Verarbeitung von Beschäftigtendaten unter dem EU-U.S.-Datenschutzschild (Privacy Shield)

Stand: 27.09.2017

Inhalt

Thilo Weichert
Waisenhofstr. 41
24103 Kiel
0431 9719742
weichert@netzwerk-datenschutzexpertise.de

Karin Schuler
Kronprinzenstraße 76
53173 Bonn
schuler@netzwerk-datenschutzexpertise.de

www.netzwerk-datenschutzexpertise.de

Transfers von Beschäftigtendaten aus Europa bzw. Deutschland in die USA sind an der Tagesordnung, zumal viele hiesige Unternehmen US-Mütter oder Tochterunternehmen haben und daher oft eine zentralisierte oder arbeitsteilige Beschäftigtendatenverarbeitung erfolgt. Außerdem wird Outsourcing in den unterschiedlichsten Formen des Cloud Computing unter Einbeziehung US-amerikanischer Dienstleister praktiziert. Nachdem der Europäische Gerichtshof (EuGH) mit Urteil vom 06.10.2015 den Safe-Harbor-Rechtsrahmen zur Daten-Übermittlung in die USA aufgehoben hatte[1] und an dessen Stelle das EU-U.S.-Datenschutzschild (Privacy Shield)[2] trat, ist die Rechtsunsicherheit groß. Für seriöse Datenschützer ist klar, dass dieses Privacy Shield, ebenso wie zuvor Safe Harbor, gegen europäische Grundrechte verstößt. Für Betriebsräte, aber auch für Arbeitergeber stellt sich daher die Frage „Was tun?“ Darauf soll hier eine Antwort gegeben werden.

1 Rechtliche Grundlagen

Die Diskussion über den Datenaustausch mit den USA ist eine Never-ending-Story mit Licht und Schatten.[3] Das Licht wird durch die in Europa geltenden Grundrechte und die diese konkretisierenden datenschutzrechtlichen Regelungen gesetzt. Von zentraler Bedeutung ist die europäische **Grundrechte-Charta** (GRCh). Diese gewährleistet in Art. 7 ein Recht auf Privat- und Familienleben einschließlich der Vertraulichkeit der Kommunikation. Art. 8 gibt jedem Mensch ein Recht auf Schutz der personenbezogenen Daten, wozu die Einhaltung der Zweckbindung, ein Anspruch auf Auskunft über die eigenen gespeicherten Daten und die Überwachung der Einhaltung der Vorschriften durch eine unabhängige Datenschutzaufsicht gehört. Art. 47 spricht jedem Menschen ein Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht zu.

In Umsetzung des Rechts auf Datenschutz wurde 1995 eine **Europäische Datenschutz-Richtlinie** (EG-DSRl) verabschiedet, deren Kapitel IV die „Übermittlung personenbezogener Daten in Drittländer“, also in Länder außerhalb des Geltungsbereichs der EU-Datenschutzgesetzgebung, regelt. Dort ist in Art. 26 Abs. 6 vorgesehen, dass die Kommission feststellen kann, dass ein Drittland aufgrund seiner Rechtsvorschriften „hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau“ gewährleistet. Eine solche Feststellung durch die EU-Kommission erfolgte mit Beschluss vom 26.07.2000 in Bezug auf die USA, wenn sich das jeweilige US-Unternehmen im Rahmen des dort festgehaltenen **Safe-Harbor-Regelwerks** über eine Selbstverpflichtung zur Beachtung bestimmter Datenschutzgrundsätze bekennt.[4] Es ist zu beachten, dass die in diesem Artikel vorrangig diskutierte Angemessenheit des Datenschutzniveaus im Empfängerland nicht die grundsätzliche Zulässigkeitsprüfung einer Übermittlung ersetzt, so wie vielfach fälschlich angenommen wird.[5]

[1] EuGH U. v. 06.10.2015, C-362/14, NJW 2015, 3151 = JZ 2016, 360.
[2] Durchführungsbeschluss (EU) 2016/1250 der EU-Kommission v. 12.07.2016 gemäß der Richtlinie 95/46/EG über die Angemessenheit des vom EU-US-Privacy-Shield gebotenen Schutzes, ABl. EU v. 01.08.2016, L 207.
[3] Dazu Anlage 2.
[4] Entscheidung 2000/520/EG, ABl. EG v. 25.08.2000, L 215/7.
[5] Vgl. hierzu auch die Ausführungen unter Ziffer 6. Empfehlungen.

