ART.-NR.: 5

THEMA – DATENSCHUTZ

Mag. Birgit Vogt-Majarek/Dr. Philipp Spring, LL.M.

Das Ende von Safe-Harbor – Erst der Anfang ...?

Entscheidungsbesprechung zu EuGH 6. 10. 2015, C-362/14

» ARD 6473/5/2015

Der EuGH erklärte in seinem aktuellen Urteil vom 6. 10. 2015 die in der Entscheidung 2000/520/EG der Europäischen Kommission bejahte „Safe Harbor"-Regelung für ungültig. (Konzern-)Unternehmen, die aufgrund dieser Ausnahmeregelung bislang regelmäßig Datentransfers in die Vereinigten Staaten durchführten, können sich daher nicht mehr auf diese Rechtsgrundlage berufen. Dies wirft zahlreiche Fragen betreffend die künftige Handhabung bzw zulässige Alternativen der Datenübermittlung (insbesondere auch im Konzern) auf.

1. Sachverhalt

In dem am 6. 10. 2015 veröffentlichten Urteil zu C-362/14 überprüfte der EuGH die Entscheidung der Europäischen Kommission zu 2000/520/EG vom 26. 7. 2000 über die **Übermittlung personenbezogener Daten** aus einem Unionsstaat **in die Vereinigten Staaten** und die darin bejahte Angemessenheit des durch die Grundsätze des „sicheren Hafens" gewährleisteten Schutzniveaus.

Im Zuge der Anmeldung zum sozialen Netzwerk *Facebook* waren alle im Unionsgebiet wohnhaften Personen angehalten, einen Vertrag mit Facebook Irland, einer Tochtergesellschaft der in den Vereinigten Staaten ansässigen Facebook Inc., abzuschließen. Dadurch erteilten die im Unionsgebiet wohnhaften Facebook-Nutzer die Erlaubnis zur Übermittlung und Verarbeitung ihrer personenbezogenen Daten an bzw durch die in den Vereinigten Staaten befindlichen Server der Facebook Inc.

Der Österreicher *Max Schrems*, Jus-Student und selbst seit Jahren Nutzer von *Facebook*, erhob gegen dieses Vorgehen (stellvertretend für viele in puncto Daten ganz ähnlich agierende US-Konzerne) am 25. 6. 2013 Beschwerde bei der irischen Datenschutzkommission. Er monierte darin den **mangelnden Schutz** der in den Vereinigten Staaten gespeicherten personenbezogenen Daten aufgrund der **willkürlichen Überwachungstätigkeit** der dortigen Bundesbehörden und verwies auch auf die von *Edward Snowden* erfolgten Enthüllungen betreffend die Zugriffsmöglichkeiten der US-Nachrichtendienste (va der National Security Agency – NSA) auf Daten.

Die irische Datenschutzbehörde wies die Beschwerde als unbegründet zurück. Einerseits lägen keine Beweise für Zugriffe der NSA auf Daten von Herrn *Schrems* vor. Zudem stehe die Übermittlung von *Facebook*-Daten in die USA im Einklang mit der Entscheidung der Europäischen Kommission vom 26. 7. 2000 betreffend die sogenannte **„Safe-Harbor-Regelung"**.[1]

Im Zuge der gegen die Entscheidung der irischen Datenschutzbehörde erhobenen Klage von *Max Schrems* beim irischen High Court stellte das Gericht zum einen fest, die elektronische Überwachung und Erfassung der aus der Europäischen Union in die Vereinigten Staaten übermittelten personenbezogenen Daten diene als notwendiges und unerlässliches Ziel dem **öffentlichen Interesse.** Der High Court räumte jedoch andererseits nach einer Beweisaufnahme ein, dass die NSA und andere Bundesbehörden, wie das Federal Bureau of Investigation (FBI), tatsächlich auf die in die USA übermittelten Daten im Rahmen der von ihnen praktizierten ***„massenhaften und wahllosen Überwachung"*** zugreifen würden.

Aufgrund der von *Max Schrems* angezweifelten Gültigkeit der Entscheidung zu 2000/520/EG sah sich der High Court gezwungen, die Frage der Bindung einer unabhängigen Datenschutzbehörde an gegenteilige Feststellungen der Europäischen Union dem EuGH im Zuge eines Vorabentscheidungsverfahrens vorzulegen.

