Datenschutzrecht: Safe Harbor ist tot – was müssen Unternehmen nun beachten?

27.10.2015

Es war die Sensationsnachricht vor drei Wochen: Der EuGH kippte in einem aufsehenerregenden Urteil das Safe-Harbor-Abkommen. In der Folge macht sich nun in den Unternehmen, die ihre Daten auf ausländischen Servern speichern oder mit Cloud-Anbietern zusammenarbeiten, deren Server in den USA stehen, große Unsicherheit breit, was sie nun tun müssen, um nicht ins Visier der Datenschützer zu geraten.

Was war Safe Harbor?

Safe Harbor war ein Abkommen zwischen der Europäischen Union und den USA, wonach personenbezogene Daten aus der EU legal in die USA übermittelt und von dort ansässigen Unternehmen verarbeitet werden durften.

Hintergrund dieses Abkommens waren die Vorschriften der Art. 25 und 26 der Europäischen Datenschutzrichtlinie

(http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML),

wonach ein Datentransfer in sog. unsichere Drittstaaten, die über kein dem EU-Recht vergleichbares Datenschutzniveau verfügen, verboten ist. Da es in den USA keine den EU-Vorschriften vergleichbaren Datenschutzregelungen gibt, sind die USA ein unsicheres Drittland i. S. d. Vorschriften.

Da der Datenaustausch mit den USA weiterhin ermöglicht werden sollte, wurde das Safe-Harbor-Abkommen geschlossen, wonach sich US-Unternehmen, die daran teilnehmen wollten, verschiedenen Datenschutzprinzipien der EU unterwerfen mussten. Eine Liste mit sich verpflichteten Unternehmen war beim US-Handelsministerium einsehbar

(Quelle: https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/SafeHarbor.html)

Generelle Zulässigkeit von Datentransfers

Generell ist nach dem Bundesdatenschutzgesetz (BDSG) die Übermittlung von personenbezogenen Daten an Dritte verboten. Erlaubt ist dies nur, wenn die Betroffenen in die Datenübermittlung gem. § 4 a BDSG eingewilligt haben oder das Unternehmen mit dem Dritten eine sog. Auftragsdatenverarbeitungsvereinbarung (ADVV) gem. § 11 BDSG geschlossen hat.

Solche Datenübermittlungen liegen z. B. vor, wenn Dritte für ein Unternehmen den Newsletterversand inkl. Datenerhebung durchführen, Agenturen Mailings oder Gewinnspiele inkl. Datenerhebung organisieren, Daten von Kunden bei einem Cloud-Anbieter gehostet werden, von einem Dritten Userdaten per Online-Tools ausgewertet werden etc.

Zwischen Unternehmen, die in der EU ansässig sind, sind Datentransfers auf Basis von ADVVs zulässig. Mit Unternehmen, die außerhalb der EU in einem Land, das ein von der EU anerkanntes angemessenes Datenschutzniveau aufweist (u. a. Schweiz, Kanada, Australien, Neuseeland, Ar-

gentinien, Andorra, Färöer, Guernsey, Isle of Man, Jersey, Israel, Uruguay), ansässig sind, können die von der EU vorgegebenen sog. Standardvertragsklauseln abgeschlossen werden.

Daneben gibt es sog. unsichere Drittstaaten (u. a. Japan, Indien, China), die kein angemessenes Datenschutzniveau aufweisen und deren Datenschutzniveau daher individuell überprüft werden muss.

Es gibt lediglich eine Ausnahme gem. § 4 c Abs. 3 Nr. 1 BDSG, die auch eine Datenübermittlung in unsichere Drittstaaten ohne Überprüfung erlaubt, nämlich wenn die Datenübermittlung notwendig ist, um vertragliche Verpflichtungen zu erfüllen, z. B. die Übermittlung von Kundenadressen im Rahmen eines Onlinekaufs zum Zwecke des Warenversands oder bei Reisebuchungen.

Das Urteil des EuGH

Der EuGH hat mit Urteil vom 6. Oktober, Az: C-362/14 , das Safe Harbor Abkommen für ungültig erklärt. Als Begründung wurde angeführt, dass die EU-Kommission keine ausreichenden Befugnisse gehabt habe, um das Safe Harbor Abkommen abschließen zu dürfen, dass die in dem Abkommen vorhandenen Öffnungsklauseln zu weitgehend gewesen seien und, dass der Datenzugriff von US-Behörden aufgrund fehlender Regelungen in dem Abkommen möglich gewesen sei.

