Arbeitsrecht im Betrieb

2016, Ausgabe 1, S. 31–34 – Kiesche/Wilke, Safe Harbor-Urteil und die Folgen

Safe Harbor-Urteil und die Folgen

von Eberhard Kiesche und Matthias Wilke

DATENSCHUTZ Der Europäische Gerichtshof hat entscheiden, dass personenbezogene Daten europäischer Bürger in den USA nicht sicher sind und das Safe Harbor-Abkommen der EU-Kommission gekippt. Das gibt neue Impulse für den Schutz von Beschäftigtendaten.

DARUM GEHT ES

1. Der EuGH hat im Oktober das Safe Harbor-Abkommen gekippt.

2. Das bedeutet, dass Datenexporte in die USA nicht mehr den Datenschutzstandards der EU entsprechen.

3. Betriebsräte sollten jetzt ihre Rechte nutzen, um den Datenaustausch rechtssicher zum Schutz der Beschäftigtendaten zu gestalten.

Der Europäische Gerichtshof in Luxemburg kippte das Safe Harbor-Abkommen.

Dank Max Schrems aus Österreich musste sich der EuGH mit der Frage auseinandersetzen, ob die Safe Harbor-Grundsätze für den Datentransfer in die USA ein angemessenes Datenschutzniveau garantieren. Der Europäische Gerichtshof (EuGH) überprüfte die Angemessenheitsentscheidung der EU-Kommission 2000/520/EG vom 26. Juli 2000 zur Datenübermittlung an US-Organisationen, die den Safe-Harbor-Grundsätzen beigetreten sind und erklärt am 6. Oktober 2015 die Safe-Harbor-Entscheidung der Kommission für ungültig. Vor dem Hintergrund der NSA-Affäre seien die personenbezogenen Daten europäischer Bürger in den USA nicht ausreichend geschützt. Geklagt hatte Max Schrems in Irland. Konkreter Anlass war, dass Schrems den Zugriff auf seine Facebook-Nutzerdaten durch amerikanische Geheimdienste befürchtete, besonders nach den Snowden-Enthüllungen. Facebook hat seine Niederlassung in Dublin. Schrems machte eine Eingabe bei der irischen Datenschutzaufsichtsbehörde, die sich weigerte, Ermittlungen gegen Facebook einzuleiten. Es gäbe keine tatsächlichen Anhaltspunkte, dass gegen die Interessen der Betroffenen verstoßen würde, so die Aufsichtsbehörde in Dublin. Daraufhin rief Max Schrems den irischen High Court (Oberstes Zivilgericht) an.
Anschließend hatte dieser beim EuGH eine Vorlage zur Verbindlichkeit von Safe Harbor eingereicht.

HINTERGRUND

Die Idee der Safe Harbor-Regelung

Safe Harbor (englisch sicherer Hafen) ist eine Entscheidung der Europäischen Kommission aus dem Jahr 2000 auf dem Gebiet des Datenschutzrechts. Danach sollte es Unternehmen ermöglicht werden, personenbezogene Daten in Übereinstimmung mit der europäischen Datenschutzrichtlinie aus einem Land der Europäischen Union in die USA zu übermitteln. Dazu mussten die Unternehmen oder Organisationen Safe Harbor beitreten. Amerikanische Unternehmen konnten sich selbst zertifizieren und in die Safe Harbor-Liste freiwillig eintragen. Damit – so die Idee der Selbstbindung – stellt das eingetragene Unternehmen das in der EU herrschende Datenschutzniveau angemessen sicher. Mehr als 4.400 Konzerne haben diesen Weg gewählt und haben nach der aktuellen Entscheidung des EuGH jetzt keine Rechtsgrundlage mehr. Es gibt keine Übergangsfrist. Auch deutsche Unternehmen, die ihre Daten in die USA übermitteln und dort verarbeiten lassen, sind betroffen.

Safe Harbor seit langem in der Kritik

Seit längerem gab es Kritik der deutschen Aufsichtsbehörden an Safe Harbor. Zuletzt wurde die Kündigung des Verfahrens gefordert. Kritisiert wurden vor allem die mangelnde Sicherstellung und Durchsetzung der Rechte der Betroffenen in den USA und der Einsatz von Unterauftragnehmern. Ebenso wurde als Vollzugsdefizit kritisiert, dass der Beitritt der Unternehmen zu Safe Harbor und die tatsächliche Rechtspraxis nicht oder höchst unzureichend überprüft werden.

