

Spies, Schröder: Cloud Computing und EU/US Safe Harbor Principles –
US-Handelsministerium bezieht Stellung

ZD-Aktuell
2013, 03566

Cloud Computing und EU/US Safe Harbor Principles – US-Handelsministerium bezieht Stellung

RA Dr. Axel Spies ist Rechtsanwalt in der Kanzlei Bingham McCutchen, Washington DC und Mitherausgeber der ZD.

RA Dr. Christian Schröder ist Rechtsanwalt und Leiter des Fachbereichs IP/IT der BDO Legal Rechtsanwaltsgesellschaft mbH in Düsseldorf und Mitglied des Wissenschaftsbeirats der ZD.

Die International Trade Administration (ITA) des US-Handelsministeriums (US Department of Commerce) hat sich nun doch bemüht, gegenüber der massiven Kritik europäischer Datenschützer in einem am 12. 4. 2013 veröffentlichten Memorandum "Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing" Stellung zu beziehen.

Die europäischen Datenschutzaufsichtsbehörden, zuletzt insbesondere die Art. 29-Datenschutzgruppe in ihrer Stellungnahme zum Cloud Computing (WP 197 v. 1.7.2012, Ziff. 3.5.1, S. 17), haben u. a. Bedenken geäußert, ob das Safe Harbor-Programm auch eine ausreichende Grundlage für Datenübermittlungen in die USA beim Cloud Computing darstellt. Deutsche Aufsichtsbehörden hatten zudem bereits in einer Stellungnahme des *Düsseldorfer Kreises* v. 27./28.4.2000 die Auffassung vertreten, dass die Einhaltung des Safe Harbor-Abkommens auf US-Seite nur unzureichend kontrolliert wird und daher den europäischen Exporteuren von Daten an Safe Harbor-zertifizierte Unternehmen Erkundigungs- und Überwachungspflichten auferlegt (Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich v. 28./29.4.2010 in Hannover – überarbeitete Fassung v. 23.8.2010; vgl. zum Streitstand *Schröder/Haag*, ZD 2012, 362 ff. und zuletzt *Schuppert/von Reden*, ZD 2013, 210 ff. m. w. N.).

1. Hintergrund des Streits

Aus EU-Sicht ist die USA für Datenübermittlungen aus der EU/dem EWR ein Land mit „inadäquatem Datenschutz“ i. S. d. Art. 25 DSRL 95/46/EG (unsicheres Drittland). Das bedeutet, dass die Übermittlung personenbezogener Daten in die USA grundsätzlich nur dann rechtmäßig ist, wenn die in dieses Land übermittelten Daten durch von den an der Übermittlung beteiligten Parteien einen dem europäischen Datenschutzniveau vergleichbaren angemessenen Schutz erfahren. Zur Gewährleistung dieses angemessenen Schutzes verweist die *EU-Kommission* auf die folgenden Möglichkeiten:

- ☐ Abschluss eines Vertrags auf Basis der EU-Standardvertragsklauseln,

- ☐ Abschluss von verbindlichen unternehmensinternen Vorschriften (Binding Corporate Rules) oder
- ☐ Beitritt des Datenimporteurs zum „US Safe Harbor-Abkommen“.

Nach dem im Jahr 2000 zwischen der *EU-Kommission* und dem *US-Handelsministerium* verhandelten Safe Harbor-Abkommen haben US-Unternehmen die Möglichkeit, sich auf der „Safe Harbor-Liste“, die das *US-Handelsministerium* seitdem betreibt und verwaltet, freiwillig für Datentransfers aus der EU (und separat für Daten aus der Schweiz) registrieren zu lassen. Diese von vielen US-Unternehmen gern genutzte Compliance-Möglichkeit besteht jedoch nicht für Unternehmen der TK-, Versicherungs- und Finanzbranche, da diese nicht unter die Jurisdiktion der *Federal Trade Commission (FTC)* fallen.

