ANALYSE UND BEWERTUNG DES EU-U.S. PRIVACY SHIELD

Safe-Harbor-Nachfolgeregelung gewährleistet kein angemessenes Schutzniveau für in die Vereinigten Staaten von Amerika übermittelte personenbezogene Daten

4. April 2016

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Digitales und Medien

Markgrafenstraße 66
10969 Berlin

digitales@vzbv.de

Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

INHALT

I. HINTERGRUND

Gemäß der EU-Datenschutzrichtlinie 95/46/EG dürfen personenbezogene Daten nur in Drittstaaten außerhalb der Europäischen Union übermittelt werden, wenn diese über ein angemessenes Datenschutzniveau verfügen. Dies ist bei den USA nicht der Fall. Damit Unternehmen aber dennoch persönliche Daten unkompliziert in die USA übermitteln können, traf die EU-Kommission im Jahr 2000 die „Safe-Harbor-Entscheidung". Demnach war die Übermittlung der Daten legal, wenn sich US-Unternehmen dafür zu grundlegenden Datenschutzregelungen verpflichteten und in eine entsprechende Liste des US-Handelsministeriums eintragen ließen.

In den Folgejahren kam immer wieder Kritik am Safe-Harbor-Programm auf. Beispielsweise zeigten Untersuchungen wiederholt, dass Unternehmen zwar angaben, dem Programm beigetreten zu sein, ohne aber in der Praxis die Grundsätze einzuhalten. Auch fanden sich auf der Liste des US-Handelsministeriums Unternehmen, die gar nicht mehr Mitglied des Programms waren.[1]

Als Reaktion auf die Kritik an Safe Harbor und die exzessive Überwachung durch die US-Geheimdienste, evaluierte die EU-Kommission das Programm und veröffentlichte im November 2013 ihre Erkenntnisse. Sie übermittelte der US-Administration 13 Empfehlungen, die bis Sommer 2014 umzusetzen seien, sonst würde sich die EU eine Kündigung des Programms vorbehalten. Seither wird über ein Nachfolgeabkommen verhandelt.[2]

Im Oktober 2015 erklärte der Europäische Gerichtshof (EuGH) die Safe-Harbor-Entscheidung für ungültig. Primär kritisierte der EuGH, dass sich die EU-Kommission nicht ausreichend mit den einschlägigen Gesetzen in den USA sowie der zur Gewährleistung der Einhaltung dieser Regeln dienenden Praxis befasst hatte und nicht feststellte, dass die USA aufgrund ihrer innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein angemessenes Schutzniveau gewährleisten. Außerdem seien die Ausnahmen für nationale Sicherheit in Safe Harbor zu weit gefasst und den Betroffenen würde kein ausreichender Rechtsschutz gegen Maßnahmen von US-Behörden eröffnet werden.[3]

Im Februar 2016 veröffentlichte die EU-Kommission ihre Vorschläge für ein Nachfolgeabkommen mit den Namen EU-U.S. Privacy Shield (folgend Privacy Shield). Neben dem Entwurf des Angemessenheitsbeschlusses wurden verschiedene Annexe veröffentlicht, die in erster Linie aus den so genannten Privacy-Shield-Prinzipien des U.S. Department of Commerce (DoC) sowie Briefen der US-Administration bestehen, die ein angemessenes Datenschutzniveau in den USA garantieren sollen.[4]

Die folgende Analyse der Dokumente bezieht sich bewusst nur auf die Maßnahmen und Garantien, die den Schutz der personenbezogenen Daten von Betroffenen in ihrer

---

[1] Galexia (2008): The US Safe Harbor - Fact or Fiction? Seite 4ff http://www.galexia.com/public/research/articles/research_articles-pa08.html

[2] EU-Kommission (2013): Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA http://europa.eu/rapid/press-release_MEMO-13-1059_de.htm

[3] Court of Justice of the European Union (2015): http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

[4] EU-Kommission (2016): Europäische Kommission stellt EU-US-Datenschutzschild vor http://europa.eu/rapid/press-release_IP-16-433_de.htm