Der Safe-Harbor-Beschluss der EU-Kommission wurde vom **Europäischen Gerichtshof** (EuGH) mit Urteil v. 06.10.2015 aufgehoben, weil der dadurch gesetzte -Rechtsrahmen gegen Art. 7, 8 und 47 GRCh verstieß.[6]

Diese Rechtsprechung des EuGH fand Eingang in die kurz danach erfolgte Beschlussfassung der Europäischen **Datenschutz-Grundverordnung** (DSGVO)[7], die am 25.05.2016 in Kraft trat und vom 25.05.2018 an die bisherige EG-DSRl ablöst. Gemäß Art. 44 DSGVO darf bei einer Übermittlung ins Drittland das durch die DSGVO „gewährleistete Schutzniveau für natürliche Personen nicht untergraben“ werden. Ob dies der Fall ist, kann gem. Art. 45, DSGVO, ebenso wie zuvor gemäß der EG-DSRl, von der Kommission festgestellt werden, wobei nun in Abs. 2 ein umfassender Katalog für die Feststellung des „angemessenen Schutzniveaus“ aufgeführt ist, der u. a. folgende Kriterien enthält: Rechtsstaatlichkeit, Achtung der Menschenrechte und Grundfreiheiten, auch in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit sowie die wirksame Funktionsweise unabhängiger Aufsichtsbehörden. Als weitere Rechtfertigung für Datentransfers in Drittländer werden die ebenso von der Kommission zu beschließenden Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c DSGVO) sowie von Aufsichtsbehörden zu genehmigende „verbindliche interne Datenschutzvorschriften“ (Binding Corporate Rules – BCR, Art. 47 DSGVO) anerkannt. Gerichtsentscheidungen im Drittland, wie den USA, sind europarechtlich ohne Verbindlichkeit (Art. 48). Art. 49 DSGVO erlaubt im Einzelfall sowie aus Gründen des öffentlichen Interesses in weiteren Fällen Drittlandsübermittlungen.

Die datenschutzrechtlichen Anforderungen an die Übermittlung in Drittländer gemäß der DSGVO unterscheiden sich formell nicht von denen der EG-DSRl. Wohl aber sind die Anforderungen der EG-DSRl vom EuGH im Safe-Harbor-Urteil präzisiert worden. Diese sowie weitere Präzisierungen haben Eingang in die Regelungen zur **Drittlandsübermittlung in der DSGVO** gefunden. Dessen ungeachtet muss aber beachtet werden, dass mit der DSGVO das Datenschutzniveau generell gegenüber dem der EG-DSRl angehoben wurde. Wird also das Angemessenheitsniveau der EG-DSRl unterschritten, so gilt dies auch für das der DSGVO. Bestand dagegen die Angemessenheit im Hinblick auf die EG-DSRl, so muss dies bzgl. der DSGVO nicht der Fall sein.[8] Gem. Art. 45 Abs. 9 DSGVO bleiben Kommissions-Beschlüsse auf Grundlage von Art. 25 Abs. 6 EG-DSRl nach Wirksamwerden der DSGVO in Kraft, bis sie geändert, ersetzt oder gekündigt werden. Der Kommissions-Beschluss zum Privacy Shield erging am 12.06.2016, also nach Inkrafttreten der DSGVO am 25.05.2016, aber rechtlich auf der Grundlage des Art. 25 Abs. 6 EG-DSRl. Prüfungsgrundlage für die Angemessenheit ist künftig ausschließlich die DSGVO.

Es ist schon lange klar, dass in den USA generell kein den europäischen Standards **entsprechendes Datenschutzniveau** besteht.[9] Das Fehlen adäquaten Datenschutzes in den USA wurde mit dem EuGH-Urteil höchstrichterlich bestätigt.

[6] EuGH (Fn. 1).
[7] Verordnung (EU) 2016/679 v. 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 v. 04./05.2016, 1 ff.
[8] Börding CR 2016, 440.
[9] Weichert, RDV 2012, 113; Däubler, Gläserne Belegschaften? 7. Aufl. 2017, Rn. 504; Schantz in Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 767.

2 Privacy Shield

An dieser grundsätzlichen Rechtslage änderte sich mit dem Wirksamwerden des Privacy Shield nichts. Ein **erster Entwurf** des Shields wurde von der Artikel-29-Arbeitsgruppe[10], vom Europäischen Datenschutzbeauftragten[11] und vom EU-Parlament[12] massiv kritisiert.[13] Nach geringfügigen Änderungen[14] wurde das Privacy Shield am 12.07.2016 von der EU-Kommission beschlossen und umgehend in Kraft gesetzt.[15]

Allerdings handelt es sich beim Privacy Shield, obwohl es zwischen den USA und der EU ausgehandelt wurde, nicht um ein internationales Abkommen.[16] Es ist vielmehr ein von der EU-Kommission vorgenommener **einseitiger Rechtsakt**, der auf einer doppelten Selbstverpflichtung der auf US-amerikanischer Seite Beteiligten basiert, sich an die formulierten Regeln zu halten. Dies sind zum einen die politischen Amtsträger der US-Administration, zum anderen die sich selbst zertifizierenden datenverarbeitenden Stellen, die vom US-Handelsministerium in einer Privacy-Shield-Liste eingetragen werden.[17] Die Verpflichtungen haben jedoch keinen bindenden rechtlichen Charakter und könnten theoretisch jederzeit zurückgezogen werden. Auch bestehen keine wirksamen Möglichkeiten, die Einhaltung der Zusagen zu erzwingen.

