

Datenübermittlungen in die USA – Fragen und Antworten zum EU-US Privacy Shield

Dieser Beitrag gibt einen Überblick über die Regelungen des EU-US Privacy Shield. Er richtet sich schwerpunktmäßig an verantwortliche Stellen. Zur Umsetzung der Angemessenheitsentscheidung der EU-Kommission über das EU-US Privacy Shield sind Abstimmungen zwischen den Aufsichtsbehörden in Deutschland und der EU erforderlich - auch um gemeinsame Verständnisse in Auslegungsfragen zu erreichen. Die folgenden Informationen werden deshalb kontinuierlich aktualisiert, erweitert und gegebenenfalls angepasst.

Bis zum 06.10.2015 konnten Datenübermittlungen in die USA über die entsprechende Angemessenheitsentscheidung der EU-Kommission auf die sogenannten Safe-Harbor-Grundsätze gestützt werden. Der Europäische Gerichtshof (EuGH) hat jedoch mit Urteil vom 06.10.2015 die Angemessenheitsentscheidung der EU-Kommission zu Safe Harbor für ungültig erklärt (Az. C-362/14). Datenübermittlungen in die USA können deshalb nicht mehr auf die Regelungen zu Safe Harbor und entsprechende Selbstzertifizierungen von US-Unternehmen gestützt werden. In Folge dieses Urteils hat die EU-Kommission mit den USA das sogenannte EU-US Privacy Shield verhandelt. Dieses soll die durch den EuGH aufgestellten Vorgaben erfüllen und Safe Harbor ersetzen.

Mit [Beschluss vom 12.07.2016](#) hat die EU-Kommission die Entscheidung getroffen, dass unter den Regelungen des EU-US Privacy Shield ein angemessenes Datenschutzniveau für Datenübermittlungen in die USA besteht.

Die Artikel-29-Gruppe, in der die europäischen Datenschutzbehörden zusammenarbeiten, begrüßt Verbesserungen im Vergleich zur Safe-Harbor-Entscheidung. Sie bedauert in ihrer [Presseerklärung vom 26.07.2016](#) jedoch, dass mit dem EU-US Privacy Shield nicht alle Bedenken ausgeräumt sind.

1. An welcher Stelle ist das EU-US Privacy Shield für verantwortliche Stellen relevant?

Bei der datenschutzrechtlichen Prüfung einer Datenübermittlung in das Ausland müssen durch die verantwortliche Stelle immer zwei Stufen berücksichtigt werden.

In der ersten Stufe muss geprüft werden, ob eine Rechtsgrundlage für die Übermittlung vorliegt (§ 4 Abs. 1 Bundesdatenschutzgesetz (BDSG)).

In der zweiten Stufe muss geprüft werden, ob die von der Übermittlung betroffenen Personen durch die Weitergabe ihrer Daten keine unverhältnismäßigen Eingriffe in ihre Persönlichkeitsrechte erfahren. Solche Eingriffe sind nicht zu befürchten, wenn personenbezogene Daten in Staaten übermittelt werden, die ein angemessenes Datenschutzniveau besitzen (dies ist zum Beispiel bei allen EU-Mitgliedstaaten der Fall). Die EU-Kommission hat mit ihrem [Beschluss vom 12.07.2016](#) zum EU-US Privacy Shield das Datenschutzniveau in den USA sektoral (in Bezug auf die selbstzertifizierte US-Unternehmen) als angemessen anerkannt. Weiterführende allgemeine Informationen zum Datenschutz bei Übermittlungen in das Ausland sind in dem Beitrag [„Wie wird der Schutz der Persönlichkeitsrechte bei der Übermittlung von Daten in das Ausland gewährleistet“](#) zusammengestellt.

Eine verantwortliche Stelle hat bestimmte zusätzliche [Prüfpflichten](#), wenn sie sich in der zweiten Stufe auf das Privacy Shield berufen möchte.

2. Darf das EU-US Privacy Shield ab sofort herangezogen werden, um ein angemessenes Datenschutzniveau für Datenübermittlungen in die USA zu gewährleisten?

