MITTELSTAND *aktuell*
Alles was Recht ist

BVMW
Bundesverband
mittelständische Wirtschaft

„SAFE HARBOR" FÜR DATENTRANSFERS IN DIE USA UNGÜLTIG: WELCHE OPTIONEN BLEIBEN?

Die Safe-Harbor-Entscheidung der EU-Kommission wurde vom Europäischen Gerichtshof (EuGH) im Verfahren C-362/14 am 06.10.2015 (Maximilian Schrems gegen die irische Datenschutzbehörde) für ungültig erklärt.

Eine enorme Tragweite hat die Entscheidung für Unternehmen, die sich beim Transfer personenbezogener Daten in die USA, etwa an Tochtergesellschaften oder Auftragnehmer, auf Safe Harbor als Legitimationsgrundlage verlassen haben. Insbesondere die Schlüsselakteure der digitalen Welt, Unternehmen aus dem Technologie- und Telekommunikationssektor sowie Cloud-Dienstleister, sind von dem Urteil betroffen, da ihr Geschäftsmodell auf dem freien Fluss von Daten in die USA beruht. Nun sind Unternehmen dazu angehalten, zusätzliche Compliance-Maßnahmen zu initiieren, um ein adäquates Datenschutzniveau beim Datentransfer von der EU in die USA zu gewährleisten. Ansonsten drohen regulatorische Maßnahmen der Datenschutzbehörden.

In diesem Beitrag beleuchten wir die Auswirkungen des Urteils für die deutsche mittelständische Wirtschaft und erläutern mögliche Schritte, die betroffene Unternehmen nun ergreifen sollten, um die Datentransfers wieder auf eine rechtssichere Basis zu stellen.

1. Das Verfahren

Im Jahre 2013 wurden im Zuge der Snowden-Affäre die Überwachungsprogramme der amerikanischen Geheimdienste publik, die überwiegend als unvereinbar mit europäischem Datenschutzrecht angesehen wurden. Vor dem Hintergrund dieser Veröffentlichungen setzte sich der Datenschutzaktivist Maximilian Schrems bei dem irischen Data Protection Commissioner (DPC) gegen den Transfer seiner personenbezogenen Daten durch Facebook auf Server in die USA zur Wehr.

Schrems begehrte mit seiner Beschwerde beim DPC die Untersuchung der Vorgänge und vertrat die Auffassung, dass die US-Behörden über einen ungehinderten Zugang zu den personenbezogenen Daten der Nutzer verfügten und Facebook insofern kein dem europäischen Recht entsprechendes Datenschutzniveau gewährleisten könne. Der DPC verfolgte die Beschwerde nicht und berief sich insbesondere darauf, dass sich Facebook bei den Datenflüssen in die USA auf die Safe-Harbor-Prinzipien stützte und die Europäische Kommission mit der Entscheidung 2000/520 verbindlich über die Angemessenheit des Datenschutzniveaus entschieden habe.

Schrems suchte gegen die Entscheidung des DPC vor dem irischen High Court Rechtsschutz, der dem EuGH die Frage vorlegte, ob die nationalen Datenschutzbehörden an die Adäquanzentscheidung der Europäischen Kommission gebunden sind oder unter Umständen über einen eigenen Beurteilungsspielraum verfügen.

Davon ausgehend entschied der EuGH, dass:

- die Safe-Harbor-Entscheidung der Kommission ungültig ist,
- die nationalen Datenschutzbehörden in absoluter Unabhängigkeit dazu imstande sein müssen, einen internationalen Datentransfer zu untersuchen und ggf. zu untersagen, wenn sie zu der Ansicht gelangen, dass das den EU-Bürgern zukommende Datenschutzniveau im Drittland unangemessen ist – eine Bindungswirkung kommt der Entscheidung der EU-Kommission damit nicht zu.

Der EuGH folgt in seinem Urteil somit überwiegend der Rechtsansicht des Generalanwalts Yves Bot, der in seiner Stellungnahme vom 23.09.2015 die Entscheidung so vorgezeichnet hatte.

2. Die Antwort der Kommission

Die Kommission bestätigte bereits, dass die Verhandlungen mit den USA zu einem „safer" Safe Harbor fortgesetzt werden. Darüber hinaus hat die Kommission eine enge Zusammenarbeit mit den Datenschutzbehörden auf nationaler und EU-Ebene angekündigt, um eine kohärente Umsetzung der Entscheidung des EuGH über die Ländergrenzen der Mitgliedsstaaten hinweg zu gewährleisten.