Jedes grundsätzlich berechnigte US-Unternehmen wird zum Safe Harbor-Abkommen zugelassen, wenn sich das Unternehmen verpflichtet, eine Reihe von durch das Abkommen festgelegten Datenschutzprinzipien intern umzusetzen – die sog. Safe Harbor-Prinzipien – und dies auch gegenüber der *FTC* öffentlich bestätigt (self-certification). Das *US-Handelsministerium* prüft bei der Aufnahme auf die Safe Harbor-Liste jedoch nicht, ob das den Beitritt beantragende Unternehmen die Prinzipien einhält. Die Einhaltung der Prinzipien muss das Unternehmen vielmehr selbst bestätigen bzw. selbst zertifizieren und diese Erklärung auch regelmäßig wiederholen, was dann in die Safe Harbor-Liste eingetragen wird. Die europäischen und deutschen Aufsichtsbehörden fordern, dass sich die Daten übermittelnde Stelle selbst von der erstmaligen und auch nachfolgenden Bestätigung über die Einhaltung der Safe Harbor-Prinzipien überzeugt (s. WP 197 der *Art. 29-Datenschutzgruppe* v. 1.7.2012, Ziff. 3.5.1, S. 17 und Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29.4.2010 in Hannover (überarbeitete Fassung v. 23.8.2010)).

Darüber hinaus vertritt die *Art. 29-Datenschutzgruppe* die Auffassung, dass bei Cloud Computing nach jeweils anwendbarem nationalen Datenschutzrecht der Beitritt zum Safe Harbor-Abkommen nicht ausreichend ist und verweist darauf, dass das Safe Harbor-Abkommen z. B. regional und auch sachlich begrenzt ist und von daher nicht sämtliche Cloud-Verarbeitungen umfassen könne. Die Europäer fordern daher von den Datenexporteuren u.a.

- ☐ den Abschluss von Auftragsdatenverarbeitungsverträgen,
- ☐ europäische Unternehmen sollten vom Cloud-Diensteanbieter Nachweise zur Einhaltung der Safe Harbor-Prinzipien verlangen, und
- ☐ die Verträge müssten Regelungen zu Unterbeauftragungen enthalten, die die Orte der Datenverarbeitung bestimmen und eine Nachverfolgbarkeit der Datenverarbeitung

gewährleisten.

Die *Art. 29-Datenschutzgruppe* äußert sogar grundsätzliche Bedenken zur Nutzung des Safe Harbor-Abkommens bei Cloud-Diensten, da das Safe Harbor-Abkommen allein möglicherweise keine hinreichende Sicherheit für die in der Cloud verarbeiteten Daten garantiere. Die *Art. 29-Datenschutzgruppe* fordert daher über das Safe Harbor-Abkommen hinausgehende Regelungen zum Schutz der in der Cloud in den USA verarbeiteten personenbezogenen Daten und empfiehlt als Alternative die Nutzung der EU-Standardvertragsklauseln. Die USA stehen hingegen auf dem Standpunkt, dass diese zusätzlichen Verpflichtungen nicht dem Safe Harbor-Abkommen entsprechen und daher nicht erforderlich sind.

2. Kernaussagen

Die *ITA des US-Handelsministeriums* trifft in dem Memo folgende Kernaussagen (Kommentare der Autoren in kursiv):

