Bundesministerium
für Wirtschaft
und Energie

Trusted Cloud

Eckpunkte zu Safe Harbor und Privacy Shield

Was Anwender wissen sollten

Version 1.0
16. Februar 2016
RA/FA IT-Recht Dr. Jens Eckhardt

TrustedCloud

Eckpunkte zu Safe Harbor und Privacy Shield als Rechtsgrundlagen zur Übermittlung von Daten in die USA – Was Anwender wissen sollten

Autor: RA/FA IT-Recht Dr. Jens Eckhardt

Werden Cloud Service aus den USA oder unter Einbindung von Unternehmen in den USA angeboten, wurde die Zulässigkeit der Datenübermittlung häufig auf die sog. Safe Harbor Principles gestützt. Diese Rechtsgrundlage hat der EuGH mit seinem Urteil vom 06.10.2015 für unwirksam erklärt. Seit dem 02.02.2016 ist ein Nachfolgeabkommen, das Privacy Shield heißen soll, abgestimmt, aber noch nicht in Kraft.

Warum das Safe Harbor-Abkommen und das Nachfolgeabkommen benötigt werden

Das deutsche und auch das europäische Datenschutzrecht fordern für die Übertragung personenbezogener Daten an einen Dritten eine datenschutzrechtliche Rechtsgrundlage, um denjenigen, um dessen Daten es geht, zu schützen. Erfasst wird auch, wenn der Dritte Zugriff auf die Daten hat; selbst wenn er sie nicht im eigentlichen Sinn verarbeiten soll. Die Rechtsgrundlage ist also erforderlich zum Schutz derjenigen, deren Daten der Cloud Service Customer mit dem Cloud Service des Cloud Service Providers verarbeiten wird.

Wenn die personenbezogenen Daten dabei in ein Land außerhalb der EU oder des EWR übertragen werden sollen, dann ist nach deutschem und europäischem Datenschutzrecht für die grenzüberschreitende Übertragung ebenfalls eine – also eine weitere – Rechtsgrundlage erforderlich.

Zusammengefasst lässt sich festhalten: Für die Verarbeitung personenbezogener Daten in einem Cloud Services außerhalb der EU bzw. des EWR müssen zwei Rechtsgrundlagen geprüft werden:
1. Zulässigkeit der Übertragung der personenbezogenen Daten an den Cloud Service Provider.
2. Die grenzüberschreitende Übertragung dieser Daten.

Das Safe Harbor-Abkommen und das Nachfolgeabkommen betreffen allein die 2. Frage: Dürfen die Daten grenzüberschreitend übertragen werden. Voraussetzung hierfür ist, dass beim Empfänger der Daten ein angemessenes Datenschutzniveau besteht.

Was das Safe Harbor-Abkommen und das Nachfolgeabkommen bewirk(t)en

Aus Sicht der EU besteht ein solches angemessenes Datenschutzniveau in den USA nicht generell. Das Safe Harbor-Abkommen war und das Privacy Shield soll ein Instrument sein, um jedenfalls beim konkreten Cloud Provider in den USA ein angemessenes Datenschutzniveau zu schaffen.

US-Unternehmen, die sich dem Safe-Harbor-Abkommen unterwarfen, mussten bestimmte Selbstverpflichtungen eingehen, um dadurch für die betroffenen Daten ein angemessenes Datenschutzniveau zu erzielen.

Warum wurde das Safe Harbor-Abkommen gekippt?

Das Safe Harbor-Abkommen wurde seit Längerem von den Datenschutzaufsichtsbehörden als unzureichendes Mittel zur Schaffung eines angemessenen Datenschutzniveaus kritisiert.

Letztlich hat der EuGH mit seinem Urteil vom 06.10.2015 (Rs. C 362/14) das Safe Harbor-Abkommen außer Kraft gesetzt. Seitdem ist das Safe Harbor-Abkommen keine Rechtsgrundlage mehr für den Datentransfer in die USA.

Der EuGH hat dies damit begründet, dass die EU-Kommission, welche das Safe-Harbor-Abkommen seinerzeit in Kraft gesetzt hatte, bei ihrer Prüfung und Entscheidung über die Schaffung eines angemessenen Datenschutzniveaus bestimmte Aspekte nicht geprüft hatte. Da diese Aspekte nicht geprüft worden waren, aber hätten geprüft werden müssen, wurde das Safe Harbor-Abkommen für unwirksam erklärt.

Der EuGH monierte – vereinfacht gesagt –, dass die EU-Kommission nicht hinreichend den Rechtsrahmen für den Zugriff staatlicher Instanzen auf die Daten, die Unterrichtung der Betroffenen hierüber und die Rechtsbehelfe der Betroffenen geprüft hatte.