Rolle als Verbraucher sicherstellen sollen und nicht auf die Fragen, die im Rahmen der Übermittlung von Beschäftigtendaten auftreten oder die durch den Zugriff der US-Behörden auf diese Daten aufgeworfen werden. Allerdings bezweifelt der Verbraucherzentrale Bundesverband (vzbv) dennoch, dass – vor dem Hintergrund der unverändert praktizierten anlasslosen Massenüberwachung durch die US-Geheimdienste – die Entscheidung der EU-Kommission vor dem EuGH Bestand haben wird. Entsprechende Klagen wurden bereits durch mehrere Akteure angekündigt. Unternehmen und Verbraucherinnen und Verbraucher[5] werden sich somit auf eine mehrjährige Rechtsunsicherheit einstellen müssen.

II. ANALYSE

1. VERPFLICHTUNG DER US-UNTERNEHMEN

US-Unternehmen, die personenbezogene Daten auf Basis des Privacy Shields übertragen wollen, müssen sich auf die Einhaltung folgender Datenschutzprinzipien gegenüber dem DoC verpflichten:

1.1 Informationspflicht („notice“)

- Unternehmen müssen verständlich über Kernelemente ihrer Datenverarbeitung informieren (beispielsweise u.a. die Art der Daten, Zwecke der Verarbeitung, Hinweis auf Recht auf Zugang und Wahlmöglichkeiten, Bedingungen für die Datenweitergabe und Verantwortlichkeit).
- Unternehmen müssen ihre Datenschutzbestimmungen mit einem Hinweis auf ihre Teilnahme am Privacy Shield veröffentlichen.
- Sie müssen auf die Privacy-Shield-Webseite des DoC und auf unabhängige Schlichtungsstellen verweisen.
- Die Informationen müssen zur Verfügung gestellt werden, wenn es praktikabel ist („as soon thereafter as is practicable“), aber bevor die Daten an Dritte weiter gegeben werden oder der Zweck geändert werden soll.

1.2 Wahlmöglichkeiten („choice“)

- Betroffene sollen der Verwendung ihrer Daten zu Werbezwecken widersprechen können.
- Betroffene sollen widersprechen können, wenn Unternehmen ihre Daten an Dritte weitergeben oder für wesentlich andere („materially different“) Zwecke verarbeiten wollen.
- Betroffene sollen ihre Einwilligung geben müssen, bevor sensitive Daten an Ditte übermittelt werden oder die Verarbeitungszwecke geändert werden.

[5] Die gewählte männliche Form bezieht sich immer zugleich auf weibliche und männliche Personen. Wir bitten um Verständnis für den weitgehenden Verzicht auf Doppelbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

1.3 Datenweitergabe („accountability for onward transfer“)

- Unternehmen müssen Richtlinien und Verfahren einrichten, mit denen sie sicherstellen, dass Dritte die Daten nur zu bestimmten und begrenzten Zwecken verwenden.
- Unternehmen müssen mit Dritten Verträge schließen, nach denen diese das gleiche Datenschutzniveau garantieren, wie es durch die Prinzipien festgelegt ist.

1.4 Sicherheit („security“)

- Unternehmen müssen vernünftige und dem Risiko angemessene Maßnahmen („reasonable and appropriate measures … taking into due account the risks“) zur Datensicherheit treffen.

1.5 Integrität der Daten und Zweckbindung („data integrity and purpose limitation“)

- Unternehmen dürfen nur Daten verarbeiten, die relevant („relevant“) sind, um die Verarbeitungszwecke zu erreichen.
- Die Daten müssen korrekt, vollständig und aktuell sein.
- Ein Unternehmen darf keine personenbezogenen Daten auf Art und Weisen verarbeiten, die mit den Zwecken unvereinbar sind, für die sie ursprünglich gesammelt wurden.

