EU – U.S. Privacy Shield – das neue „Datenschutzschild" ersetzt die „Safe Harbor"-Regelung

Im Oktober 2015 erklärte der Europäische Gerichtshof (EuGH) die „Safe-Harbor-Regelung", auf deren Grundlage bislang viele in Europa ansässige Unternehmen ihren Datenexport in die USA hatten laufen lassen, für ungültig. Die Existenz eines angemessenen, d.h. gleichwertigen, Datenschutzniveaus in den USA sei durch die Europäische Kommission nicht festgestellt worden. Im Hinblick auf die 2013 bekannt gewordenen umfassenden Eingriffsmöglichkeiten U.S.-amerikanischer Behörden sei der Zugriff auf in den USA (auch) bei privaten Unternehmen gespeicherte personenbezogene Daten (im Folgenden: „Daten") nicht auf absolut notwendige Maßnahmen beschränkt. Vielmehr erfolgen solche Eingriffe – entgegen des in der EU geltenden Rechts – ohne Differenzierung, Einschränkung oder Ausnahmen. Zudem gebe es keine wirksamen Rechtsschutzmöglichkeiten für betroffene EU-Bürger.

Nach umfassenden Verhandlungen mit den zuständigen U.S.-amerikanischen Behörden über rechtliche Garantien und künftiges Vorgehen, hat die Europäische Kommission am 12.07.2016 eine neue Entscheidung zur Angemessenheit des Datenschutzniveaus in den USA verabschiedet. Der als „Privacy Shield" oder auch „Datenschutzschild" eingeführte Beschluss ist seit dem 01.08.2016 in Kraft. Der Beschluss stellt nunmehr wieder die dritte Rechtsgrundlage für den Datentransfer in die USA neben den verbindlichen unternehmensinternen Richtlinien (*binding corporate rules, BCR)* und dem Abschluss von Verträgen basierend auf den sog. Standardvertragsklauseln dar. Voraussetzung ist, dass sich empfangende U.S.-amerikanische Unternehmen entsprechend des „Privacy Shield" haben zertifizieren lassen.

Wie funktioniert das Privacy Shield?

Das Privacy Shield formuliert sieben Datenschutzgrundsätze: Informationspflicht, Datenintegrität und Zweckbindung, Bestehen einer Wahlmöglichkeit, Sicherheit, Auskunftsrecht, Rechtsschutz, Durchsetzung und Haftung, sowie Verantwortlichkeit für die Weitergabe von personenbezogenen Daten. Zudem werden weitere sog. Rahmengrundsätze zur Durchführung bestimmt.

Im Ganzen soll die Verpflichtung zur Einhaltung dieser Grundsätze ein Datenschutzniveau ergeben, das mit dem im europäischen Wirtschaftsraum herrschenden vergleichbar ist. Soweit eine konkrete Verarbeitung unter EU-Recht fällt, wird dessen Anwendbarkeit nicht durch das Privacy Shield verdrängt.

U.S.-amerikanische Unternehmen, die auf Grundlage des Privacy Shields Daten aus der EU empfangen möchten, müssen sich zertifizieren. Das U.S.-Handelsministerium führt eine Liste („Datenschutz-Liste") mit allen zertifizierten Unternehmen, die öffentlich einsehbar ist (https://www.privacyshield.gov/welcome). Die Unternehmen müssen sich jährlich rezertifizieren. Ebenfalls öffentlich einsehbar ist, wenn ein Unternehmen nicht mehr zertifiziert ist, d.h. seine Zertifizierung nicht erneuert hat oder wegen Verstößen gegen das Privacy Shield gestrichen wurde. Die Einhaltung der Grundsätze unterliegt der Kontrolle des U.S.-Handelsministeriums. Dieses kann ggf. selbst rechtliche Schritte gegen Unternehmen einleiten oder da Verfahren an eine im Einzelfall zuständige andere Behörde abgeben.

Die Wirksamkeit der Privacy-Shield-Mechanismen wird jährlich überprüft. Beteiligt hieran sind jedenfalls das U.S.-Handelsministerium und die *Federal Trade Commission,* sowie die EU-Kommission und betroffene Datenschutzbehörden.

Wie funktioniert die Zertifizierung?

Bei der Zertifizierung handelt es sich um eine Selbstzertifizierung, d.h. das Unternehmen verpflichtet sich gegenüber dem amerikanischen Handelsministerium zur Einhaltung der normierten Grundsätze und beantragt die Aufnahme auf die Datenschutz-Liste. Um aufgenommen zu werden, muss es insbesondere den Kontrollbefugnissen bestimmter U.S.-amerikanischer Behörden unterliegen, öffentlich – d.h. in der Regel auf der Unternehmens-Website – erklären, die Grundsätze einzuhalten und seine entsprechenden Datenschutzbestimmungen offenlegen. Schließlich muss es sich auch dementsprechend verhalten.