3. Die Konsequenzen

Nachdem nun bereits mehrere Wochen seit dem Urteil vergangen sind, ist aber schon festzustellen, dass sich die Behörden sehr schwer tun, eine einheitliche Linie zu finden. Eine unter ihnen abgestimmte Position ist noch nicht verlautbart worden. Im Gegenteil preschen nun teilweise schon einzelne Behörden mit einer sehr restriktiven Betrachtung der verbleibenden Möglichkeiten vor. Folgende unmittelbaren Konsequenzen ergeben sich für die mittelständische Wirtschaft:

a) US-Technologieunternehmen müssen ihre Schutzmaßnahmen verstärken

Unternehmen, die in den USA ansässige IT-Dienstleister einsetzen und sich bei internationalen Datentransfers auf deren Safe-Harbor-Mitgliedschaft gestützt haben, stehen nun vor einer unsicheren Rechtslage, welche die Ergreifung alternativer Lösungsansätze erfordert. Bis zum Abschluss eines revidierten Safe-Harbor-Abkommens werden die Datenschutzbehörden als Voraussetzung für Datenflüsse in die USA aller Voraussicht nach einen belastbaren Nachweis über die Gewährleistung des Datenschutzes sowie weitere Sicherungsmaßnahmen – etwa Binding Corporate Rules (bei unternehmensinternen Datentransfers) oder EU-Standardverträge – fordern. Es hat den Anschein, als ob die Aufsichtsbehörden hier teilweise eine sehr strikte Linie fahren, so jedenfalls die schleswig-holsteinische Aufsichtsbehörde ULD laut einem Positionspapier vom 14.10.2015.

Eine weitere Unsicherheit liegt darin, den Zeitpunkt zu ermitteln, zu dem Unternehmen in Zusammenarbeit alternative Maßnahmen ergriffen haben müssen. Die Safe-Harbor-Entscheidung ist mit dem Urteil des EuGH jedenfalls mit sofortiger Wirkung außer Kraft gesetzt worden. Unternehmen sollten sich vor diesem Hintergrund vergegenwärtigen, dass die Genehmigungsverfahren für „Binding Corporate Rules" Monate dauern können und auch Standardverträge – soweit sie denn überhaupt möglich bleiben – evtl. den Aufsichtsbehörden vorgelegt werden müssen.

b) Umfassendere Prüfungskompetenz der Datenschutzbehörden

Bei Zweifeln über die Angemessenheit des Schutzniveaus können Datenschutzbehörden internationale Datentransfers nun unabhängig überprüfen und untersagen. Auf der Grundlage des wegweisenden Urteils könnten vermehrt Anfragen von Betroffenen bei den Unternehmen im Hinblick auf den datenschutzkonformen Transfer ihrer Daten eingehen. Betroffene könnten sich zudem mit Beschwerden an die Datenschutzbehörden richten, um nachdrücklich den Vollzug der europäischen Datenschutzregeln gegen rechtswidrig handelnde Unternehmen zu fordern.

Die Datenschutzbehörden sind einer erheblichen Ausweitung des Verwaltungsaufwands ausgesetzt. Ihre gegenwärtige Mittelausstattung wird eine angemessene Bearbeitung der zu erwartenden Erhöhung von Beschwerden und Anfragen von Betroffenen kaum ermöglichen. Insofern ist mit der Verkündung neuer Richtlinien für die Gewährleistung datenschutzkonformer Datenflüsse zu rechnen. Das ULD in Schleswig-Holstein hat dies in einem Positionspapier vom 14.10.2015 für Unternehmen in Schleswig-Holstein schon getan. Sofern Unternehmen ihre Datentransfers in die USA mit den Safe-Harbor-Prinzipien legitimiert haben, gilt es, die erwähnten Richtlinien der Aufsicht zur Kenntnis zu nehmen und möglichst zeitnah umzusetzen. Unternehmen werden vor allem ihre Dienstleister in den USA mit besonderer Sorgfalt auf die Gewährleistung eines angemessenen Datenschutzniveaus und auf potentielle Verletzungen überprüfen müssen, da ansonsten regulatorische Maßnahmen drohen.

c) Implikationen für andere Datentransferlösungen

Die Entscheidung des EuGH, dass die nationalen Datenschutzbehörden hinsichtlich der Feststellung eines angemessenen Datenschutzniveaus nicht an die Wertung der Kommission in der Safe-Harbor-Entscheidung gebunden sind, dürfte in entsprechender Weise auf die Adäquanzentscheidungen der Kommission zu anderen Jurisdiktionen, etwa Israel oder Neuseeland, aber auch auf andere Datentransfer-Lösungen (z.B. auf EU-Standardverträge) übertragbar sein. Auch diese Lösungen sind deshalb kein Allheilmittel mehr zur datenschutzrechtlichen Absicherung von Datentransfers. Es ist durchaus denkbar, dass die Datenschutzbehörden von ihren Prüfungsbefugnissen auch bei Datenflüssen in andere Drittstaaten Gebrauch machen werden.

