Datenübermittlung in die USA: Was passiert nach dem EuGH-Urteil zu Safe Harbor?

26. Oktober 2015

1. Was ist das „Safe Harbor“-Abkommen?

Die Übermittlung personenbezogener Daten in die USA ist nach deutschem und europäischem Datenschutzrecht nur unter sehr engen Voraussetzungen gestattet. Die USA gelten als „unsicherer Drittstaat“, dessen Gesetze den Betroffenen kein „angemessenes Schutzniveau“ bieten, das mit europäischen Datenschutzstandards vergleichbar ist.

Um eine Datenübermittlung in die USA zu erleichtern, hat die EU-Kommission mit dem US-Handelsministerium im Jahr 2000 das sogenannte Safe-Harbor-Abkommen geschlossen. US-Unternehmen können dem Safe-Harbor-Abkommen im Wege einer Selbstzertifizierung beitreten, indem sie sich den darin geregelten datenschutzrechtlichen Pflichten und Prinzipien unterwerfen und sich öffentlich verpflichten, diese einzuhalten. Die Liste der Beitrittsunternehmen ist unter http://safeharbor.export.gov/list.aspx abrufbar.

Bislang galt, dass mit dem Beitritt eines US-Unternehmens zum Safe-Harbor-Abkommen dieses als „datenschutzrechtlich sicher“ angesehen wurde. Eine Übermittlung personenbezogener Daten an Beitrittsunternehmen war damit zumindest prinzipiell möglich (auch wenn im Einzelfall noch weitere Voraussetzungen und Details vorliegen mussten – insbesondere nach Auffassung der deutschen Datenschutz-Aufsichtsbehörden).

2. Was hat der EuGH entschieden?

Der EuGH (Urt. v. 6.10.2015, Rs. C-362/14) hat die Entscheidung der Kommission 2000/520/EC vom 26.7.2000, nach welcher das Safe-Harbor-Abkommen ein angemessenes Schutzniveau gewährleistet, für ungültig erklärt. Der EuGH hat dies damit begründet, dass das Safe-Harbor-Abkommen nur für Beitrittsunternehmen gilt, nicht aber für amerikanische Behörden. Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses und der Durchführung von Gesetzen der USA haben Vorrang vor den Safe-Harbor-Regelungen, so dass US-Unternehmen verpflichtet sind, die Safe-Harbor-Regelungen nicht anzuwenden, wenn sie diesen Erfordernissen widersprechen. Zwar sagt der EuGH in dem Urteil nicht explizit, dass in den USA kein angemessenes Schutzniveau für personenbezogene Daten besteht, doch er führt aus, dass amerikanische Behörden auf die aus der EU in die USA übermittelten personenbezogenen Daten zugreifen und sie in einer Weise verarbeiten können, die über das hinausgeht, was zum Schutz der nationalen Sicherheit absolut notwendig und verhältnismäßig ist. Eine Regelung, die es Behörden gestattet, generell und ohne irgendeine Differenzierung auf den Inhalt elektronischer Kommunikation zuzugreifen, verletze das Grundrecht auf Achtung des Privatlebens. Trotz Safe-Harbor sind also Eingriffe amerikanischer Behörden in Persönlichkeitsrechte der Betroffenen, deren Daten übermittelt werden, in einem Umfang möglich, der unverhältnismäßig ist und damit Grundrechte der EU-Bürger verletzt.

3. Welche Vertragsverhältnisse / Auftragnehmer / Subunternehmer sind betroffen?

Grundsätzlich sind alle Vertragsbeziehungen betroffen, bei denen personenbezogene Daten direkt oder indirekt in die USA übermittelt werden. Beispiele:

- Cloud-Anbieter (z.B. Salesforce, Google Apps, Dropbox, Microsoft 365)
- Hosting-/Infrastruktur-Anbieter (z.B. Amazon AWS, Microsoft Azure)
- Website-Analyse und Werbenetzwerke, Social-Media-Plugins (da auch IP-Adressen derzeit als personenbezogene Daten angesehen werden!), z.B. Google Analytics, Google Adwords, Facebook Retargeting.