2. Entscheidung des EuGH

Der EuGH kommt in seinem Urteil zum Ergebnis, dass eine nationale **Kontrollstelle** durch die Entscheidung der Europäischen Kommission **nicht an der Prüfung** der Eingabe einer Person **gehindert** sei, die sich auf den Schutz ihrer Rechte und Freiheiten im Zusammenhang mit dem Transfer personenbezogener Daten aus einem Mitgliedstaat in ein Drittland beziehe, in dem **kein angemessenes Schutzniveau** gewährleistet werde.

Die **Entscheidung zu 2000/520/EG** der Europäischen Kommission erklärt der Europäische Gerichtshof für **ungültig**, weil sie

1 2000/520/EG: Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (bekannt gegeben unter Aktenzeichen K (2000) 2441).

gegen die Anforderungen der Richtlinie 95/46/EG[2] verstoße, und begründet dies zusammenfassend wie folgt:

Art 25 der RL 95/46/EG verbiete Übermittlungen personenbezogener Daten in ein Drittland, das kein „angemessenes Schutzniveau" gewährleiste, wobei kein in der Unionsrechtsordnung garantiertes, identisches Schutzniveau verlangt werde. Der Kommission obliege die Prüfung des Schutzniveaus in regelmäßigen Abständen, weil das in einem Drittland gewährte Schutzniveau naturgemäß Schwankungen unterworfen sei.

Die Entscheidung zu 2000/520/EG treffe laut EuGH keine hinreichenden Feststellungen zu jenen Maßnahmen, durch die ein angemessenes Schutzniveau in den Vereinigten Staaten gewährleistet werde. Sie räume den „Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen" insofern Vorrang ein, als gestützt auf diese ein **Eingriff in die Grundrechte** jener Personen, deren personenbezogene Daten aus der Europäischen Union in die Vereinigten Staaten übermittelt würden, ermöglicht werde. Jedoch seien die Ausnahmen vom Schutz personenbezogener Daten auf das **absolut Notwendige zu beschränken** (vgl EuGH 8. 4. 2014, C-293/12, C-594/12, *Digital Rights Ireland*).

Der Europäische Gerichtshof sieht ferner in einer Regelung, die den Behörden den generellen Zugriff auf elektronische Kommunikation erlaubt, eine Verletzung des in Art 7 der Charta garantierten **Grundrechts auf Achtung des Privatlebens** (vgl EuGH 8. 4. 2014, C-293/12, C-594/12, *Digital Rights Ireland*).

Des Weiteren sei der in Art 47 der EU-Charta verankerte Anspruch auf wirksamen gerichtlichen Rechtsschutz laut EuGH durch den Mangel eines Rechtsbehelfs, mit dem Bürger die sie betreffenden personenbezogenen Daten tatsächlich kontrollieren könnten, verletzt (vgl EuGH 11. 9. 2008, C-428 bis C-434/06).

Ferner beschränke die Entscheidung zu 2000/520/EG die Befugnisse der Kontrollstellen, weil diese angesichts der erwähnten Entscheidung keine Maßnahmen zur Gewährleistung der Einhaltung der Richtlinie 95/46/EG durchführen dürften. Zu dieser Beschränkung sei die Europäische Kommission allerdings laut EuGH nicht berechtigt.

3. Anmerkungen

3.1. Unionsrechtliche Rahmenbedingungen für die Datenübermittlung an Drittländer

Im Zusammenhang mit dem Transfer von personenbezogenen Daten ist ganz entscheidend, dass aufgrund der „Richtlinie über die Verarbeitung personenbezogener Daten"[3] eine Übermittlung derartiger Daten in ein Drittland[4] auch innerhalb eines Konzerns, wie dies aus Praktikabilitäts- und weitergehenden Überlegungen häufig der Fall ist, grundsätzlich nur dann zulässig ist, wenn das **Drittland** ein **angemessenes Schutzniveau** gewährleistet. Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, ist unter Berücksichtigung aller Umstände im Hinblick auf eine Übermittlung von Daten oder eine bestimmte Kategorie von Datenübermittlungen zu beurteilen.

