



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

---

A background graphic consisting of a network of light blue lines connecting various sized light blue dots, creating a web-like pattern across the page.

# LEITFADEN ZUM SWISS-US PRIVACY SHIELD

QUELLE:

GUIDE TO THE EU-U.S. PRIVACY SHIELD  
European Commission  
Directorate-General for Justice and Consumers

© European Union, 2016  
Reproduction is authorised provided the source is acknowledged.





# Inhalt

Einleitung	7
Verpflichtungen der für Privacy Shield zertifizierten Unternehmen und Rechte der betroffenen Personen	9
Wie kann Beschwerde gegen ein für Privacy Shield zertifiziertes Unternehmen erhoben werden?	15
Die Ombudsstelle: Anlaufstelle für Beschwerden betreffend Personendatenbearbeitungen durch US Behörden	19



# Einleitung

## Was ist der Swiss-US Privacy Shield und warum brauchen wir ihn?

Die Schweiz und die Vereinigten Staaten (USA) unterhalten enge Handelsbeziehungen. Die Übermittlung personenbezogener Daten ist ein wichtiger und unverzichtbarer Bestandteil der transatlantischen Beziehungen, insbesondere in der heutigen globalen, digitalisierten Wirtschaft. Viele Transaktionen umfassen die Erhebung und Verwendung personenbezogener Daten wie zum Beispiel Name, Telefonnummer, Geburtsdatum, Wohnanschrift, E-Mail-Adresse, Kreditkartennummer, Nutzernamen, Geschlecht und Familienstand oder andere Informationen, mit denen Personen identifiziert werden können. Diese Daten können in der Schweiz durch eine Zweigniederlassung oder einen Geschäftspartner eines amerikanischen Unternehmens erhoben und in den USA weiter bearbeitet werden.

Dies ist der Fall, wenn Sie als Kunde Waren und Dienstleistungen online erwerben, als Privatperson soziale Medien oder Cloud-Speicherdienste nutzen oder wenn ein in der Schweiz ansässiges Unternehmen personenbezogene Daten seiner Mitarbeitenden oder Kunden zur Bearbeitung an ein Unternehmen in den USA (z. B. an die Muttergesellschaft) übermittelt.

Nach Schweizer Recht müssen personenbezogene Daten, die in die USA übermittelt werden, einem angemessenen Datenschutzniveau unterliegen. Dazu dient der Swiss-US Privacy Shield. Dank diesem neuen Rechtsrahmen können personenbezogene Daten aus der Schweiz an ein Unternehmen in den USA übermittelt werden, wenn sich dieses an eine Reihe von Vorschriften und Garantien zum Schutz dieser Daten hält. Der Schutz gilt für alle in der Schweiz wohnhaften Personen.

## Wie funktioniert der Privacy Shield?

Bei der Übermittlung personenbezogener Daten aus der Schweiz in die USA stehen verschiedene Instrumente wie Vertragsklauseln, verbindliche unternehmensinterne Datenschutzvorschriften (sog. Binding Corporate Rules, BCR) und der Privacy Shield zur Verfügung, um für ein angemessenes Datenschutzniveau zu sorgen. Um den Privacy Shield verwenden zu können, müssen sich amerikanische Unternehmen zuerst beim US-Handelsministerium (Department of Commerce, DOC) registrieren. Die Verpflichtungen der Unternehmen im Rahmen des Privacy Shield sind in den Datenschutzgrundsätzen des Rechtsrahmens ([vgl. Swiss-US Privacy Shield Framework/ANNEX Principles and Arbitration](#)) aufgeführt. Das DOC ist für das Management und die Verwaltung des Privacy Shield zuständig und hat sicherzustellen, dass Unternehmen ihren Verpflichtungen nachkommen. Zertifizierungswillige Unternehmen müssen über Datenschutzbestimmungen verfügen, die mit den Grundsätzen des Privacy Shield im Einklang stehen. Sie müssen ihr Zertifikat, d.h. ihre „Mitgliedschaft“ im Privacy Shield, jährlich erneuern.

