COMPLIANCEBERATER.TEAM

EuGH Urteil: Safe-Harbour gewährt kein angemessenes Datenschutz Niveau.

Heute hat der EuGH in der Rechtssache C-362/14 (Maximillian Schrems gegen die irische Datenschutz-Aufsichtsbehörde) eine weitreichende und folgenschwere Entscheidung getroffen:

> „Wahrend allein der Gerichtshof dafür zuständig ist, einen Rechtsakt der Union für ungültig zu erklären, können die mit einer Beschwerde befassten nationalen Datenschutzbehörden, auch wenn es eine Entscheidung der Kommission gibt, in der festgestellt wird, dass ein Drittland ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet, prüfen, ob bei der Übermittlung der Daten einer Person in dieses Land die Anforderungen des Unionsrechts an den Schutz dieser Daten eingehalten werden, und sie können, ebenso wie die betroffene Person, die nationalen Gerichte anrufen, damit diese ein Ersuchen um Vorabentscheidung zur Prüfung der Gültigkeit der genannten Entscheidung stellen“
>
> **EuGH, Az.: C-362/14**

Die Richtlinie über die Verarbeitung personenbezogener Daten[1] bestimmt, dass die Übermittlung solcher Daten in ein Drittland grundsätzlich nur dann zulässig ist, wenn das betreffende Drittland ein "angemessenes Schutzniveau" bzw. "ausreichendes Schutzniveau" dieser Daten gewährleistet. Ferner kann nach der Richtlinie die Kommission feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen ein angemessenes Schutzniveau gewährleistet. Dies hat die Kommission für die USA getan [2] und so US-amerikanischen Unternehmen ermöglicht, sich als Safe-Harbour zertifizieren zu lassen. Auch für andere Staaten wurde ein entsprechendes „ausreichendes Datenschutzniveau“ festgestellt.[3] Schließlich sieht die Richtlinie vor, dass jeder Mitgliedstaat eine oder mehrere öffentliche Stellen benennt, die in seinem Hoheitsgebiet mit der Überwachung der Anwendung der zur Umsetzung der Richtlinie erlassenen nationalen Vorschriften beauftragt sind („Datenschutzbehörden“).

COMPLIANCEBERATER.TEAM

Welche Auswirkungen hat diese Entscheidung auf den Datentransfer Ihres Unternehmens in die USA?

Die Entscheidung des EuGH hat die quasigesetzliche Entscheidung der Europäischen Kommission, dass bei U.S.-amerikanischen Unternehmen, welche sich dem Safe-Harbour Abkommen unterworfen haben, ein „angemessenes Datenschutzniveau“ im Sinne des § 4b BDSG besteht, relativiert und der vollständigen Prüfung der datenschutzrechtlichen Aufsichtsbehörden unterworfen:

---

[1] 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)
[2] Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments
[3] Eine ausführliche Liste mit den entsprechenden Fundstellen und gesetzlichen Grundlagen finden sie hier (http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm).

> „Aus all diesen Gründen erklärt der Gerichtshof die Entscheidung der Kommission vom 26. Juli 2000 für ungültig. Dieses Urteil hat zur Folge, dass die irische Datenschutzbehörde die Beschwerde von Herrn Schrems mit aller gebotenen Sorgfalt prüfen und am Ende ihrer Untersuchung entscheiden muss, ob nach der Richtlinie die Übermittlung der Daten der europäischen Nutzer von Facebook in die Vereinigten Staaten auszusetzen ist, weil dieses Land kein angemessenes Schutzniveau für personenbezogene Daten bietet."
>
> **EuGH, Az.: C-362/14**

Vor dieser Aussage des Gerichts, welche natürlich noch durch die ausführlichen Urteilsgründe zu bestätigen ist, dürften Datenübermittlungen auch in die U.S.A auf der Grundlage nach § 4b Abs. 2bis 6 BDSG weiterhin zulässig bleiben, bis die zuständige Datenschutzbehörde mit aller gebotenen Sorgfalt geprüft und am Ende ihrer Untersuchung entschieden hat, ob nach der Richtlinie die Übermittlung der Daten der europäischen Betroffenen in die Vereinigten Staaten auszusetzen ist, weil dieses Land kein angemessenes Schutzniveau für personenbezogene Daten bietet.

Welche Konsequenzen können sich daraus ergeben?

An dieser Stelle ist die Frage zu stellen, auf welche Rechtsvorschriften die Übermittlung personenbezogener Daten von Kunden oder Beschäftigten an andere, auch konzernangehörige Gesellschaften, gestützt werden können. Dies ist insbesondere interessant für Unternehmen, die mit Schwester- oder Muttergesellschaften im nicht-europäischen Ausland besonders eng zusammen arbeiten. Hier müssen bei der Prüfung der Zulässigkeit der Übermittlung der Daten die besonderen Anforderungen der §§ 4b Abs. 2bis 6 und 4 c BDSG erfüllt werden.

COMPLIANCEBERATER.TEAM

Hierzu stehen grundsätzlich folgende Möglichkeiten zur Verfügung:

- beim Datenempfänger ist ein angemessenes Datenschutzniveau gewährleistet (§ 4b Abs. 2, Abs. 3 BDSG), oder
- es liegt einer der Ausnahmetatbestände gemäß. § 4c Abs. 1 BDSG vor, oder
- die Übermittlung wird von der Datenschutzbehörde gem. § 4c Abs. 2 S.1 BDSG genehmigt, weil ausreichende Datenschutzgarantien erbracht werden.

<u>Angemessenes Datenschutzniveau im Drittstaat</u>

In § 4b Abs. 2 BDSG ist von der Angemessenheit des Datenschutzniveaus beim Datenempfänger die Rede. Die hier zugrunde liegende Vorschrift des Art. 25 Abs. 1 und Abs. 2 der EU-Datenschutzrichtlinie (95/46/EG) stellt jedoch nicht auf das Datenschutzniveau beim Empfänger (also z. B. der Konzernmutter), sondern auf das Drittland insgesamt, in dem der Empfänger die Daten verarbeitet und in dem die

Daten somit gesandt werden sollen und das dort herrschende Datenschutzniveau, ab. Die Europäische Kommission hat gem. Art. 25 Abs. 6 der EU-Datenschutzrichtlinie (95/46/EG) die Möglichkeit, das Bestehen eines solchen angemessenen Datenschutzniveaus festzustellen. Hiervon hat sie auch Gebrauch gemacht und solche Entscheidungen für Andorra, Argentinien, Kanada, Schweiz, Färöer Inseln, Guernsey, Israel, Isle of Man, Jersey, Neuseeland und Uruguay getroffen.[4]

Daraus folgt, dass personenbezogene Daten aus Deutschland auch ohne Überprüfung der Angemessenheit des Datenschutzniveaus übermittelt werden dürfen, sofern auch die Voraussetzungen für die Datenübermittlung im Allgemeinen erfüllt sind. Die Übermittlung bedarf nicht der Genehmigung durch die Datenschutzbehörde, da § 4b BDSG ein solches Erfordernis nicht erhält. Die Feststellungen der Europäischen Kommission für diese Länder sind auch nicht von der hier besprochenen EuGH Entscheidung betroffen. Die EuGH hat festgestellt, dass nur er die Verwerfungskompetenz besitzt, einen solchen Rechtsakt der Union für ungültig zu erklären.

Darüber hinaus hat die Europäische Kommission diese Entscheidung, dass ein ausreichendes Datenschutzniveau besteht, auch für U.S.-amerikanische Unternehmen, die sich dem Safe-Harbour Abkommen unterwerfen, getroffen. Diese Entscheidung der Kommission ist Gegenstand der hier behandelten Entscheidung des EuGH. Ob die Entscheidung des EuGH unmittelbare Auswirkungen auf die Annahme eines ausreichenden Datenschutzniveaus in diesem Zusammenhang hat, oder ob hierfür erst eine rechtsmittelfähige Entscheidung der jeweils zuständigen Datenschutzbehörde notwendig ist, die diese Annahme des ausreichenden Datenschutzniveaus negiert, wird wohl erst den ausführlichen Urteilsgründen entnommen werden können. Wie oben bereits ausgeführt, spricht die Pressemitteilung des EuGH für letztere Alternative. Daher können wohl derzeit noch Unternehmen von einem ausreichenden Datenschutzniveau im Zusammenhang mit dem Safe-Harbour Abkommen ausgehen und ihre Datenübermittlungen in die U.S.A. auf § 4b Abs. 2 bis 6 stützen.

COMPLIANCEBERATER.TEAM

Sollte jedoch diese Annahme durch gerichtliche oder behördliche Entscheidung erschüttert werden, bleiben nur noch die Alternativen des § 4c BDSG, um eine Datenübermittlung in die U.S.A. zu rechtfertigen.

Ausnahmetatbestände gem. § 4c Abs. 1 BDSG

In § 4c Abs. 1 BDSG sind Ausnahmen enthalten, aufgrund derer personenbezogene Daten an Empfänger in Drittstaaten auch ohne angemessenes Datenschutzniveau übermittelt werden dürfen.

Im Wesentlichen praxisrelevant dürften die Ausnahmetatbestände nach § 4c Abs. 1 Nr. 1 bis 3 BDSG sein, wobei hier starke Abstriche bei der wirksamen Umsetzung aufgrund starker Einschränkungen wegen der Zweckbindung der Daten zu machen sind.

[4] Eine vollständige und vor allem auch aktuelle Liste findet sich unter: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Wie so oft ist die Einwilligung des Betroffenen eine Ausnahme hier nach § 4c Abs. 1 Nr. 1 BDSG. Hier ist jedoch auf die Schwierigkeit der ausreichenden Dokumentation einer wirksamen Einwilligung hinzuweisen. Die Datenschutzbehörden erheben an der Wirksamkeit der Einwilligung häufig Zweifel, insbesondere, wenn die Einwilligung im Rahmen eines Beschäftigungsverhältnisses erteilt wurde, vielleicht noch in einer Klausel des Arbeitsvertrages, oder die im unmittelbaren Zusammenhang mit dem Beginn des Beschäftigungsverhältnisses erteilte Genehmigung. Insbesondere die Hessische Datenschutzbehörde hat hier darauf hingewiesen, dass Zweifel an der Wirksamkeit der Einwilligung von Beschäftigten in besonderer Weise angebracht sind, wenn Beschäftigtendaten in einen unsicheren Drittstaat übermittelt werden sollen.[5]

An die Einwilligung sind daher sehr hohe Anforderungen zu stellen, wenn sie als Grundlage für die Übermittlung von Beschäftigtendaten in unsichere Drittstaaten dienen soll.

Gemäß § 4c Abs. 1 Nr. 2 BDSG sind Übermittlungen in unsichere Drittstaaten erlaubt, wenn sie zur Vertragsabwicklung oder zur Durchführung vorvertraglicher Maßnahmen erforderlich sind. Hierbei ist jedoch auf die strenge Zweckbindung zu achten. Es dürfen nur solche Daten übermittelt werden, die unbedingt erforderlich sind. Dieser Ausnahmetatbestand kommt auch für Datenübermittlung in konzernbezogenen Beschäftigtenverhältnissen in Betracht. Hier ist jedoch noch einmal auf die in Abgrenzung zu den „berechtigten Interessen“ aus den §§ 27 f. BDSG in § 4c Abs. 1 Nr. 2 notwendige „Erforderlichkeit“ hinzuweisen. Die berechtigten Interessen des übermittelnden oder empfangenden Konzernunternehmens reichen für die Erfüllung des Tatbestandes nach § 4 c Abs. 1 Nr. 2 nicht aus. Die in Konzernen typischerweise verfolgten Interessen der Konzentration und des konzerninternen Outsourcings von Aufgaben zum Zwecke der Verschlankung von Arbeitsprozessen und der Gewinnung von Synergieeffekten oder auch zur Zentralisierung und Vereinheitlichung bestimmter Entscheidungen erfüllen das Merkmal der Erforderlichkeit für die Durchführung des Vertrages nicht.