DIE ENTSCHEIDUNG

Das Urteil des EuGH zu »Safe-Harbor«, abrufbar unter http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=85155

USA PATRIOT ACT

Der USA PATRIOT Act ist ein US-amerikanisches Bundesgesetz, das am 25. Oktober 2001 vom Kongress im Zuge des Krieges gegen den Terrorismus verabschiedet wurde. Es war eine direkte Reaktion auf die Terroranschläge am 11. September 2001 und die wenig später erfolgten Milzbrand-Anschläge. Das Gesetz bringt eine Einschränkung der amerikanischen Bürgerrechte in größerem Maße mit sich.

Besondere Probleme bereitet der amerikanische »Patriot Act«. Dieses im Zuge der Terrorabwehr beschlossene US-Gesetz verpflichtet alle US-Unternehmen, im Rahmen des Antiterrorkampfs Daten an US-Behörden zu übermitteln. Dazu können Daten gehören, die nach deutschem Recht dem Datenschutz oder der betrieblichen Mitbestimmung unterliegen, so zum Beispiel Beschäftigtendaten und Daten über Telefongespräche oder E-Mail-Verbindungen.

Das bahnbrechende Urteil

Grundlage für das EuGH-Urteil waren die EU-Grundrechtecharta von 2009 mit dem Recht auf Datenschutz in Artikel 8 und die Datenschutzrichtlinie 95/46/EG. Der EuGH beschäftigt sich mit zwei Fragen:

1. Sind nationale Aufsichtsbehörden für den Datenschutz an die Entscheidung der Kommission zu Safe Harbor gebunden?
2. Ist weiterhin das Safe-Harbor-Abkommen zulässig?

Irische Aufsichtsbehörde hätte tätig werden müssen

Der EuGH stellt fest, dass die nationale Aufsichtsbehörde sich nicht gegen eine Angemessenheitsentscheidung der Kommission grundsätzlich stellen kann. Aber im Einzelfall muss die Aufsichtsbehörde bei Individualbeschwerden selbst entscheiden, ob

eine Datenübermittlung in den jeweiligen Drittstaat im Einklang mit europäischen Datenschutzgrundsätzen steht. Dies gilt dann, wenn tatsächliche Anhaltspunkte für die Gefährdung eines angemessenen Datenschutzniveaus vorliegen. Die Eingabe von Max Schrems hätte von der Dubliner Behörde entgegengenommen und geprüft werden müssen.

Safe Harbor-Abkommen ist unzulässig

Der EuGH beschäftigt sich des Weiteren mit der Zulässigkeit des Safe-Harbor-Abkommens. Es stellt fest, dass im Europäischen Datenschutzrecht eine Definition des »angemessenen Datenschutzniveaus« fehlt, so in Art. 25 Abs. 2 der Richtlinie 95/46/EG. Dies zwingt dazu, bei der Übermittlung von Daten alle rechtlichen und faktischen Umstände zu berücksichtigen.

Die Kommission muss entweder nationale Vorschriften des Drittstaates oder internationale Übereinkommen und Verpflichtungen und somit die faktische und rechtliche Geltung der angemessenen Datenschutzgarantien ausreichend prüfen. Das Safe Harbor-Abkommen hat keine Bindungswirkung für staatlich veranlasste und anlasslose Zugriffe auf europäische Daten. Zudem liegen nur Grundsätze vor, aber keine staatlichen Rechtsnormen oder internationale Verpflichtungen. Insofern stellt der EuGH fest, dass keine ausreichenden Maßnahmen nach Art. 25 Abs. 6 der EG-Datenschutzrichtlinie für den Rechtsschutz bei der Übermittlung von Daten in die USA vorliegen. Der EuGH attestiert der EU-Kommission eine »unechte Angemessenheitsentscheidung«, denn europäische Daten seien in den USA nicht sicher. Hat die Kommission Hinweise auf Zweifel, beispielsweise aufgrund des USA Patriot Act, muss sie nach dem EuGH ihre getroffene Entscheidung regelmäßig überprüfen. Bislang hat sie nur Empfehlungen zur Verbesserung des Safe Harbor-Systems ausgesprochen. Nach Snowden hat sie die Entscheidung nicht grundsätzlich in Frage gestellt. Zurzeit ist sie in Verhandlungen mit der US-Regierung.

