unternehmen immer noch keine Bereitschaft zur Behebung der von der Aufsichtsbehörde gerügten Mängel oder Rechtsverletzungen zeigt, kann die Behörde die Übermittlung personenbezogener Daten in die USA im Einzelfall als »ultima ratio« verbieten.

4. **Widerspruch:** Unternehmen haben grundsätzlich die Möglichkeit eines Widerspruchs gegen diesen Verwaltungsakt der Behörde einzulegen.

Es gibt in Ausnahmefällen die Möglichkeit, das sofortige Verbot eines Verfahrens zu erzwingen. Aufgrund des Grundsatzes der Verhältnismäßigkeit und der Tatsache, dass der EuGH weder abschließend geklärt hat, dass die USA kein angemessenes Datenschutzniveau hat noch eine offizielle Umstellungsfrist auf andere Transfermechanismen gesetzt hat, sollte eine sofortige Untersagung nicht zu erwarten sein.

Bußgeld: Ein Bußgeldbescheid kann, unabhängig von anderen Maßnahmen (wie der Untersagung des Datentransfers) drohen. Generell kann ein Bußgeld in Höhe von bis zu 300.000 Euro drohen. Das Datenschutzgesetz setzt aber voraus, dass das Unternehmen vorsätzlich oder fahrlässig gehandelt hat. Der Fahrlässigkeitsmaßstab ist die im Verkehr erforderliche Sorgfalt bei der Verarbeitung personenbezogener Daten. Die Unternehmen, die sich die letzten 15 Jahre auf Safe Harbor gestützt haben, genießen einen Vertrauensschutz und müssen für den **bisherigen Datentransfer** in die USA keine Maßnahmen seitens der Aufsichtsbehörden befürchten. Für einen **zukünftigen Datentransfer** sollten Unternehmen jedoch aktiv werden und mindestens eine Bestandsaufnahme der bestehenden Verträge machen sowie weitere Schritte planen. Eine kurzfristige Verhängung eines Bußgelds ohne dass einem Unternehmen eine angemessene Zeit zur Umstellung der Prozesse gewährt wird, sollte nicht verhältnismäßig sein.

Welche Auswirkungen hat Safe Harbor auf die Datenschutzgrundverordnung?

Die Datenschutzgrundverordnung befindet sich derzeit im Trilog, in dem sich EU-Kommission, EU-Parlament und der Ministerrat wahrscheinlich bis Ende 2015 auf gemeinsame Datenschutzregeln einigen, die dann zwei Jahre später in Kraft treten. Kapitel V der Verordnung, das von den Parteien schon vor dem EuGH-Urteil weitestgehend ausgehandelt wurde, betrifft die Übermittlung personenbezogener Daten in Drittländer. Im Nachgang der Entscheidung muss also geprüft werden, ob die ausgehandelten Kompromisse der Verordnung den Anforderungen des EuGH standhalten. Auch interessant sind Kapitel VI und VII, die Vorschriften für die Zuständigkeit der Aufsichtsbehörde und deren Zusammenarbeit auf europäischer Ebene festlegen. So wird die Gründung eines Europäischen Datenausschusses diskutiert (»European Data Protection Board«), das als übergeordnete Instanz dienen und im Gegensatz zur Artikel-29-Gruppe bindende Entscheidungen in bestimmten Bereichen fällen soll. Dies könnte zu mehr Einheitlichkeit bei der Auslegung der EU-Datenschutzregelungen bei den nationalen Aufsichtsbehörden führen.

Fest steht bereits, dass Unternehmen, die Daten außerhalb der EU verarbeiten, ihre Dienste aber auch innerhalb der EU anbieten, künftig den Regelungen der Europäischen Union unterliegen sollen (so genanntes Marktortprinzip). Datenschutzrechtliche Prozesse und Verträge müssen daher von amerikanischen und europäischen Unternehmen nicht nur in Hinblick auf Kapitel V, sondern der gesamten Grundverordnung angepasst werden.

Welche Auswirkungen könnte das Safe Harbor auf andere Abkommen haben?

- **Vorratsdatenspeicherung:** Der massenhafte Zugriff auf personenbezogene Daten ist kein reines US-amerikanisches Phänomen. ↗2014 hat der EuGH die EU-Richtlinie zur Sicherung von Telefon- und E-Mail-Informationen gekippt. Die Speicherung von Kommunikationsdaten ohne Verdacht auf Straftaten sei nicht mit EU-Recht vereinbar. Auch in den einzelnen Mitgliedsstaaten (z. B. Niederlande, Deutschland, Frankreich) sind Gesetze zur Vorratsdatenspeicherung verabschiedet worden oder auf dem Weg. Es steht aber zur Diskussion, ob die EU Kompetenzen hat, diese nationalen Gesetze in Frage zu stellen. Unabhängig davon kann aber über den nationalen Weg eine Verfassungsbeschwerde drohen.

- **Fluggastdatenspeicherung:** Mit knapper Mehrheit hat der ↗federführende Ausschuss des Europa-Parlaments im Juli 2015 für die europaweite Speicherung von Fluggastdaten (PNR) gestimmt. Damit könnten künftig die Passagierdaten von Flügen in die EU und aus der EU für bis zu fünf Jahre gespeichert werden. Innereuropäische und nationale Flüge sind von der Speicherung ausgenommen. Festgehalten werden pro Passagier und Flug bis zu 60 Einzelangaben. Die Richtlinie zur Fluggastdatenspeicherung befindet sich derzeit in den Trilogverhandlungen und soll bis Ende des Jahres abgeschlossen werden. Datenschützer kritisieren, die Regelung beinhaltet einen Eingriff von großem Ausmaß und besonderer Schwere in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten. Die Safe Harbor Entscheidung könnten dazu führen, dass auch diese Richtlinie auf die vom EuGH gemachten Kriterien hin überprüft wird.

- **Internationale Handelsabkommen:** Derzeit wird zwischen der EU und den Vereinigten Staaten ein internationales Freihandelsabkommen (↗»TTIP«) verhandelt. Ebenfalls auf dem Weg ist ein Abkommen über den Handel mit Dienstleistungen (↗»TISA«) in Form eines völkerrechtlichen Vertrags zwischen 23 Parteien einschließlich der USA. Datenschutzfragen werden grundsätzlich nicht im Rahmen dieser Verträge verhandelt. Allerdings betrifft der Datenschutz z. B. auch handelsbezogene Kommunikation etwas bei Dienstleistungen im ITK-Bereich oder E-Commerce. Einige EU-Parlamentarier haben daher die Frage nach den Auswirkungen der Safe Harbor Entscheidung aufgeworfen. Die Kommission, der unter EU-Recht die Kompetenz zugewiesen ist diese Handelsverträge auszuhandeln, versichert jedoch, dass der EU-Datenschutz nicht durch die Verträge betroffen sei.

Bitkom vertritt mehr als 2.300 Unternehmen der digitalen Wirtschaft, davon gut 1.500 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom