Datenübermittlung in Nicht-EU-Staaten: rechtliche Probleme

Von Jens Chr. Hammersen und Ulrich Eisenried

Das Outsourcing an Dienstleister außerhalb der EU ist mit Vorsicht zu genießen. Beim Datenexport in Länder ohne „Angemessenheitsentscheidung" der EU-Kommission (wie sie beispielsweise für die Schweiz existiert) empfehlen die Autoren, grundsätzlich die EU-Standardvertragsklauseln durchzusetzen. Von dem Datenexport in die USA können sie trotz eines mit dem US-Außenministerium ausgehandelten „Safe-Harbor-Paket" nur abraten. Denn die deutschen Datenschutzbehörden stehen dem nicht erst seit Prism sehr kritisch gegenüber. Red.

Angesichts der Globalisierung sehen sich viele Unternehmen mit der Frage konfrontiert, ob und gegebenenfalls in welche Länder Dienstleistungen ausgelagert werden können. Dabei muss sich das Unternehmen immer häufiger zwischen Angeboten von Anbietern innerhalb und außerhalb des Europäischen Wirtschaftsraums (EWR) entscheiden. Entscheidet sich das Unternehmen für einen Dienstleister außerhalb des EWR, wirft dies nicht nur eine Reihe praktischer Probleme auf, sondern stellt das auslagerungswillige Unternehmen auch rechtlich vor komplexe Herausforderungen.

Besondere Brisanz besitzt in diesem Zusammenhang das für nahezu jedes Unternehmen essenzielle Thema „Datenschutz", dem insbesondere aufgrund der Datenschutzskandale in der jüngsten Vergangenheit auch in der Öffentlichkeit große Aufmerksamkeit gewidmet wird.

Als prominentestes Beispiel für einen solchen Datenschutzskandal ist die Überwachung des E-Mail-Verkehrs durch den US-Geheimdienst mittels der Spähsoftware „Prism" zu nennen. Der vorliegende Beitrag behandelt die Frage, ob es für deutsche Unternehmen datenschutzrechtlich möglicherweise sicherer oder zumindest ebenso sicher ist, auf Dienstleister beispielsweise in der Schweiz, Uruguay, Russland und Moldawien zurückzugreifen als auf solche in den USA.

Drittländer mit „Angemessenheitsentscheidung" der EU-Kommission

Als Drittländer werden alle Länder bezeichnet, die außerhalb der EU und des EWR liegen. Gemäß § 4 b Abs. 2 BDSG sind Datenübermittlungen in Drittländer nur dann zulässig, wenn ein Erlaubnistatbestand im Sinne des § 4 Abs. 1 BDSG (das heißt eine Einwilligung des Betroffenen oder eine gesetzliche Erlaubnisnorm) vorliegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Ein der Übermittlung entgegenstehendes schutzwürdiges Interesse des Betroffenen wird angenommen, wenn in dem betreffenden Drittland kein angemessenes Datenschutzniveau gegeben ist. Die EU-Kommission ist durch Art. 25 Abs. 6 EU-Datenschutzrichtlinie 95/46/EG (EU-DatSchRL) ermächtigt, durch eine sogenannte „Angemessenheitsentscheidung" formell festzustellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder anwendbarer internationaler Verpflichtungen über ein angemessenes Datenschutzniveau verfügt.

USA dank Abkommen ein „Safe Harbor"

Drittländer, für die eine sogenannte „Angemessenheitsentscheidung" der EU-Kommission vorliegt, sind neben europäischen Insel- und Kleinststaaten auch Argentinien, Australien, Israel, Kanada, Schweiz sowie neuerdings Neuseeland und überraschenderweise Uruguay. Nach Auffassung der EU-Kommission besitzen diese Länder aufgrund ihrer internen Gesetzgebung ein den Grundsätzen der EU-DatSchRL im We-

Zu den Autoren

Jens Chr. Hammersen und **Dr. Ulrich Eisenried** sind Rechtsanwälte bei HAMMERSENs RECHTSANWÄLTE, München.

sentlichen entsprechendes Datenschutzniveau.

Auch für die USA existiert eine Angemessenheitsentscheidung der EU-Kommission. Den USA wird jedoch nicht aufgrund ihrer Gesetzgebung – in den USA existieren keine mit denen der EU vergleichbaren Datenschutzgesetze –, sondern nur auf Grundlage des mit dem US-Außenministerium ausgehandelten sogenannten „Safe-Harbor-Pakets" ein ausreichendes Datenschutzniveau bescheinigt.

Wesentliche Inhalte des Safe-Harbor-Pakets: Das Safe-Harbor-Paket besteht aus den „Safe-Harbor-Grundsätzen", die durch als Leitplanken dienende „Häufig gestellte Fragen" (FAQs) sowie weitere Anhänge ergänzt werden. Darin sind grundlegende Datenschutzrechte von Personen enthalten, wie zum Beispiel das Recht des durch die Datenverarbeitung Betroffenen, darüber informiert zu werden, wer seine Daten für welche Zwecke verwendet und an welchen Empfänger die Daten gegebenenfalls übermittelt werden. Geregelt werden außerdem Maßnahmen zur Datensicherheit sowie Berichtigungs- und Beschwerderechte des Betroffenen.

Für zuständig für die Überprüfung von Beschwerden und gegebenenfalls die Geltendmachung von Unterlassungs- und Schadensersatzansprüchen werden die Federal Trade Commission und das US-Verkehrsministerium erklärt.

Kritikpunkte an Safe Harbor

Die Angemessenheitsentscheidung der EU-Kommission in Bezug auf Safe Harbor unterliegt allerdings in zahlreichen Punkten der Kritik.

So wird beispielsweise der durch die Datenverarbeitung betroffenen Person eine Wahlmöglichkeit („opt out") eingeräumt. Die maßgebliche Passage in Anhang I der Safe-Harbor-Entscheidung lautet: „Die Organisation muss Privatpersonen die Möglichkeit geben zu wählen („opt out"), ob ihre personenbezogenen Daten a) an Dritte weitergegeben werden sollen oder b) für einen Zweck verwendet werden sollen, der mit dem ursprünglichen oder dem nachträglich von der betreffenden Person genehmigten Erhebungszweck unvereinbar ist."

Die betroffene Person kann hiernach widersprechen, wenn das Safe-Harbor-Unternehmen die Daten des Betroffenen an Dritte weitergibt oder wenn das Safe-Harbor-Unternehmen die Daten des Betroffenen für einen anderen als den ursprünglichen Erhebungszweck (oder als den nachträglich vom Betroffenen genehmigten Erhebungszweck) verwendet. Diese Wahlmöglichkeit ist deshalb befremdlich, da sie entgegen Art. 6 Abs. 1 lit. b) der EU-DatSchRL den Eindruck vermittelt, dass die zweckentfremdete Verwendung von Daten des Betroffenen den Normalfall bildet – so muss sich der Betroffene aktiv gegen eine zweckentfremdete Verwendung seiner Daten entscheiden, um eine solche auszuschließen.[1)]

Die Schwierigkeiten bei der Anwendung von Safe Harbor werden dadurch verstärkt, dass der Anwendungsbereich dieser Grundsätze zwischen EU-Stellen und deutschen Behörden uneinheitlich gesehen wird.

Die deutschen Aufsichtsbehörden stellen sich auf den Standpunkt, dass die Safe-Harbor-Grundsätze auf die Funktionsübertragung[2)] zugeschnitten sind und daher nicht alle Safe-Harbor-Grundsätze auf eine Auftragsdatenverarbeitung passen.

Die Aufsichtsbehörden haben aber in entsprechenden Beratungen gegenüber Unternehmen die Ansicht geäußert, dass wesentliche Datenschutzgrundsätze auch für Safe-Harbor-zertifizierte Auftragsdatenverarbeiter gelten müssen. Der Informationsgrundsatz kann hingegen bei der Auftragsdatenverarbeitung nur sinngemäß gelten, da informationspflichtig nach EU-Datenschutzrecht nur der deutsche Datenexporteur als verantwortliche Stelle ist.

Daher muss Safe Harbor im Fall der Auftragsdatenverarbeitung (wenn also der US-amerikanische Datenimporteur nicht zur verantwortlichen Stelle wird) so ausgelegt werden, dass das US-Unternehmen dem EU-Exporteur alle nach deutschem Datenschutzrecht erforderlichen Informationen zur Verfügung stellen muss, die dieser benötigt, um seine datenschutzrechtlichen Auskunftspflicht gegenüber dem Betroffenen erfüllen zu können. Dies muss der EU-Exporteur vertraglich (zum Beispiel im Vertrag entsprechend § 11 BDSG) gegenüber dem US-Auftragsverarbeiter sicherstellen.

Keine effektive Kontrolle der Einhaltung von Mindeststandards gewährleistet

Allein das formale Safe-Harbor-Zertifikat wird für den Nachweis eines angemessenen Schutzniveaus nicht als ausreichend bewertet. Die praktische Erfahrung mit dem Zertifizierungssystem von Safe Harbor hat gezeigt, dass keine effektive Kontrolle der Einhaltung der datenschutzrechtlichen Mindeststandards gewährleistet ist. Die im Dezember 2008 veröffentlichte sogenannte „Galexia"-Studie deckt insbesondere auf, dass sich Unternehmen mit einer „Safe-Harbor-Zertifizierung" schmücken, obwohl sie diesem Abkommen überhaupt nicht beigetreten sind beziehungsweise die Mindestanforderungen dieses Abkommens nicht einhalten.

Ursächlich dafür dürfte maßgeblich sein, dass nach dem Safe-Harbor-Prinzip US-amerikanische Unternehmen die Möglichkeit haben, sich durch die bloße Abgabe der Erklärung, die Safe-Harbor-Prinzipien einzuhalten sowie durch eine entsprechende Meldung an die Federal Trade Commission (FTC) selbst zertifizieren zu lassen. Ob diese Unternehmen im Bereich Datensicherheit die dafür erforderlichen Voraussetzungen erfüllen, wird von den US-Behörden nicht weiter geprüft. In der „Galexia"-Studie wurde

festgestellt, dass in zehn Jahren nur ein einziger Safe-Harbor-Fall überhaupt von einem Gericht überprüft wurde.

Schriftlichen Nachweis verlangen

Vor diesem Hintergrund hat der Düsseldorfer Kreis – als Zusammenschluss der Datenschutz-Aufsichtsbehörden im Unternehmensbereich – am 29. April 2010 beschlossen, dass sich der deutsche Datenexporteur einen schriftlichen Nachweis über die Safe-Harbor-Zertifizierung von seinem US-amerikanischen Datenimporteur vorlegen lassen muss. Zudem muss er sich im Fall der Funktionsübertragung nachweisen lassen, dass sein Datenimporteur die im Safe-Harbor-Abkommen festgelegten Informationspflichten gegenüber dem Betroffenen wahrnimmt. Für den Fall, dass der US-amerikanische Datenimporteur als Auftragsdatenverarbeiter tätig wird, muss der deutsche Datenexporteur als verantwortliche Stelle nachweisen, dass er die erforderlichen Vereinbarungen getroffen hat, um seinen eigenen Informationspflichten gegenüber dem Betroffenen zu genügen. Dokumente, die zum Nachweis der vorstehenden Mindeststandards dienen, sollte der deutsche Datenexporteur sorgfältig aufbewahren, da dieser als verantwortliche Stelle auf Anforderung der Datenschutzbehörden verpflichtet ist, diese vorzulegen.

Datenübertragung nach Uruguay sicherer als in die USA

Abschließend ist damit festzuhalten, dass für deutsche Unternehmen die Datenübertragung in die USA mit erhebliche praktischen Schwierigkeiten verbunden ist, da eine effektive Kontrolle der Einhaltung der Safe-Harbor-Grundsätze nicht besteht und die aufsichtsbehördlichen Anforderungen – wie oben dargestellt – umfangreich und kompliziert sind.

Bezüglich der anderen Länder, für die die EU-Kommission eine Angemessenheitsentscheidung erlassen hat, – also auch für Uruguay – bestehen hingegen nach Auffassung der EU-Kommission grundsätzlich keine durchgreifenden rechtlichen Bedenken, da sich die Angemessenheit des Datenschutzniveaus dort unmittelbar aus geltendem nationalem Recht ergibt. Die Datenübermittlung in diese Länder erscheint damit sicherer als in die USA.

Dies wird dadurch bestätigt, dass die Datenschutzkonferenz als oberstes Gremium der deutschen Datenschutzbehörden in ihrer Pressemitteilung vom 24. Juli 2013 festgestellt hat, dass angesichts der Datenzugriffe durch die US-Sicherheitsbehörden Datenübermittlungen in die USA grundsätzlichen Bedenken begegnen. Die Behörden haben sich vor diesem Hintergrund darauf verständigt, dass vorerst keine neuen Genehmigungen im Sinne von § 4 c BDSG für Datenübermittlungen in die USA erteilt werden sollen, sowie zu prüfen, ob bestehende Übermittlungen auszusetzen sind. Welche nächsten Schritte die Aufsichtsbehörden unternehmen werden, bleibt abzuwarten. Es empfiehlt sich daher für den deutschen Datenexporteur, die weitere Entwicklung im Auge zu behalten.

EU-Standardvertragsklauseln in Ländern ohne Angemessenheitsentscheidung

Steht nun fest, dass die Sicherheit der Datenübertragung in die USA in der praktischen Ausgestaltung ein geringeres Niveau hat als bei den übrigen Ländern, für die eine Angemessenheitsentscheidung besteht, stellt sich die Frage, ob das US-Datenschutzniveau zumindest gegenüber den sonstigen Drittländern als höher einzuschätzen ist.

Festzuhalten ist dabei zunächst, dass völkerrechtliche Vereinbarungen zum Datenschutz nur dann eine ausreichende Grundlage für ein angemessenes Datenschutzniveau darstellen können, wenn sie in den unterzeichnenden Staaten unmittelbar gelten. Die Europäische Daten-

bank und markt
Zeitschrift für Retailbanking

Verlag und Redaktion:

Verlag Fritz Knapp GmbH
Aschaffenburger Straße 19, 60599 Frankfurt am Main,
Postfach 111151, 60046 Frankfurt am Main,
Telefon 069/970833-0, Telefax 069/7078400,
www.kreditwesen.de,
E-Mail: red.bum@kreditwesen.de

Herausgeber: Klaus-Friedrich Otto

Chefredaktion: Dr. Berthold Morschhäuser, Swantje Benkelberg, Philipp Otto

Redaktion: Lars Haugwitz, Barbara Hummel, Frankfurt am Main.

Redaktionssekretariat: Elke Hildmann

Die mit Namen versehenen Beiträge geben nicht immer die Meinung der Redaktion wieder. Bei unverlangt eingesandten Manuskripten ist anzugeben, ob dieser oder ein ähnlicher Beitrag bereits einer anderen Zeitschrift angeboten worden ist. Beiträge werden nur zur Alleinveröffentlichung angenommen.

Die Zeitschrift und alle in ihr enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig.

Manuskripte: Mit der Annahme eines Manuskripts zur Veröffentlichung erwirbt der Verlag vom Autor das ausschließliche Verlagsrecht sowie das Recht zur Einspeicherung in eine Datenbank und zur weiteren Vervielfältigung zu gewerblichen Zwecken in jedem technisch möglichen Verfahren. Die vollständige Fassung der Redaktionsrichtlinien finden Sie unter www.kreditwesen.de.

Verlags- und Anzeigenleitung: Uwe Cappel

Anzeigenverkauf: Hans-Peter Schmitt, Tel. 069/970833-43.

Anzeigendisposition: Anne Guckes, Tel. 69/970833-26, sämtl. Frankfurt am Main, Aschaffenburger Straße 19.

Zurzeit gilt Anzeigenpreisliste Nr. 42 vom 1.1.2013.

Erscheinungsweise: Am 1. jeden Monats.

Bezugsbedingungen: Abonnementspreise incl. MwSt. und Versandkosten: jährlich € 409,50. Bei Abonnements-Teilzahlung: ½jährlich € 210,40. Ausland: jährlich € 419,42. Preis des Einzelheftes € 22,00 (zuzügl. Versandkosten).

Verbundabonnement mit der „Zeitschrift für das gesamte Kreditwesen": jährlich € 767,85. Bei Abonnements-Teilzahlung: ½jährlich € 403,40. Ausland: jährlich € 795,21.

Studentenabonnement: 50% Ermäßigung (auf Grundpreis).

Der Bezugszeitraum gilt jeweils für ein Jahr. Er verlängert sich automatisch um ein weiteres Jahr, wenn nicht einen Monat vor Ablauf dieses Zeitraumes eine schriftliche Abbestellung vorliegt.

Bestellungen aus dem In- und Ausland direkt an den Verlag oder an den Buchhandel.

Probeheftanforderungen bitte unter
Tel.-Nr. 069/970833-25

Als Supplement liegt „cards Karten cartes" jeweils am 1. Februar, 1. Mai, 1. August und 1. November dieser Zeitschrift bei.

Bei Nichterscheinen ohne Verschulden des Verlages oder infolge höherer Gewalt entfallen alle Ansprüche.

Bankverbindungen: Postbank Frankfurt 60482-609 (BLZ 50010060), Landesbank Hessen-Thüringen-Girozentrale 10555001 (BLZ 50050000), sämtliche in Frankfurt am Main.

Druck: Druckerei Hassmüller Graphische Betriebe GmbH & Co. KG, Königsberger Straße 4, 60487 Frankfurt.

ISSN 1433-5204

schutzkonvention[3], die beispielsweise von Moldawien, Aserbaidschan und Russland, nicht aber den USA ratifiziert wurde, kann insofern nicht als Übermittlungsgrundlage dienen, da dieser keine unmittelbare Geltung zukommt. Sie enthält zwar für automatisiert, das heißt mit IT-Unterstützung, verarbeitete Daten, bestimmte elementare Datenschutzprinzipien, die in innerstaatliches Recht umzusetzen waren. Dies beinhaltet unter anderem

- den Grundsatz der Datenverarbeitung nach Treu und Glauben,
- den Zweckbindungsgrundsatz,
- das Erforderlichkeitsprinzip
- sowie den Informationsanspruch des Betroffenen.

Die Europäische Datenschutzkonvention entspricht jedoch nicht dem datenschutzrechtlichen Standard der EU. Sie enthält lediglich einige rudimentäre Datenschutzgrundsätze, zu deren Umsetzung in innerstaatliches Recht sich die unterzeichnenden Staaten verpflichtet haben. Es gelten daher auch für diese Länder die allgemeinen Anforderungen für die Übermittlung der Daten in Drittländer.

In diesem Zusammenhang ist der Abschluss der sogenannten „EU-Standardvertragsklauseln" zu empfehlen. Durch die unveränderte Verwendung dieser von der EU-Kommission verabschiedeten datenschutzrechtlichen Klauseln wird ein angemessenes Schutzniveau im Sinne § 4 b Abs. 2 S. 2 BDSG sichergestellt. Eine aufsichtsrechtliche Genehmigung der Datenübermittlung ist dann entbehrlich.[4] Die Einhaltung der Standardvertragsklauseln durch den ausländischen Dienstleister ist vom deutschen Datenexporteur sicherzustellen.

Vergleicht man die EU-Standardvertragsklauseln mit den Safe-Harbor-Grundsätzen, stellt man fest, dass das Safe-Harbor-Niveau nicht höher ist als das der EU-Standardvertragsklauseln. Datenschutzrechtlich nachteilig ist in beiden Fällen, dass ausschließlich eine privatrechtliche Überwachung durch den Datenexporteur, aber keine staatliche Kontrolle stattfindet.

Besser EU-Standardvertragsklauseln als Safe Harbor

Aus Unternehmenssicht könnte die Anwendung der EU-Standardvertragsklauseln gleichwohl vorzuziehen sein, da in Bezug auf die Safe-Harbor-Grundsätze noch keine einheitliche behördliche Auffassung zu praktisch wichtigen Fragen der Anwendbarkeit existiert. Auch ist darauf hinzuweisen, dass die EU-Standardvertragsklauseln – abgesehen von der oben dargestellten Kontrolle – vollumfänglich den Standards der EU-Richtlinie und des BDSG entsprechen. Demgegenüber bleibt Safe Harbor beispielsweise hinsichtlich des geschilderten Wahlrechts des Betroffenen bezüglich der Verwendung seiner Daten hinter dem maßgeblichen EU-Recht zurück.

Daher ist es aus Sicht eines deutschen Datenexporteurs in der Regel vorteilhafter zu versuchen, auch im Falle einer Datenübermittlung in die USA an Stelle von Safe Harbor den Abschluss der EU-Standardvertragsklauseln durchzusetzen. Allerdings ist auch die Übermittlung personenbezogener Daten auf Basis von Standardvertragsklauseln in die USA derzeit nach Ansicht der deutschen Aufsichtsbehörden vor dem Hintergrund der „Prism"-Berichterstattung grundlegenden Zweifeln ausgesetzt. Es empfiehlt sich, die weitere Entwicklung, insbesondere Äußerungen der Datenschutzaufsichtsbehörden laufend zu verfolgen.

EU-weite Vereinheitlichung durch Datenschutzgrundverordnung

Die Problematik der Übermittlung von Daten eines EU-Bürgers in ein Drittland wird sich künftig möglicherweise einfacher und datenschutzrechtlich sicherer darstellen.

So soll die aus dem Jahr 1995 stammende EU-DatSchRL unter anderem durch eine sogenannte Datenschutz-Grundverordnung der EU ersetzt werden. Durch diese Datenschutz-Grundverordnung, die in allen Mitgliedstaaten der EU unmittelbar gelten soll, würde die Verarbeitung personenbezogener Daten durch private Unternehmen EU-weit vereinheitlicht. Eine Möglichkeit, durch nationale Gesetze von dieser Verordnung abzuweichen, bestünde nicht.

Ein wesentlicher Grundsatz dieser Verordnung soll sein, dass diese auch für nicht in der EU niedergelassene Unternehmen gilt, sofern diese ihre Waren und Dienstleistungen EU-Bürgern anbieten.[5] Das würde insbesondere US-Unternehmen wie zum Beispiel Google oder Facebook betreffen.

Sollte die Datenschutz-Grundverordnung in Kraft treten, wäre damit insbesondere auch das mit den USA ausgehandelte Safe-Harbor-Abkommen obsolet. Im praktischen Ergebnis liefe das Inkrafttreten der Verordnung daher auf eine Stärkung der Datenschutzrechte der EU-Bürger hinaus.

Allerdings hilft auch das beste Gesetz nichts, wenn es nicht beachtet wird. Das zeigt nicht zuletzt die durch die Snowden-Enthüllungen publik gewordene E-Mail-Überwachung durch den britischen Geheimdienst, die im geltenden EU-Recht wohl kaum eine Stütze finden dürfte.

Fußnoten

[1] Vgl. Simitis, BDSG, 7. Auflage 2011, § 4 b Rn. 73).
[2] Die Funktionsübertragung grenzt sich von der Auftragsdatenverarbeitung dadurch ab, dass neben der Datenverarbeitung auch die zugrunde liegende Aufgabe ganz oder teilweise an das Auslagerungsunternehmen abgegeben wird. So ist zum Beispiel in dem bloßen Zurverfügungstellen von Speicherkapazität oder einer Übermittlungstechnologie eine Auftragsdatenverarbeitung zu sehen, wohingegen bei der Auslagerung von ganzen IT- und Telekommunikationsbereichen eine Funktionsübertragung vorliegt.
[3] „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten.
[4] Vgl. zum Beispiel Innenministerium Baden-Württemberg, Hinweise zum BDSG für die Privatwirtschaft Nr. 40, B 2.8 – Bekanntmachung vom 18. Februar 2002, Az. 2-0552.1/17).
[5] Vgl. Art. 3 Nr. 2 des Verordnungsentwurfs.