Die datenempfangenden Unternehmen in den USA (US-Unternehmen), die sich den Regelungen des EU-US Privacy Shields unterwerfen wollen, können sich seit dem 01.08.2016 beim US-Handelsministerium selbstzertifizieren. Das Ministeri-

um stellt eine offizielle [Liste](#) der aktiven zertifizierten sowie inaktiven Unternehmen zur Verfügung. Sie steht ausschließlich in einer englischen Sprachversion zur Verfügung. Sobald ein US-Unternehmen in dieser Liste aufgeführt ist, kann das EU-US Privacy Shield auf der zweiten Stufe (siehe hierzu [Frage 1](#)) grundsätzlich herangezogen werden, um Daten in die USA zu übermitteln. Eine verantwortliche Stelle hat bestimmte [Prüfpflichten](#), wenn sie sich auf das Privacy Shield berufen möchte.

Die [Bedenken der europäischen Aufsichtsbehörden](#) zu Datenübermittlungen in die USA können ebenfalls Auswirkungen haben.

3. Welche Bedenken bestehen auf Seiten der europäischen Datenschutzbehörden und welche Auswirkungen haben sie?

Die Art-29-Gruppe hat in ihrer [Presseerklärung vom 26.07.2016](#) weiterhin Bedenken gegen das EU-US Privacy Shield geäußert. Diese betreffen sowohl kommerzielle Aspekte (beispielsweise das Fehlen von konkreten Regelungen zu automatisierten Entscheidungen und zu einem allgemeinen Widerspruchsrecht) als auch den Zugang der staatlichen US-Behörden zu den Daten, die aus der EU unter dem EU-US Privacy Shield übermittelt werden.

Im Rahmen der ersten gemeinsamen jährlichen Überprüfung des EU-US Privacy Shield werden die nationalen Vertreter der Art-29-Gruppe deshalb nicht nur bewerten, ob die verbleibenden Probleme gelöst sind, sondern auch, ob die Schutzmaßnahmen des EU-US Privacy Shield funktionsfähig und effektiv sind. Daraus können sich Maßnahmen der Aufsichtsbehörden ergeben. Außerdem können sich die Ergebnisse der Prüfung hinsichtlich des Zugangs von staatlichen Behörden zu Daten, die unter dem EU-US Privacy Shield übermittelt werden, auch auf andere Übermittlungsinstrumente wie verbindliche Unternehmensregelungen (BCRs) und Standardvertragsklauseln auswirken.

Die LDI NRW behält sich vor, aufgrund von Ergebnissen der jährlichen Überprüfung des EU-US Privacy Shield und eigenen Erkenntnissen, Datenübermittlungen unter dem EU-US Privacy Shield gegebenenfalls in Einzelfällen auszusetzen. Die irische Datenschutzbehörde hat außerdem ein gerichtliches Verfahren zur Überprüfung der EU-Standardvertragsklauseln vor dem irischen Commercial Court angestrengt. Die EU-Standardvertragsklauseln sind ein weiteres Instrument, mit denen bei Datenübermittlungen in Drittstaaten Garantien für den [Schutz der Persönlichkeitsrechte](#) erreicht werden können. Die Verhandlung ist für Februar 2017 angesetzt worden. Entscheidungen im weiteren Verfahren (letztendlich wohl des Europäischen Gerichtshofes) können Auswirkung speziell auf die Wirksamkeit des Beschlusses der EU-Kommission zu den Standardvertragsklauseln als auch allgemein auf andere Übermittlungsinstrumente haben.

4. Welche Prüfpflichten obliegen verantwortlichen Stellen?

Verantwortliche Stellen müssen bei jeder Datenverarbeitung prüfen, ob diese [datenschutzrechtlich zulässig](#) ist. Im Rahmen der sorgfältigen Auswahl eines selbstzertifizierten US-Unternehmens müssen sich verantwortliche Stellen vergewissern, dass das datenempfangende US-Unternehmen eine gültige Zertifizierung besitzt und dass diese auch eingehalten wird. Die verantwortliche Stelle muss dafür mindestens klären, ob die Zertifizierung tatsächlich vorliegt, diese noch gültig ist (diese muss jährlich erneuert werden) und ob die zu übermittelnden Daten von der Zertifizierung abgedeckt sind.

Verantwortliche Stellen sollten sich ebenfalls nachweisen lassen, wie das US-Unternehmen seinen Informationspflichten gegenüber den von der Datenverarbeitung betroffenen Personen nachkommt.

Soweit US-Unternehmen die Übergangsregelungen in Bezug auf den Grundsatz der Verantwortlichkeit der Weitergabe in Anspruch nehmen ([Frage 5](#)), sollten sich verantwortliche Stellen die vollständige Umsetzung des Grundsatzes nach Ablauf der Übergangszeit nachweisen oder zumindest bestätigen lassen.