Grundlage des Privacy Shield-Beschlusses mit 155 Erwägungsgründen ist – wie bei Safe Harbor – ein Grundsatztext, sowie ein Wust von Briefen von US-Amtsträgern, die sämtlich nach dem Regierungswechsel in den USA von Obama zu Trump nicht mehr im Amt sind. Diese Briefe und deren Anlagen, die gemeinsam mit dem Kommissions-Beschluss ein stattliches eng beschriebenes **Kompendium von 111 Seiten** ergeben, lassen keine Struktur erkennen. Dass es sich hierbei um ein vollkommen chaotisch zusammengestelltes, unübersichtliches Konvolut handelt, lässt sich u. a. daran ablesen, dass

- selbst im offiziellen Veröffentlichungsblatt der EU die als Annexe zum EU-Kommissions-Beschluss gekennzeichneten Briefe und deren Annexe einmal als Anhang dann als Anlage bezeichnet werden und zudem mit einer undurchsichtigen Zählweise markiert sind,
- ein Dokument (Schiedsmodell) in der Eile versehentlich zweimal veröffentlicht wurde, wobei es einmal als „Anlage 2“, das andere Mal als „Anlage 1“ gekennzeichnet ist,[18]
- Anlagen A keine Anlagen B folgen,[19]

[10] Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision, Working Paper (WP) 238; dazu von dem Bussche in Plath, BDSG DSGVO, 2. Aufl. 2016; § 4b BDSG Rn. 31e; Ritzmann/Hänig K&R Beilage 1 zu Heft 9/2916, 43.
[11] Europäischer Datenschutzbeauftragter, Opinion 4/2016 v. 30.05.2016 on the EU-U.S. Privacy Shield draft adequacy decision.
[12] Entschließung v. 26.05.2016 zur transatlantischen Datenübermittlung 2016/2727(RSP).
[13] Ausführliche Kritik Weichert, Privacy Shield – Darstellung und rechtliche Bewertung, 07.03.2016; http://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_privacyshield.pdf; ders. ZD 2016, 209.
[14] Zusammenfassung bei Schröder in Kühling/Buchner, DS-GVO, 2017, Art. 45 Rn. 45.
[15] EU-Kommissions-Beschluss (Fn. 2).
[16] Von Lewinski in Auernhammer, DSGVO BDSG, 5. Aufl. 2017 Art. 96 DSGVO Rn. 7.
[17] EU-Kommissions-Beschluss (Fn. 2), ErwGr 14, 32, L207/3, 7; Weichert ZD 2016, 211; diese Liste ist zu finden unter https://www.privacyshield.gov/list.
[18] EU-Kommissions-Beschluss (Fn. 2), Anhang I Anlage 2, Anhang II Anlage 1, L 207/45 u. L 207/68.
[19] So zu den EU-Kommissions-Beschluss (Fn. 2) Anhängen III und IV, L 207,72, 85; zum oben Stehenden insgesamt siehe die Anlage 1 des vorliegenden Gutachtens (S. 16) mit dem Inhaltsverzeichnis des EU-Kommissions-Beschlusses.

- ein Schreiben aus dem US-Justizministerium ohne Absender im Amtsblatt der EU abgedruckt wurde,[20]
- im Kommissions-Beschluss eine Vielzahl von Fußnoten enthalten sind, die auf weitere Dokumente außerhalb und innerhalb des Privacy Shields verweisen, was der Klarheit nicht eben förderlich ist.

Über den Rechtscharakter und die **Verbindlichkeit der Briefe** findet sich im gesamten Regelwerk des Privacy Shields keine Aussage. Auch die normativen und prozeduralen Aussagen, die in den Anhängen der Briefe zu finden sind, verlieren sich oft in Unklarheit oder in Unverbindlichkeit. Von der Datenverarbeitung betroffene Beschäftigte sind überfordert, wenn sie die Rechtskonformität einer Datenverarbeitung prüfen wollen; genauso aber auch jeder Jurist, der sich nicht auf Datenschutz mit US-Bezug spezialisiert hat und intensiv in das Studium des Privacy-Shield-Regelwerks eingestiegen ist. Schon dem europäischen Datenschutzrecht wird vorgeworfen, es sei wegen seiner Vielschichtigkeit für die Betroffenen nicht und nur noch schwer zu überschauen. Gegenüber dem Regelungskonglomerat des Privacy Shields erscheinen die europäischen Datenschutznormen geradezu als Paradebeispiel für Klarheit und Verbindlichkeit.

