EU-Kommission billigt den EU-US-Privacy-Shield

RA Dr. Axel Spies, Morgan Lewis & Bockius, Washington DC/Frankfurt/M.

Die Abreden zum EU-US-Privacy-Shield, die nach dem wegweisenden Safe Harbor-Urteil des EuGH (ZD 2015, 549 m. Anm. Spies) die transatlantischen Datenübertragungen erleichtern sollen, haben am 12.6.2016 die letzten Hürden genommen. Einige Datenschutzbehörden und Vertreter der Art. 29-Datenschutzgruppe äußerten bis zuletzt Kritik. Die neuen Privacy Shield-Grundsätze sollen ab dem 1.8.2016 für US-Datenimporteure anwendbar sein. Diese Möglichkeit wird von zahlreichen US-Organisationen begrüßt werden, die bis zum EuGH-Urteil nach Safe Harbor zertifiziert waren. Allerdings hat die Registrierung in den USA auch einige Nachteile für die US-Unternehmen und die Datenexporteure.

Die *EU-Kommission* ist der festen Ansicht, dass die Garantien der *US-Regierung* und der US-Strafverfolgungsbehörden ausreichend sind, auch wenn sie keinen völkerrechtlichen Vertrag mit den USA vorweisen können. Die EU-Kommissare *Ansip* und *Jourova* haben erklärt, dass die Abreden zum Privacy Shield „klare und eindeutige Verpflichtungen für Unternehmen" enthalten, die sich auf die Privacy Shield-Liste setzen lassen. Die neue *Kommissions*-Entscheidung zur Angemessenheit des Privacy Shield tritt mit sofortiger Wirkung in Kraft. Sie wird mit ziemlicher Sicherheit vor Gericht angefochten werden. US-Unternehmen sollen sich gleichwohl ab den 1.8.2016 in die Liste eintragen können. Zuständig ist, wie bei Safe Harbor, das *US-Department of Commerce* (*DOC*).

I. Strengere Regelung als bei Safe Harbor

Die wichtigsten Grundsätze des neuen Privacy Shield, verglichen mit Safe Harbor, sind:

- **Strenge Verpflichtungen für die registrierten Unternehmen:** Im Rahmen der neuen Vereinbarung wird das *DOC* regelmäßige Updates vornehmen und Bewertungen der teilnehmenden Unternehmen durchführen, um sicherzustellen, dass die Unternehmen den neuen Regeln folgen und bei Weiterübermittlungen von personenbezogenen Daten an Dritte das Schutzniveau gewahrt ist.

- **Massenhafte Sammlung von Daten in den USA unter bestimmten Voraussetzungen möglich.** Die US-Behörden sichern zu, dass der Zugang der Behörden zu Zwecken der Strafverfolgung und nationalen Sicherheit Beschränkungen unterliegt. Zu diesem Zwecke gibt es neue Kontrollmechanismen, von denen EU-Bewohner profitieren sollen, sowie ein neues Streitbeilegungsverfahren in diesem Bereich. Das *Büro des Direktors der National Intelligence* sichert zu, dass die massenweise Erfassung von Daten nur unter bestimmten Voraussetzungen möglich sein soll. Bei Konflikten soll ein Ombudsmann im *US-Department of State* eine Klärung herbeiführen.

- **Besserer Schutz der Persönlichkeitsrechte:** Jedem EU-Bewohner, der der Auffassung ist, dass seine Daten im Rahmen des Privacy Shield missbraucht werden, steht ein neuer Streitbeilegungsmechanismus offen. Idealerweise hilft die datenverarbeitende Stelle selbst der Beschwerde ab. Wenn nicht, soll eine neue alternative Streitbeilegung zum Zuge kommen. Die Betroffenen können sich auch an ihre jeweilige nationale Datenschutzbehörde wenden, die dann in einem relativ komplizierten Verfahren mit der *Federal Trade Commission* (*FTC*) und dem Unternehmen zusammenarbeitet, um den Konflikt zu lösen.

- **Neuer gemeinsamer Überprüfungsmechanismus**: Eine gemeinsame jährliche Überprüfung soll die Funktionsweise des Privacy Shield überwachen, einschließlich der Verpflichtungen, der für die Strafverfolgung und nationalen Sicherheitszwecke genutzten personenbezogenen Daten. Die *EU-Kommission* und das *DOC* werden bei der Überprüfung einige *National Intelligence-Experten* aus den USA und die *EU-Datenschutzbehörden* mit zu Rate ziehen. Die *Kommission* wird auf alle anderen

Informationsquellen zurückgreifen und dann einen öffentlichen Bericht an das *EU- Parlament* und den *Rat* senden. Die *Kommission* erhofft sich von der Möglichkeit der Aussetzung des Privacy Shield, dass sie bei Konflikten zu Gunsten der Betroffenen Druck auf die *US-Regierung* ausüben kann.