- ☐ Safe Harbor und die Entscheidung der *EU-Kommission* zur „Angemessenheit“ bei Safe Harbor-zertifizierten Unternehmen finden für sämtliche Vereinbarungen Anwendung, welche die Übermittlung personenbezogener Daten aus der EU zu Unternehmen betreffen, die in den Vereinigten Staaten niedergelassen sind. Dies gilt auch für Cloud Computing-Dienstleistungsverträge. – *Es gibt also keine Sonderregeln für das Cloud Computing.*
- ☐ Der von der *Art. 29-Datenschutzgruppe* neben dem Safe Harbor-Beitritt geforderte zusätzliche Abschluss von Auftragsdatenverarbeitungsverträgen ist generell zutreffend. – *Den Parteien wird bei der Abfassung jedoch ein weiter Spielraum zugestanden. Mit anderen Worten es müssen nicht die Standardklauseln benutzt werden.*
- ☐ Wenn es um die bloße Verarbeitung von Daten geht, stellen die EU-Standardvertragsklauseln für Auftragsdatenverarbeitung eine Alternative zur Safe Harbor-Zertifizierung dar – nicht eine zusätzliche Anforderung (d.h. jede der beiden Alternativen steht einem Diensteanbieter zur Verfügung, um ein „adäquates“ Maß an Datenschutz zu gewährleisten). – *Der Cloud-Anbieter in den USA kann folglich zwischen beiden Alternativen wählen. Die ITA weist hiermit die Empfehlung zur Nutzung der Standardvertragsklauseln zusätzlich zur Safe Harbor-Registrierung zurück.*
- ☐ Die *EU-Kommission* hat keine über das bisherige Safe Harbor-Abkommen hinausgehenden Anforderungen gestellt. Die von der *Art. 29-Datenschutzgruppe* geforderten zusätzlichen Nachweispflichten über die regelmäßig wiederholte Selbst-Zertifizierung bzw. das Einhalten der Safe Harbor-Prinzipien sind daher nicht maßgeblich. Die geforderten Nachweise können auch durch Einblick in die vom *US-*

Handelsministerium veröffentlichte Safe Harbor-Listen erhalten werden. – Nach Ansicht der ITA kann die EU (einschließlich der Art. 29 Datenschutzgruppe – WP 196) dem Datenexporteur nicht die zusätzliche Pflicht zur Prüfung auferlegen, ob die Safe Harbor-Registrierung gültig erfolgt ist oder ob sie nicht wirksam ist. Die Datenexporteure müssten sich auf die Eintragung verlassen können.

□ Das Safe Harbor-Abkommen sieht ausdrücklich vor, dass eine Unterbeauftragung auch in andere Drittländer möglich ist, sofern sich der Unterauftragnehmer zu einem Schutz der Daten verpflichtet, dessen Niveau die Safe Harbor-Prinzipien nicht unterschreitet. – *Hiermit weist die ITA die von der Art. 29-Datenschutzgruppe behauptete geografisch begrenzte Anwendbarkeit des Safe Harbor-Abkommens bei Cloud-Dienstleistungen zurück.*

□ Die Safe Harbor-Anforderung, nach der angemessene Vorkehrungen zum Datenschutz getroffen werden müssen, erfüllt die Vorgabe der DSRL 95/46/EG nach angemessenem Datenschutz durch technische und organisatorische Maßnahmen. Allerdings müssen die Parteien einer Datenübermittlung diese Maßnahmen auch für die vereinbarten Dienstleistungen vertraglich konkretisieren. – *Der Cloud-Vertrag muss technische und sicherheitsrelevante Maßnahmen und Organisationsvorkehrungen für die sichere Verarbeitung der übermittelten Daten enthalten. Genaue Vorgaben gibt es hierfür aus US-Sicht nicht. Allerdings stellt sich die ITA damit auch nicht den weitergehenden Cloud-spezifischen Anforderungen der Art. 29-Datenschutzgruppe entgegen.*

□ Keine europäische Aufsichtsbehörde darf die Übermittlung von Daten an US-Cloud-Diansteanbieter, die dem Safe Harbor-Abkommen beigetreten sind, wegen behaupteter mangelnder Angemessenheit des Datenschutzes untersagen.

□ Die geplante DS-GVO der EU wird aller Voraussicht nach nicht zur Beendigung des Safe Harbor-Abkommens führen.

□ US-Unternehmen, die auf den US Patriot Act angesprochen werden, sollen auf die Rede des US-Botschafters bei der EU, *William Kennard*, v. 4.12.2012 verweisen. Danach bestehen in der transatlantischen Diskussion über den Schutz der Privatsphäre erhebliche Missverständnisse über das US-Rechtssystem.

Auf die Reaktion der europäischen Datenschützer auf das Memorandum darf man gespannt sein. Es ist durchaus möglich, dass das Abkommen über die Safe Harbor-Prinzipien und dessen Ausweitung zum Thema der gerade anlaufenden Gespräche über eine „Investment Partnerschaft“ (Trade and Investment Partnership Agreement – TITIP) zwischen den Amerikanern und Europäern wird.