Humanistische Union

Netzwerk Datenschutzexpertise

Anforderungen an einen Export-Import-Vertrag für Datenübermittlungen ins Drittausland ohne angemessenen Datenschutz

In: vorgänge 212 (4/2015), S. 144-150

Am 6. Oktober 2015 hat der Europäische Gerichtshof die Übermittlung personenbezogener Daten aus der Europäischen Union (EU) in die Vereinigten Staaten von Amerika (USA) nach dem sog. Safe Harbor-Verfahren gestoppt. Ausgangspunkt war eine Vorlage des Irischen High Courts zur Frage, inwiefern bei Beschwerden nationale Datenschutz-Kontrollstellen die rechtlichen Voraussetzungen für solche Datentransfers materiell prüfen müssen. In Irland hatte der Österreicher Maximilian Schrems geklagt, der sich gegen die Speicherung von Benutzerdaten der Firma Facebook auf amerikanischen Servern wehrt. Schrems machte dabei geltend, dass nach den Enthüllungen Edward Snowdens nicht mehr davon ausgegangen werden könne, dass amerikanische Unternehmen die Bedingungen des Safe Harbor-Verfahrens erfüllen (etwa die Information der Betroffenen über die Datenweitergabe an staatliche Stellen). Das Safe Harbor-Verfahren basiert im Kern auf einer Selbstverpflichtung der betreffenden Unternehmen gegenüber dem amerikanischen Handelsministerium. Auf der Grundlage dieses Verfahrens hatte die EU-Kommission die USA mit ihrer Entscheidung 2000/520/EG vom 26.7.2000 zum „sicheren Hafen" erklärt, was seitdem die vereinfachte Datenübermittlung in die USA erlaubt. Diese Deklaration wurde vom EuGH jetzt für nichtig erklärt. Von der Entscheidung des EuGH sind tausende hierzulande tätige Unternehmen betroffen, darunter auch Firmen wie Google oder Amazon.
Dr. Thilo Weichert und Karin Schuler fassen in einem kürzlich vom Netzwerk Datenschutzexpertise veröffentlichten Gutachten die Folgen dieser Entscheidung zusammen und geben Hinweise, wie Firmen eine datenschutzkonforme Lösung entwickeln können.

1 Einleitung

Der Europäische Gerichtshof (EuGH) hat in seinem Urteil vom 06.10.2015 zur Inanspruchnahme von „Safe Harbor" durch „Facebook" entschieden, dass Datenübermittlungen von Europa in die – aus Datenschutzsicht unsicheren – Vereinigten Staaten von Amerika (USA) auf dieser rechtlichen Grundlage unzulässig sind, weil dort kein hinreichendes Schutzniveau besteht (Az. C-362/14). Das Urteil hob damit nicht nur die Safe-Harbor-Entscheidung der Kommission der Europäischen Union (EU) auf, sondern definierte rechtliche Bedingungen für personenbezogene Datenübermittlungen in einen Staat, der kein dem EU-Recht angemessenes Datenschutzniveau vorweisen kann.
Damit formulierte der EuGH auch Anforderungen an die bestehenden Standardvertragsklauseln und Binding Corporate Rules (BCRs). Die Standardvertragsklauseln und die BCRs behalten vorläufig formell weiterhin ihre Gültigkeit. Doch die von der EU-Kommission anerkannten Standardvertragsklauseln sowie wohl die meisten der von Datenschutzaufsichtsbehörden anerkannten BCRs genügen materiellrechtlich nicht den Angemessenheitskriterien des EuGH. Dies hat zur Folge, dass diese formell gültigen Regeln zurückgenommen und durch materiell-rechtlich dem EuGH-Urteil entsprechende Vertragsregeln ersetzt werden müssen.
Im Folgenden werden unter 2. die wesentlichen Aussagen des EuGH dargestellt. Unter 3. werden die Positionen der zuständigen Behörden dargestellt. Unter 4. und 5. werden vom „Netzwerk Datenschutzexpertise" Vorschläge gemacht, wie diesen Anforderungen inhaltlich in Export-Import-Verträgen entsprochen werden kann. Unter 6. wird dargestellt, wer welche Maßnahmen ergreifen muss, um zeitnah bei Datenübermittlungen in Drittstaaten grundrechtskonforme Verhältnisse herzustellen.

2 Grundrechtliche Anforderungen an grenzüberschreitende Datenübermittlungen

Der EuGH stellte klar, dass bei Datentransfers ins Ausland den Datenschutzbehörden eine zentrale Funktion zukommt: „Jede von ihnen (ist) zu der Prüfung befugt, ob bei einer Übermittlung personenbezogener Daten aus ihrem Mitgliedstaat in ein Drittland die … aufgestellten Anforderungen eingehalten werden“ (Rn. 47). Auch „der Person, von der die Eingabe stammt, … (muss) der Rechtsweg offenstehen, damit sie eine solche sie beschwerende Entscheidung vor den nationalen Gerichten anfechten kann“ (Rn. 64). Gefordert ist ein „angemessenes Schutzniveau“ im Drittland, das dem in der Europäischen Union (EU) „im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist“ (Rn. 73) und das sich „in der Praxis als wirksam erweisen“ muss (Rn. 74). Dabei sind „alle Umstände zu berücksichtigen …, die bei einer Übermittlung personenbezogener Daten in ein Drittland eine Rolle spielen“ (Rn. 75). Der Grundrechtsschutz verlangt, „dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken“ (Rn. 92). „Eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, (verletzt) den Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens“ (Rn. 94). Regelungen, die keine Möglichkeit eines Rechtsbehelfs in Bezug auf Auskunft, Berichtigung oder Löschung vorsehen, verletzen „den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz“ (Rn. 95).

3 Die bisherigen behördlichen Handlungskonzepte

Die EU-Kommission will nun mit den USA verhandeln, um bei der dortigen Datenverarbeitung das vom EuGH geforderte Datenschutzniveau zu erreichen. Die europäischen Datenschutzbehörden haben signalisiert, dass bis Ende Januar 2016 ein Ergebnis vorgelegt werden müsse.
Es dürfte klar sein, dass die USA – schon gar nicht bis dahin – nicht bereit und in der Lage sein werden, ihr Datenschutzniveau anzupassen. Hierfür bedürfte es der Einrichtung einer unabhängigen Datenschutzkontrolle und der Verabschiedung eines Datenschutzgesetzes, das den Betroffenen Ansprüche zuspricht, wie sie in Europa aus dem Grundrecht auf Datenschutz gemäß Art. 8 Europäische Grundrechte-Charta abgeleitet werden. Es ist bisher nicht ansatzweise zu erkennen, dass die US-Regierung diesen Anforderungen entsprechen will, geschweige denn wird. Derzeit ist auch nicht zu erwarten, dass das oberste US-Gericht, der Supreme Court, ein Grundrecht auf Datenschutz anerkennt, so wie dies US-Juristen seit Jahren immer wieder fordern. Bisher akzeptiert der Supreme Court lediglich „reasonable expectations of privacy“ ohne grundrechtliche Absicherung. Den Betroffenen wird damit keine Verhältnismäßigkeitsprüfung bei der Verarbeitung von personenbezogenen Daten und keine Einklagbarkeit ihrer Datenschutzansprüche zugestanden, schon gar nicht gegenüber privaten Firmen.

3.1 Die EU-Kommission

Mit Datum vom 06.11.2015 veröffentlichte die EU-Kommission eine Mitteilung an das Europäische Parlament und den Rat über den Transfer von Personendaten von der EU in die Vereinigten Staaten von Amerika (USA) gemäß Richtlinie 95/46/EG in Reaktion auf das Urteil des Europäischen Gerichtshofs im Fall C-362/14 (Schrems)(COM(2015) 566/endg.). Darin wird signalisiert, dass nach Wegfall von Safe Harbor vorläufig auf andere Instrumente, namentlich sog. „Standardvertragsklauseln“ und „Binding Corporate Rules“ (BCRs), die behördlich genehmigt worden sind, zurückgegriffen werden können, wohl wissend, dass auch diese Instrumente nicht den EuGH-Anforderungen genügen. In ihrem Statement vom 06.11.2015 weist die EU-Kommission darauf hin, dass beim Rückgriff auf Standardvertragsklauseln oder BCRs, „wenn der Datenimporteur Gründe zur Annahme hat, dass die im Empfängerland anwendbare Gesetzgebung ihn an der Erfüllung seiner vertraglichen Verpflichtungen hindert, er umgehend den Datenexporteur in der EU informieren muss. In einer solchen Situation obliegt es dem Exporteur, die nötigen angemessenen Maßnahmen zur Sicherstellung des Datenschutzes zu ergreifen. Dies können technische, organisatorische, auf das Geschäftsmodell bezogene oder rechtliche Maßnahmen sein, und bis dahin gehen, dass der Datentransfer oder der zugrundeliegende Vertrag suspendiert wird.“
Es ist nach dem EuGH-Urteil offensichtlich, dass der Datenimporteur in den USA im Konfliktfall seinen vom europäischen Grundrechtsschutz ausgehenden Pflichten nicht nachkommen kann, etwa wenn – ohne

administrative oder gerichtliche Kontrolle – US-Behörden aus Europa stammende Daten herausverlangen.

3.2 Die Datenschutzaufsichtsbehörden

Die in der Artikel-29-Arbeitsgruppe versammelten europäischen Datenschutzaufsichtsbehörden erklärten am 15.10.2015, sie würden „weiter untersuchen, wie sich das EuGH-Urteil auf andere Übermittlungsinstrumente auswirkt." Bis dahin gingen sie davon aus, „dass Standardvertragsklauseln und BCR weiter verwendet werden können. Dies wird die Datenschutzbehörden jedoch nicht davon abhalten, bestimmte Fälle zu untersuchen, zum Beispiel auf der Grundlage von Beschwerden, und ihre Befugnisse zum Schutz von Einzelpersonen auszuüben." Weitergehende Maßnahmen werden nicht angekündigt. Vielmehr wird den Unternehmen geraten, „über die Risiken nach(zu)denken, die sie bei der Datenübermittlung letztendlich eingehen, und die rechtzeitige Einführung rechtlicher und technischer Lösungen in Erwägung (zu) ziehen, um diese Risiken zu minimieren und den EU-Datenschutz-Acquis einzuhalten."
Darüber hinausgehend kündigten die deutschen Datenschutzbehörden in ihrem Positionspapier vom 26.10.2015 an, „keine neuen Genehmigungen für Datenübermittlungen in die USA auf Grundlage von verbindlichen Unternehmensregelungen (BCR) oder Datenexportverträgen (zu) erteilen."

4 Export-Import-Vertrag

Was bedeutet dies für den Datentransfer in die USA, der nicht durch die explizite Einwilligung des oder durch einen Vertrag zugunsten des Betroffenen legitimiert werden kann? Das Sinnvollste und Sicherste ist es, den Datentransfer in die USA zu stoppen und die nötigen Verarbeitungen in Europa vorzunehmen. Dies ist insbesondere für Betriebsräte, die die Verarbeitung von Beschäftigtendaten durch Betriebsvereinbarung legitimieren wollen, der Königsweg.
Sollte dies kurzfristig nicht möglich sein, besteht nur eine Möglichkeit: Der Datenexporteur in Europa muss mit dem Datenimporteur in den USA einen Vertrag abschließen, der Folgendes vorsieht: Fordert eine europäische Datenschutzaufsichtsbehörde oder ein Betroffener Auskunft über die in den USA erfolgende weitere Verarbeitung oder in Bezug auf die exportierten Daten Löschung, Sperrung oder Berichtigung, so ist der Importeur dazu zu verpflichten, dem gemäß den für den Exporteur geltenden europäischen Datenschutzvorschriften zu entsprechen. Letztlich muss der Datenimporteur umfassend auf die Einhaltung des europäischen Datenschutzrechts verpflichtet werden – einschließlich Zweckbindung, technisch-organisatorische Vorkehrungen und Betroffenenrechten. Um insbesondere die unverhältnismäßige Massenüberwachung durch die National Security Agency oder durch andere US-Behörden grundrechtlich einzuhegen, muss der Datenimporteur verpflichtet werden, den Datenexporteur hierüber umgehend zu benachrichtigen, damit dieser die nötigen Vorkehrungen ergreifen kann.
Weiterhin ist zu regeln, dass Datentransfers und diese begründende Vertragsgrundlagen suspendiert, also zumindest vorläufig gestoppt werden, wenn den nach europäischem Recht gerechtfertigten Auskunfts- und Korrekturanforderungen oder sonstigen europarechtlich begründeten Verarbeitungsbeschränkungen durch den Importeur nicht genügt wird. Als weitere Sanktionen können und sollten bei geringeren Verletzungen des EU-Rechts in den USA Vertragsstrafen-und Schadenersatzzahlungen vorgesehen werden. Ob diese Vertragsregelungen zwischen Exporteur und Importeur ausreichend sind, müssen sowohl die zuständige europäische Datenschutzbehörde wie auch der Betroffene überprüfen können. Ist dies nicht möglich, und sei es wegen einer Schweigeverpflichtung nach US-amerikanischem Recht, dann muss im Zweifel zumindest für die Zukunft der weitere Datentransfers in die USA gestoppt werden. Es dürfte kaum ein Weg daran vorbeigehen, dass der Export-Import-Vertrag mit seinen datenschutzrelevanten Inhalten veröffentlicht wird, da zumindest bei Massendatenverarbeitungen nur so die Betroffenen hiervon Kenntnis erlangen können.
Akzeptiert ein Betriebsrat einen solchen Export-Import-Vertrag als Grundlage der Verarbeitung von Beschäftigtendaten in den USA, so sollte die korrespondierende Betriebsvereinbarung folgende Anforderungen erfüllen:

Der Export-Import-Vertrag sollte als Anlage Teil der Betriebsvereinbarung (BV) werden
Das Berechtigungskonzept (ebenfalls Anlage der BV) muss auch die Rollen und Berechtigungen der US-amerikanischen Zugangsberechtigten aufführen.

Benachrichtigungen des Datenimporteurs müssen dem Betriebsrat unverzüglich mitgeteilt werden.
Die Beschäftigten sollten vollständig und verständlich über ihre Rechte als Betroffene aufgeklärt werden. Es sollte ein Prozess beim Arbeitgeber etabliert werden, der Beschäftigte bei der Wahrnehmung ihrer Rechte unterstützt.
Das verbriefte Recht des Betriebsrats, die Einhaltung abgeschlossener Betriebsvereinbarungen zu überprüfen, muss in geeigneter Weise für die US-amerikanische Datenverarbeitung konkretisiert werden. Mindestens ist ein nicht abzulehnendes Konsultations- und Fragerecht (mit resultierender Auskunftspflicht) bei namentlich zu benennenden Verantwortlichen auf US-amerikanischer Seite zu vereinbaren. Dies muss zusätzlich in den Export-Import-Vertrag aufgenommen werden.

5 Rechtsschutz

Solange in den USA kein angemessenes Datenschutzniveau besteht – einschließlich Zweckbindung, Verhältnismäßigkeitsprüfung, unabhängige Kontrolle und Rechtsschutz – müssen bei Datentransfers in die USA administrative Kontrolle und Rechtsschutz über den Exporteur gewährleistet werden. D. h. die Betroffenen müssen ihre Datenschutzrechte, auch soweit sie in den USA tangiert werden, bei der exportierenden Stelle durchsetzen können. Dies erfolgt zunächst durch Anrufung der unabhängigen für den Exporteur zuständigen Datenschutzbehörde. Diese kann das gesamte BDSG-Instrumentarium in Anspruch nehmen. Die einzige bittere Pille nach dem derzeit bestehenden Datenschutzrecht dürfte darin bestehen, dass rechtlicher Anknüpfungspunkt für die Rechtskontrolle nur der Export sein kann. D. h. bei Datenschutzverletzungen insbesondere im Bereich des Importeurs kann nur reagiert und für die Zukunft sanktioniert werden; präventiver Datenschutz kann sich zunächst nur auf die Vertragsprüfung beziehen. Unklar ist, ob der Export-Import-Vertrag vorsehen muss, dass der europäischen Datenschutzbehörde – über die Auskunftspflicht des Datenimporteurs hinausgehend – in den USA ein Kontrollrecht eingeräumt werden kann bzw. muss. Das zur Datenschutzkontrolle Gesagte gilt letztlich aber auch für Betroffenenklagen gegen Verarbeitungsprozesse in den USA vor dem für den Exporteur zuständigen Gericht sowie für Gerichtsprozesse wegen Verfügungen der Datenschutzbehörde.

6 Anstehende Aufgaben

Das Jammern der Verantwortlichen in den USA ob der oben dargestellten Rechtslage sollte sich in Grenzen halten. Die USA zeigen keinerlei Zurückhaltung bei ihren rechtlichen Restriktionen, wenn es um die Verhinderung von auch nur befürchteten Rechtsverstößen etwa durch chinesische Datenverarbeiter geht. Es ist leider so, dass es sich bei den USA in Sachen Datenschutz nicht um das „Land der Freien“, sondern um das Land der Vogelfreien handelt. Dass sich dies ändert, liegt ausschließlich in der Hand der US-Politik und der US-Rechtsprechung.
Dies darf aber die zuständigen europäischen Behörden, insbesondere die EU-Kommission und die Datenschutzbehörden, nicht dazu verleiten, die Hände in den Schoß zu legen und die Verantwortung für die Umsetzung des EuGH-Urteil anderen zuzuschreiben. Durch neue Standardvertragsklauseln auf der Grundlage der unter 4. und 5. vorgenommenen Erwägungen sowie durch entsprechende Vorgaben für einzelvertraglichen Lösungen müssen die zuständigen Behörden umgehend aktiv werden.

Autor_innen: Dr. Thilo Weichert und Karin Schuler
im Rahmen des Netzwerks Datenschutzexpertise

DAS NETZWERK DATENSCHUTZEXPERTISE ist ein in diesem Jahr gegründeter Zusammenschluss von DatenschutzexpertInnen, die durch wissenschaftliche und praxisorientierte Beiträge die öffentliche Diskussionen über Fragen des Datenschutzes sowie von Grund- und Menschenrechten in der digitalen Welt voranbringen wollen. Es versteht sich als ExpertInnennetzwerk, das mit qualifizierten Stellungnahmen und Positionstexten die Bemühungen der bestehenden in diesem Bereich aktiven NGOs sinnvoll ergänzt.
Die Stellungnahmen des Netzwerks behandeln Grundsatzfragen als auch konkrete Sachverhalte, Gesetzentwürfe oder Stellungnahmen. Sie berücksichtigen informationstechnische, rechtliche, sozioökonomische sowie weitere relevante Aspekte. Weitere Informationen & Kontakt:
http://www.netzwerk-datenschutzexpertise.de

.

---

https://www.humanistische-union.de/publikationen/vorgaenge/212-vorgaenge/publikation/netzwerk-datenschutzexpertise/
Abgerufen am: 01.10.2022