Die Europäische Kommission kann sohin auf der Grundlage von Art 25 Abs 6 Datenschutzrichtlinie 95/46/EG feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder aufgrund internationaler Verpflichtungen, die es eingegangen ist, ein angemessenes Schutzniveau hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen gewährleistet.

3.2. Die Safe-Harbor-Regelung

Gestützt auf diese Möglichkeit stellte die Europäische Kommission mit ihrer Entscheidung aus dem Jahr 2000 fest, dass die **„Safe-Harbor-Regelung"** ein taugliches Instrument sei, um ein angemessenes Datenschutzniveau in den USA zu gewährleisten.

Hintergrund der Safe-Harbor-Regelung war kurz zusammengefasst, dass einzelne US-Unternehmen sich beim US-Department of Commerce freiwillig einer Art **„Zertifizierung"** unterwerfen konnten und ihnen damit ein nach europäischen Standards **angemessenes Datenschutzniveau zugebilligt** wurde. Diese US-Unternehmen galten somit als „sicherer Hafen" im Sinne des Datenschutzrechts für Datenübermittlungen aus Europa.

3.3. Unabhängigkeit der nationalen Kontrollstellen

Die wesentlichsten Aussagen des EuGH in seiner aktuellen Entscheidung beziehen sich einerseits darauf, dass eine Entscheidung der Europäischen Kommission, wie sie betreffend die oben beschriebene „Safe-Harbor-Regelung" erfolgt sei, die **Befugnisse der nationalen Datenschutzbehörde weder beschränken noch beseitigen** könne. Somit kann die nationale Behörde grundsätzlich in völliger Unabhängigkeit von der Entscheidung der Europäischen Kommission, insbesondere im Lichte der durch die EU-Charta garantierten Grundrechte[5] (va der Grundrechte auf Achtung der Privatsphäre und auf Schutz personenbezogener Daten) überprüfen, ob die mit der Datenschutzrichtlinie aufgestellten Anforderungen für die Übermittlung von Daten in ein Drittland tatsächlich gewahrt werden. Allerdings ist im Streitfall nur der EuGH selbst befugt, eine Kommissionsentscheidung für ungültig zu erklären, sodass es der Vorlage der maßgeblichen Fragen an den EuGH bedarf, wie dies auch im vorliegenden Fall erfolgte.

2 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

3 Datenschutzrichtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

4 Drittstaaten oder Drittländer sind Staaten, die nicht Mitgliedstaaten der Europäischen Union sind.

5 Charta der Grundrechte der Europäischen Union (2000/C 364/01).

3.4. Kein angemessenes Schutzniveau in den USA, keine Rechtsbehelfe

Der EuGH setzte sich in seinem Urteil, wie erwähnt, mit der Gültigkeit der Entscheidung der Europäischen Kommission zu 2000/520/EG auseinander. In diesem Zusammenhang führte der Gerichtshof aus, dass im Rahmen der Prüfung der Kommission, ob ein Drittland über ein angemessenes Schutzniveau verfügt, näher untersucht werden muss, ob dieses Drittland tatsächlich ein **Schutzniveau** der Freiheiten und Grundrechte gewährleistet, das dem in der Europäischen Union aufgrund der Datenschutzrichtlinie garantierten Niveau (zumindest) **gleichwertig** ist. Das mit der Entscheidung der Kommission festgestellte angemessene Schutzniveau muss in regelmäßigen Abständen und zudem immer dann überprüft werden, wenn konkrete Anhaltspunkte vorliegen, die Anlass zu begründeten Zweifeln über die Angemessenheit des Schutzes geben, wie dies im Zusammenhang mit der erwähnten Safe-Harbor-Regelung der Fall war.