Das US-Handelsministerium stellt eine offizielle [Liste](#) der aktiven zertifizierten sowie inaktiven Unternehmen zur Verfügung. Sie steht ausschließlich in einer englischen Sprachversion zur Verfügung.

5. Gibt es Übergangsregelungen?

Die Regelungen des EU-US Privacy Shield gelten grundsätzlich unmittelbar vom Zeitpunkt der Zertifizierung an. Damit müssen auch die Anforderungen an zertifizierte US-Unternehmen grundsätzlich unmittelbar vom Zeitpunkt der Zertifizierung an vollständig umgesetzt werden. Die Angemessenheitsentscheidung der EU-Kommission enthält jedoch in Anhang II, Abschnitt III.6.e Übergangsregelungen im Zusammenhang mit dem Grundsatz der Verantwortlichkeit für die Weitergabe. Damit ist die Verantwortlichkeit für die Weitergabe von übermittelten Daten durch das datenempfangende Unternehmen in den USA (US-Unternehmen) an eine andere Stelle gemeint. Das US-Unternehmen muss nach seiner Selbstzertifizierung so schnell wie möglich, spätestens jedoch innerhalb von neun Monaten, die Anforderungen aus dem Grundsatz der Verantwortlichkeit für die Weitergabe umsetzen. Um die Übergangsregelungen in Anspruch nehmen zu können müssen folgende Anforderungen erfüllt sein:

- Das US-Unternehmen muss bereits vor der Selbstzertifizierung geschäftliche Beziehungen zu den Dritten unterhalten, an die Daten weitergegeben werden sollen.
- Das US-Unternehmen muss sich innerhalb von zwei Monaten nach Inkrafttreten der Entscheidung in den USA (01.08.2016) selbstzertifizieren.
- Bei Weiterübermittlungen von Daten an Dritte muss das US-Unternehmen auch während der Übergangszeit die Grundsätze der Informationspflicht und Wahlmöglichkeit anwenden.
- Bei der Weitergabe an Dritte, die im Auftrag und auf Weisung des US-Unternehmens tätig werden, muss sich das US-Unternehmen vergewissern, dass der Beauftragte mindestens das Schutzniveau gewährleistet, das in den Grundsätzen gefordert wird.

Das EU-US Privacy Shield kann dann auch schon in diesem Übergangszeitraum herangezogen werden.

6. Können alle US-Unternehmen an der Selbstzertifizierung teilnehmen?

Es können solche US-Unternehmen an der Selbstzertifizierung des EU-US Privacy Shield teilnehmen, die den Untersuchungs- und Durchsetzungsbefugnissen der Federal Trade Commission (FTC), des US-Verkehrsministeriums (Department of Transportation) oder anderer gesetzlicher Organe, die die Einhaltung der Grundsätze effektiv gewährleisten, unterliegen. Die EU kann dazu weitere US-Behörden anerkennen. Diese würden dann als Anhang dem Beschluss der EU-Kommission beigefügt (Anhang II, Abschnitt I.2 des Beschlusses der EU-Kommission; Anhang II enthält die Grundsätze des EU-US Privacy Shields). Besondere Rahmenbedingungen bestehen in Bezug auf [Personaldaten](#).

7. Welche Inhalte haben die Grundsätze des EU-US Privacy Shield?

In Anhang II, Abschnitt II der [Angemessenheitsentscheidung der EU-Kommission](#) zum EU-US Privacy Shield sind Datenschutzgrundsätze definiert, die von den selbstzertifizierten US-Unternehmen eingehalten werden müssen. Diese Struktur wurde aus dem Safe-Harbor-Abkommen beziehungsweise der Angemessenheitsentscheidung der EU-Kommission zu Safe Harbor weitergeführt. Die hier zusammengestellten Informationen können von verantwortlichen Stellen beispielsweise im Rahmen von Auswahlentscheidungen oder bei der Unterstützung von betroffenen Personen, etwa im Beschäftigungsverhältnis, herangezogen werden:

- **Informationspflicht** (Anhang II, Abschnitt II.1)