Betroffen sind insbesondere auch Konstellationen, in denen Daten zwar in EU-Rechenzentren gespeichert werden, der Auftragnehmer sich aber z.B. zu Wartungs- oder Entwicklungszwecken Zugriff durch Mitarbeiter oder Subunternehmer aus den USA vorbehält.

4. Wie kann ich jetzt noch rechtmäßig Daten in die USA übermitteln?

Deutsches und europäisches Datenschutzrecht sehen neben Safe Harbor weitere Möglichkeiten zur „Legalisierung“ einer Datenübermittlung in die USA vor:

a. Einwilligungen der Betroffenen

Eine Datenübermittlung in unsichere Drittstaaten ist zulässig, wenn alle Betroffenen (d.h. alle Personen, deren Daten übermittelt werden) ausdrücklich ihre Einwilligung erklären. Dieser Weg ist praktisch nicht umsetzbar, da so gut wie nie alle Betroffenen tatsächlich erreichbar und auch bereit sind, eine Einwilligung abzugeben. Die Einwilligung müsste zudem „informiert“ erfolgen, d.h. es müssten alle tatsächlichen und potentiellen Datenempfänger in den USA genannt werden und es müsste umfassend über die mit der Übermittlung verbundenen Risiken aufgeklärt werden. Eine Einwilligung von Arbeitnehmern ist ebenfalls problematisch, da diese nach Auffassung der Aufsichtsbehörden i.d.R. nicht freiwillig abgegeben wird. Einwilligungen sind zudem jederzeit widerruflich, was eine Datenverarbeitung allein auf dieser Grundlage für Unternehmen im Grunde ausschließt.

b. Abschluss von Verträgen nach den EU-Standardvertragsklauseln

Die EU-Kommission hat in den letzten Jahren Standardvertragsklauseln für die Übermittlung von Daten an Empfänger in unsicheren Drittstaaten veröffentlicht. Wenn die Parteien diese Standardvertragsklauseln unverändert (!) in einem Vertrag verwenden, ist auf dieser Basis ein Datentransfer auch an Empfänger in den USA bisher grundsätzlich erlaubt. Allerdings schließen US-Unternehmen ungern Verträge auf Basis der EU-Standardvertragsklauseln ab – insbesondere weil sie sich damit dem Recht und der Datenschutzaufsicht Deutschlands (bzw. des jeweiligen EU-Staates des Vertragspartners) unterwerfen.

c. Implementierung von Binding Corporate Rules (BCR)

Internationale Konzerne können sich verbindliche Konzernregelungen zum Datenschutz auf Basis des europäischen Datenschutzrechts auferlegen (sog. Binding Corporate Rules). So kann für alle Konzernunternehmen ein „angemessenes Datenschutzniveau“ hergestellt werden. Die Datenübermittlung an Konzernunternehmen in den USA wäre damit grundsätzlich erlaubt. Allerdings müssen die Datenschutzbehörden aller EU-Länder, in denen Konzernunternehmen ihren Sitz haben, den konkreten BCR zustimmen. Der administrative Aufwand ist daher erheblich und der Abschluss von BCR bedarf aufgrund der erforderlichen Genehmigungen einer langen Vorlaufzeit.

Achtung:

Der **EuGH** hat sich zur Wirksamkeit der EU-Standardvertragsklauseln und BCR in seinem Urteil vom 6.10.2015 **nicht** geäußert. Die Begründung des EuGH zur Unwirksamkeit von Safe-Harbor betrifft der Sache nach aber auch die EU-Standardvertragsklauseln und BCR: Auch in diesen Fällen können US-Behörden unabhängig von den vertraglichen Vereinbarungen unbeschränkten Zugriff auf personenbezogene Daten nehmen. Andererseits haben die EU-Standardvertragsklauseln und BCR einen anderen rechtlichen Ansatz, denn diese finden gerade auf die Datenübermittlung in ein Empfängerland Anwendung, das kein angemessenes Datenschutzniveau gewährleistet. Die EU-Kommission verweist daher in einer Pressemitteilung ausdrücklich auf die weiterhin bestehende Möglichkeit der Verwendung von EU-Standardvertragsklauseln und BCR.