Ob ein US-Unternehmen dem Privacy Shield angeschlossen ist, erfährt man aus der Liste auf der Website des DOC (<https://www.privacyshield.gov/welcome>). Diese Liste enthält Angaben zu allen Unternehmen, die für Privacy Shield zertifiziert sind, zur Art der verwendeten Personendaten und den angebotenen Dienstleistungen. Auf der Website befindet sich zudem eine Liste von Unternehmen, die nicht mehr dem Privacy Shield angeschlossen sind und somit keine personenbezogenen Daten im Rahmen des Privacy Shield mehr erhalten dürfen. Diese Unternehmen dürfen die noch unter dem gültigen Zertifikat erhaltenen Personendaten nur weiter aufbewahren und bearbeiten, wenn sie dem DOC die Anwendung der Datenschutzgrundsätze für diese Daten zusichern.



# Verpflichtungen der für Privacy Shield zertifizierten Unternehmen und Rechte der betroffenen Personen

Unternehmen sind verpflichtet, personenbezogene Daten im Einklang mit den Datenschutzgrundsätzen des Privacy Shield zu bearbeiten.

## 1. Informationspflicht

Ein für Privacy Shield zertifiziertes Unternehmen muss die betroffenen Personen darüber informieren,

- welche Arten von personenbezogenen Daten es bearbeitet;
- zu welchen Zwecken es diese Daten bearbeitet;
- ob es beabsichtigt, personenbezogene Daten an ein anderes Unternehmen weiterzugeben, und falls ja, aus welchen Gründen;
- dass betroffene Personen das Recht haben, vom Unternehmen Zugang zu ihren Daten zu verlangen;
- dass betroffene Personen das Recht haben, darüber zu bestimmen, ob ein zertifiziertes Unternehmen ihre Daten an Dritte bekannt geben darf oder ob es diese in einer Art verwenden darf, die sich vom ursprünglich genehmigten Verwendungszweck „wesentlich unterscheidet“. Dabei genügt es, wenn das Unternehmen der betroffenen Person das „Recht zu widersprechen“ („Opt-out“-Recht) gibt. Handelt es sich bei den Daten um besonders schützenswerte Personendaten (beispielsweise Daten zur ethnischen Herkunft oder zum Gesundheitszustand, s. Artikel 3 des Datenschutzgesetzes, DSG), muss das Unternehmen eine ausdrückliche Einwilligung der betroffenen Personen einholen („Opt-in“-Recht);
- wie betroffene Personen das Unternehmen kontaktieren können, um eine Beschwerde über die Verwendung ihrer Daten einzureichen;
- an welche Stelle für alternative Streitbeilegung (Alternative Dispute Resolution body, ADR) in der Schweiz oder in den USA Beschwerden eingereicht werden können;
- welches die zuständige US-Regierungsbehörde für die Untersuchung und Durchsetzung der im Rahmen des Privacy Shield bestehenden Verpflichtungen des Unternehmens ist;

- dass es auf rechtmässige Anfrage von US-Behörden gerechtfertigt sein kann, Informationen über betroffene Personen offenzulegen.

Das dem Privacy Shield angeschlossene Unternehmen muss einen Link zu seinen Datenschutzbestimmungen bereitstellen, wenn es über eine öffentliche Website verfügt, oder andernfalls darauf hinweisen, wo diese Bestimmungen eingesehen werden können. Es muss zudem den Link zur Privacy-Shield-Liste des DOC angeben, damit die betroffenen Personen die Gültigkeit des Privacy-Shield-Zertifikats des Unternehmens überprüfen können.