Folgen der Entscheidung

Eine Datenübermittlung allein aufgrund der Safe Harbor-Entscheidung der Kommission vom 26.7.2000 ist nicht mehr zulässig. Unternehmensleitungen müssen ihre Datenexporte in die USA der Rechtsprechung des EuGH anpassen. Der EuGH hat die Position der europäischen Aufsichtsbehörden deutlich gestärkt. Ihnen wird die Kompetenz zugesprochen, den Sachverhalt zu überprüfen, selbst tätig zu werden und den Rechtsweg zu beschreiten. Es müssen jedoch konkrete Anhaltspunkte für den Verdacht einer Verletzung europäischer Grundfreiheiten vorliegen. Die Datenschutzbehörden der EU-Mitgliedstaaten müssen jetzt Wege definieren, wie der Datenverkehr mit den USA datenschutzkonform zu gestalten ist. Das Urteil des EuGH hat Auswirkungen auf den Datenverkehr mit den USA oder mit weiteren Drittstaaten. Es gibt andere Rechtsgrundlagen für den Datenexport in Drittländer, so die Standardklauseln der Kommission, die Einwilligung nach § 4c Abs. 1 Nr. 3 BDSG, Einzelfallgenehmigungen oder die verbindlichen Unternehmensregelungen (Binding Corporate Rules – BCRs). Auch diese Datentransfers und Speicherungen sind vor US-Geheimdiensten nicht sicher. Ab sofort werden auch diese Rechtsgrundlagen im Lichte der EuGH-Entscheidung in Frage gestellt. Hier sind Stellungnahmen der deutschen Aufsichtsbehörden, beispielsweise des Unabhängiges Landeszentrum für Datenschutz in Schleswig Holstein, zu berücksichtigen, inwieweit und in welchem Ausmaß die Instrumente betroffen sind.[1]

CLOUD COMPUTING

Unter Cloud Computing (deutsch etwa Rechnen in der Wolke) wird das Speichern von Daten in einem entfernten Rechenzentrum verstanden, aber auch die Ausführung von Programmen, die nicht auf dem lokalen Arbeitsplatzcomputer oder Server installiert sind, sondern eben entfernt in der Wolke.

Auf der Sondersitzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) am 21. Oktober 2015 wird im Positionspapier (Nr. 7) bekräftigt, dass die Datenschutzbehörden derzeit keine neuen Genehmigungen für Datenübermittlungen in

die USA auf Grundlage von BCR oder Datenexportverträgen erteilen werden. Beim Export von Beschäftigtendaten oder wenn gleichzeitig Daten Dritter betroffen sind, kann die Einwilligung nur in Ausnahmefällen eine zulässige Grundlage für eine Datenübermittlung in die USA sein (DSK 26.10.2015, Nr. 9 und 10). Die Kommission hat nun unverzüglich regulatorische Maßnahmen zur Garantie eines angemessenen Schutzniveaus mit den US-Behörden zu verhandeln und zu vereinbaren. Das benötigt jedoch Zeit. Kurzfristig kann jeder Datentransfer in die USA durch nationale Aufsichtsbehörden in Frage gestellt werden. Die EU-Kommission wird von der DSK aufgefordert, die Rechtslage und Rechtspraxis in Drittstaaten zu überprüfen.

Handlungsmöglichkeiten der Betriebsräte

Betriebsräte von Tochtergesellschaften amerikanischer Konzerne, die ihre Kunden- oder Beschäftigtendaten in den USA speichern und verarbeiten, sollten ihre (Konzern-)Betriebsvereinbarungen für Übermittlungen von Beschäftigtendaten in die USA überprüfen, aufkündigen oder nachverhandeln. Betriebsräte von betroffenen Unternehmen sollten zudem von der Unternehmensleitung einen Zeitplan fordern, wann und in welchen Schritten Datenübermittlungen auf der Grundlage von Safe-Harbor gestoppt oder nachgebessert werden.[2] Betriebsräte von Unternehmen, die andere Instrumente zum Datentransfer in Drittstaaten einsetzen, sollten von ihren Geschäftsführungen eine Stellungnahme anfordern, inwieweit diese Rechtsgrundlagen mit der EuGH-Rechtsprechung noch vereinbar sind.