Es bleibt abzuwarten, welche Haltung die Datenschutz-Aufsichtsbehörden hierzu einnehmen und ob sie trotz Abschluss von EU-Standardvertragsklauseln oder BCR kein „angemessenes Datenschutzniveau“ mehr annehmen werden und eine Datenübermittlung in die USA bis zu einer gesetzlichen Neuregelung generell unzulässig sein wird.

5. Was ist jetzt zu tun?

Folgende Schritte bieten sich an:

- **Bestandsaufnahme:** Es sollte festgestellt werden, welche Vertragsverhältnisse / Partner / Subunternehmer überhaupt betroffen sind, entweder
  - weil es sich um US-Unternehmen handelt, an die direkt Daten übermittelt werden oder
  - weil es sich um EU-Vertragspartner handelt, die sich eine Weiterübertragung von Daten an Subunternehmer in den USA vorbehalten (das ist z.B. regelmäßig Fall bei Verträgen mit den europäischen Töchtern von Microsoft, Facebook, Google, IBM, Amazon usw.).
- Nach Feststellung welche Vertragsverhältnisse betroffen sind, sollten diese nach ihrer Bedeutung für das Unternehmen **priorisiert** werden.
- Wird in den o.g. Fällen die Datenübermittlung auf Safe Harbor gestützt, ist sie nach der Rechtsprechung des EuGH unzulässig. In diesen Fällen könnten die o.g. **Alternativen** in Betracht kommen, etwa der Abschluss von Verträgen auf Basis der EU-Standardvertragsklauseln aber auch der eher langfristige Ansatz des Einsatzes von BCRs.
- Beim Einsatz von Dienstleistern mit Sitz in den USA, die bisher Safe Harbor zertifiziert waren, sollten **alternative Garantien** angefragt werden.
- Es sollte nach Möglichkeit **dokumentiert** werden, dass sich das Unternehmen darum bemüht, Alternativen für eine rechtmäßige Datenübermittlung zu suchen.
- In jedem Fall sollten die Positionen der deutschen **Aufsichtsbehörden beobachtet** werden.

6. Was machen die deutschen Datenschutz-Aufsichtsbehörden? Drohen Maßnahmen und Bußgelder?

a. Aktueller Stand

Die offiziellen Stellungnahmen der deutschen Aufsichtsbehörden beschränken sich bisher (Stand 6.10.2015) weitgehend auf die grundsätzliche Begrüßung des Urteils.

Die Aufsichtsbehörden haben angekündigt, in den nächsten Tagen ihr Vorgehen auf nationaler und europäischer Ebene zu koordinieren. Aus einer ersten Stellungnahme des Hamburger Datenschutzbeauftragten ist aber auch abzuleiten, dass diese Behörde durchaus auch die Instrumente Standardvertragsklauseln und BCR auf den Prüfstand stellen will. Wörtlich heißt es dort: „Es ist zu prüfen, ob und inwieweit Datentransfers in die USA auszusetzen sind. Dies gilt auch, wenn sie auf andere Rechtsgrundlagen wie Standardvertragsklauseln, Einwilligung oder Binding Corporate Rules gestützt werden.“ (https://www.datenschutz-hamburg.de/news/detail/article/eugh-kippt-transatlantisches-safe-harbor-abkommen.html).

In einer ersten Stellungnahme des Ersten Vizepräsidenten der EU-Kommission Frans Timmermans und der EU-Kommissarin für Justiz, Verbraucherschutz und Gleichstellung Vera Jourová heißt es hingegen: „In the meantime, transatlantic data flows between companies can continue using other mechanisms for international transfers of personal data available under EU data protection law. The EU data protection rules provide for several other mechanisms that provide safeguards for international transfers of personal data, for instance through standard data protection clauses in contracts between companies exchanging data across the Atlantic or binding corporate rules for transfers within a corporate group.” Die Kommission geht also offensichtlich davon aus, dass Datenübermittlungen auf der Grundlage der Standardvertragsklauseln und BCRs weiter zulässig bleiben.