1.6 Auskunftsrecht („access“)

- Betroffene haben das Recht Informationen darüber zu erhalten, ob ein Unternehmen personenbezogene Daten verarbeitet, die sie betreffen. Unternehmen müssen diese Informationen innerhalb eines angemessenen Zeitraums und für eine nicht-exzessive („non-excessive“) Gebühr zur Verfügung stellen.
- Betroffene haben das Recht auf Auskunft, Berichtigung, Änderung oder Löschung ihrer Daten, wenn diese nicht korrekt sind oder entgegen der Datenschutzprinzipien verarbeitet wurden, es sei denn, dies würde einen übermäßigen Aufwand für das Unternehmen bedeuten.

1.7 Durchsetzung („recourse, enforcement and liability“)

- Unternehmen müssen gewährleisten, dass ihre Datenschutzbestimmungen den Datenschutzprinzipien entsprechen und diesen auch gefolgt wird. Dies kann beispielsweise über jährliche Selbstzertifizierung erfolgen.
- Unternehmen müssen sicherstellen, dass sie Beschwerden von europäischen Betroffenen rasch (innerhalb von 45 Tagen) kostenfrei bearbeiten.
- Unternehmen müssen alternative Schlichtungsstellen benennen, die Konflikte lösen sollen.

2. AUFSICHT UND DURCHSETZUNG DURCH DAS U.S. DEPARTMENT OF COMMERCE UND DIE FEDERAL TRADE COMMISSION

- Das DoC wird eine Privacy-Shield-Liste mit den teilnehmenden Unternehmen veröffentlichen und aktuell halten. Das DoC kann selbständig überprüfen, ob falsche Angaben gemacht werden und Hinweisen der EU-Datenschutzbeauftragten folgen.
- Das DoC kann, beispielsweise durch Fragebögen, Überprüfungen durchführen, wenn es Beschwerden oder andere glaubhafte Hinweise erhält, dass sich ein Unternehmen nicht an die Datenschutzprinzipien hält.
- Verstößt ein Unternehmen dauerhaft gegen die Vorgaben des DoC, kann es von der Liste gelöscht werden. Widersetzt es sich den Anordnungen einer Aufsichtsbehörde, kann die Löschung dauerhaft sein.
- Wird ein Unternehmen von der Liste gelöscht, weil es sich nicht an die Prinzipien hält, muss es die Daten löschen. Außerdem darf es nicht mehr den Anschein erwecken, als würde an am Privacy Shield teilnehmen.
- Die Federal Trade Commission (FTC) bleibt primäre Durchsetzungsbehörde und soll Beschwerden (von Betroffenen, Schlichtungsstellen, dem DoC oder EU-Datenschutzbeauftragten) mit hoher Priorität bearbeiten. Sie soll Schnittstellen zu den EU-Datenschutzbeauftragten einrichten.
- Die FTC ist berechtigt (aber nicht verpflichtet) Überprüfungen vorzunehmen und Sanktionen (gegen unfaire und trügerische Geschäftspraktiken) zu verhängen. Die FTC kann Unterlassungsverfügungen erlassen und vor US-Gerichten klagen. Außerdem kann die FTC Bußgelder verhängen, wenn gegen eine Unterlassungsverfügung oder eine Anordnung eines Gerichts verstoßen wird.
- Unternehmen können sich freiwillig der Aufsicht durch EU-Datenschutzbeauftragte unterwerfen. In diesem Fall müssen sie auf deren Anfragen reagieren und den Anordnungen der Behörden zur Abhilfe oder des Ausgleichs Folge leisten. Die EU-Datenschutzbeauftragten können dabei vom DoC und der FTC unterstützt werden. Verstöße sollen sanktioniert werden.