US-Unternehmen müssen betroffenen Personen eine Reihe von Informationen zur Verfügung stellen. Dies sind unter anderem Angaben zu den Arten der erfassten personenbezogenen Daten, der Identität von Dritten, an

die die Daten weitergegeben werden, sowie der Zweck der Weitergabe. Ebenfalls müssen die US-Unternehmen auf das Auskunftsrecht der betroffenen Personen und das gewählte Streitbeilegungsgremium hinweisen. Zertifizierte US-Unternehmen müssen betroffene Personen außerdem darüber informieren, dass sie aufgrund rechtmäßiger Behördenanfragen zu den Zwecken der nationalen Sicherheit oder der Strafverfolgung verpflichtet sind, Daten offenzulegen. Im Sinne einer bestmöglichen Umsetzung der Grundsätze sollten US-Unternehmen konkret darüber informieren, in welchen Fällen zu diesen Zwecken bei ihnen regelmäßig [zulässige Ausnahmen](#) von den Grundsätzen Anwendung finden werden. US-Unternehmen können außerdem, soweit rechtlich zulässig, Transparenzberichte über die Anzahl der Anträge von Behörden auf Datenzugriff aus Gründen der Strafverfolgung oder nationalen Sicherheit veröffentlichen.

Die Informationspflichten enthalten spiegelbildlich ein Recht auf Information der betroffenen Personen.

- **Wahlmöglichkeit** (Anhang II, Abschnitt II.2)

Sollen Daten durch das US-Unternehmen an Dritte weitergegeben werden oder Daten zu anderen Zwecken verarbeitet werden, die wesentlich von dem ursprünglichen Zweck abweichen, muss der betroffenen Person diesbezüglich eine Wahlmöglichkeit gegeben werden (davon umfasst sind auch Abweichungen von dem Zweck, dem die betroffene Person nachträglich zugestimmt hat).

Diese Wahlmöglichkeit ist als Widerspruchsrecht („opt-out“) oder als ausdrückliche Zustimmung („opt-in“) umgesetzt. Eine ausdrückliche Zustimmung ist bei sensiblen Daten erforderlich. Diese umfassen die besonderen Arten personenbezogener Daten nach dem Bundesdatenschutzgesetz (BDSG). Bei nicht wesentlichen Zweckänderungen muss der betroffenen Person keine Wahlmöglichkeit eingeräumt werden.

Gibt das zertifizierte US-Unternehmen Daten an einen Dritten weiter, der in seinem Auftrag tätig ist (Auftrags(daten)verarbeiter), ist der Grundsatz

der Wahlmöglichkeit nicht anwendbar. Das US-Unternehmen muss dafür jedoch einen Vertrag mit dem Beauftragten abschließen (siehe auch den Grundsatz der Verantwortlichkeit für Weitergabe sowie zu den Grenzen von Zweckänderungen den Grundsatz der Datenintegrität und Zweckbindung).

- **Verantwortlichkeit für Weitergabe** (Anhang II, Abschnitt II.3)

US-Unternehmen dürfen Daten, die sie unter dem EU-US Privacy Shield erhalten haben, unter bestimmten Umständen an ein anderes Unternehmen weitergeben:

Sollen Daten an einen Dritten, der als verantwortliche Stelle tätig wird, weitergegeben werden, muss das US-Unternehmen mit diesem einen Vertrag schließen. Darin ist zu regeln, dass die Daten nur im Rahmen der (festzulegenden) zulässigen Zweckbestimmungen verarbeitet werden dürfen. Der Dritte muss sich dazu verpflichten, das gleiche Schutzniveau vorzusehen wie die Grundsätze des EU-US Privacy Shield. Er muss sich außerdem dazu verpflichten, das zertifizierte US-Unternehmen zu unterrichten, sollte er diese Verpflichtung nicht mehr erfüllen können. In einem solchen Fall muss die Datenverarbeitung durch den Dritten entweder eingestellt werden oder er muss mit anderen sinnvollen und geeigneten Maßnahmen Abhilfe schaffen.

Sollen Daten an einen Dritten, der im Auftrag und auf Anweisung des zertifizierten US-Unternehmens tätig wird (Auftrags(daten)verarbeiter) weitergegeben werden, muss das US-Unternehmen mit diesem ebenfalls einen Vertrag abschließen. Der Grundsatz geht hier jedoch detaillierter auf die Dinge ein, die das zertifizierte US-Unternehmen sicherstellen muss (und deshalb auch gegebenenfalls detaillierter vertraglich regeln sollte). Zusätzlich müssen auf Verlangen die vereinbarten Regelungen zum Datenschutz dem US-Handelsministerium vorgelegt werden. Das US-Unternehmen haftet außerdem für Verstöße des verarbeitenden Dritten gegen die Grundsätze des EU-US Privacy Shield, außer es kann nachweisen, für das Schadensereignis nicht verantwortlich zu sein.