Welche rechtlichen Verbesserungen bietet das Privacy Shield für Betroffene?

Alle Personen, deren Daten im europäischen Wirtschaftsraum verarbeitet und in die USA zu einem Privacy-Shield-zertifizierten Unternehmen übermittelt werden, erhalten durch das Privacy Shield neue Rechtsschutzmöglichkeiten.

In den USA bestehen für Nicht-U.S.-Bürger vom Grundsatz her weniger Rechtsschutzmöglichkeiten gegen Eingriffe in ihr Grundrecht auf Datenschutz (bzw. nach amerikanischem Verständnis „right to privacy“) als für U.S.-Amerikaner. Grund hierfür ist, dass U.S.-amerikanische Verfassungsrechte nur für U.S.-Bürger gelten. Nicht-U.S.-Bürgern bleibt nur der privatrechtliche Klageweg auf Grundlage einiger U.S.-amerikanischer Gesetze. Diese setzen jedoch in der Regel den Eintritt eines tatsächlichen Schaden (über die Tatsache dass – unberechtigt – auf private Daten zugegriffen wurde hinaus) voraus und sind zudem kostspielig, d.h. nicht für jedermann zugänglich.

Das Privacy Shield bietet nun verschiedene Rechtsschutzmöglichkeiten. Insbesondere wurde ein öffentlicher Ombudsmechanismus eingeführt, der in Europa lebenden Personen Zugang zu einer unabhängigen Ombudsperson in den USA und so zu einer kostenfreien Prüfung des eigenen Anliegens verschafft. Anders als auf dem offiziellen Klageweg muss nicht nachgewiesen werden, dass man in einem konkreten Fall von einer Dateneinsicht oder -speicherung durch U.S.-amerikanische Behörden betroffen ist, um eine Eingabe machen zu können. Die Ombudsperson wird den dargelegten Sachverhalt auf Übereinstimmung mit U.S.-amerikanischem Recht prüfen und mitteilen, dass keine Rechtsverstöße vorliegen bzw. vorab einen vorliegenden Rechtsverstoß abstellen.

Welche Rechtsbehelfe haben Betroffene jetzt konkret?

Basiert eine Datenverarbeitung in den USA auf dem Privacy Shield und haben Betroffene den Verdacht, dass ihre personenbezogenen Daten durch das U.S.-Unternehmen nicht entsprechend den Datenschutzgrundsätzen verarbeitet werden, haben sie verschiedene Handlungsoptionen. Dem Grundsatz des Rechtsschutzes, der Durchsetzung und Haftung nach sind die Beschwerdemöglichkeiten für Verbraucher grds. kostenfrei.

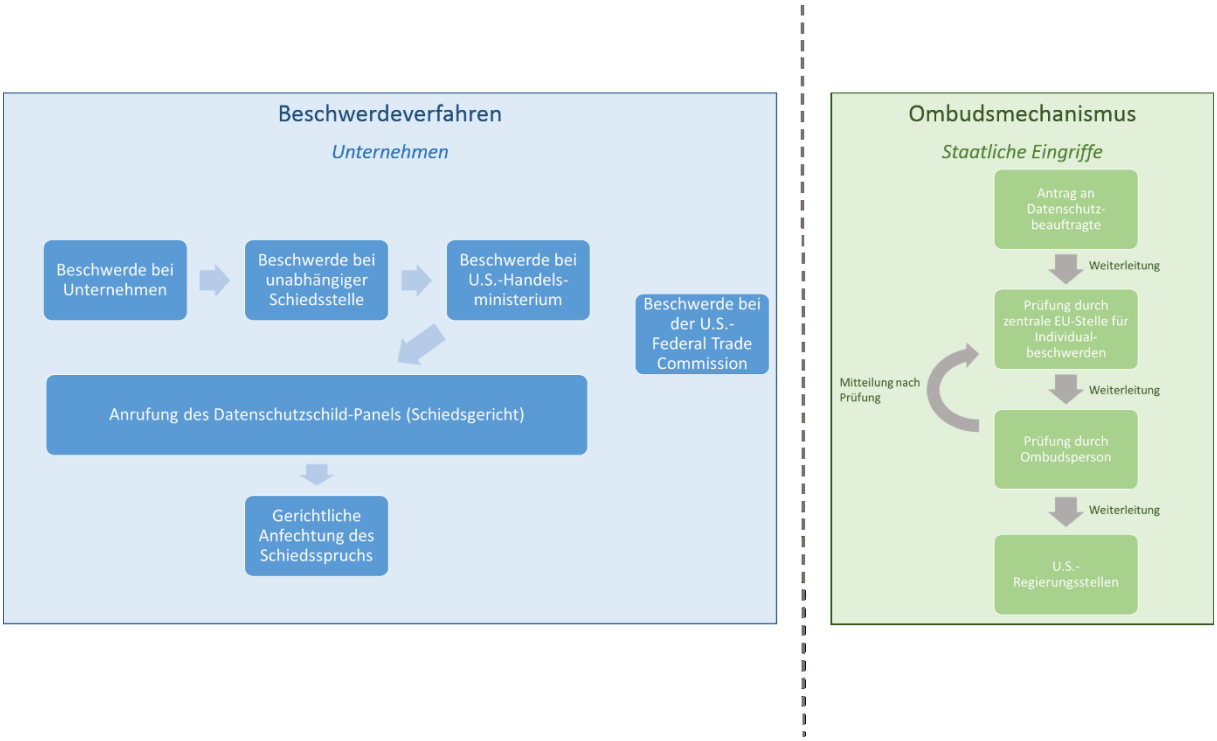

Abb.: Übersicht – Rechtsschutz Privacy Shield

Unternehmen selbst

Betroffene können sich – und sollten dies auch zunächst tun – in jedem Fall direkt an das Unternehmen wenden. Unternehmen müssen eine Kontaktperson benennen und auf dort eingehende Beschwerden innerhalb von 45 Tagen in Bezug auf den Beschwerdeinhalt reagieren.

Unabhängige Beschwerdestellen

Unternehmen können sich einer unabhängigen Beschwerdestelle unterwerfen, die dann ermächtigt ist, das Unternehmen anzuweisen, bzw. zu sanktionieren. In diesem Fall müssen Unternehmen auf ihren Websites diese Beschwerdestelle verlinken. Auf der Website der Beschwerdestelle sollten alle Details zum Beschwerdeverfahren bei der Stelle einsehbar sein. Es können Kriterien für die Zulässigkeit von Beschwerden aufgestellt werden. Die Beschwerdestelle muss Angaben zu Bearbeitungsdauer und möglichen Abhilfemaßnahmen machen. Offensichtlich unbegründete oder nicht ernst gemeinte Beschwerden müssen nicht beantwortet werden.

Die Beschwerdestellen müssen bei Missachtung ihrer Entscheidung die Gerichte anrufen oder die zuständige Behörde; zudem müssen sie das U.S.-Handelsministerium unterrichten.

Unternehmen können sich auch einer europäischen Datenschutzbehörde als unabhängiger Beschwerdestelle unterwerfen. Wenn das Unternehmen das Privacy Shield auch zur Übermittlung von Beschäftigtendaten nutzen möchte, muss es sich insofern zur Zusammenarbeit verpflichten.

Datenschutzbeauftragte (U.S.-Handelsministerium/Federal Trade Commission)

Betroffene können eine Beschwerde an das U.S.-Handelsministerium formulieren. Diese kann bei der Datenschutzbeauftragten auf Deutsch oder Englisch eingereicht werden. Die Datenschutzbeauftragte übersetzt die Beschwerde ggf. und leitet sie an die zuständige Stelle im U.S.-Handelsministerium weiter. Binnen 90 Tagen erhält sie eine Antwort, die sie sodann an die Betroffenen weitergibt.

Betroffene können sich jederzeit direkt an die Datenschutzbeauftragte wenden, statt selbst eine Beschwerde an ein U.S.-Unternehmen zu formulieren. Die Datenschutzbeauftragte hat – sofern sich ein Unternehmen nicht ihr als unabhängige Schlichtungsstelle unterworfen hat – keine Anordnungsbefugnisse gegenüber den Unternehmen. Jedoch wird sie die Beschwerde des Betroffenen prüfen und binnen 60 Tagen eine Empfehlung an das U.S.-Unternehmen senden. Auf diese muss das Unternehmen innerhalb von 25 Tagen reagieren. Tut es das nicht oder nicht ausreichend, kann die Datenschutzbeauftragte die U.S.-amerikanische Federal Trade Commission um Rechtsdurchsetzung ersuchen und das U.S.-Handelsministerium informieren, sodass das Unternehmen ggf. von der Privacy Shield-Liste gestrichen wird.