Hintergrund des Urteils ist ein Rechtsstreit eines Datenschutz-Aktivisten Max Schrems gegen Facebook Irland. Schrems hatte den irischen Datenschutzbeauftragten aufgefordert, Facebook den Datentransfer in die USA zu untersagen, was der Datenschutzbeauftragte mit Verweis auf eine Safe-Harbor-Zertifizierung von Facebook ablehnte und seine Prüfungsbefugnis beschränkt sah. Der oberste Gerichtshof Irlands hatte daraufhin diese Fragen dem EuGH zur Vorabentscheidung vorgelegt.

Das Urteil des EuGH hat zur Folge, dass die Übermittlung personenbezogener Daten in die USA und deren dortige Verarbeitung nunmehr unzulässig sind. Sowohl das Unternehmen, das die Daten übermittelt, als auch das Unternehmen, das die Daten in den USA verarbeitet, verstoßen gegen die Datenschutzregelungen, was neben Schadensersatzansprüchen der Betroffenen auch Bußgelder der Datenschutzbehörden bis zu 300.000 EUR zur Folge haben kann.

Gibt es Alternativen zu Safe Harbor?

Da viele Unternehmen Leistungen von US-Anbietern in Anspruch nehmen, stellt sich für diese nun die Frage, ob es Alternativen zum Safe Harbor Abkommen gibt, die den Datentransfer zulässig machen.

Die gute Nachricht ist: Es gibt Alternativen. Die schlechte Nachricht ist: Diese sind aufgrund der derzeitigen Rechtslage ebenfalls nicht 100 % sicher.

Wechsel zu einem Anbieter in einem sicheren Drittland:
Sofern dies praktikabel ist, sollte zu einem Anbieter gewechselt werden, der seinen Sitz innerhalb der EU oder in einem sicheren Drittland, s. o., hat. Dann ist nur eine ADVV erforderlich.

Einwilligung der Betroffenen:
Zulässig und rechtssicher, aber bei großen Unternehmen wohl nicht praktikabel, ist die Einholung der schriftlichen Einwilligung der Betroffenen, deren Daten übermittelt werden sollen. Dies erfordert selbstverständlich vorab eine umfassende Aufklärung über den Umfang der Datenübermittlung.

Standardvertragsklauseln der EU:
Eine weitere Möglichkeit ist der Abschluss sog. Standardvertragsklauseln mit einem Anbieter, der in einem unsicheren Drittstaat sitzt.
Hierbei handelt es sich um von der EU vorgegebene Standardverträge, die den Vertragspartner verpflichten, sich den wesentlichen geltenden Datenschutzregelungen der EU zu unterwerfen.
Allerdings muss sich der Dienstleister auch an die Vorgaben der Standardvertragsklauseln halten, was ggfs. von dem Auftraggeber kontrolliert werden muss. Es gibt auch bereits Unternehmen, die von sich aus den Abschluss dieser Verträge anbieten.
Verweigert ein Unternehmen den Abschluss dieser Vertragsklauseln, kann evtl. ein außerordentliches Kündigungsrecht bestehen.
Diese Verträge sind jedoch auch nicht sicher, da alle Landesdatenschutzbeauftragten bereits angekündigt haben, diese Standardvertragsklauseln ebenfalls überprüfen lassen zu wollen.

Individueller Vertrag:
Unternehmen können auch einen individuellen Vertrag mit dem Anbieter schließen, der den Anbieter auf die Einhaltung der wesentlichen Bestimmungen des deutschen Datenschutzrechts verpflichtet und die Einhaltung in geeigneter Weise garantiert. Ein solcher Vertrag muss jedoch von der zuständigen Datenschutzbehörde ausdrücklich genehmigt werden. Ein solches Genehmigungsverfahren ist recht aufwändig, setzt Kontrollen voraus und garantiert letztlich nicht die Genehmigung der Behörde.