Möglicherweise werden Übergangsfristen zur Umstellung auf „rechtmäßige“ Vertragsmodelle eingeräumt – sofern es solche Modelle nach Auffassung der Aufsichtsbehörden unter Berücksichtigung des EuGH-Urteils überhaupt noch geben wird. Denkbar ist auch, dass Übergangsfristen bis zum Inkrafttreten eines neuen – derzeit in Verhandlung befindlichen – Safe Harbor-Abkommens gewährt werden.

Es ist aber auch nicht auszuschließen, dass es zu der Problematik unterschiedliche Positionen auf EU-Ebene (EU-Kommission) und auf nationaler Ebene (deutsche Datenschutzaufsichtsbehörde) geben wird, was zu einer erheblichen Rechtsunsicherheit führen würde.

b. Aktuelles Risiko von Maßnahmen und Sanktionen

In der augenblicklichen Phase der Rechtsunsicherheit ist nicht damit zu rechnen, dass die deutschen Datenschutzbehörden **kurzfristig** Maßnahmen gegen Unternehmen ergreifen oder gegen diese Bußgelder verhängen, die personenbezogene Daten bislang auf der Basis von Safe Harbor in die USA übermittelt haben und weiterhin übermitteln.

c. Instrumentarium der Aufsichtsbehörden

Mittelfristig ist aber nicht auszuschließen, dass die Datenschutzbehörden das Übermittlungsverbot gegen Unternehmen durchsetzen. Den Aufsichtsbehörden steht hierzu grundsätzlich das folgende **Instrumentarium** zur Verfügung:

- Verlangen nach Auskunft
- Prüfbesuche vor Ort
- Anordnungsverfügungen
- Untersagungsverfügungen
- Verhängung von Bußgeldern
- Einleitung eines Strafverfahrens

Je nach der weiteren Entwicklung sollte das Unternehmen auf entsprechende Maßnahmen und Verfahrensschritte vorbereitet sein.

7. Arbeitsrecht: Kollektivrechtliche Auswirkungen des Urteils des EuGH vom 6.10.2015 (C-362/14) in mitbestimmten Unternehmen

Die Übermittlung von Beschäftigtendaten innerhalb von (internationalen) Konzernen entspricht einer weit verbreiteten Praxis und einem ebenso weit verbreiteten praktischen Bedürfnis.

In mitbestimmten Unternehmen gehört die Überwachung der Einhaltung datenschutzrechtlicher Bestimmungen zu den Aufgaben des Betriebsrats. Die Übermittlung von Beschäftigtendaten ins EU-Ausland wird daher zumeist in **Betriebsvereinbarungen** geregelt, weil Betriebsvereinbarungen aufgrund ihrer normativen Wirkung als Erlaubnisnormen im Sinne von § 4 Abs. 1 BDSG gelten. Soweit es speziell um den Datentransfer von deutschen Konzernunternehmen zu Konzerngesellschaften (meistens zur Konzernmutter) mit Sitz in den USA geht, enthalten solche Betriebsvereinbarungen häufig den Vorbehalt, dass die jeweiligen US-Unternehmen einen angemessenen Datenschutz-Standard herstellen müssen, indem sie dem Safe Harbor-Abkommen beitreten bzw. sich dessen Grundsätzen verbindlich unterwerfen.

Nach dem Urteil des EuGH vom 6.10.2015 in der Rechtssache C-362/14 gewährleisten die Safe Harbor-Grundsätze jedoch kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG.

Wenngleich das Urteil keine unmittelbare Auswirkung auf den Inhalt oder den rechtlichen Bestand von Betriebsvereinbarungen entfaltet, die auf Safe Harbor verweisen, stellt sich die Frage, ob und inwieweit solche Betriebsvereinbarungen noch als Erlaubnisnormen im Sinne von § 4 Abs. 1 BDSG wirken können, nachdem ihre Geschäftsgrundlage gleichsam weggefallen ist. Zwar dürfen (nach umstrittener Auffassung) Betriebsvereinbarungen den im BDSG festgelegten Mindeststandard an Datenschutz unterschreiten, doch müssen die Persönlichkeitsrechte der betroffenen Arbeitnehmer insgesamt angemessen berücksichtigt werden. Ein Verweis auf Safe Harbor genügt hierfür nun nicht (mehr).