Die Vorgaben der Grundsätze der Informationspflicht und Wahlmöglichkeit sind dabei immer einzuhalten – der Grundsatz der Wahlmöglichkeit gilt nicht für Weitergaben von Daten durch das zertifizierte US-Unternehmen an einen Dritten, der im Auftrag und auf Anweisung tätig wird (Auftrags(daten)verarbeiter), siehe Grundsatz der Wahlmöglichkeit.

Erhält das US-Unternehmen selbst Daten als Auftrags(daten)verarbeiter, muss die datenübermittelnde verantwortliche Stelle außerdem die [Anforderungen aus § 11 BDSG](#) beachten.

- **Sicherheit** (Anhang II, Abschnitt II.4)
US-Unternehmen müssen unter dem EU-US Privacy Shield angemessene und geeignete Maßnahmen zum Schutz vor Verlust, Missbrauch und unbefugtem Zugriff, Weitergabe, Änderung und Zerstörung ergreifen.
- **Datenintegrität und Zweckbindung** (Anhang II, Abschnitt II.5)
Personenbezogene Daten müssen auf die Informationen beschränkt sein, die für den rechtmäßigen Verarbeitungszweck erheblich sind. Sie dürfen nur so lange aufbewahrt werden, wie dies zur Zweckerfüllung erforderlich ist. In besonderen Fällen kann hiervon abgewichen werden, z.B. bei Verarbeitungen zur Archivierung im öffentlichen Interesse, für journalistische Zwecke oder für die wissenschaftliche oder historische Forschung.

Grundsätzlich darf das datenempfangende US-Unternehmen personenbezogene Daten nur für die Zwecke verwenden, für die sie ursprünglich erhoben wurden, oder für solche Zwecke, denen die betroffene Person nachträglich zugestimmt hat. Daten dürfen außerdem nie für andere Zwecke weiterverwendet werden, die mit dem ursprünglichen Erhebungszweck oder mit dem Zweck unvereinbar sind, dem die betroffene Person nachträglich zugestimmt hat. Ansonsten hängt die Zulässigkeit der Verwendung der Daten für einen anderen Zweck davon ab, wie stark der ursprüngliche Zweck von der neuen Zweckbestimmung abweicht (siehe Grundsatz der Wahlmöglichkeit).

- **Auskunftsrecht** (Anhang II, Abschnitt II.6)
Betroffene Personen haben einen Auskunftsanspruch gegenüber den US-Unternehmen, die personenbezogene Daten unter dem EU-US Privacy Shield empfangen. Der Anspruch bezieht sich auf die über sie gespeicherten oder verarbeiteten Daten. Dies schließt auch eine Auskunft darüber ein, ob das US-Unternehmen überhaupt Daten der Person speichert oder verarbeitet. Die betroffene Person muss grundsätzlich die Möglichkeit haben, Daten zu korrigieren, zu ändern oder zu löschen, wenn sie falsch sind oder unter Verstoß gegen die Grundsätze verarbeitet wurden.
- **Rechtsschutz, Durchsetzung und Haftung** (Anhang II, Abschnitt II.7; Abschnitt III.11)
Zertifizierte US-Unternehmen müssen anlassunabhängige Kontrollverfahren einsetzen um sich zu vergewissern, dass die Vorgaben des EU-US Privacy Shield tatsächlich umgesetzt werden. Die Kontrollen müssen mindestens einmal jährlich durchgeführt werden und können entweder durch die Unternehmen selbst oder durch externe Stellen durchgeführt werden. Hinzu kommen bestimmte Dokumentationspflichten.

Im Rahmen des EU-US Privacy Shield müssen teilnehmende US-Unternehmen selbst für Nachfragen und Beschwerden zur Verfügung stehen und innerhalb von 45 Tagen nach Eingang einer Beschwerde antworten. Sie müssen zusätzlich ein kostenfreies Beschwerde-/Abhilfeverfahren bei unabhängigen Beschwerdestellen (auch Streitbeilegungsgremien genannt) anbieten. US-Unternehmen können grundsätzlich frei unter Durchsetzungsmechanismen entscheiden, welche die Anforderungen der Grundsätze des EU-US Privacy Shield erfüllen. Folgende mögliche Mechanismen sind in den Grundsätzen ausdrücklich aufgeführt:

1. Befolgung von Datenschutzprogrammen privater Anbieter für alternative Streitbeilegung aus der EU oder den USA (in den Programmen sind die Grundsätze und wirksame Durchsetzungsmechanismen integriert),

2. indem sich die zertifizierten US-Unternehmen gesetzlich oder durch Rechtsverordnung vorgesehenen Kontrollorganen (in den USA) unterwerfen, die Beschwerden von Einzelpersonen nachgehen und Streitigkeiten schlichten oder
3. indem sie sich zur Zusammenarbeit mit den EU-Datenschutzbehörden verpflichten.