## 2. Zweckbindung

Grundsätzlich kann ein für Privacy Shield zertifiziertes Unternehmen personenbezogene Daten nur zu dem Zweck verwenden, zu dem sie ursprünglich erhoben wurden oder für den eine nachträgliche Einwilligung vorliegt. Will es Daten zu einem anderen Zweck verwenden, hängt die Zulässigkeit davon ab, wie sehr der neue Zweck vom ursprünglichen abweicht:

- Die Verwendung von Daten für einen Zweck, der mit dem ursprünglichen Zweck unvereinbar ist, ist unter keinen Umständen zulässig.
- Wenn sich der neue Zweck vom ursprünglichen Zweck „wesentlich unterscheidet“, jedoch mit diesem zusammenhängt, darf das für Privacy Shield zertifizierte Unternehmen Daten nur dann nutzen, wenn kein Einwand erhoben wird (Opt-out) oder – im Falle besonders schützenswerter Personendaten – eine ausdrückliche Einwilligung vorliegt (Opt-in).
- Unterscheidet sich der neue Zweck vom ursprünglichen Zweck nur unwesentlich, ist eine entsprechende Verwendung zulässig.

Hat beispielsweise ein Arbeitgeber Personaldaten zur Bearbeitung in die USA übermittelt, könnte das US-amerikanische Unternehmen diese Daten verwenden, um den Mitarbeitenden ein Angebot für eine Versicherung oder die Altersvorsorge zu machen, solange sie einer solchen Verwendung nicht widersprechen (Opt-out). Hingegen darf es Daten nicht zu kommerziellen Zwecken an Dritte veräussern, weil dies keinen direkten Bezug zum Anstellungsverhältnis hat.

Betroffene Personen haben auch das Recht zu entscheiden, ob ein für Privacy Shield zertifiziertes Unternehmen personenbezogene Daten an ein anderes Unternehmen in den USA oder in einem Drittstaat weitergeben darf. Werden Daten durch das Unternehmen an einen Auftragsdatenbearbeiter weitergegeben, müssen die beiden Unternehmen einen schriftlichen Vertrag abschliessen, der dieselben Datenschutzgarantien wie der Swiss-US Privacy Shield enthält. Das zertifizierte Unternehmen kann für Handlungen des Auftragnehmers haftbar gemacht werden, wenn sich dieser nicht an diese Vorschriften hält.

### 3. Verhältnismässigkeit

Das für Privacy Shield zertifizierte Unternehmen darf nur diejenigen personenbezogenen Daten bearbeiten, die für die Zwecke der Bearbeitung relevant sind. Zudem muss es dafür sorgen, dass die verwendeten Daten richtig, vollständig und auf dem neuesten Stand sind. Personenbezogene Daten dürfen ausserdem nur so lange gespeichert werden, wie dies für den Zweck der Bearbeitung erforderlich ist. Längere Aufbewahrungszeiträume sind nur zulässig, wenn sie durch spezifische Interessen wie z.B. Archivierung, Literatur, Kunst, Journalismus, wissenschaftliche oder historische Forschung oder statistische Analyse gerechtfertigt sind. Auch in diesen Fällen müssen die Datenschutzgrundsätze eingehalten werden.

### 4. Datensicherheit

Das Unternehmen muss sicherstellen, dass Personendaten in einer sicheren Umgebung aufbewahrt und vor Verlust, missbräuchlicher Nutzung, unbefugtem Zugriff, unbefugter Weitergabe, Veränderung und Vernichtung gesichert sind, wobei der Art der Daten und den mit der Bearbeitung verbundenen Risiken gebührend Rechnung zu tragen ist.

### 5. Datenübermittlung an Dritte

Wie bereits unter Punkt 2 angemerkt, kann das für Privacy Shield zertifizierte Unternehmen Daten unter bestimmten Bedingungen und unter Berücksichtigung des ursprünglichen Verwendungszwecks an ein anderes Unternehmen weitergeben. Ungeachtet seines Standorts inner- oder ausserhalb der USA muss das Drittunternehmen, das die Daten empfängt, das Schutzniveau sicherstellen, das im Rahmen des Privacy Shield garantiert ist. Dies erfordert einen Vertrag zwischen den beiden Unternehmen, in dem die Bedingungen festgelegt werden, unter denen Personendaten bearbeitet werden dürfen. Insbesondere ist das Drittunternehmen zu verpflichten, das für Privacy Shield zertifizierte Unternehmen von Situationen zu unterrichten, in denen es seinen Verpflichtungen nicht mehr nachkommen kann. Sollte dieser Fall eintreten, muss es die Bearbeitung der Daten einstellen. Strengere Regeln gelten, wenn ein Dritter als Auftragnehmer eines zertifizierten Unternehmens handelt. In diesem Fall kann Letzteres für die Handlungen des Auftragnehmers, der gegen seine Verpflichtungen zum Schutz personenbezogener Daten verstösst, haftbar gemacht werden.

