SAFE HARBOR: Schonfrist vorbei

Was Cloud-Anbieter und -Kunden jetzt beachten sollten

Dr. Jens Eckhardt, Rechtsanwalt und Fachanwalt für Informationstechnologierecht sowie Datenschutzauditor (TÜV), Vorstand EuroCloud Deutschland_eco e. V.

Seit knapp fünf Monaten heißt es: Safe Harbor adé. Leider haben immer noch viele von der Entscheidung des Europäischen Gerichtshofs betroffene Unternehmen ihre Regelungen für den internationalen Datentransfer nicht an die neue Rechtslage angepasst. Die Schonfrist der Datenschutzaufsichtsbehörden ist aber nun endgültig vorbei: Erste Bußgeldverfahren wurden gegen mehrere Unternehmen in Hamburg eingeleitet – es drohen Bußgelder bis 300.000 Euro. Bis zur tragfähigen Umsetzung des Nachfolgeabkommens EU-US Privacy Shield sind EU-Standardverträge derzeit die beste datenschutzkonforme Alternative – allerdings gibt es auch hier Bedenken. EuroCloud Deutschland hat die wichtigsten Informationen für Cloud-Anbieter und -Kunden zusammengefasst.

Für viel Aufsehen sorgte die Entscheidung des Gerichtshofs der Europäischen Union (EuGH), der mit Urteil vom 06.10.2015 Safe-Harbor-Vereinbarungen für unwirksam erklärte. Seit diesem Tag, ohne Übergangsfrist, ist es europäischen Unternehmen nicht mehr gestattet, auf Safe-Harbor-Basis personenbezogene Daten in die USA zu transferieren, sie dort zu speichern oder zu verarbeiten. Die Richter begründeten das Urteil unter anderem mit mangelndem Rechtsschutz gegen Grundrechtseingriffe von EU-Bürgern und den umfangreichen Befugnissen von US-Behörden, auf die Daten zuzugreifen. Unternehmen, die Daten auf der Grundlage des Safe-Harbor-Abkommens übermittelt hatten, mussten nach der EuGH-Entscheidung schnellstens reagieren. Denn bei einer unzulässigen Datenübertragung in Drittstaaten drohten Bußgelder und sogar die Untersagung der Datenverarbeitung. Außerdem konnte Nichtstun zu Haftungsfallen führen, wenn etwa Dienstleister ihre Kunden nicht rechtzeitig angemessen informierten.

Die verabschiedete EU-Datenschutzgrundverordnung (EU-DSGVO) hat an der Aktualität des Themas nichts geändert, denn sie ist noch nicht in Kraft getreten. Selbst wenn, wären ihre Regelungen erst ab 2018 unmittelbar anwendbar. Die aktuellen Herausforderungen der EuGH-Entscheidung sind damit nicht gelöst und auch nicht vertagt.

Seit 2. Februar 2016 haben sich die EU-Kommission und die USA als Nachfolgeregelung zum Safe-Harbor-Abkommen auf das so genannte **EU-US Privacy Shield** verständigt. **Es ist jedoch noch nicht in Kraft und entfaltet damit keine rechtliche Wirkung!** Alle Beteiligten sollten sich bemühen, dass mit dem Nachfolgeabkommen Privacy Shield schnell eine tragfähige Rechtsgrundlage geschaffen wird, die den in der Safe-Harbor-Entscheidung genannten Anforderungen des EuGH entspricht. **Doch Abwarten ist keine Option! Dies machen insbesondere die in Hamburg eingeleiteten Bußgeldverfahren nachdrücklich deutlich.**

Datenübermittler, aber auch Dienstleistungskunden müssen handeln

Betroffen sind zum einen Unternehmen, die personenbezogene Daten auf Basis von Safe Harbor aus der EU in die USA übermitteln. Das können zum Beispiel europäische Tochtergesellschaften von US-Unternehmen sein, deren Personalmanagement im Mutterkonzern erfolgt. Oder deutsche Cloud Service Provider, die für ihr Angebot ein Rechenzentrum in den USA nutzen, ihre Softwarepflege/-entwicklung oder den Support dort erledigen lassen.