Binding Corporate Rules:
Für Konzerne und Firmengruppen, die intern Daten in unsichere Drittstaaten übermitteln, kommen sog. Binding Corporate Rules (BCRs) in Frage. Hierbei handelt es sich um verbindliche Unternehmensrichtlinien, die den Datenschutz und die Übermittlung personenbezogener Daten ausschließlich innerhalb des Konzerns regeln. Der Inhalt kann individuell gestaltet werden, muss aber einige Pflichtregelungen z. B. zu einem Sicherheitskonzept, Audit, Schulungen, enthalten.
Problematisch ist jedoch, dass die BCRs im Rahmen eines sog. Mutual Recognition-Verfahrens von den europäischen Datenschutzbehörden anerkannt werden müssen, was bis zu 2 Jahren dauern kann (Quelle: https://de.wikipedia.org/wiki/Binding_Corporate_Rules).

Außerdem stehen auch die BCRs nunmehr auf dem Prüfstand der Datenschützer.

Was werden die Datenschutzbehörden nun unternehmen?

Die Landesdatenschutzbeauftragten stürzen sich nun natürlich auf dieses Thema. Der neue Landesdatenschutzbeauftragte von Rheinland-Pfalz, Dieter Kugelmann, studierter Jurist, kündigte in einem Interview mit der Allgemeinen Zeitung (Rhein Main Presse) bereits an, dass in den nächsten Wochen wohl hunderte Unternehmen in Rheinland-Pfalz Anfragen von seiner Behörde erhalten werden, in denen sie Auskunft darüber geben müssen, auf welcher rechtlichen Grundlage sie Daten in die USA senden. Kugelmann hat ferner angekündigt, dass auch Bußgelder bis zu 300.000 EUR verhängt werden können, wenn trotz des Safe Harbor-Urteils noch Daten in die USA versandt werden.

Am 21. Oktober gab es auf einer Konferenz des Datenschutzbeauftragten des Bundes und der Länder auch ein Treffen der Landesdatenschutzbeauftragten, die sich auf ein gemeinsames Vorgehen geeinigt haben. Eine Stellungnahme ist am 26. Oktober 2015 veröffentlicht worden (Quelle: https://www.datenschutz.hessen.de/ft-europa.htm#entry4521), wonach man sich u. a. auf Folgendes geeinigt hat:

- Jegliche Datenverarbeitungen, die bisher auf Basis des Safe Harbor Abkommens durchgeführt wurden, sind nunmehr unzulässig.
- Erhalten die Behörden hiervon Kenntnis, werden sie diese Datenübermittlungen untersagen.
- Auch Datenübermittlungen aufgrund von Standardvertragsklauseln und BCRs sind in Frage gestellt.
- Die Behörden werden derzeit keine BCRs oder andere Verträge über Datenübermittlungen in die USA genehmigen.
- Unternehmen sollen unverzüglich den Datentransfer datenschutzgerecht gestalten.
- Einwilligungen zum Datentransfer können eine Grundlage hierfür sein.

Es wurde ebenfalls angekündigt, dass man bis zum 31.01.2016 auf eine Entscheidung der EU zur Zulässigkeit der Standardvertragsklauseln warte, danach aber Anhörungen von Unternehmen in die Wege leiten werde. Nach solchen schriftlichen Anhörungen können dann Untersagungsverfügungen erlassen und bei Weigerung Bußgelder verhängt werden.
Allerdings werden die Behörden im Falle von Beschwerden von Betroffenen auch schon früher tätig werden, da sie hierzu verpflichtet sind.

Was müssen Unternehmen nun veranlassen?

Das Urteil betrifft alle Unternehmen, die selbst Daten in die USA weiterleiten oder von dort ansässigen Dienstleistern, z. B. Cloud-Anbietern, in den USA verarbeiten lassen, somit insbesondere Unternehmen, die im Online-Marketing tätig sind und Analysen, E-Mail Marketing, sowie Cloud Computing betreiben. Es genügt bereits, wenn ein Unternehmen einen US-Anbieter wählt, der z. B. den Newsletterversand abwickelt, da in diesem Fall personenbezogene Daten wie E-Mail-Adressen und Namen auf dem Server des US-Anbieters gehostet werden.
Unternehmen, die mit Anbietern aus den USA zusammenarbeiten, sollten daher Maßnahmen in die Wege leiten, die im Falle einer Anhörung durch den Landesdatenschutzbeauftragten dokumentieren, dass man sich um den Datenschutz kümmert und versucht, dass Safe Harbor Urteil umzusetzen. Solche Maßnahmen, die immer schriftlich dokumentiert werden sollten, enthalten z. B. eine datenschutzrechtliche Prüfung des Vertragspartners in den USA, sofern dies in der Praxis möglich ist. Geprüft werden sollte u. a., ob es eine Datenschutzerklärung bzw. privacy policy gibt, ob diese den deutschen Vorschriften entspricht, ob die dort genannten Regelungen auch umgesetzt werden, ob es eine ausreichende Datenverschlüsselung gibt etc.
Daneben sollten, nach Ansicht der Datenschutzbeauftragten, derzeitige Verträge mit US-Anbietern gekündigt und neue, angepasste Verträge geschlossen werden. Letztlich sollte auf den Abschluss von EU-Standardvertragsklauseln gedrängt werden, auch wenn diese derzeit noch auf dem Prüfstand stehen.

