Europäischer Gerichtshof kippt Safe Harbor-Regelung. Was heißt das für die betriebliche Praxis ?

Der Europäische Gerichtshof (EuGH) ist das oberste Gericht in der Europäischen Union. Der EuGH prüft, ob die Rechtsprechung innerhalb der EU auch tatsächlich den Verträgen, Richtlinien und Verordnungen entspricht. EuGH-Urteile sind daher richtungsweisend für die nationalstaatliche Rechtsprechung.

Was bedeutet Safe Harbor eigentlich?
Es handelt sich um eine Regelung zwischen EU-Kommission und US-Handelsministerium. Mittels Safe Harbor können US-Unternehmen zusichern, dass personenbezogene Daten europäischer NutzerInnen bei ihnen ebenso gut geschützt sind wie in Europa. Aufgrund dieser Selbstverpflichtungserklärung dürfen dann personenbezogene Daten aus Europa in die USA zum Safe Harbor zertifizierten Unternehmen transferiert und dort verarbeitet werden. Und zwar ohne die sonst für Nicht-EU-Mitgliedsstaaten erforderliche Genehmigung durch die Datenschutzbehörde.

Zur Vorgeschichte:
Wie in den Medien der letzten Tage ausführlich berichtet, erfolgte das aktuelle Urteil aufgrund einer Klage von Max Schrems gegen eine Entscheidung der irischen Datenschutzbehörde. Dort war er zuvor mit seinem Anliegen abgeblitzt: Schon 2011 hatte Schrems nämlich in Irland, dem europäischen Sitz von Facebook, eine Prüfung beantragt, inwieweit die in den USA über ihn gespeicherten Facebook-Daten sicher vor Massenüberwachung seien. Die irische Behörde war der Ansicht, es genüge, dass Facebook nach Safe Harbor zertifiziert sei. Deshalb dürfe die Datenschutzbehörde die beantragte Prüfung gar nicht durchführen. Seit damals stellt sich – zusätzlich befeuert durch Bekanntwerden der NSA-Affäre 2013 – die Frage: **Sind Grundrechte wie jenes auf Datenschutz für den oder die Einzelne/n durchsetzbar oder existieren sie nur auf dem Papier?** Der Gerichtshof hat nun in dieser Frage eine Entscheidung getroffen.

Die wichtigsten Aussagen des EuGH

IT-Systeme, die nicht ausreichend vor Massenüberwachung schützen, verletzen die Grundrechte:

„Die Datenverarbeitungssysteme stehen im Dienste des Menschen. Sie haben (…) deren Grundrechte und -freiheiten und insbesondere deren Privatsphäre zu achten und zum (…) Wohlergeben der Menschen beizutragen." (zitiert aus den Erwägungsgründen der derzeit noch geltenden Datenschutzrichtlinie 95/46). Die Grundrechte, insbesondere das Recht auf Achtung des Privat- und Familienlebens, genießen als Teil des Unionsrechtes Vorrang vor einzelstaatlichen Regelungen und EU-Kommissionsentscheidungen. Ziel sei es, in der Europäischen Gemeinschaft ein hohes Schutzniveau sicherzustellen und Datentransfers daher nur in solche Drittstaaten zuzulassen, die ein Datenschutzniveau gewährleisten, das dem europäischen gleichwertig ist.

Safe Harbor = ungültig:
Die von der EU-Kommission erlassene „Safe Harbor-Regelung" wurde vom EuGH für ungültig erklärt, weil es in den USA weder Regelungen gibt, die Grundrechtseingriffe der Behörden begrenzen würden, noch wirksamer Rechtsschutz gegen solche Eingriffe besteht.

Nationale Datenschutzbehörde prüft unabhängig, ob im Drittstaat (im konkreten Fall USA) angemessener Datenschutz besteht oder nicht.

„Die Gewährleistung der Unabhängigkeit nationaler Kontrollstellen (…) ist ein wesentliches Element zur Wahrung des Schutzes der Personen bei der Verarbeitung personenbezogener Daten." so der EuGH in seiner Urteilsbegründung. Daraus ist abzuleiten, dass Melde- und Genehmigungspflichten bei der Österreichischen Datenschutzbehörde ernst genommen werden müssen und die Befugnisse der Datenschutzbehörde *nicht* unter Berufung auf Safe Harbor unterlaufen werden dürfen. Der EuGH hält dazu ausdrücklich fest, dass die nationalen Datenschutzbehörden in ihren Prüf- und Genehmigungsbefugnissen durch Kommissionsentscheidungen nicht eingeschränkt werden dürfen.

Fraglich wird sein, ob schon bisher abseits von Safe Harbor bestehende Entscheidungen der EU-Kommission zum Datentransfer in Nicht-EU-Länder (z.B. Standardvertragsklauseln) aufgrund der Argumentation des EuGH nun ebenfalls die Gültigkeit verlieren – zumindest in Bezug auf die USA – und damit als alternative Legitimation von Datentransfers in die USA ausscheiden.

Was kann der Betriebsrat nun tun?

- Keine anlassbezogenen Zustimmungs- und Einverständniserklärungen (weder kollektiv noch individuell) im Betrieb zulassen.
- Darauf bestehen, dass allfällige Datenüberlassungen und -übermittlungen in die USA von der Österreichischen Datenschutzbehörde genehmigt werden müssen.
- Bestehende Betriebsvereinbarungen und Dienstleisterverträge zum Thema Datenverarbeitung in den USA überprüfen. Falls Safe Harbor die Rechtsgrundlage für den Datentransfer in die USA darstellt, sollte wegen geänderter Voraussetzungen neu verhandelt werden.
- Jetzt wäre die Gelegenheit günstig, eine Betriebsvereinbarung zu diversen betrieblichen Datenverwendungen zu fordern – auch im Interesse der Geschäftsführung, die dann auf konkrete, rechtlich abgesicherte Vereinbarungen zurückgreifen kann.
- Jetzt wäre ein passender Zeitpunkt, einen betrieblichen Datenschutzbeauftragten bzw. die Einsetzung eines betrieblichen Datenschutzausschusses zu fordern.
- Generell ist nun ein guter Zeitpunkt um gemeinsam mit den Beschäftigten und der GPA-djp der Geschäftsleitung zu vermitteln, dass betrieblicher Datenschutz einen wichtigen Aspekt der betrieblichen Sozialpartnerschaft darstellt. Nur mit dem Betriebsrat und der Belegschaft gemeinsam kann Datenmissbrauch hintangehalten werden.
- Anregen, dass europäische Dienstleister zur Datenverarbeitung in Anspruch genommen werden.

Was können Beschäftigte nun tun?

- Keine Einverständniserklärungen unterschreiben!
- Auskunftsbegehren, wie sie im Datenschutzgesetz vorgesehen und sogar im Verfassungsrang abgesichert sind, an den Arbeitgeber stellen; also nachfragen, *wer welche personenbezogenen Daten zu welchem Zweck wo* verarbeitet.
- Das Thema Datenschutz gemeinsam mit dem Betriebsrat (wieder) auf die betriebliche Agenda bringen; z.B. bei Betriebsversammlungen, der Forderung nach einem betrieblichen Datenschutzausschuss, einer neuen Betriebsvereinbarung …

Unter welchen Voraussetzungen dürfen Daten nun ins Ausland gesendet werden?

Der/die ArbeitgeberIn muss für den Transfer von Daten in Nicht-EU-Staaten, die keinen angemessenen Datenschutz haben, grundsätzlich die Genehmigung der Datenschutzbehörde (DSB) einholen. Erteilt wird die Genehmigung, wenn sich herausgestellt hat, dass die personenbezogenen Daten aus Österreich auch im jeweiligen Nicht-EU-Ausland gut vor Missbrauch geschützt sind.

Um die Vorgehensweise bei Datenübermittlung in Drittstaaten zu vereinfachen hat die EU-Kommission Standardvertragsklauseln entwickelt, die angemessene Garantien für die Übermittlung personenbezogener Daten von der EU in Drittländer gewährleisten sollen. Diese Klauseln betreffen nur die Datenweitergabe zwischen Auftraggebern, nicht aber zwischen Auftraggeber und Dienstleister. 2004 entschloss sich die EU-Kommission eine zusätzliche Möglichkeit der Datenübermittlung an Drittstaaten einzuführen, da die Standardvertragsklauseln von Unternehmen kaum angewendet wurden; die alternativen Standardvertragsklauseln. Sie sollen den Datentransfer erleichtern, betreffen aber ebenfalls nur die Datenweitergabe von einem Auftraggeber an einen anderen. Am 15. Mai 2010 beschloss die EU-Kommission Standardvertragsklauseln für die Überlassung personenbezogener Daten an einen Dienstleister in einem Drittstaat.

Keine Genehmigung der DSB ist laut verschiedenen Beschlüssen der EU-Kommission für bestimmte Drittstaaten erforderlich, bei denen die EU-Kommission davon ausgeht, dass sie ein angemessenes Schutzniveau für personenbezogene Daten bieten; dies sind **Norwegen, Lichtenstein, Island, Andorra, Schweiz, Argentinien, Guernsey, Jersey, Uruguay, Neuseeland, Israel, Isle of Man sowie die Färöer Inseln**.