COMPLIANCEBERATER.TEAM

Übermittlung wird genehmigt (EU-Standardvertragsklauseln)

Wenn das angemessene Datenschutzniveau (§ 4b Abs. 2, 3 BDSG) bzw. keiner der Kriterien des § 4c Abs. 1 BDSG erfüllt sind, muss die Datenübermittlungen auf eine andere Grundlage gestützt werden:

Zur Erfüllung der datenschutzrechtlichen Anforderung an die Übermittlung von personenbezogenen Daten in unsichere Drittstaaten stellen die von der Europäischen Kommission auf der Grundlage von Art. 26 Abs. 4 der EU-Datenschutzrichtlinie (95/46/EG) verabschiedeten Standardvertragsklauseln das in der Praxis wohl wichtigste Instrument dar.

Diese EU-Standardvertragsklausen enthalten alle erforderlichen datenschutzrechtlichen Vertragsklauseln, um die Übermittlung in einen unsicheren Drittstaat zu legitimieren. Hier ist insbesondere zu berücksichtigen, dass bei Verwendung der unveränderten Standardvertragsklauseln die Datenexporte

[5] (vgl. hierzu: Hess. Landesreg., 14. Bericht über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden, Nr. 9)

nach Ansicht der meisten Datenschutzbehörden wohl nicht genehmigungspflichtig sind. Die Datenschutzbehörden verlangen regelmäßig lediglich eine Vorlage des Vertragswerkes, um die Unveränderlichkeit der EU-Standardvertragsklausen überprüfen zu können. Ob sich hierbei jedoch im Nachgang zu der hier besprochenen EuGH-Entscheidung im Zusammenhang mit den U.S.A. Verwerfungen ergeben werden, bleibt abzuwarten.

Diese Standardvertragsklauseln bieten ein verwendbares Instrument, das häufig mit vertretbarem Aufwand umgesetzt werden kann. Gerne beraten wir Sie und Ihr Unternehmen bei der Implementierung der EU-Standardvertragsklauseln in Ihre Verträge.

Für Konzerne und größere Unternehmen können auch sogenannte Binding Corporate Rules eine sehr interessante Möglichkeit zur Erfüllung der datenschutzrechtlichen Anforderungen für die Übermittlung von Daten ins Ausland darstellen. Durch diese können die zahlreichen grenzüberschreitenden Datenverarbeitungsprozesse gebündelt und einheitlich geregelt werden. Gerne unterstützen wir Sie auch bei der Erstellung und Integration von Binding Corporate Rules.

Bei Fragen zum Thema wenden Sie sich bitte an die Teammitglieder

Rechtsanwälte Gmerek & Manthe
Wilhelm-Theodor-Römheld-Straße 14
55130 Mainz
Tel: 06131-908301-0
Fax: 06131-908301-9
E-Mail: jgmerek@complianceberater.team
jmanthe@complianceberater.team
tgmerek@complianceberater.team

COMPLIANCEBERATER.TEAM

Bei Fragen zum COMPLIANCEBERATER.TEAM wenden Sie sich bitte an

Rechtsanwalt Jürgen Möthrath
Carl-Ulrich-Straße 3
67547 Worms
Tel: 06241-93800-0
Fax: 06241-93800-8
E-Mail: jmoethrath@complianceberater.team