Ausblick

Die EU-Kommission verhandelt derzeit mit den USA über eine Novelle der Safe-Harbor-Regelungen. Ob und wann es jedoch eine neue Vereinbarung geben wird, ist fraglich.

Bis Ende Januar 2016 soll seitens der EU geklärt werden, ob die Standardvertragsklauseln bzw. die BCRs noch zulässig sind bzw. diese angepasst werden.

Fazit

Auch wenn die Rechtslage derzeit sehr unsicher ist, sollten Sie auf keinen Fall in Panik verfallen. Allerdings dürfen Sie nun auch nicht gänzlich untätig bleiben. Als erstes sollten Unternehmen her-

ausfinden, ob sie überhaupt mit Dienstleistern aus den USA zusammenarbeiten oder Software von US-Anbietern nutzen bzw. wo übermittelte Daten verarbeitet werden. Sofern Sie danach von dem Safe Harbor Urteil betroffen sind, sollten Sie sich aktiv um Datenschutzmaßnahmen bemühen. Wir empfehlen daher, zumindest die o. g. Maßnahmen in die Wege zu leiten und zu versuchen, gemeinsam mit Ihren US-Anbietern eine Regelung zu finden bzw. EU-Standardvertragsklauseln abzuschließen. Achten Sie auf eine schriftliche Dokumentation für den Fall, dass Sie demnächst eine Anhörungsmitteilung des Landesdatenschutzbeauftragten erhalten.

Falls Sie Fragen zum Datenschutzrecht haben, können Sie uns gerne kontaktieren.
Wir helfen Ihnen schnell und kompetent.

Ihr Ansprechpartner für weitere Fragen ist:

Rechtsanwältin Daniela Wagner-Schneider LL.M.
Fachanwältin für Gewerblichen Rechtsschutz

WAGNER Rechtsanwälte webvocat® - Small.Different.Better

WAGNER Rechtsanwälte webvocat®

Weitere interessante News finden Sie auf unserer Webseite www.webvocat.de
Wenn Sie diesen Newsletter nicht mehr erhalten möchten, senden Sie bitte eine E-Mail an: wagner@webvocat.de

---

Impressum

WAGNER Rechtsanwälte webvocat® Partnerschaft, Attorneys at Law
Großherzog-Friedrich-Str. 40, D-66111 Saarbrücken,
Fon: +49 (0) 681/958282-0, Fax: +49 (0) 681/958282-10,
E-Mail: wagner@webvocat.de,
Internet: www.webvocat.de / www.geistigeseigentum.de

Mitglieder der Rechtsanwaltskammer des Saarlandes / Members of the Bar Association of the Saarland; USt-Id/Vat-No.: DE 265452894; Partnerschaftsregister / Partnership Register: Amtsgericht Saarbrücken Nr./No. 98, Vertretungsberechtigte Partner/ authorized representatives: Manfred Wagner, Daniela Wagner-Schneider; Verantwortlich für den Inhalt: Rechtsanwältin Daniela Wagner LL.M.

Rechtliche Hinweise

ren Inhalte nicht zu Eigen. Die Webseiten Dritter unterliegen der Haftung der jeweiligen Betreiber. Zum Zeitpunkt der Linksetzung waren keine Rechtsverstöße auf den verlinkten Webseiten ersichtlich. Im Falle von Rechtsverstößen auf den Webseiten Dritter distanzieren wir uns ausdrücklich von den Inhalten der entsprechenden Seiten. Eine ständige Kontrolle aller externen Links ist uns ohne konkrete Hinweise auf Rechtsverstöße nicht zumutbar. Bei Kenntnis von Rechtsverstößen werden wir jedoch derartige externe Links unverzüglich löschen.