Sollte die Prüfung der Beschwerde ergeben, dass die Übermittlung an das U.S.-Unternehmen nicht im Einklang mit europäischem Recht steht, kann die Datenschutzbeauftragte im Rahmen ihrer Zuständigkeit gegen das übermittelnde europäische Unternehmen vorgehen.

Federal Trade Commission

Betroffene können den auch U.S.-Bürgern offenstehenden Weg nutzen und selbst Beschwerde bei der Federal Trade Commission (FTC) einreichen (www.ftc.gov/complaint).

Privacy Shield Schiedsmodell – „Datenschutzschild-Panel"

Durch das Privacy Shield wird ein Schiedsverfahren implementiert. Unter der Voraussetzung, dass Betroffene ordnungsgemäß Beschwerde bei dem Unternehmen eingelegt haben, das unabhängige Beschwerdeverfahren durchlaufen haben und die Angelegenheit über die Datenschutzbeauftragte dem U.S.-Handelsministerium zur Klärung zugeleitet haben, kann in der Regel das Schiedsverfahren beantragt werden.

Betroffene müssen das Unternehmen unter Beschreibung der bisher unternommenen Schritte und der Rechtsverletzung darüber informieren, dass sie nunmehr das Datenschutzschild-Panel anrufen wollen. Hierbei kann Unterstützung von der Datenschutzbeauftragten in Anspruch genommen werden. Das Unternehmen hat 45 Tage Zeit, auf die Information zu reagieren.

Wenn das Datenschutz-Panel eine Rechtsverletzung feststellt, kann es gegenüber dem Unternehmen Einsicht in die betroffenen Daten, Berichtigung, Löschung oder Rückgabe anordnen. Das Verfahren findet in den USA binnen 90 Tagen nach der Information an das Unternehmen statt. Betroffene können der Verhandlung telefonisch oder per Video-Konferenz beiwohnen. Die Datenschutzbeauftragte darf das Verfahren über die Information an das Unternehmen hinaus nicht begleiten.

Soweit kein Rechtsanwalt in Anspruch genommen wird, ist das Schiedsverfahren für Betroffene grds. kostenfrei. Die Beantragung einer gerichtlichen Überprüfung des Schiedsspruches ist den Betroffenen und den Unternehmen möglich.

Ombudsstelle

Durch das Privacy Shield wird zudem ein Ombudsmechanismus implementiert. Dieser dient als Rechtsschutzmöglichkeit in Bezug auf die U.S.-amerikanische „Signalaufklärung", d.h. in der Regel geheimdienstliche Aktivitäten. Das bedeutet, anders als die zuvor genannten Beschwerdemöglichkeiten, können bei der Ombudsstelle Sachverhalte eingereicht werden, die sich nicht um Verstöße von privaten Unternehmen gegen die Grundsätze drehen, sondern um staatliches Handeln durch U.S.-amerikanische Behörden.

Die Aufgabe der Ombudsstelle ist es, Sachverhalte daraufhin zu überprüfen, ob sie in Einklang mit U.S.-amerikanischem Recht stehen. Sie arbeitet hierzu mit den beteiligten U.S.-Sicherheitsbehörden und

bestehenden Aufsichtsmechanismen zusammen. Die Ombudsstelle ist dem U.S.-Außenministerium nachgeordnet und frei in ihren Entscheidungen.

Anträge können schriftlich bei der Datenschutzbeauftragten eingereicht werden. Diese leitet sie weiter an die zentrale EU-Stelle für Individualbeschwerden, wo Anträge insbesondere auf Vollständigkeit – inklusive der Identität des Antragstellers – geprüft werden. Der Antrag sollte Angaben darüber enthalten, um welchen Sachverhalt es geht, welches Ziel verfolgt wird, welche U.S.-Behörden vermutlich involviert sind und was bisher zur Aufklärung des Sachverhalts unternommen wurde. Ein Nachweis über eine tatsächlich erfolgte Signalaufklärung ist nicht erforderlich.

Nach Abschluss ihrer Ermittlungen teilt die Ombudsstelle der EU-Stelle für Individualbeschwerden mit, dass sie Beschwerde ordnungsgemäß geprüft hat und dass kein Verstoß gegen U.S.-amerikanisches Recht vorliegt bzw. ein solcher abgestellt wurde. Ob eine Überwachung vorlag wird nicht mitgeteilt. Anträge werden auch an die zuständigen U.S.-Regierungsstellen weitergeleitet. Die zuständigen Überwachungsstellen – Generalinspekteure und Datenschutz- und Bürgerrechtsbeauftragte – haben die Möglichkeit, Rechtsverstöße oder anderes Fehlverhalten zu ahnden.