Zum anderen sind Unternehmen betroffen, die Dienstleistungen nutzen, bei denen der Anbieter oder ein Subunternehmer in den USA sitzt. Dabei ist es egal, ob Daten aktiv in die USA übertragen werden oder aus den USA darauf zugegriffen werden kann.

EU-Standardverträge beste datenschutzkonforme Alternative

Um zu reagieren, bleiben den Unternehmen drei Möglichkeiten:

1. Sie holen sich für den Datentransfer in die USA die **Einwilligung** aller Betroffenen. Das ist aber langwierig und unwahrscheinlich, dass jeder zustimmt. Entscheidend ist allerdings auch, dass die Einwilligung jederzeit widerrufen werden kann. Damit besteht keine Planungssicherheit.

2. Sie stützen den Datentransfer auf „verbindliche Unternehmensregelungen“ (**Binding Corporate Rules – BCR**) oder ihr Dienstleister stützt die Weiterleitung in seinem Unternehmensverbund auf so genannte **Processor Binding Corporate Rules (PBCR)**. BCR und PBCR kommen grundsätzlich nur beim transnationalen Austausch von Daten innerhalb eines Unternehmensverbunds zum Einsatz und die Entwicklung eines entsprechenden Maßnahmenkatalogs, die Genehmigung auf europäischer und jeweils nationaler Ebene sowie die anschließende Umsetzung in allen beteiligten Unternehmen können sich über Jahre hinziehen. Hinzu kommt, dass die deutschen Datenschutzaufsichtsbehörden einstweilen die benötigten Genehmigungen nicht erteilen.

3. Die dritte Möglichkeit sind die so genannten **EU-Standardverträge** zur Datenübermittlung. Der Abschluss dieser Vereinbarung zwischen dem datenübermittelnden und dem -empfangenden Unternehmen schafft ein datenschutzrechtlich angemessenes Schutzniveau bei dem Datenempfänger. Die Vertragsklauseln sind relativ schnell und einfach implementierbar. Die Inhalte sind, wie der Name schon sagt, standardisiert: Die Unternehmen müssen keine aufwändige Prüfung vornehmen, sondern sind darauf beschränkt, die Freifelder mit sachlichen Beschreibungen der Zusammenarbeit auszufüllen. Obwohl die EU-Standardverträge mittlerweile eine Unterauftragnehmer-Klausel enthalten, ist zu beachten: Sitzt der Auftragnehmer in der EU, der Unterauftragnehmer aber in den USA, muss der EU-Standardvertrag unmittelbar zwischen Auftraggeber und Unterauftragnehmer geschlossen werden.

Wurden die vorgegebenen Standardtexte unverändert übernommen, mussten die EU-Standardverträge nach deutscher Praxis bislang nicht den Datenschutzaufsichtsbehörden zur Genehmigung vorgelegt werden. Zu dieser Aufsichtspraxis sind die Datenschutzaufsichtsbehörden nach deren Verständnis nicht gesetzlich verpflichtet. Sie halten nach jüngsten Informationen aber – jedenfalls einstweilen – an dieser Praxis fest.

Nach ersten Stellungnahmen halten die Datenschutzbehörden aber jeglichen Transfer von personenbezogenen Daten in die USA, auch auf Basis von EU-Standardverträgen oder (P)BCR, für rechtlich problematisch. Daher wollen sie diese in Einzelfällen prüfen und haben auch die Möglichkeit, die Übermittlung (im Einzelfall) auszusetzen.

Was sollten Unternehmen tun, die Cloud-Lösungen nutzen?