## 6. Auskunfts- und Berichtigungsrecht

Jede betroffene Person hat das Recht, vom für Privacy Shield zertifizierten Unternehmen Auskunft über ihre Daten zu verlangen.

Sie hat das Recht, Auskunft über den Zweck der Datenbearbeitung, die Kategorien der bearbeiteten Personendaten und die Empfänger (oder die Kategorien der Empfänger), an die die Daten weitergegeben werden, zu erhalten. Die betroffene Person kann das Unternehmen auffordern, die Daten zu ändern oder zu löschen, wenn sie nicht richtig oder veraltet sind oder unter Verletzung der Privacy-Shield-Vorschriften bearbeitet wurden.

Ein Auskunftsgesuch bedarf keiner Begründung. Ist das Ersuchen zu weit gefasst oder zu vage, kann das Unternehmen jedoch eine Begründung verlangen. Das Unternehmen muss innerhalb einer angemessenen Frist auf das Gesuch reagieren. Es kann die Auskunftsrechte nur in bestimmten Fällen einschränken, z. B. wenn die Gewährung der Auskunft die Vertraulichkeit verletzen, gegen das Berufsgeheimnis verstossen oder mit rechtlichen Verpflichtungen kollidieren würde.

## 7. Beschwerderecht und Rechtsschutz

Hält sich das zertifizierte Unternehmen nicht an die Vorschriften des Privacy Shield und verstösst gegen seine Verpflichtung zum Schutz personenbezogener Daten, können betroffene Personen Beschwerde einlegen und unentgeltlichen Rechtsschutz verlangen. Zertifizierte Unternehmen sind verpflichtet, unabhängige Beschwerdeverfahren anzubieten. Die Unternehmen können sich für die alternative Streitbeilegung (Alternative Dispute Resolution body, ADR) entscheiden oder sich der Aufsicht des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) unterstellen.

Betroffene können bei folgenden Stellen Beschwerde einlegen:

1. beim für Privacy Shield zertifizierten US-Unternehmen selbst;
2. bei einer unabhängigen Beschwerdestelle, beispielsweise einer Stelle für alternative Streitbeilegung (ADR) oder dem EDÖB;
3. via den EDÖB beim DOC;
4. bei der Federal Trade Commission (oder beim US-Verkehrsministerium, d.h. dem U.S. Department of Transportation, falls die Beschwerde eine Fluggesellschaft oder eine Fahrkartenverkaufsstelle betrifft);
5. beim für den Privacy Shield zuständigen Schiedsgericht, falls alle anderen Rechtsbehelfe erfolglos waren.

- **Stelle für alternative Streitbeilegung (ADR)**

Eine Stelle für alternative Streitbeilegung (Alternative Dispute Resolution body, ADR) ist eine private Organisation, die sich u.a. mit Datenschutzbeschwerden gegen Unternehmen befasst. Wird die alternative Streitbeilegung gewählt, muss das für Privacy Shield zertifizierte Unternehmen entscheiden, ob es sich in der Schweiz oder in den Vereinigten Staaten der alternativen Streitbeilegung unterstellt. Das Verfahren wird durch die ausgewählte Streitbeilegungsstelle bestimmt.

- **EDÖB**

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte ist als Beratungs- und Aufsichtsstelle auf nationaler Ebene für datenschutzrechtliche Anliegen zuständig.