Besonders entscheidend wird dabei die Frage sein, ob die Aufsichtsbehörden es nach wie vor zulassen werden, Datenübermittlungen in die USA (aber auch in andere „kritische" Jurisdiktionen wie z.B. China) auf Basis der so genannten EU-Standardvertragsklauseln zuzulassen. Formal sind diese zwar von der EuGH-Entscheidung nicht berührt. Erste Aufsichtsbehörden schlagen hier aber kritische Töne an. Unternehmen sollten deshalb zunächst eruieren, welchen Standpunkt die für sie zuständige Behörde einnimmt und ggf. welche Anforderungen sie an eine Verwendung der Standardvertragsklauseln stellt.

d) Verstärkter Druck auf die EU und die USA bei den Verhandlungen eines neuen Safe-Harbor-Abkommens

Das Urteil wird den Druck auf die EU und die USA erhöhen, die gegenwärtigen Verhandlungen hinsichtlich eines neuen Safe-Harbor-Abkommens zum Abschluss zu bringen oder andere Lösungen für die gerügten Mängel – insbesondere dem unverhältnismäßigen Zugriff der amerikanischen Behörden auf die personenbezogenen Daten von EU-Bürgern ohne etwaige Rechtsschutzmöglichkeiten – zu finden. Die Datenschutzbehörden haben allerdings selbst bei Abschluss eines revidierten Abkommens die Möglichkeit, Datenflüsse auf seiner Grundlage zu untersagen, wenn sie von der Angemessenheit des Datenschutzniveaus nicht überzeugt sind.

4. Konkrete Maßnahmen zur Sicherstellung der Compliance

Folgende Ad Hoc-Maßnahmen sollte nun jedes Unternehmen ergreifen:

- Überprüfung bestehender Datentransfers: Ermitteln Sie die effektiven Maßnahmen, die Ihr Kooperationspartner in den

USA zur Gewährleistung eines angemessenen Schutzes der übermittelten personenbezogenen Daten getroffen hat. Stellen Sie fest, ob diese Maßnahmen auf Safe Harbor aufbauen oder nicht.
- Neue Richtlinien der Datenschutzbehörden beachten: Die Datenschutzbehörden werden aller Voraussicht nach Richtlinien mit Kriterien zur Herstellung eines angemessenen Datenschutzniveaus in Jurisdiktionen außerhalb der EU und den drohenden regulatorischen Maßnahmen bei Nichteinhaltung der Standards erlassen. Diesbezüglich sollten Sie beachten, dass die Richtlinien sich je nach Drittstaat und Datenschutzbehörde unterscheiden können.
- Überarbeitung der Service Provider-Verträge: Implementieren Sie zusätzliche vertragliche Pflichten Ihrer IT Service-Provider, um einerseits die notwendigen Compliance-Schritte durchzuführen und um andererseits die regulatorischen Vorgaben der zuständigen Datenschutzbehörde umzusetzen.
- Vorausschauend sein und alternative Datentransfer-Lösungen etablieren: Eine rechtskonforme Alternativlösung könnte je nach individueller Fallgestaltung darin bestehen, statt auf Safe Harbor auf Instrumente wie die EU-Standardverträge oder evtl. sogar verbindliche Unternehmensregelungen zurückzugreifen. Solche Alternativen sollten geprüft werden.
- Alternative Auftragsdatenverarbeitungsmöglichkeiten in Betracht ziehen: Überprüfen Sie, ob Ihr Auftragsdatenverarbeiter Lösungen anbietet, die keinen Transfer von personenbezogenen Daten an den Safe-Harbor-Prinzipien unterliegenden Unternehmen vorsieht; z.B. weil eine Datenhaltung innerhalb der EU möglich ist.

Dr. Christoph Torwegge LL.M. (University of Bristol), Hamburg
Partner bei Osborne Clarke
www.osborneclarke.com

Dr. Flemming Moos, Hamburg
Fachanwalt für Informationstechnologierecht Partner bei Osborne Clarke
www.osborneclarke.com

Kontakt:

Bundesverband mittelständische Wirtschaft (BVMW) e. V.
Kommission Recht
Leipziger Platz 15, D-10117 Berlin
Tel.: +49 (0)30 533206-0, Fax: +49 (0)30 533206-50
politik@bvmw.de, www.bvmw.de