3. EINZELBESCHWERDEN UND RECHTSSCHUTZ

- Betroffene können sich bei Beschwerden direkt an die Unternehmen wenden. Die Unternehmen müssen die dafür notwendigen Informationen bereitstellen. Die Beschwerden müssen innerhalb von 45 Tagen bearbeitet werden.
- Unternehmen müssen alternative Schlichtungsstellen („independent dispute resolution body“ bzw. „independent recourse mechanism“) in den USA oder der EU benennen, an die sich Betroffene kostenlos wenden können. Sanktionen durch diese Schlichtungsstellen sollen ausreichend streng („sufficiently rigorous“) sein (z.B.: Veröffentlichung der Schlichtungsergebnisse, Löschung der Daten, Entfernung eines Siegels und Unterlassung).
- Betroffene können sich an ihre nationalen EU-Datenschutzbeauftragten wenden. Das DoC wird Verfahren einrichten, über die die EU-Datenschutzbeauftragten Beschwerden weiterleiten und deren Verlauf verfolgen können. Solche Beschwerden sollen innerhalb von 90 Tagen bearbeitet werden. Über dieses Verfahren soll es jährliche Berichte geben.
- Sollten alle vorherigen Beschwerdemechanismen erfolglos oder für den Betroffenen unbefriedigend verlaufen sein, können diese sich an ein Schiedsgericht namens „Privacy Shield-Panel“ wenden („arbitration option“). Das Schiedsgericht besteht

aus einem Pool von 20 Schiedsrichtern, die durch das DoC und der EU-Kommission benannt werden. Die Parteien des Rechtsstreits wählen aus diesem Pool einen oder drei Schiedsrichter aus. Die genauen Prozeduren des Schiedsgerichtsverfahrens sollen durch die EU-Kommission und das DoC vereinbart werden. Das Schiedsgerichtsverfahren soll in den USA stattfinden, der Betroffene kann über (Video-)Telefonie teilnehmen. Kostenlose Übersetzungen sollen in Ausnahmefällen möglich sein, soweit die Kosten nicht zu hoch werden. Der Betroffene kann bei der Vorbereitung durch einen EU-Datenschutzbeauftragten unterstützt werden, dieser darf aber nicht an dem Verfahren selbst teilnehmen. Sollte ein Anwalt bestellt werden, müssen die Parteien diesen selbst bezahlen, allerdings soll es einen Fond geben, der durch das DoC eingerichtet und durch die Unternehmen finanziert wird, der die Kosten bis zu einer Höchstgrenze (die durch die EU-Kommission und das DoC festgelegt wird) übernimmt. Das Schiedsgericht kann nur für den konkreten Einzelfall nicht-monetäre, gerechte Linderung („non-monetary equitable relief“) (wie individueller Zugang, Korrektur, Löschung oder Rückgabe der Daten) herbeiführen. Die Entscheidungen sind bindend, können aber vor den Gerichten des Bezirks, in denen das Unternehmen seinen Sitz hat, angefochten werden.

- Betroffene können keinen Schadenersatz im Rahmen des Schiedsgerichtsverfahrens erhalten. Mit Verweis auf das Verfahrensergebnis steht ihnen die Option offen, Schadenersatz im Rahmen von zivilrechtlichen Klagen vor den regulären US-Gerichten zu erstreiten.

4. JÄHRLICHE ÜBERPRÜFUNG

- Die Privacy-Shield-Entscheidung soll einer jährlichen Überprüfung unter Berücksichtigung aller beteiligten Institutionen unterliegen.
- In diesem Rahmen wird die EU-Kommission umfassende Informationen vom DoC über die aufgetretenen Beschwerden und durchgeführten Überprüfungen erhalten und auch andere Quellen (Presse, NGOs, Informationsfreiheitsanfragen, etc.) berücksichtigen.
- Auf dieser Basis wird die EU-Kommission einen jährlichen Bericht erstellen.
- Sollten beispielsweise Beschwerden systematisch nicht ausreichend verfolgt werden, kann die EU-Kommission ihre Entscheidung korrigieren oder revidieren.

III. BEWERTUNG

1. ALLGEMEINES

- Privacy Shield basiert nicht auf Gesetzen oder Abkommen, sondern lediglich auf Zusagen in Briefen der US-Administration.
- Die Dokumente sowie die Verfahren sind undurchsichtig und kompliziert. Eine klare Ordnung der Bestimmungen ist nicht zu erkennen. Teilweise werden beispielsweise in den Dokumenten der US-Administration unterschiedliche Terminologien für identische Verfahren verwendet (zum Beispiel „independent dispute resolution body“ vs. „independent recourse mechanism“).