- U.S. Department of Commerce (DOC) und U.S. Federal Trade Commission (FTC)

Beschwerden an das DOC und/oder die FTC müssen beim EDÖB eingereicht werden.

- Für den Privacy Shield zuständiges Schiedsgericht

Das Schiedsgericht besteht aus drei neutralen Schiedsrichtern und ermöglicht eine Streitbeilegung ohne Anrufung eines Gerichts. Seine Entscheidungen sind verbindlich und vor US-Gerichten durchsetzbar. Die betroffene Person kann unter bestimmten Bedingungen das Schiedsverfahren vor dem zuständigen Schiedsgericht in Anspruch nehmen (insbesondere müssen alle anderen zur Verfügung stehenden Rechtsbehelfe ausgeschöpft sein). Zertifizierte Unternehmen können dem Schiedsgericht keine Beschwerden zum Entscheid vorlegen, da dieses nur für natürliche Personen vorgesehen ist.

## 8. Rechtsschutz im Fall des Datenzugriffs durch US-Behörden

Der Schutz personenbezogener Daten kann auch durch den Zugriff von US-Behörden beeinträchtigt werden. Der Privacy Shield stellt sicher, dass ein Zugriff nur in dem Masse erfolgt, wie dies für die Verfolgung eines Zieles von hohem öffentlichem Interesse, zum Beispiel der nationalen Sicherheit oder des Strafvollzuges, erforderlich ist. Zwar sind im US-Recht Schutzmechanismen und Rechtsbehelfe auf dem Gebiet der Strafverfolgung vorgesehen, doch wird mit dem Privacy Shield erstmals ein besonderes Instrument, die Ombudsstelle, geschaffen, das sich mit Fragen des Datenzugriffs im Namen der nationalen Sicherheit befasst (siehe Abschnitt C)..n oder sich der Aufsicht des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) unterstellen.

## Wie kann Beschwerde gegen ein für Privacy Shield zertifiziertes Unternehmen erhoben werden?

Der Privacy Shield bietet eine Reihe von Möglichkeiten, um Beschwerde gegen ein Unternehmen einzureichen, beispielsweise wenn dieses personenbezogene Daten nicht korrekt bearbeitet oder andere Vorschriften missachtet.

Der Rechtsbehelf kann den individuellen Bedürfnissen entsprechend frei gewählt werden.

Bei folgenden Stellen kann eine Beschwerde eingereicht werden:

1. **Beim für Privacy Shield zertifizierten US-Unternehmen direkt.** Ein zertifiziertes Unternehmen muss detailliert informieren, wie im Beschwerdefall vorzugehen ist. Das Unternehmen muss innerhalb von 45 Tagen nach Eingang einer Beschwerde antworten. Aus der Antwort muss hervorgehen, ob die Beschwerde begründet ist, und wenn ja, wie das Unternehmen Abhilfe schafft. Es ist verpflichtet, jeder eingehenden Beschwerde nachzugehen, die nicht offensichtlich unbegründet ist.
2. **Bei der unabhängigen Stelle für alternative Streitbeilegung (ADR),** falls sich das zertifizierte Unternehmen für die alternative Streitbeilegung entschieden hat. Die Website des Unternehmens muss Informationen über die ADR und den Link zu deren Website enthalten, die Aufschluss über die angebotenen Dienste und das zu befolgende Verfahren gibt. Diese Stelle muss in der Lage sein, wirksame Abhilfemaßnahmen und Sanktionen festzulegen, damit sichergestellt ist, dass das für Privacy Shield zertifizierte Unternehmen seiner Verpflichtung zum Schutz personenbezogener Daten nachkommt. Das Schiedsverfahren ist für die betroffene Person unentgeltlich.
3. **Beim EDÖB.** Ein für Privacy Shield zertifiziertes Unternehmen kann den EDÖB als unabhängige Beschwerdestelle wählen. Da bei der Bearbeitung von Personaldaten die Aufsicht durch den EDÖB zwingend vorgeschrieben ist, können sich Arbeitnehmer mit Beschwerden in Bezug auf ihre beschäftigungsrelevanten Daten, die an ein zertifiziertes Unternehmen übermittelt werden, immer an den EDÖB wenden. Dies gilt auch dann, wenn sich das Unternehmen nicht zur Zusammenarbeit mit dem EDÖB entschieden hat. Der EDÖB wird die Beschwerde an die zuständige US-Behörde weiterleiten.