Es besteht gemäß „Freedom Of Information Act“ (vergleichbar mit den Informationsfreiheits-, bzw. Transparenzgesetzen in einigen Bundesländern) die Möglichkeit, Zugang zu behördlichen Dokumenten zu bekommen. Ausgenommen sind als geheimhaltungsbedürftig eingestufte Dokumente. Informationen hierzu finden sich unter www.FOIA.gov und http://www.justice.gov/oip/foia-resources.

Der Ombudsmechanismus gilt gleichermaßen für Daten, die gemäß dem Privacy Shield, den Standardklauseln, den verbindlichen unternehmensinternen Datenschutzregelungen, sowie „Ausnahmeregelungen“ oder „etwaigen künftigen Ausnahmeregelungen“ von der EU in die USA übermittelt werden.

Privates Klagerecht

Die je nach Verarbeitungszusammenhang sich aus verschiedenen U.S.-amerikanischen Gesetzen ergebenden Rechte können weiterhin privatrechtlich in den USA eingeklagt werden. Ein Beispiel wäre der „Wiretap Act“ (18 U.S.C. § 2520), wonach die Betroffenen einer Überwachung von leitungsgebundener, mündlicher oder elektronischer Kommunikation gegen die USA oder einen Regierungsbeamten klagen können. Allerdings entstehen u.U. hohe Prozesskosten und der Verstoß muss vom Klagenden bewiesen werden.

Welche Besonderheit besteht bei Beschäftigtendaten?

Soweit ein U.S.-Unternehmen Beschäftigtendaten verarbeitet (Bsp.: der U.S.-amerikanische Mutterkonzern erhält die Beschäftigtendaten der Beschäftigten des europäischen Tochterunternehmens), trifft das Privacy Shield eine Sonderregelung: Wenn ein Privacy Shield-zertifiziertes Unternehmen Beschäftigtendaten übermittelt bekommen hat, darf es diese nur offenlegen oder für andere Zwecke nutzen, soweit diese Zwecke nicht unvereinbar mit dem Zweck sind, für den sie ursprünglich erhoben wurden. Die Beschäftigten müssen für eine solche andere Nutzung (z.B. Direktmarketing) um Erlaubnis gebeten werden und haben das Recht, nicht zuzustimmen, ohne dass ihnen hierdurch berufliche Nachteile entstehen.

Wie verlässlich ist das Privacy Shield?

Abschließend muss erwähnt werden, dass trotz der verbesserten Rechtsstellung der Betroffenen, Zusagen der beteiligten U.S.-Behörden, sowie vereinzelter Rechtsänderungen und –ergänzungen in den USA, umstritten bleibt, ob der Kernkonflikt, nämlich der Zugriff auf gespeicherte personenbezogene Daten ohne (aus europäischer Sicht ausreichende) Differenzierung, Einschränkung oder Ausnahmen durch insbesondere U.S.-Sicherheitsbehörden, durch das Privacy Shield aufgelöst wird. Sowohl die Datenschutz-Konferenz (auf deutscher Ebene), als auch die Art. 29-Arbeitsgruppe (auf europäischer Ebene) haben sich diesbezüglich kritisch geäußert. Voraussichtlich wird auch dieser Durchführungsbeschluss durch Betroffene vor den erstinstanzlich zuständigen nationalen Gerichten angegriffen werden. Aus dem Urteil des EuGH geht weiterhin hervor, dass es auch den Datenschutzbeauftragten möglich sein muss, auf Eingaben, die die Rechtmäßigkeit der Kommissionsentscheidung in Frage stellen, rechtliche Mittel zur Überprüfung anzuwenden.

Die nationalen Gerichte werden die Frage, ob die Europäische Kommission rechtlich einwandfrei festgestellt hat, dass ein angemessenes Datenschutzniveau in den USA besteht und dementsprechend das Privacy Shield verabschieden durfte, letztlich erneut dem EuGH vorlegen.

Bis aber dort eine Entscheidung vorliegt, ist eine Datenübermittlung in die USA an Privacy Shield-zertifizierte Unternehmen jedenfalls als rechtmäßig anzusehen.

Unabhängig von eventuellen Gerichtsverfahren wird die Funktionsweise des Privacy Shield jährlich überprüft und die Rechtslage neu bewertet. Theoretisch ist es denkbar dass – etwa durch Änderungen maßgeblicher U.S.-amerikanischer Gesetze – eine solche Prüfung ergibt, dass kein angemessenes Datenschutzniveau in den USA mehr besteht und der Durchführungsbeschluss zum Privacy Shield daher abgeändert oder aufgehoben wird.