Der EuGH kritisierte im aktuellen Urteil, dass sich die Kommission in ihrer Entscheidung nur darauf beschränkt habe, zu überprüfen, ob aufgrund der Safe-Harbor-Regelung ein angemessenes Schutzniveau für jene US-Unternehmen geschaffen werde, die sich freiwillig einer Art „Zertifizierung" beim US-Department of Commerce unterwerfen. Dieses Schutzniveau gelte jedoch ausschließlich für diese zertifizierten US-Unternehmen, wohingegen **US-Behörden** dadurch **nicht gebunden** seien. Die Entscheidung enthalte sohin keine Feststellungen darüber, dass die USA entsprechende Maßnahmen getroffen hätten, um ein angemessenes Schutzniveau im Sinne der EU-Datenschutzrichtlinie zu gewährleisten. Vielmehr führte die Entscheidung der Europäischen Kommission sogar aus, dass US-amerikanische Bestimmungen jedenfalls dann absoluten Vorrang[6] gegenüber den Safe-Harbor-Regelungen hätten, wenn sie in Widerstreit zu den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses sowie der Durchführung von Gesetzen stünden.

Ferner beanstandete der Europäische Gerichtshof im Hinblick auf die oben erläuterten europarechtlichen Datenschutzbestimmungen und die Vorgaben in puncto „angemessenes Schutzniveau" uE zu Recht, dass die Europäische Kommission auch keine Feststellungen dazu getroffen habe, ob es in den USA staatliche Regeln gebe, um mögliche **Eingriffe** von staatlichen Stellen **in Grundrechte zu begrenzen**, sowie, ob es überhaupt einen wirksamen **gerichtlichen Rechtschutz** gegen derartige Eingriffe gebe. Dass die Kommission ungeachtet ihrer Bejahung der Angemessenheit selbst Bedenken im Hinblick auf das Schutzniveau von in die USA übermittelten Daten hatte, beweisen zwei Mitteilungen der Kommission,[7] die beide am 27. 11. 2013 erlassen wurden. Darin stellte die Europäische Kommission fest, dass US-Behörden auf personenbezogene Daten zugegriffen und diese in einer Weise verarbeitet hätten, die mit den Zielsetzungen der Übermittlung unvereinbar gewesen sei und die über jenes Ausmaß hinausginge, das zum Schutz der nationalen Sicherheit absolut notwendig und verhältnismäßig gewesen sei. Darüber hinaus standen den Betroffenen, was der EuGH in seinem aktuellen Urteil ebenfalls betonte, auch keine entsprechenden Rechtsbehelfe zur Verfügung, um Einblick in die in den Vereinigten Staaten verarbeiteten Daten nehmen zu können und diese zu berichtigen oder zu löschen. Spätestens zu diesem Zeitpunkt hätte die Europäische Kommission ihre Safe-Harbor-Entscheidung laut EuGH überdenken müssen.

Aus den vorgenannten Gründen erklärte der Europäische Gerichtshof sohin die **gesamte Entscheidung** der Kommission für **ungültig**, was die irische Datenschutzbehörde, die sich nunmehr erneut mit der Beschwerde von *Max Schrems* auseinandersetzen muss, entsprechend zu berücksichtigen hat.

Damit folgte der EuGH der Meinung von Generalanwalt *Yves Bot*, der in seinem Schlussantrag[8] ebenfalls die Meinung vertrat, dass die Entscheidung 2000/520/EG ungültig sei, und dies insbesondere darauf stützte, dass die Überwachung der US-Geheimdienste „massiv und willkürlich" („*massive and indiscriminate*") erfolge.

3.5. Schlussfolgerungen

3.5.1. Betroffene Unternehmen

Es sieht so aus, als hätte *Max Schrems* mit seiner Beharrlichkeit und seiner durchaus nachvollziehbaren Gegenwehr gegen den europarechtlichen Standards klar widersprechende Eingriffsmöglichkeiten in personenbezogene Daten, die aus der EU in Drittstaaten übersendet werden, die Büchse der Pandora geöffnet. Die konkreten rechtlichen und faktischen Konsequenzen der EuGH-Entscheidung sind derzeit noch nicht im Detail absehbar.