Der EDÖB übermittelt dem zertifizierten Unternehmen seine Stellungnahme so schnell wie möglich, spätestens aber innerhalb von 60 Tagen nach Eingang der Beschwerde. Die beschwerdeführende Person wird über diese Empfehlung

informiert, die in der Regel veröffentlicht wird. Das Unternehmen hat 25 Tage Zeit, um der Stellungnahme des EDÖB nachzukommen. Folgt das Unternehmen der Stellungnahme nicht, kann der EDÖB den Fall an die Federal Trade Commission (FTC) weiterleiten, damit diese Vollzugshandlungen einleitet. Er kann aber auch das DOC über die Weigerung des Unternehmens informieren und die Löschung der Gesellschaft aus der Privacy-Shield-Liste verlangen, falls das Unternehmen seine Verpflichtungen weiterhin nicht erfüllt.

Geht aus einer Beschwerde zudem hervor, dass die Übermittlung personenbezogener Daten an ein für Privacy Shield zertifiziertes Unternehmen in der Schweiz gegen das Schweizer Datenschutzrecht verstösst, kann der EDÖB auch gegen das Unternehmen in der Schweiz vorgehen und das Einstellen der Datenübermittlung anordnen.

4. **Beim DOC.** Auch wenn der EDÖB keine direkten Aufsichtsbefugnisse über zertifizierte amerikanische Unternehmen hat, gegen das sich eine Beschwerde richtet, kann er die Beschwerde an das DOC (US-Handelsministerium) weiterleiten. Das DOC prüft die Beschwerde und antwortet dem EDÖB innerhalb von 90 Tagen, oder es kann die Beschwerde auch an die Federal Trade Commission (oder das U.S. Department of Transportation, Verkehrsministerium) weiterleiten.
5. **Bei der Federal Trade Commission (FTC).** Es besteht auch die Möglichkeit, eine Beschwerde direkt bei der amerikanischen Federal Trade Commission einzureichen: [www.ftc.gov/complaint](http://www.ftc.gov/complaint). Denselben Weg beschreiten auch US-Bürgerinnen und -Bürger.
6. **Beim für den Privacy Shield zuständigen Schiedsgericht.** Bleibt eine Beschwerde nach Rückgriff auf die anderen Rechtsbehelfe immer noch ganz oder teilweise ungeklärt oder ist der Beschwerdesteller weiterhin unzufrieden, steht als letztes Rechtsmittel ein verbindliches Schiedsverfahren zur Verfügung.

## Wer kann ein Schiedsverfahren verlangen und in welchem Fall?

Ein solches Verfahren kann nur durch eine betroffene Einzelperson persönlich eingeleitet werden und ist für das für Privacy Shield zertifizierte Unternehmen bindend.



Die Möglichkeit der Anrufung des Schiedsgerichts kann jedoch erst gewählt werden, nachdem alle anderen Rechtsbehelfe erfolglos waren. Das Schiedsverfahren steht nicht zur Verfügung, wenn eine Beschwerde bereits Gegenstand eines Schiedsverfahrens war, ein anderes Gericht bereits über dieselbe Beschwerde mit denselben Verfahrensparteien entschieden hat, die Parteien bereits eine Einigung erzielt haben oder der EDÖB die Beschwerde direkt mit dem Unternehmen geklärt hat. Im Übrigen kann die Federal Trade Commission parallel zum Schiedsverfahren Untersuchungen aufnehmen.