Für das Beschwerde-/Abhilfungsverfahren bei den EU-Datenschutzbehörden ist ein informelles Gremium der Datenschutzbehörden vorgesehen. Soweit Personaldaten unter dem EU-US Privacy Shield übermittelt werden sollen, müssen sich US-Unternehmen in Bezug auf diese Daten zwingend zur Zusammenarbeit mit den EU-Datenschutzbehörden verpflichten ([hierzu auch Frage 10, Personaldaten](#)). Erhält ein US-Unternehmen sowohl Personaldaten als auch andere Datenarten, dürfen US-Unternehmen für die anderen Datenarten ein separates Beschwerde-/Abhilfungsverfahren auswählen. Entsprechend sieht die Privacy-Shield-Liste des US-Handelsministeriums separate Felder für Beschwerde-/Abhilfungsverfahren vor.

Betroffene Personen können sich auch direkt an die [Federal Trade Commission als Durchsetzungsbehörde](#) oder an die für sie zuständige EU-Datenschutzbehörde wenden. Je nach Einzelfall kann die Datenschutzbehörde dann tätig werden:

Sie kann im Rahmen ihrer Zuständigkeit gegenüber der datenübermittelnden verantwortlichen Stelle in der EU handeln.

Wenn sich das Unternehmen zur Zusammenarbeit mit den EU-Aufsichtsbehörden verpflichtet hat, kann sie im Rahmen des Beschwerde-/Abhilfungsverfahrens über das Gremium der EU-Datenschutzbehörden gegenüber dem US-Unternehmen tätig werden.

Sie hat außerdem die Möglichkeit, die Beschwerde über eine spezielle Kontaktstelle an das US-Handelsministerium weiterleiten.

Zertifizierte US-Unternehmen haften für eigene Verstöße gegen die Regelungen des EU-US Privacy Shield sowie grundsätzlich auch für Verstöße von Dritten, die im Auftrag und auf Anweisung des zertifizierten US-Unternehmens tätig werden (Auftrags(daten)verarbeiter).

Zusätzlich sieht das EU-US Privacy Shield für betroffene Personen die Möglichkeit eines kostenpflichtigen Schiedsgerichtsverfahrens für so genannte „Restansprüche“ vor. Betroffene Personen können dieses Verfahren daher nicht direkt, sondern erst nach Erschöpfung anderer Beschwerde-/Abhilfemechanismen in Gang setzen. Das Schiedsverfahren kann nicht in Anspruch genommen werden, sofern EU-Datenschutzbehörden zuständig sind oder befugt sind, geltend gemachte Verstöße direkt zu klären. Nicht eindeutig sind die Regelungen des EU-US Privacy Shield zu der Frage, ob die betroffene Person vor Beantragung des Schiedsverfahrens zwingend alle anwendbaren Abhilfemechanismen kumulativ durchlaufen muss.

Verstöße eines zertifizierten US-Unternehmens gegen die Grundsätze des EU-US Privacy Shield sind außerdem durch die für die Durchsetzung zuständigen US-Behörden als unlautere und irreführende Praktiken verfolgbar.

Diese Grundsätze werden in Zusatzgrundsätzen (Anhang II, Abschnitt III) konkretisiert und an einzelnen Stellen eingeschränkt.

8. Gibt es Ausnahmen von den Grundsätzen des EU-US Privacy Shield?

Die Einhaltung der Grundsätze des EU-US Privacy Shield kann begrenzt sein, soweit Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Strafverfolgung Rechnung getragen werden muss.

Einschränkungen können durch Gesetzesrecht, staatliche Regulierungsvorschriften oder Fallrecht erfolgen. Aus diesen müssen sich Verpflichtungen oder ausdrückliche Ermächtigungen ergeben, die den Grundsätzen des EU-US Privacy Shield widersprechen. Dabei muss das US-Unternehmen nachweisen, dass es

die Grundsätze nur im erforderlichen Maß zur Erfüllung der übergeordneten Interessen nicht einhält.