Prüfen Sie,

- in welchen Konstellationen und durch welche Dienstleister ein Datentransfer in die USA erfolgt.
- in welchen Konstellationen und durch welche Dienstleister ein Zugriff auf die personenbezogenen Daten aus den USA erfolgen kann (auch wenn sie in der Praxis nicht darauf zugreifen)
- welche Ihrer Vertragspartner oder Sub-Unternehmer sich auf das Safe-Harbor-Abkommen berufen haben,
- welche dieser Datenübertragungen für Ihr Geschäft am allerwichtigsten sind und stellen Sie alle – beginnend bei denen mit höchster Priorität – kurzfristig auf EU-Standardverträge um.

Beruft sich ein Dienstleister darauf, Safe-Harbor-zertifiziert zu sein, hat mit Ihnen aber einen EU-Standardvertrag geschlossen, dann stellt das kein Problem dar. Hauptsache der Datentransfer stützt sich nicht ausschließlich auf Safe Harbor.

Sie sind selbst ein Dienstleister, der bislang Safe Harbor genutzt hat?

Dann gestalten Sie umgehend EU-Standardverträge und beachten Sie dabei die ergänzenden Regelungen der Auftragsdatenverarbeitung, der Leistungsbeschreibung und technisch-organisatorischen Maßnahmen. Informieren Sie Ihre Kunden/Auftraggeber darüber, dass Sie Safe-Harbor-Vereinbarungen genutzt haben und nun auf EU-Standardverträge umstellen.

Für alle gilt:

Behalten Sie die Entwicklungen in den nächsten Monaten aufmerksam im Blick, da sich hier noch geschäftskritische Änderungen ergeben könnten. Vergessen Sie nicht, all Ihre Materialien wie Datenschutzerklärungen und Flyer an die neuen Vorgaben anzupassen.

Hintergrund: Ehemalige Sonderregelung Safe Harbor

Für die USA existierte bis zum 06.10.2015 eine Sonderregelung, das so genannte „Safe-Harbor"-Abkommen, das im Jahr 2000 zwischen den USA und der EU geschlossen wurde, um den Online-Datenverkehr zu vereinfachen und zu beschleunigen. Nach diesem Abkommen war eine Datenübermittlung an ein dort ansässiges Unternehmen oder Unternehmensteile zulässig, wenn sie sich verpflichten, ein dem europäischen beziehungsweise deutschen Datenschutz entsprechendes Niveau einzuhalten. Es handelte sich dabei um eine Art Selbstzertifzierung des Unternehmens mit Unterwerfung unter Sanktionen durch US-Aufsichtsinstanzen. Dieses Safe-Harbor-Abkommen wurde in Deutschland jedoch von den Datenschutzaufsichtsbehörden erheblich kritisiert, weil bezweifelt wurde, dass diese Verfahren tatsächlich das angestrebte Schutzniveau schaffen. Mit Urteil vom 06.10.2015 erklärte der Europäische Gerichtshof (EuGH) die Entscheidung 2000/520/EG der EU-Kommission, auf welcher dieses Safe Harbor-Prinzip beruhte, für unwirksam (Az. C-362/14). Das Safe-Harbor-Abkommen ist keine Rechtsgrundlage mehr für einen Datentransfer in die USA oder einen Zugriff auf Daten in der EU aus den USA.

Weitere Informationen

Hilfreiche Informationen bietet das Trusted Cloud Datenschutzprofil (TCDP), das als Prüfstandard für die Datenschutz-Zertifizierung von Cloud-Diensten zum Einsatz kommt und datenschutzrechtliche Anforderungen auf der Seite des Cloud-Anbieters beschreibt. Das TCDP wurde unter Beteiligung von EuroCloud vom Kompetenzzentrum Trusted Cloud im Auftrag des Bundesministeriums für Wirtschaft und Energie entwickelt. Es steht hier zum kostenfreien Download bereit: http://bit.ly/1QRD5El.

Grundlegende Informationen zum Datenschutz bei Cloud Services gibt es außerdem im „Leitfaden – Datenschutz und Cloud Computing", der unter Leitung von Dr. Jens Eckhardt erstellt wurde: bit.ly/1RDtPAz.