### Vorgehen für die Anrufung des Schiedsgerichts

Vor der Einleitung des Schiedsverfahrens muss die Absicht dem betreffenden Unternehmen formell mitgeteilt werden. Die Mitteilung muss eine Beschreibung der mutmasslichen Verletzung der Privacy Shield Vorschriften und eine Zusammenfassung der bisher unternommenen Beschwerdeschritte enthalten. Der Beschwerde können auch Belege oder relevante Rechtsunterlagen beigelegt werden.

### Ort des Schiedsgerichtsverfahrens

Das Schiedsverfahren findet in den USA statt, da die für Privacy Shield zertifizierten Unternehmen ihren Sitz in den USA haben.

### Vorteile des Schiedsgerichtsverfahrens

- das Recht, den EDÖB um Hilfestellung bei der Erstellung einer Beschwerde zu ersuchen;
- die Möglichkeit, dem Verfahren per Telefon oder Videokonferenz beizuwohnen, sodass eine persönliche Anwesenheit in den USA nicht erforderlich ist;
- die Möglichkeit, unentgeltliche Dolmetschdienste in Anspruch zu nehmen und Unterlagen aus dem Englischen in eine Amtssprache übersetzen zu lassen;
- die Begleichung der Kosten des Schiedsverfahrens (mit Ausnahme der Anwaltskosten) aus einem vom Handelsministerium eigens dazu eingerichteten Fonds, der sich aus den jährlichen Beiträgen der für Privacy Shield zertifizierten Unternehmen finanziert.

## Dauer des Schiedsverfahrens

Das Schiedsverfahren wird innerhalb von 90 Tagen abgeschlossen ab dem Tag, an dem das betroffene Unternehmen über die Einleitung des Verfahrens informiert wurde.

## Rechtsbehelfe innerhalb des Schiedsgerichtsverfahrens

Das Schiedsgericht kann dem Beschwerdeführer Ansprüche wie Zugang, Berichtigung, Löschung oder Herausgabe seiner Daten zuerkennen. Es kann zwar keinen Schadenersatz zusprechen. Beschwerdeführer haben aber die Möglichkeit, ihre Ansprüche vor Gericht nach dem US-Gesetz über Schiedsverfahren (Federal Arbitration Act) geltend zu machen, falls das Ergebnis des Schiedsverfahrens unbefriedigend ausgefallen ist.

## Die Ombudsstelle: Anlaufstelle für Beschwerden betreffend Personendatenbearbeitungen durch US Behörden

Mit der Ombudsstelle errichtet der Privacy Shield eine neue unabhängige Beschwerdestelle im Bereich der nationalen Sicherheit.

Es handelt sich dabei um einen leitenden Beamten (Privacy Shield Ombudsperson) im US-Aussenministerium (US-Department of State), der seine Tätigkeit unabhängig von den US-amerikanischen Geheimdiensten ausübt. Er sorgt mit seinen Mitarbeitenden dafür, dass Beschwerden ordnungsgemäss und zeitnah behandelt werden. Beschwerdeführer erhalten eine Bestätigung, dass die einschlägigen amerikanischen Gesetze eingehalten oder die Mängel beseitigt wurden, falls gegen Rechtsvorschriften verstossen wurde.

Die Ombudsstelle arbeitet in ihrem Zuständigkeitsbereich eng mit anderen unabhängigen Aufsichts- und Ermittlungsbehörden zusammen, um alle für die Behandlung einer Beschwerde erforderlichen Informationen betreffend die Vereinbarkeit von Überwachungsmaßnahmen mit US-Recht zu erhalten. Diesen Behörden obliegt die Aufsicht über die verschiedenen amerikanischen Geheimdienste.

### Zuständigkeitsbereich der Ombudsstelle

Die Ombudsstelle befasst sich mit sämtlichen Beschwerden im Zusammenhang mit personenbezogenen und kommerziellen Datenübermittlungen aus der Schweiz an Unternehmen in den USA. Auch wenn das Daten übermittelnde US-Unternehmen dem Privacy Shield nicht angeschlossen ist und Daten gestützt auf alternative Transferinstrumente – wie Standardvertragsklauseln oder verbindliche unternehmensinterne Vorschriften – übermittelt.