Es liegt somit (jetzt erst recht) an den Unternehmen als verantwortliche Stelle, und an den Betriebsräten, zu prüfen, ob und wie ein angemessenes Schutzniveau innerhalb des Konzerns gewährleistet werden kann. Ob den Konzernen eine massenhafte (außerordentliche?) Kündigung oder Lossagung von bestehenden Betriebsvereinbarungen durch die Betriebsräte ins Haus steht, bleibt abzuwarten. Empfehlenswert erscheint dies nicht. Soweit nämlich infolgedessen auch eine Nachwirkung entfällt, entstünde ein nicht erstrebenswerter, regelungsfreier Zustand, in dem die Persönlichkeitsrechte der betroffenen Arbeitnehmer erst Recht nicht zur Geltung kommen können.

Ratsamer dürfte es sein, dass sich die Betriebsparteien nach dem Urteil des EuGH unverzüglich mit der Frage befassen, wie bestehende **Betriebsvereinbarungen angepasst** werden können und müssen. Ein Anspruch auf

Anpassungsverhandlungen lässt sich nach der Rechtsprechung des BAG im Falle des Wegfalls der Geschäftsgrundlage auch ohne Kündigung durchsetzen.

8. Fazit

Alle weiteren zu unternehmenden Schritte hängen im Wesentlichen davon ab, wie sich die deutschen Datenschutzbehörden zu dem Problem positionieren, insbesondere ob sie

- alternative Wege wie die Vereinbarung auf Basis der EU-Standardvertragsklauseln (unverändert mit den bisherigen Musterklauseln) oder BCRs weiterhin akzeptieren,
- andere Lösungswege aufzeigen,
- Übergangsfristen einräumen, oder
- das gesetzliche Übermittlungsverbot flächendeckend durchsetzen.

Auch ist der zügige Abschluss eines neuen Safe-Harbor-Abkommens möglich, das die Datenübermittlung in die USA zulassen würde.

Wir werden Sie über die aktuelle Entwicklung und die möglicherweise notwendigen Schritte auf dem Laufenden halten und dieses **Whitepaper periodisch aktualisieren**. Für Fragen stehen wir Ihnen natürlich immer gerne zur Verfügung.

Die Autoren sind Rechtanwälte der Kanzlei „TCI Rechtsanwälte“ mit Branchenfokus in den Bereichen Technology, Communications, Information, auf denen die Kurzbezeichnung „TCI“ beruht.

TCI Rechtsanwälte München (Tel. 089 / 38367880):

- Dr. Thomas Stögmüller, LL.M. (Berkeley), Fachanwalt für Informationstechnologierecht; tstoegmueller@tcilaw.de
- Dr. Michael Karger, Fachanwalt für Informationstechnologierecht, Fachanwalt für Verwaltungsrecht; mkarger@tcilaw.de
- Harald Krüger, Fachanwalt für Arbeitsrecht; hkrueger@tcilaw.de
- Dr. Truiken Heydn; theydn@tcilaw.de

TCI Rechtsanwälte Berlin (Tel. 030 / 2005420):

- Carsten Gerlach, Fachanwalt für Informationstechnologierecht; cgerlach@tcilaw.de

TCI Rechtsanwälte Mainz (Tel. 06131 / 30290460):

- Stephan Schmidt, Fachanwalt für Informationstechnologierecht; sschmidt@tcilaw.de
- Christian Welkenbach, Fachanwalt für Informationstechnologierecht, Fachanwalt für gewerblichen Rechtsschutz; cwelkenbach@tcilaw.de

Weitere Informationen: www.tcilaw.de und www.it-rechts-praxis.de.

(Version 1.0; Stand: 26.10.2015)

Dieses Merkblatt wurde im Rahmen der Kooperation IT-Sicherheit für Familienunternehmen der IHK Schwaben mit dem Branchennetzwerk aitiRaum e.V. erstellt.

Ansprechpartner:

Kristin Joel
Stettenstraße 1 + 3 | 86150 Augsburg
Tel 0821 3162-406 | Fax 0821 3162-342
kristin.joel@schwaben.ihk.de