Einschränkungen können sich auch aus Ausnahmeregelungen der Richtlinie oder des nationalen Rechts ergeben (beispielsweise bei der Weiterverarbeitung von Personaldaten oder bei einer Datenübermittlung an ein selbstzertifiziertes US-Unternehmen im Rahmen einer Auftrags(daten)verarbeitung).

Die möglichen Ausnahmen wirken sich auch auf die [Informationspflichten](#) der selbstzertifizierten Unternehmen aus.

9. Welche Betroffenenrechte ergeben sich aus dem EU-US Privacy Shield?

Die Betroffenenrechte unter dem EU-US Privacy Shield sind

- Recht auf Information,
- Wahlmöglichkeit (Anhang II, Abschnitt II.2),
- Auskunftsrecht (Anhang II, Abschnitt II.5),
- Recht auf Inanspruchnahmen der Beschwerde-/Abhilfeverfahren (Anhang II, Abschnitt II.7) und
- Recht auf Einreichung eines Antrags zur Anrufung der Ombudsperson (Anhang III, Anlage A).

In Anhang II, Abschnitt III sind hierzu besondere Regelungen enthalten.

Ausführlichere Informationen zu den Betroffenenrechten werden zurzeit erstellt.

10. Sind besondere Vorgaben hinsichtlich Personaldaten zu beachten?

Für Übermittlungen von Personaldaten unter dem EU-US Privacy Shield sind besondere Rahmenbedingungen zu beachten. Zunächst ist geregelt, unter welchen Umständen die Grundsätze des EU-US Privacy Shield auf Übermittlungen von Personaldaten anwendbar sind. US-Unternehmen müssen dann besondere Anforderungen erfüllen, um sich für den Erhalt von Personaldaten unter dem EU-

US Privacy Shield zu zertifizieren. Sie müssen sich beispielsweise dazu verpflichten, mit der (den) Datenschutzbehörde(n) in der EU zusammenzuarbeiten und den Empfehlungen der Behörden nachzukommen. Für die eigentlichen Übermittlungen werden ebenfalls besondere Rahmenbedingungen aufgestellt. Die folgenden Anforderungen können auch direkte Auswirkung für die datenübermittelnden verantwortlichen Stellen in der EU haben:

- Die Grundsätze des EU-US Privacy Shield sind auf Übermittlungen von Personaldaten anwendbar, wenn die verantwortliche Stelle in der EU Daten über ihre (früheren oder derzeitigen) Beschäftigten im Rahmen des Beschäftigungsverhältnisses erhoben hat und diese entweder an eine Mutterorganisation, eine verbundene Organisation oder eine Dienstleistungsorganisation übermittelt.
- Der Grundsatz der Wahlmöglichkeit ist unter Umständen eingeschränkt, da allgemeine Regelungen in EU-Mitgliedstaaten zur Datenübermittlung gegebenenfalls zweckändernde Weiterverarbeitungen in Drittstaaten ausschließen können. Solche Einschränkungen erkennt auch das EU-US Privacy Shield an. Datenübermittelnde verantwortliche Stellen müssen US-Unternehmen in solchen Fällen darauf hinweisen und sollten dies gegebenenfalls vertraglich regeln.
- Macht ein Beschäftigter gemäß des Grundsatzes der Wahlmöglichkeit von seinem Widerspruchsrecht Gebrauch oder erteilt er nicht seine Einwilligung, darf dies keine Minderung seiner Berufschancen zur Folge haben. Es wird in diesem Zusammenhang außerdem zusätzlich klargestellt, dass dies keine Sanktionen zur Folge haben darf.
- Individuellen Datenschutzbedürfnissen der Beschäftigten ist angemessen Rechnung zu tragen. Als Beispiele werden die Beschränkung des Zugriffs auf bestimmte Daten oder Anonymisierung beziehungsweise Pseudonymisierung genannt.

11. Welche staatlichen Stellen überwachen die Einhaltung des EU-US Privacy Shield?

1. EU-Datenschutzbehörden

Die EU-Datenschutzbehörden bleiben uneingeschränkt zuständig nach dem jeweils anwendbaren nationalen Recht. Sie können im Rahmen ihrer Zuständigkeit immer gegenüber der datenübermittelnden verantwortlichen Stelle in der EU tätig werden. Soweit sich zertifizierte US-Unternehmen zur Zusammenarbeit mit den EU-Datenschutzbehörden als unabhängige Beschwerdestellen/Streitbelegungs-gremium verpflichtet haben, sind sie insoweit auch für US-Unternehmen zuständig.