## Verfahren für die Einreichung einer Beschwerde an die Ombudsstelle

Der Antrag muss beim EDÖB schriftlich eingereicht werden. Er sollte eine Begründung, sowie die Art der gewünschten Antwort oder erwarteten Unterstützung enthalten; ausserdem Informationen über die US-Regierungsstellen, die an den Überwachungsmaßnahmen beteiligt sein könnten, sowie andere Massnahmen, die in dieser Angelegenheit eventuell bereits getroffen wurden und etwaige bereits erhaltene Antworten. Aus dem Antrag muss jedoch nicht hervorgehen, dass ein Zugriff auf personenbezogene Daten durch den US-Geheimdienst tatsächlich stattgefunden hat.

Vor der Übermittlung an die Ombudsstelle wird geprüft, ob dem Antrag ein berechtigtes Anliegen zugrunde liegt. Dabei wird Folgendes überprüft:

- die Identität des Antragstellers, um sicherzustellen, dass dieser ausschliesslich für sich selbst und nicht für eine Regierung oder eine zwischenstaatliche Organisation handelt;
- die Vollständigkeit der darin enthaltenen Informationen,
- ob es sich um eine Übermittlung personenbezogener Daten in die Vereinigten Staaten handelt;
- dass der Antrag nicht schikanös oder missbräuchlich erfolgt.

## Ablauf des Verfahrens vor der Ombudsstelle

Die Ombudsstelle bearbeitet den Antrag und setzt sich mit dem EDÖB in Verbindung, falls sie noch Fragen hat oder zusätzliche Informationen benötigt.

Sobald der Antrag vollständig ist, wird er an die entsprechende US-Stelle weitergeleitet. Bezieht sich der Antrag auf die Vereinbarkeit der Überwachung mit dem US-Recht, kann die Ombudsstelle mit einer der unabhängigen Kontrollstellen mit Ermittlungsbefugnissen zusammenarbeiten. Die Ombudsstelle ist auf die erforderlichen Auskünfte angewiesen, um auf gestellte Beschwerden antworten zu können. Sie wird in der Antwort bestätigen, dass die Beschwerde ordnungsgemäss bearbeitet und das US-Recht eingehalten wurde oder andernfalls mitteilen, dass Verstösse gegen US-Recht behoben wurden. Der Antwort ist nicht zu entnehmen, ob die antragstellende Person von amerikanischen Geheimdiensten überwacht wurde.

## Öffentlichkeitsprinzip

Jede Person kann gestützt auf den Freedom of Information Act (FOIA) Zugang zu Aufzeichnungen beantragen, die sich im Besitz der US-Regierung befinden. Die offiziellen Websites jedes Ministeriums enthalten Informationen darüber, wie Zugang zu Dokumenten beantragt werden kann. Weitere Informationen zur Beantragung sind den Websites [www.FOIA.gov](http://www.FOIA.gov) und <http://www.justice.gov/oip/foia-resources> zu entnehmen.

Es wird jedoch kein Zugang zu als Verschlussachen eingestuften Informationen zur nationalen Sicherheit, personenbezogenen Informationen von Dritten sowie Informationen über strafrechtliche Ermittlungen gewährt. Dies gilt gleichermassen für Amerikaner und Nicht-Amerikaner.

Bei Streitigkeiten im Zusammenhang mit einem nach dem FOIA beantragten Zugang kann der Verwaltungsrechtsweg eingeschlagen und anschliessend ein Bundesgericht in den USA angerufen werden. Das Gericht kann daraufhin entscheiden, ob die beantragten Aufzeichnungen ordnungsgemäss zurückgehalten werden; gegebenenfalls kann es die Regierung zwingen, Zugang zu diesen Unterlagen zu gewähren. Die Gerichte können die Anwaltskosten erstatten, aber es wird kein Schadenersatz geleistet.