Stand: 22.08.2018

# FAQ für verantwortliche Stellen

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

Vor einer Datenübermittlung muss die datenübermittelnde Stelle die Einhaltung des anwendbaren Datenschutzrechts sicherstellen. Bei der datenschutzrechtlichen Prüfung einer Datenübermittlung in das Ausland muss sie zwei Stufen berücksichtigen.

In der ersten Stufe muss der Verantwortliche prüfen, ob eine Rechtsgrundlage für die Übermittlung vorliegt (Art. 5 Abs. 1 lit. a), Art. 6 EU Datenschutz-Grundverordnung). Außerdem müssen alle allgemeinen Anforderungen an die Datenverwendung eingehalten werden (zum Beispiel der Zweckbindungs- und Erforderlichkeitsgrundsatz, Informationspflichten). Auftragsverarbeiter müssen die sie als Auftragsverarbeiter treffenden allgemeinen Pflichten erfüllen. Informationen zum Thema Auftragsverarbeitung enthält das Kurzpapier Nr. 13 (Auftragsverarbeitung).

Werden personenbezogene Daten unter dem EU-US Privacy Shield an ein US-Unternehmen als verantwortliche Stelle übermittelt, muss der datenübermittelnde Verantwortliche die Betroffenen über die Identität der Empfänger ihrer Daten informieren und darüber, dass die Daten vom Schutz des EU-US Privacy Shield profitieren. Damit können die Betroffenen ihre Rechte aus dem EU-US Privacy Shield gegenüber der datenempfangenden verantwortlichen Stelle wahrnehmen. Zu beachten ist außerdem, dass Datenübermittlungen an andere Unternehmen außerhalb der EU/des Europäischen Wirtschaftsraums (EWR) in Leistungsverträgen (etwa mit Geschäftspartnern) ausgeschlossen sein können.

Bei Datenübermittlungen in Länder außerhalb der EU/des EWR (Drittländer) ist in der zweiten Stufe zu prüfen, ob in einem Empfängerstaat ein dem Rechtsrahmen der Europäischen Union gegenüber angemessenes Datenschutzniveau gegeben ist bzw. geeignete oder angemessene Garantien umgesetzt sind (Art. 45-47DS-GVO) oder ob eine der Ausnahmeregelungen des Art. 49 DS-GVO anwendbar ist. 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 den Selbstzertifizierungsmechanismus des Privacy Shield) als angemessen anerkannt. Weiterführende allgemeine Informationen zum Datenschutz bei Übermittlungen in das Ausland sind in dem Beitrag „Welche Anforderungen sind bei der Übermittlung von Daten in das Ausland zu beachten?“ zusammengestellt.

Eine datenübermittelnde Stelle hat bestimmte zusätzliche Prüfpflichten (siehe Frage 6), wenn sie sich auf das EU-US Privacy Shield berufen möchte.

## 2. Wann ist das EU-US Privacy Shield einschlägig?

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. Auf der Internetseite des Ministeriums werden Informationen zur Selbstzertifizierung bereitgestellt. Dort steht ebenfalls eine offizielle Liste der aktiven zertifizierten sowie inaktiven Unternehmen zur Verfügung (ausschließlich in Englisch). 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 datenübermittelnde Stelle hat bestimmte Prüfpflichten (siehe Frage 3), wenn sie sich auf das Privacy Shield berufen möchte. US-Unternehmen, die nicht mehr an dem Privacy-Shield-Selbstzertifizierungsmechanismus teilnehmen, dürfen keine personenbezogenen Daten mehr unter dem Privacy Shield erhalten. Sie müssen jedoch die Privacy-Shield-Prinzipien weiter auf die Daten anwenden, die sie unter ihrer aktiven Zertifzierung erhalten haben. Für Datenübermittlungen an US-Unternehmen, die nicht mehr an dem Privacy-Shield-Mechanismus teilnehmen, können alternative Übermittlungsinstrumente genutzt werden. Weitere Informationen hierzu sind in dem Beitrag „Welche Anforderungen sind bei der Übermittlung von Daten in das Ausland zu beachten?“ zusammengestellt.

Die Bedenken der europäischen Aufsichtsbehörden (siehe Frage 5) zu Datenübermittlungen in die USA können ebenfalls Auswirkungen haben.

## 3. Welche Prüfpflichten haben verantwortliche Stellen?

Datenübermittelnde Stellen müssen bei jeder Datenverarbeitung prüfen, ob diese datenschutzrechtlich zulässig (siehe Frage 1) ist. Im Rahmen der sorgfältigen Auswahl eines selbstzertifizierten US-Unternehmens müssen sich datenübermittelnde Stellen vergewissern, dass das datenempfangende US-Unternehmen eine gültige Zertifizierung besitzt. Die datenübermittelnde Stelle muss dafür mindestens klären, ob die Zertifizierung tatsächlich vorliegt, diese noch gültig ist (sie

muss jährlich erneuert werden) und ob die zu übermittelnden Daten von der Zertifizierung abgedeckt sind. Dazu müssen Unternehmen die offizielle Liste der aktiven zertifizierten sowie inaktiven Unternehmen einsehen. Diese wird durch das US-Handelsministerium bereitgestellt. Sie steht ausschließlich in einer englischen Sprachversion zur Verfügung.

Soweit US-Unternehmen die Übergangsregelungen in Bezug auf den Grundsatz der Verantwortlichkeit der Weitergabe in Anspruch genommen haben, sollten sich verantwortliche Stellen die vollständige Umsetzung des Grundsatzes nach Ablauf der Übergangszeit nachweisen oder zumindest bestätigen lassen (siehe Frage 6).

## 4. 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) oder des US-Verkehrsministeriums (Department of Transportation) unterliegen. Dies bedeutet, dass sich beispielsweise gemeinnützige Organisationen, Banken, Versicherungsunternehmen und Telekommunikationsdienstleister (hinsichtlich allgemeiner carrier activities) nicht selbstzertifizieren können, da sie nicht unter die Zuständigkeit der FTC oder des DoT fallen.

Weitere gesetzliche Organe der USA können hinzukommen. 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 (siehe Frage 11).

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

Die Artikel-29-Gruppe äußerte in ihrer Presseerklärung vom 26.07.2016 weiterhin Bedenken gegen das EU-US Privacy Shield. Ihre Bedenken betrafen 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.

Bedenken bestehen auch nach der ersten gemeinsamen jährlichen Überprüfung des Privacy-Shield-Mechanismus im Herbst 2017.

Die LDI NRW behält sich vor, aufgrund von Ergebnissen der jährlichen Überprüfungen des EU-US Privacy Shield sowie 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 High Court angestrengt. Die EU-Standardvertragsklauseln sind ein weiteres Instrument, mit denen bei Datenübermittlungen in Drittstaaten Garantien für den Schutz der Persönlichkeitsrechte erreicht werden können. Der irische High Court hat dem EuGH Fragen zu dem Inhalt des Verfahrens vorgelegt. Dieses Vorabentscheidungsersuchen wird unter dem Aktenzeichen C-311/18 geführt. Die Entscheidung des EuGH steht noch aus.

## 6. Gab es Übergangsregelungen und haben solche weiterhin Auswirkungen?

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. Die US-Unternehmen, die diese Ausnahme in Anspruch genommen haben, mussten nach der Selbstzertifizierung so schnell wie möglich, spätestens jedoch innerhalb von neun Monaten, die Anforderungen aus dem Grundsatz der Verantwortlichkeit für die Weitergabe umsetzen.

Datenübermittelnde Stellen sollten sich in solchen Fällen nach Ablauf der Übergangszeit die vollständige Umsetzung des Grundsatzes nachweisen oder bestätigen lassen.

## 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)

  Selbstzertifizierte 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. Die 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 (siehe Frage 8). 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 Stelle außerdem die Anforderungen aus Art. 28 EU Datenschutz-Grundverordnung beachten (siehe Frage 13).

- **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-/Abhilfeverfahren 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 (siehe auch Frage 10). Erhält ein US-Unternehmen sowohl Personaldaten als auch andere Datenarten, dürfen US-Unternehmen für die anderen Datenarten ein separates Beschwerde-/Abhilfeverfahren auswählen. Entsprechend sieht die Privacy-Shield-Liste des US-Handelsministeriums separate Felder für Beschwerde-/Abhilfeverfahren vor.

Betroffene Personen können sich auch direkt an die Federal Trade Commisson als Durchsetzungsbehörde (siehe Frage 11) 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 die Aufsichtsbehörde im Rahmen des Beschwerde-/Abhilfeverfahrens 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-Unternehmes 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 (siehe Frage 7).

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

In Anhang II, Abschnitten II und III (Grundsätzen und Zusatzgrundsätzen des EU-US Privacy Shield) sowie in Anhang III der Angemessenheitsentscheidung der EU-Kommission zum EU-US Privacy Shield (Grundsätze und Zusatzgrundsätze) sind die Rechte der Betroffenen unter dem EU-US Privacy Shield geregelt:

- Recht auf Information,
- Wahlmöglichkeit (Anhang II, Abschnitt II.2),
- Auskunftsrecht (Anhang II, Abschnitt II.6),
- 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 den Zusatzgrundsätzen (Anhang II, Abschnitt III) sind hierzu besondere Regelungen enthalten.

Ausführlichere Informationen zu den Betroffenenrechten, einschließlich der Beschwerdemöglichkeiten, finden Sie in den Informationen für Betroffene zum EU-US Privacy Shield.

## 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 verpflich-

ten, 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/Streitbelegungsgremium 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 so genannte „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/Streitbeilegungsgremien 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, erfolgen 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 Ombuds-

person 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 datenübermittelnde Stellen neben den Zulässigkeitsvoraussetzungen der „zweiten Stufe" der Datenverarbeitung (Art. 44f. EU Datenschutz-Grundverordnung) auch die Anforderungen des Art. 28 EU Datenschutz-Grundverordnung erfüllen. Denn die Voraussetzungen des Art. 28 EU Datenschutz-Grundverordnung für eine wirksame Auftragsverarbeitung betreffen die so genannte 1. Stufe des Datenumgangs und müssen daher unabhängig davon eingehalten werden, wo die Auftragsdatenverarbeitung stattfindet. Davon umfasst ist auch die Pflicht zum Abschluss eines Vertrages oder Etablierung eines anderen Rechtsinstrumentes gemäß Art. 28 Abs. 3 EU Datenschutz-Grundverordnung.

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