LINKTIPP
Thilo Weichert vom 7.10.2015 – Safe Harbor – was Betriebsräte wissen müssen, unter: **www.bund-verlag.de/zeitschriften/arbeitsrecht-im-betrieb/aktuelles/news/2015/10/10-fragen-zum-safe-harbor-urteil.php**

Auch Personalabteilungen betroffen

Ebenso sind von dem Urteil Personalabteilungen und Betriebsräte großer Unternehmensgruppen betroffen, wenn die Grundlagen des Austausches von Personal-Daten (HR-Daten) zwischen Personalabteilungen in der EU und den USA wegfallen. Datenübermittlungen in die USA, die ausschließlich auf die Safe Harbor-Prinzipien gründen und von denen die Aufsichtsbehörden Kenntnis erlangen, werden untersagt. Übergangsfristen der Aufsichtsbehörden sind zu beachten.
Betriebsräte sollten schnellstens Verhandlungen mit der Arbeitgeberseite führen, ob oder inwieweit zusätzliche Garantien zum Schutz des Rechts auf Datenschutz gerade bei dem Export von Beschäftigtendatenschutz geschaffen werden müssen. Hier ist an Gewährleistungen insbesondere im Hinblick auf Zweckbindung, die Weitergabe an Sicherheitsbehörden im Fall von gesetzlichen Verpflichtungen, die Betroffenenrechte oder den Rechtsschutz und die Datenschutzkontrolle zu denken.[3] Betriebsräte können hierfür vor allem auf den Abschluss oder an die Änderung von Konzernbetriebsvereinbarungen nach § 4 Abs. 1 BDSG setzen. Sie sollten für Datenexporte in die USA die Verschlüsslung der Beschäftigtendaten fordern (siehe Anlage zu § 9 BDSG, Satz 2).

Innerbetriebliche Prüfung notwendig

Betriebsparteien sollten auch bei der Übermittlung in weitere Drittstaaten das Problem staatlich veranlasster Datenzugriffe oder Abgriffe seitens von Geheimdiensten prüfen und daraus Konsequenzen ziehen.[4] Das bedeutet, weitere Angemessenheitsentscheidungen der Kommission innerbetrieblich prüfen und mit weiteren Rechtsgarantien Datenübermittlungen rechtssicher gestalten. Beim Cloud Computing sollte seitens der Unternehmen auf zertifizierte Cloud-Anbieter in Europa zurückgegriffen werden, wenn sie bisher ihre Daten in der Cloud bei US-Dienstleistern verarbeiten oder speichern lassen. Sie sollten vom bisherigen Cloud-Anbieter zusätzliche Gewährleistungen für den Datenschutz fordern. Die Nutzung von MS Office 365 ist hinsichtlich der rechtlichen Zulässigkeit in Frage zu stellen.[5]

Beschäftigte, die von einem Datenexport in die USA betroffen sind, können sich an ihre Betriebsräte, ihren jeweiligen Datenschutzbeauftragten und die zuständige Aufsichtsbehörde mit einer Beschwerde wenden. Betriebsräten und Personalabteilungen ist zudem anzuraten, strikt bei einem geplanten Datenexport oder auch bei der Entwicklung einer Betriebsvereinbarung zu Datenübermittlungen in Drittstaaten die nationalen Aufsichtsbehörden hinzuziehen und deren Zustimmung einzuholen.

Neue Impulse für die Datenschutzkontrolle

Dieses wichtige Urteil des EuGH ermöglicht Datenschützern, den Datenaustausch mit den USA rechtssicherer als bisher zu gestalten. Weitere Instrumente für den Datenexport in die USA aber auch in andere Drittstaaten werden ab sofort auf den Prüfstand gestellt. Der Europäische Datenschutz und auch der Beschäftigtendatenschutz gehen aus diesem Urteil gegenüber amerikanischen Konzernen wie beispielsweise Facebook, Apple, Google oder Amazon gestärkt hervor. Der EuGH verschafft dem Recht auf Datenschutz in der EU-Grundrechtecharta die gebührende Geltung. Für ihre vom EuGH geklärten neuen Aufgaben benötigen die deutschen Aufsichtsbehörden dringend mehr Personal.

Dr. Eberhard Kiesche, Arbeitnehmerorientierte Beratung (AoB), Bremen.
eberhard.kiesche@t-online.de

Matthias Wilke, Datenschutz- und Technologieberatung (dtb), Kassel.
info@dtb-kassel.de

---

[1] Positionspapier vom 14.10.2015.

[2] Weichert vom 7.10.2015, http://www.bund-verlag.de/zeitschriften/arbeitsrecht-im-betrieb/aktuelles/news/2015/10/10-fragen-zum-safe-harbor-urteil.php.

[3] Weichert ebenda.

[4] Wedde, Cloud Computing, CuA 7–8/2014, 14.

[5] Weichert, a.a.O. Nr. 6.