Faktum ist, dass die Ungültigkeit der Kommissions-Entscheidung aus 2000 auch viele nationale Unternehmen betrifft, weil ein **Datentransfer in die Vereinigten Staaten**, wie dieser insbesondere in internationalen Konzernunternehmen an der Tagesordnung ist, **nicht mehr**, wie bisher, auf die **Safe-Harbor-Regelung gestützt** werden kann. Wie viele Unternehmen davon in Österreich betroffen sind, ist schwer zu sagen. Die ARGE Daten hält eine Zahl von bis zu 4.000 Unternehmen für realistisch.[9]

Von besonderer Relevanz ist das aktuelle Urteil insbesondere auch für jene nationalen Unternehmen, die in jüngster Vergangenheit ihre **Kunden- und Mitarbeiterdaten an US-Cloud-Anbieter** (wie zB Microsoft, Google, Apple etc) transferiert haben. Die meisten dieser Anbieter haben ein sogenanntes „follow-the-sun-data-center" in Betrieb und stützen den Transfer auf die

6 Anhang IV Abschnitt B der Entscheidung 2000/520/EG: „*Es steht jedoch eindeutig fest, dass, wenn aufgrund des US-amerikanischen Rechts eine den Grundsätzen des sicheren Hafens entgegenstehende Verpflichtung auferlegt wird, die US-Unternehmen die Gesetze einhalten müssen, und zwar ungeachtet dessen, ob sie auf die Grundsätze des sicheren Hafens verpflichtet sind oder nicht.*"

7 Mitteilung COM(2013) 846 und Mitteilung COM(2013) 847.

8 http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62014CC0362&from=EN.

9 Der Standard vom 17. 10. 2015: „ARGE Daten zu Safe Harbor: Firmen unter Abkommen brauchen Genehmigung".

Safe-Harbor-Regelung. Um die Zugriffszeiten auf die Daten in der Cloud möglichst kurz zu halten, wird versucht, die Distanz zwischen Server und User zu verringern. Die Daten werden dabei rund um den Globus transferiert, wobei die Daten des jeweiligen Users grundsätzlich auf jenem Server bereitgestellt werden, der dem User örtlich am nächsten ist. Da die meisten Menschen tagsüber arbeiten, wandern die Daten mit der Sonne während der Bürozeiten. In der Nacht werden dann entsprechende Backups auf den Servern durchgeführt.

3.5.2. Konkrete Alternativen zur Safe-Harbor-Regelung?

Die österreichische Datenschutzbehörde (DSB) hält auf ihrer Website unter Anführung der entsprechenden Gesetzesbestimmungen fest, dass es gemäß §§ 12 und 13 Datenschutzgesetz 2000 (DSG 2000) mehrere andere **Alternativen** gäbe, um personenbezogene Daten in die USA zu senden.[10]

Darunter fällt insbesondere der Transfer von Daten in die Vereinigten Staaten zur Erfüllung von eindeutig im Interesse des Betroffenen abgeschlossenen **Verträgen** oder die Weitergabe von Daten mit **Zustimmung des Betroffenen**. Die letztgenannte Zustimmungs-Variante klingt zwar recht einfach, ist aber in der Praxis aufgrund der diesbezüglichen rechtlichen Vorgaben sehr aufwendig und daher nur eingeschränkt praktikabel.

Nach Ansicht des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein,[11] das in seiner Beurteilung als sehr streng gilt, scheidet die Einholung einer wirksamen Zustimmungserklärung des von der Datenübermittlung Betroffenen aus folgenden Gründen aus: Eine Datenverarbeitung muss aufgrund der diesbezüglichen Vorgaben in der Datenschutzrichtlinie grundsätzlich für den konkreten Fall bzw für eine konkrete Datenanwendung abgegeben werden. Aufgrund der wie erwähnt nicht überschaubaren, willkürlichen Überwachungsmaßnahmen der US-Behörden ist die Abgabe einer solchen Zustimmung schwer vorstellbar. Aber selbst wenn eine ausreichende Information zu den konkreten Datenanwendungen vorliegt, greift die erwähnte Überwachung der Geheimdienste wohl in den Wesensgehalt des Grundrechts auf Achtung des Privatlebens ein. Derartige Eingriffe sind jedoch der Disposition des Einzelnen entzogen und können daher an sich auch nicht im Wege einer individuellen Zustimmung erfolgen.