II. Problematische Registrierung für US-Unternehmen beim DOC

Der Privacy Shield ist keine pauschale Rechtsgrundlage für den internationalen Datentransfer. Ohne eine Registrierung hilft er nicht weiter. Ob sich viele Unternehmen in die neue Privacy Shield-Liste freiwillig eintragen werden, ist derzeit fraglich. Die Compliance-Vorgaben der Privacy Shield-Principles sind streng und die praktische Handhabung ihrer Überwachung und Einhaltung noch unklar. Z. B. muss das Unternehmen Kontaktadressen in der EU angeben und die Dritten benennen, an die personenbezogene Daten übermittelt werden. Die neuen Privacy Shield-Principles beinhalten auch eine Reihe von neuen Inhaltsvorgaben für die Verträge zwischen dem Datenimporteur und solchen Dritten. Manche US-Unternehmen werden mit der Zweckbegrenzung für die Datenverarbeitung in den Privacy Shield-Principles und den damit einhergehenden Löschungspflichten vermutlich ihre Schwierigkeiten haben. Unternehmen, die das Privacy Shield verlassen, müssen ihre gespeicherten EU-Daten weiter nach den Privacy Shield-Principles verarbeiten oder diese löschen bzw. zurückgeben. Manche US-Unternehmen werden davor zurückscheuen, sich durch ihre Aufnahme in die Liste gegenüber der *FTC* oder dem *Department of Transportation* zu exponieren, die zu behördlichen Verfahren und/oder neuen Klagen in den USA bei Konflikten führen könnte. Für eine ganze Reihe von US-Unternehmen ist die Aufnahme in die Liste ohnehin nicht möglich, da sie nicht durch eine dieser beiden Behörden beaufsichtigt werden. Das gilt z. B. für den gesamten TK-Sektor, der von der *Federal Communications Commission* (*FCC*) überwacht wird. Manche Fragen sind vermutlich erst dann sicher zu beantworten, wenn das *DOC* interpretierende Anweisungen zur Privacy Shield-Liste veröffentlicht.

III. Pflichten der Datenexporteure unklar

Weitgehend ungeklärt ist zum gegenwärtigen Zeitpunkt, welche Verpflichtungen die Datenexporteure in der EU/EWR bei einer Datenübermittlung an ein Unternehmen haben, das sich auf der Privacy Shield-Liste über das *DOC* eingetragen hat. Z. B. ob § 11 BDSG zur Auftragsdatenverarbeitung mit seinem Anforderungskatalog weiterhin wie bei der Übermittlung an einen Dienstleister in Deutschland gilt. Wann müssen die Datenexporteure dafür gerade stehen, dass sich die Datenimporteure nicht an die anwendbaren Regeln (z. B. über die Zweckbindung oder die Weitergabe an Dritte) halten? Sind die Datenexporteure in ihrem Heimatland haftbar, wenn die Empfänger in den USA doch massenweise Daten an US-Behörden übermitteln (wozu die Empfänger nach höherrangigem US-Recht jetzt oder möglicherweise künftig verpflichtet sind) oder wenn sie Dritten unrechtmäßigen Zugang zu den Daten gewähren? Welche Dokumentations- und Mitteilungspflichten haben die Datenexporteure vor dem Datenexport in die USA? Wann muss der Betriebsrat vorab zustimmen? Was gilt für die Umsetzung der neuen Regelungen der DS-GVO (z. B. für das Recht auf Vergessenwerden)? Die *Art. 29-Datenschutzgruppe* will sich zu den neuen Regeln erst noch äußern. Dann wird sich zeigen, ob die Datenschutzbehörden zu diesen Themen eine einheitliche Linie vertreten.

IV. Alternative EU-US-Datenübertragungen und Brexit

Es gibt für diese Unternehmen zum Glück weiterhin andere Optionen, persönliche Daten an die USA zu übertragen, wie das Mittel der ausdrücklichen Zustimmung, Verwendung von Binding Corporate Rules (BCRs) oder vornehmlich die von der EU zugelassenen Mustervereinbarungen (EU-Standardvertragsklauseln – Standard Contractual Clauses). Letztere werden gerade nach dem *EuGH*-Urteil zu Safe Harbor von Unternehmen häufig verwendet. Ihre Verwendung wurde vor kurzem von *Schrems* in einem neuen Verfahren in Irland (ZD-Aktuell 2016, 05167) in Frage gestellt, das vermutlich der *EuGH* entscheiden wird. Damit hätte der *EuGH* zum zweiten Mal nach Safe Harbor die Möglichkeit, in die Regeln für den Datenexport in die USA korrigierend einzugreifen.

Auch der Brexit wirft seine Schatten voraus: Nach dem Brexit-Referendum Großbritanniens wird der Privacy Shield erst einmal auch für GB-US-Transfers wirksam. Erst wenn die neue Premierministerin *May* eine formelle Mitteilung nach Art. 50 des Lissabon-Vertrags zum Austritt in Brüssel einreicht, stellt sich die Frage nach der Zukunft des Privacy Shield. In diesem Fall müssen die *britische Regierung* und die *US-Regierung* entscheiden, ob sie die gleichen Beschränkungen für die grenzüberschreitende Datenübermittlungen behalten oder eine alternative Lösung, wie einen neuen GB-US-Privacy-Shield, suchen wollen. In diesem Fall wird sich für die *britische Regierung* dieselbe Frage wie für die Datenschützer sonst in der EU/EWR stellen, wie eine Massenüberwachung und eine anlasslose Datensammlung der Behörden begrenzt werden kann. Welche Regeln dann für den Datenfluss aus der EU nach Großbritannien gelten (z. B. ein vergleichbarer EU-GB-Privacy -Shield), ist derzeit unklar.

Weiterführende Links

Vgl. auch ZD-Aktuell 2016, 05230; ZD-Aktuell 2016, 05233; zu Standardvertragsklauseln *Schmitz/von Dall'Armi,* ZD 2016, 217; ZD-Aktuell 2016, 05171; *Filip*, ZD-Aktuell 2016, 05108; zum Privacy Shield *Weichert*, ZD 2016, 209; *Smagon*, ZD 2016, 55 und *Schreiber/Kohm*, ZD 2016, 255.