Auch für **Kanada** gibt es eine Entscheidung der Kommission, wobei sich aber der angemessene Schutz auf einen eingeschränkteren Bereich bezieht. So wird Kanada als ein Land angesehen, das ein angemessenes Schutzniveau garantiert, wenn die Datenempfänger dem kanadischen Gesetz über personenbezogene Informationen und elektronische Dokumente unterliegen.

Für Datentransfers in die **USA** wurde ausgehandelt, dass der von den **Grundsätzen des „Sicheren Hafens"** (vorgelegt vom Handelsministerium der USA) gewährleistete Schutz dem europäischen Datenschutzniveau angemessen ist. An Unternehmen, die sich den Prinzipien des „Sicheren Hafens" unterwerfen, konnten somit Daten übermittelt werden. Im Jänner 2014 forderte das EU-Parlament, das Safe Harbor-Abkommen auszusetzen, da im Zuge der NSA-Spionage das Vertrauen in das Abkommen wesentlich erschüttert wurde. Mit seiner Entscheidung im Oktober 2015 hat der EuGH das Abkommen nun für ungültig erklärt, **sodass die Prüfung, ob in den USA ein angemessenes Datenschutzniveau gilt, wieder bei der nationalen Datenschutzbehörde liegt.**

Davon abgesehen können Daten ganz unbeschadet in Drittstaaten verwendet werden, wenn

- sie zuvor anonymisiert wurden, also kein Bezug zu einer Person mehr besteht.
- Gesetze zu dem Transfer verpflichten.
- sie für private Zwecke oder für publizistische Tätigkeiten übermittelt werden.
- ein vom/von der AuftraggeberIn mit dem/der Betroffenen oder mit einem Dritten eindeutig im Interesse des/der Betroffenen abgeschlossener Vertrag nicht anders als durch Übermittlung der Daten ins Ausland erfüllt werden kann.
- die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor ausländischen Behörden erforderlich ist und die Daten rechtmäßig ermittelt wurden.

- die Übermittlung oder Überlassung in einer Standardverordnung (§ 17 Abs 2 Z 6) oder Musterverordnung (§ 19 Abs 2) ausdrücklich angeführt ist.
- es sich um Datenverkehr mit österreichischen Dienststellen im Ausland handelt.

Wie geht's jetzt auf europäischer Ebene mit der Datenschutzgrundverordnung (DSGVO) weiter?

Grundrechtliche Bedenken liegen auch bei der derzeit im Trilog verhandelten Fassung zur DSGVO vor. Das Urteil des EuGH kann als stichhaltiges Argument verwendet werden, um die Umsetzung der Grundrechte in der Datenschutzgrundverordnung zu stärken.

In den derzeitigen Entwürfen wird z.B. der betrieblichen Mitwirkung keine große Bedeutung beigemessen. Da Mitwirkung aber zu den Grundwerten der europäischen Gemeinschaft zählt, kann dieses Urteil als strategische Unterstützung verwendet werden, um die *Mitwirkungsrechte des Betriebsrates* bei betrieblichen Datenanwendungen explizit zu verankern.

Auch die Frage nach einem wirksamen Rechtsbehelf (der ja vom EuGH in den USA als unzureichend eingestuft wurde) stellt sich in Zusammenhang mit der DSGVO. Derzeit wäre ja geplant, dass sich die örtliche Zuständigkeit für die Geltendmachung von Datenschutzrechten am Sitz der Hauptniederlassung eines Konzerns orientieren soll. Die Situation in der Max Schrems sich bei seiner facebook-Auseinandersetzung befand – nämlich nach Irland fahren zu müssen um sein Auskunftsbegehren zu stellen – wäre somit auch im neuen EU-Recht Standard. Mit Bürgernähe und zumutbarem Zugang zum Recht hätte das wenig zu tun. Ob das ein „wirksamer Rechtsbehelf" im Sinne der EU-Grundrechtecharta ist, darf bezweifelt werden.

Und was bedeutet das für TTIP?

Auch für die weiteren Verhandlungen des zwischen EU und USA derzeit hinter verschlossenen Türen besprochenen Freihandelsabkommens TTIP ist das Safe Harbour Urteil brisant. Datentransfers spielen im Freihandel eine große Rolle, schon lange gibt es Befürchtungen, dass über TTIP versucht wird, das europäische Datenschutzniveau zu untergraben. Das Urteil des EuGH erschwert dies nun und es ist möglich, dass die Verhandlungen sich dadurch verzögern. Umso wichtiger ist es weiter darauf zu pochen, dass keine Einschränkungen von Datenschutzbestimmungen in TTIP verankert werden.

Mehr Facts zu TTIP gibt's in der Abteilung EKI (Europa-Konzerne-Internationales) der GPA –djp sowie unter https://edri.org/ttip-and-digital-rights-the-booklet/