2. Federal Trade Commission und das US-Verkehrsministerium (Department of Transportation)

Die Federal Trade Commission (FTC) und das US-Verkehrsministerium sind sogenannte „Durchsetzungsbehörden“. Sie sind befugt, die Zusagen der US-Unternehmen im Rahmen ihrer Selbstzertifizierungen durchzusetzen. Andere gesetzliche (US-)Organe, die die Einhaltung der Grundsätze effektiv gewährleisten und von der EU entsprechend anerkannt werden, können zukünftig in einem zusätzlichen Anhang als Durchsetzungsbehörden aufgeführt werden. Diese Stellen können die Zusagen von zertifizierten US-Unternehmen zur Einhaltung des EU-US Privacy Shield durchsetzen, zum Beispiel durch Unterlassungsanordnungen. Deshalb können die unabhängigen privaten Beschwerdestellen/Streitbelegungs-gremien bei Missachtung ihrer Entscheidungen entweder die Gerichte anrufen oder die zuständige Durchsetzungsbehörde als entscheidungsbefugte Behörde verständigen. Verstöße eines zertifizierten US-Unternehmens gegen die Grundsätze des EU-US Privacy Shield sind außerdem durch die für die Durchsetzung zuständigen US-Behörden als unlautere und irreführende Praktiken verfolgbar.

3. US-Handelsministerium (Department of Commerce)

Das US-Handelsministerium war Verhandlungspartner der EU-Kommission für das EU-US Privacy Shield und ist für den Selbstzertifizierungsprozess insgesamt zuständig. Die Erklärungen der US-Unternehmen zur Selbstzertifizierung, erfol-

gen deshalb ihm gegenüber. Das Ministerium prüft auch das Vorliegen der formalen Anforderungen und stellt die Liste der zertifizierten bzw. nicht mehr zertifizierten Unternehmen zur Verfügung. Über eine Kontaktstelle bei dem Ministerium können EU-Datenschutzbehörden eingegangene Beschwerden, für die sie nicht selbst zuständig sind, weiterleiten. Das Ministerium bemüht sich um Klärung der Beschwerden und kontrolliert außerdem von Amts wegen die Einhaltung der Zusagen der zertifizierten US-Unternehmen unter dem EU-US Privacy Shield. Es schaltet gegebenenfalls die zuständige Durchsetzungsbehörde ein. US-Unternehmen, die die Grundsätze des EU-US Privacy Shield fortgesetzt missachten, werden von dem Ministerium von der Privacy Shield Liste gestrichen.

12. Welche Rolle hat die Ombudsperson des EU-US Privacy Shield inne?

Der Ombudsperson-Mechanismus ist ein neues Abhilfeverfahren für den Bereich der nationalen Sicherheit. Darüber sollen Anfragen und Beschwerden von betroffenen Personen zum Zugriff auf Daten, die die nationale Sicherheit betreffen, koordiniert und beantwortet werden. Die Rolle der Ombudsperson wird durch einen höheren Beamten im US-Außenministerium eingenommen. Die Ombudsperson steht der Ombudsstelle des EU-US Privacy Shield vor. Dieser Mechanismus ist nicht nur auf Sachverhalte im Zusammenhang mit dem EU-US Privacy Shield beschränkt. Er ist für sämtliche Datenübermittlungen von der EU in die USA anwendbar. Weitere Ausführungen zum Verfahren sind in dem Schreiben des US-Außenministeriums an die EU-Kommission (Anhang III des [Beschlusses der EU-Kommission](#)) enthalten.

13. Welche Anforderungen sind zu beachten wenn ein datenempfangendes US-Unternehmen als Auftrags(daten)verarbeiter tätig wird?

Sollen personenbezogene Daten aus der EU in den USA im Auftrag verarbeitet werden, müssen verantwortliche Stellen neben den Zulässigkeitsvoraussetzungen der „zweiten Stufe“ der Datenverarbeitung (§§ 4b, 4c BDSG) auch die An-

forderungen des § 11 BDSG erfüllen. Denn die Voraussetzungen des § 11 BDSG betreffen die so genannte 1. Stufe des Datenumgangs und müssen daher unabhängig davon eingehalten werden, wo die Auftragsdatenverarbeitung stattfindet.

Die Selbstzertifizierung eines datenempfangenden US-Unternehmens (Auftrags(daten)verarbeiter) unter dem EU-US Privacy Shield bezieht sich dabei auf die Zulässigkeitsvoraussetzungen der zweiten Stufe der Datenverarbeitung.