2. VERPFLICHTUNG DER US-UNTERNEHMEN

Die Prinzipien sind vage, lassen viel Spielraum und werden nach US-Recht ausgelegt:

- Wenige Vorgaben zu Grundprinzipen des Datenschutzes (z.B. der Rechtmäßigkeit der Verarbeitung) und zu verschiedenen Verarbeitungsschritten (wie Erhebung, Nutzung, Speicherung).
- Daten dürfen soweit verarbeitet werden, wie sie zum Erreichen „von Verarbeitungszwecken“ „relevant“ und nicht wie im EU-Recht „für einen Zweck erforderlich“ sind.
- Regelungen zur Zweckbindung und Datenweitergabe sind schwach: Zwecke müssen nicht eindeutig sein und können sehr breit definiert werden. Verbraucher haben lediglich ein Widerspruchsrecht, wenn Daten an Dritte weitergegeben oder für einen „wesentlich“ anderen Zweck verarbeitet werden sollen.
- Informationspflichten der Unternehmen im Vergleich zu EU-Regelungen sind zu schwach (z.B. keine Angaben über Quellen der Daten). Informationen müssen erst gegeben werden, bevor die Daten an Dritte weiter gegeben werden oder der Zweck geändert werden soll.
- Der Auskunftsanspruch wird stark eingeschränkt. Zugang zu Daten ist nicht grundsätzlich kostenlos. Zugang kann auch verweigert werden, wenn die Kosten zu hoch sind, bei Geschäftsgeheimnissen oder wenn Daten lediglich zu wissenschaftlichen / statistischen Zwecken verarbeitet werden.
- Es bestehen kaum Vorgaben zur Datensicherheit.

3. AUFSICHT UND DURCHSETZUNG DURCH DAS U.S. DEPARTMENT OF COMMERCE UND DIE FEDERAL TRADE COMMISSION

- Keine klaren Vorgaben für Selbstzertifizierung oder externe Gutachten.
- FTC und besonders DOC sind Teil der Exekutive und damit nicht unabhängig.
- Durchsetzung / Maßnahmen durch die FTC und DOC scheinen unverbindlich („kann“ aber nicht „muss“).

4. EINZELBESCHWERDEN UND RECHTSSCHUTZ

- Beschwerdeverfahren sind umständlich, kompliziert, äußerst langwierig und richten sich an US-Recht aus.
- Das Schiedsgerichtsverfahren ist für den Verbraucher nachteilig und aufgrund der Ausgestaltung quasi nicht in zumutbarer Weise ein gangbarer Weg (in den USA, Englisch, keine Vertretung durch europäische Datenschutzbeauftragte, Anwaltskosten, US-Regeln).
- Die Schiedsrichter werden durch die Exekutive benannt und sind somit nicht unabhängig.
- Ergebnisse des Schiedsgerichtsverfahrens sind nur auf den Einzelfall bezogen und beinhalten keine klaren, wirksamen Sanktionen.
- Der Weg vor die Gerichte ist umständlich (beziehungsweise erst möglich, wenn die anderen Verfahren durchlaufen wurden? An dieser Stelle sind die Dokumente nicht eindeutig).

IV. FORDERUNGEN

Auch abgesehen von der bislang ungelösten Problematik der Massenüberwachung durch die US-Sicherheitsdienste genügt nach Ansicht des vzbv der EU-U.S. Privacy Shield auch im nicht-öffentlichen Bereich nicht dem europäischen Recht und darf daher in dieser Form nicht verabschiedet werden. Mindestanforderungen an einen akzeptablen Safe-Harbor-Nachfolger aus Verbrauchersicht wären:

1. VERPFLICHTUNGEN DER US-UNTERNEHMEN

- Die Prinzipien, die dem Privacy Shield zugrunde liegen, müssen geschärft und im Kern dem europäischen Datenschutzrecht gleichwertig sein. Den Grundregeln des EU-Datenschutzes (Rechtmäßigkeit, Einwilligung, Zweckbindung, Erforderlichkeit und Datensparsamkeit, Transparenz und Betroffenenrechte, Datensicherheit und Kontrolle) muss daher auch im Privacy Shield bzw. über einen entsprechenden Rechtsrahmen verbindlich entsprochen werden.
- Der Verarbeitungszweck muss eindeutig sein und für Zweckänderungen müssen klare Kriterien definiert werden. Lediglich die Möglichkeit des nachträglichen Widerspruchs, wenn Daten an Dritte weitergegeben oder für einen „wesentlich“ anderen Zweck verarbeitet werden sollen, ist nicht ausreichend.
- Informationen müssen dem Verbraucher vor Beginn der Datenverarbeitung zur Verfügung gestellt werden. Die Ausübung seiner Rechte (wie das Auskunftsrecht) muss für den Betroffenen grundsätzlich kostenlos sein und darf nicht unverhältnismäßig beschränkt werden.

2. AUFSICHT UND DURCHSETZUNG DURCH DAS U.S. DEPARTMENT OF COMMERCE UND DIE FEDERAL TRADE COMMISSION

- Da im Rahmen des Privacy Shields in erster Linie an einer Selbstzertifizierung festgehalten werden soll, müssen wirksame Überwachungs- und Kontrollmechanismen geschaffen werden, die es erlauben, in der Praxis etwaige Verstöße zu ermitteln und zu ahnden. Die Veröffentlichung der Datenschutzbestimmungen und eine reine Erklärung der Unternehmen, sich an die Privacy-Shield-Prinzipien zu halten, dürfen nicht ausreichend sein. Die Unternehmen sollten hingegen wirksam belegen müssen, dass sie diese Prinzipien in der täglichen Praxis tatsächlich einhalten, bevor sie auf die Privacy-Shield-Liste aufgenommen werden.
- Es muss eine effektive Kontrolle und Rechtsdurchsetzung durch tatsächlich unabhängige US-Aufsichtsbehörden sichergestellt werden, die auch Einzelbeschwerden von Verbrauchern vehement verfolgen.
- Bei einem festgelegten Anteil der Unternehmen sollten anlassunabhängige vor-Ort-Kontrollen durch diese US-Aufsichtsbehörden durchgeführt werden. Außerdem sollte immer eine eingehende Überprüfung eines Unternehmens durch die US-Aufsichtsbehörden erfolgen müssen, sobald eine europäische Datenschutzbehörde die Einhaltung der Bestimmungen bezweifelt.

3. EINZELBESCHWERDEN UND RECHTSSCHUTZ

- Den Betroffenen muss die Möglichkeit effektiver Rechtsschutzmechanismen eröffnet werden. Hinsichtlich der alternativen Schlichtungsverfahren müssen verbindliche Qualitätskriterien festgelegt werden, insbesondere in Bezug auf die Unabhängigkeit und Unparteilichkeit der Schlichtungsstellen (beispielsweise durch eine paritätische Besetzung der Träger unter Beteiligung der Verbraucherverbände), der Transparenz des Verfahrens, der Aufsicht über die Stellen sowie der möglichen Sanktionen.
- Schiedsstellen dürfen nicht nur in den USA angesiedelt sein, auch in Europa muss es solche Stellen mit klaren und transparenten Verfahrensvorgaben geben, die an europäischem Recht ausgerichtet sind. Betroffene müssen mit geringem Aufwand und ohne wesentliches Kostenrisiko an den Schiedsverfahren teilnehmen und sich dabei durch europäische Datenschutzbeauftragte vertreten lassen können. Darüber hinaus müssen auch bei diesen Einrichtungen klar definierte, wirksame Sanktionen ausgesprochen werden können, wenn gegen Verfahrensvorschriften verstoßen wird.
- In jedem Fall müssen europäische Verbraucher stets – also auch ohne zuvor eine Schlichtungsstelle oder ein Schiedsgericht angerufen zu haben – vor europäischen Gerichten ihre Rechte (wie das Auskunftsrecht oder das Recht auf Löschung der Daten) einklagen sowie Schadenersatz erstreiten können, wenn Privacy-Shield-zertifizierte Unternehmen ihre Daten auf eine unzulässige Weise verarbeiten.