Der EuGH machte damit gleichzeitig entsprechende Garantien zum Schutz der Betroffenen zur Voraussetzung für ein Nachfolgeabkommen und den Datentransfer in die USA.

Alternativen zu Safe Harbor als Rechtsgrundlage

Das Safe Harbor-Abkommen war und ist nicht die einzige Rechtsgrundlage für eine Übertragung von Daten in die USA. Es kommen weitere Rechtsinstrumente in Betracht: sog. EU-Standard-verträge, sog. Binding Corporate Rules und die Einwilligung der Betroffenen.

Das bedeutet, dass die Übertragung personenbezogener Daten in die USA mit dem Kippen der Safe Harbor-Principles nicht generell unzulässig geworden ist.

Binding Corporate Rules (BCR) kommen grundsätzlich nur im Unternehmensverbund zum Einsatz. In Gestalt der sogenannten Processor Binding Corporate Rules (PBCR) sind sie eine Möglichkeit für den Cloud Service Provider, seine Unternehmensstruktur über Binding Corporate Rules zu verbinden. Der grenzüberschreitende Datentransfer im Unternehmensverbund des Cloud Service Providers wäre damit legitimiert. Solche PBCR müssen allerdings als Wirksamkeitsvoraussetzung durch die Datenschutzaufsichtsbehörden genehmigt und dann die der Genehmigung zugrunde liegenden Mechanismen in den beteiligten Unternehmen implementiert werden. In der Praxis sind dafür erhebliche Zeiträume einzuplanen. Sofern diese nicht ohnehin eingeführt sind, kommen sie nicht als „kurzfristige Reaktion“ in Betracht.

Die Einwilligung als Alternative setzt voraus, dass jeder, dessen Daten in der Cloud verarbeitet werden sollen, transparent über den Datentransfer in oder den Zugriff aus den USA informiert wird und dann auch noch zustimmt. Hinzukommt, dass jeder Betroffene grundsätzlich seine Einwilligung jederzeit widerrufen kann. Vor diesem Hintergrund erscheint die Einwilligung kaum als „kurzfristige Reaktion“ und nachhaltige Strategie.

Es kommt ein „Ausweichen“ auf sog. EU-Standardverträge in Betracht. Hierbei handelt es sich um eine vertragliche Vereinbarung zwischen dem Cloud Service Customer und dem Unternehmen außerhalb der EU bzw. des EWR. Der Inhalt des Vertrages ist im Wesentlichen durch die EU-Kommission vorgegeben. Wenn der Vertrag insoweit unverändert abgeschlossen wird, dann wird dadurch beim Empfänger ein angemessenes Datenschutzniveau geschaffen.
Nach der bisherigen Praxis der deutschen Datenschutzaufsichtsbehörden musste bei unveränderter Übernahme der Textvorgabe auch keine Genehmigung der Aufsichtsbehörden für den Datentransfer in die USA eingeholt werden.

Allerdings wurde auch die Verwendung dieser alternativen Rechtsinstrumente im Lichte der Begründung des EuGH zur Unwirksamkeit der Safe Harbor-Principles nachhaltig durch die Datenschutzaufsichtsbehörden in Frage gestellt.

Status Quo

Die EU-Kommission teilte am 02.02.2016 mit, dass mit den USA eine Einigung auf ein Nachfolgeabkommen mit dem Namen Privacy Shield erfolgt ist. Diese Einigung muss nun in der Folgezeit umgesetzt werden. Bis dahin entfaltet das Privacy Shield keine unmittelbare Rechtswirkung.

Eine mittelbare Wirkung entfaltete die Ankündigung gleichwohl: Die Datenschutzaufsichtsbehörden haben einstweilen ihre Bedenken auch gegen die alternativen Rechtsinstrumente zurückgestellt und betrachten diese als weiterhin wirksam. Es soll zunächst eine detaillierte Prüfung des Privacy Shield und damit verbunden insgesamt eine Bewertung des Datentransfers in die USA erfolgen.

Was bedeutet das für Praxis?

Für den Transfer personenbezogener Daten in die USA im Rahmen von Cloud Services muss und kann (einstweilen) auf die alternativen Rechtsinstrumente zurückgegriffen werden: sog. EU-Standardverträge, sog. Binding Corporate Rules und die Einwilligung der Betroffenen. Hierbei treten die sog. EU-Standardverträge im Rahmen der Nutzung von Cloud Services in den Vordergrund.

Bundesministerium
für Wirtschaft
und Energie

Trusted Cloud

Impressum

Redaktion

Kompetenznetzwerk Trusted Cloud e. V.

c/o INNOVA Beratungsgesellschaft mbH

Lückhoffstraße 33

14129 Berlin