Aus **arbeitsrechtlicher Sicht** ist zudem zu berücksichtigen, dass ein Arbeitnehmer im Rahmen seines Beschäftigungsverhältnisses eine Zustimmungserklärung nur innerhalb bestimmter Rahmenbedingungen, wie gefordert, freiwillig und ohne Zwang abgeben kann. Ein Zwang ergibt sich nach Ansicht von Teilen der Lehre aus dem regelmäßig unterstellten Abhängigkeitsverhältnis des Betroffenen vom Arbeitgeber. Tatsächlich kann eine wirksame **Zustimmung** in der Praxis sehr wohl erfolgen und die **rechtliche Situation für Arbeitgeber** jedenfalls **verbessern**. Sie muss jedoch, wie erwähnt, entsprechend den jeweiligen Umständen angepasst werden und kann nur schwer als Vorabzustimmung für alle Zukunft erteilt werden, weil der Arbeitnehmer auch über die zu verwendenden Daten zu informieren ist. Wesentlich ist für eine wirksame Zustimmung nach datenschutzrechtlichen Maßstäben zudem auch, dass die Arbeitnehmer grundsätzlich jederzeit ihre Zustimmung ohne Angabe von Gründen **widerrufen** können.

Unter Bezugnahme auf die Stellungnahme der Europäischen Kommission vom 6. 10. 2015[12] hat die DSB in ihrer Bekanntmachung ferner festgehalten, dass ein Transfer von personenbezogenen Daten in die Vereinigten Staaten auch künftig auf **Standardvertragsklauseln**[13, 14] und auf **Binding Corporate Rules**[15] gestützt werden kann.

Bei den Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (2001/497/EG), den Alternativen Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (2004/915/EG) sowie den Standardvertragsklauseln für die Weitergabe personenbezogener Daten an Auftragsverarbeiter in Drittländern (2010/87/EG) handelt es sich jeweils um von der Europäischen Kommission gefasste Entscheidungen über Standardvertragsklauseln, die angemessene Garantien für die Übermittlung personenbezogener Daten von der EU in Drittländer gewährleisten sollen, und die ua die Pflichten des Datenexporteurs und des -importeurs sowie die Haftung regeln.

➡ **Hinweis:** Zu beachten ist, dass trotz Verwendung der Standardvertragsklauseln der Datentransfer von Österreich in ein Drittland (im Gegensatz zur Rechtslage in manch anderem EU-Mitgliedstaat) der Genehmigung durch die DSB bedarf, die nach den bisherigen Erfahrungen (zumindest) mehrere Monate dauern würde.

Auch wenn die Gültigkeit der bereits bisher vorhandenen **Standardvertragsklauseln** durch das aktuelle EuGH-Urteil nicht in Abrede gestellt wird, sind diese – wie zB das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein betont – **nur bedingt praktikabel** und uE im Lichte der aktuellen EuGH-Entscheidung durchaus mit Vorsicht zu verwenden. Solange nämlich die USA aufgrund ihrer oben erwähnten umfangreichen Überwachungsmaßnahmen durch staatliche Behörden ua nicht als sicheres Drittland eingestuft werden könne, stellt sich – so das Un-

10 http://www.dsb.gv.at/site/6218/default.aspx.
11 https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-Positionspapier-zum-EuGH-Urteil.pdf.
12 http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm.
13 2001/497/EG, 2004/915/EG oder 2010/87/EG.
14 Die Europäische Kommission hat Standardvertragsklauseln verabschiedet, die ihrer Einschätzung nach angemessene Garantien bei der Übermittlung personenbezogener Daten von der EU in Drittländer gewährleisten. Die Standardvertragsklauseln enthalten eine rechtlich durchsetzbare Erklärung („Garantie"), nach der sowohl der „Datenexporteur" als auch der „Datenimporteur" sich verpflichten, die Daten nach Maßgabe bestimmter Datenschutzgrundsätze zu verarbeiten.
15 Diese sind ein von der Artikel-29-Datenschutzgruppe entwickelter Rahmen für verbindliche konzerninterne Richtlinien zum Umgang mit personenbezogenen Daten. Die Artikel-29-Datenschutzgruppe ist das unabhängige Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes.

abhängige Landeszentrum – die Frage, ob ein Transfer in die USA nicht dennoch unzulässig sei.

Auch technische Maßnahmen zur Herstellung des Einklangs mit der EuGH-Entscheidung, wie die „Rückholung" der Daten aus den USA und die **Speicherung auf Servern in Europa**, könnten eine mögliche Alternativlösung sein. Dabei ist jedoch zu beachten, dass diese Maßnahmen unter Umständen die Verpflichtung zur Einholung der **Zustimmung des Betriebsrates** gemäß § 96a Abs 1 Z 1 ArbVG (= Einführung von Personaldatensystemen) auslösen können und daher näher zu prüfen wäre, inwieweit die Vorgaben des österreichischen Arbeitsverfassungsgesetzes hier erfüllt werden, oder inwieweit etwa nur Arbeitnehmerdaten verarbeitet werden, die für die Erfüllung gesetzlicher, kollektivvertraglicher oder arbeitsvertraglicher Verpflichtungen notwendig sind, sodass es insofern keiner Betriebsvereinbarung bedarf.

Auch wenn es für Unternehmen **keine Übergangsfrist** für die Umstellung von bisher auf der „Safe-Harbor-Regelung" basierenden Datentransfers auf andere, oben erwähnte, legale Übermittlungsmöglichkeiten gibt, empfiehlt die Art-29-Datenschutzgruppe den nationalen Datenschutzbehörden in ihrer Stellungnahme vom 16. 10. 2015[16], mit entsprechenden Vollstreckungsmaßnahmen gegenüber Unternehmen bis Ende Jänner 2016 zuzuwarten. Es ist daher uE recht unwahrscheinlich, dass die DSB bereits davor – und vor allem ohne Vorankündigung – entsprechende Sanktionen verhängt. Bei Datentransfers ohne entsprechende gesetzliche Ausnahme oder behördliche Genehmigung drohen gemäß § 52 Abs 2 DSG 2000 Geldstrafen bis zu € 10.000,- für jeden Transfer.

Vor diesem Hintergrund sollte von Seiten der Unternehmen **möglichst rasch nach Alternativen** – zumindest für einen Übergangszeitraum – **gesucht** werden, weil uE zu bezweifeln ist, dass bis Jänner 2016 eine zufriedenstellende Lösung gefunden wird, mit der im Hinblick auf die obigen Ausführungen und die aufgezeigten Interessengegensätze alle Seiten gut leben können. Angekündigt wurde auch schon, dass seitens der Europäischen Kommission eine „Safe-Harbor-Regelung II" gefasst werden wird, in der den Vorgaben des EuGH laut dem aktuellen Urteil so weit wie möglich nachgekommen wird. Ob und wann ein solches Vorhaben tatsächlich umgesetzt wird, ist noch offen.

16 http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

Die Autorin:

Mag. **Birgit Vogt-Majarek** ist seit 2004 Partnerin bei KSW und leitet mit Georg Schima die Arbeitsrechts- und Ius Laboris-Task Force. Sie berät in- und ausländische Unternehmen zu allen Themen des individuellen und kollektiven Arbeitsrechts sowie Executives in allen Fragen von der Vertragserstellung bis zu dessen Beendigung. Birgit Vogt-Majarek ist ferner Autorin und Vortragende zu verschiedensten arbeitsrechtlichen und HR-spezifischen Themen.

birgit.vogt-majarek@ksw.at
lesen.lexisnexis.at/autor/Vogt-Majarek/Birgit

Foto: KSW

Der Autor:

Dr **Philipp Spring**, LL.M. (UPenn) ist Rechtsanwalt bei Kunz Schima Wallentin Rechtsanwälte OG. Er berät und vertritt nationale und internationale Unternehmen auf dem Gebiet des Immaterialgüterrechts und gewerblichen Rechtsschutzes, sowie des IKT-Rechts mit besonderem Schwerpunkt auf dem Datenschutzrecht. Weiterer Schwerpunkt seiner Tätigkeit ist das Sportrecht. Zahlreiche Publikationen in Fachzeitschriften.

philipp.spring@ksw.at
lesen.lexisnexis.at/autor/Spring/Philipp

Foto: beigestellt