Die schon in Safe Harbor formulierten **Grundsätze** werden im Privacy Shield fortgeschrieben, wobei jedoch der Detaillierungsgrad teilweise erhöht wurde, ohne dass, wegen der Einseitigkeit der Erklärung, hiermit ein Gewinn an Rechtssicherheit und Rechtsschutzmöglichkeiten verbunden wäre. Zusätzlich zu der bisherigen Selbstzertifizierung und der Aufsicht durch die Federal Trade Commission (FTC) bzw. des Department of Transport (DOT) ist ein abschließendes Streitschlichtungsverfahren vorgesehen. Dieses soll in den USA in englischer Sprache durchgeführt werden und für alle Beteiligten verbindlich sein; europäische Aufsichtsbehörden können dabei als Streithelfer der Betroffenen nicht direkt eingebunden werden.

Hinsichtlich der **behördlichen Nutzung** von aus Europa transferierten Daten werden mehrere grundsätzlich mögliche Kontrollprozesse erwähnt. Eine Einschränkung der Massenüberwachung wird zunächst in Aussicht gestellt, doch sichert keine der erwähnten Regelungen und der angebotenen Verfahren für die Betroffenen Transparenz geschweige denn die Durchsetzung eines subjektiven Rechtsanspruchs. Die Zahl der angebotenen Rechtsschutzwege steht im umgekehrten Verhältnis zu deren Transparenz, Verbindlichkeit, Praktikabilität und Durchsetzungsmöglichkeit.[21]

Wie bei Safe Harbor ist eine **Selbstzertifizierung** vorgesehen, die durch die Organisation selbst vorgenommen werden kann und in deren Rahmen diese sich und der Welt bestätigt, dass ihre „Datenschutzbestimmungen den Grundsätzen des Privacy-Shields entsprechen“.

Bezüglich der tatsächlichen Schutzwirkung für Beschäftigte (materiell-rechtlich) bleibt das Privacy Shield weit hinter den europäischen Standards zurück: Es werden wie bei Safe Harbor keine festen Normen etabliert, sondern lediglich Grundsätze formuliert. Diese werden bezeichnet mit

- 1. Informationspflicht,
- 2. Wahlmöglichkeit,

[20] EU-Kommissions-Beschluss (Fn. 2) Anhang VI an US Department of Commerce u. International Trade Administration, L 207/105.
[21] Weichert ZD 2016, 213 f.

- 3. Verantwortlichkeit bei der Weitergabe,
- 4. Sicherheit,
- 5. Datenintegrität und Zweckbindung,
- 6. Auskunftsrecht und
- 7. Rechtsschutz, Durchsetzung und Haftung.

Nicht nur bzgl. ihrer Bezeichnung, sondern auch inhaltlich bleiben diese Grundsätze unverbindlich, selbst wenn bei deren Beschreibung Verbindlichkeit („muss“, „darf nur“) vorgetäuscht wird. So kommt es z. B. bei der Zweckbindung nicht auf die Erforderlichkeit, sondern auch die Erheblichkeit zur Zweckerreichung an; verboten sind nur mit dem ursprünglichen Zweck unvereinbare Zwecke.

Für die **Durchsetzung** von Betroffenenrechten werden „belastbare Mechanismen“ als Rechtsbehelfe gefordert, die sich dann aber selbst im nicht-öffentlichen Bereich wieder in Beliebigkeit, großem Aufwand und Unverbindlichkeit verlieren (direkter Kontakt mit Unternehmen, Behandlung durch Handelsministerium oder FTC/DOT, unabhängige Beschwerdestelle, Inkenntnissetzung eines Gerichts, Durchführung eines Schiedsverfahrens in einem Privacy-Shield-Panel, Behandlung durch EU-Datenschutzbehörde).[22] Wenig erfolgversprechend für die Betroffenen ist das oben erwähnte Streitschlichtungsverfahren (Schiedsmodell), für das sich diese als Gerichtsersatz entscheiden können. Die ergehenden Schiedssprüche sind für die Betroffenen verbindlich. Eine gerichtliche Überprüfung erfolgt auf Antrag „nach US-Recht gemäß Federal Arbitration Act“.[23] Mit dieser Regelung ist die umfassende Überprüfung der Selbstverpflichtungen der US-Unternehmen nach europäischen Rechtsstandards nicht gesichert.

Bei einer sachlichen Prüfung erweist es sich als offensichtlich, dass das Privacy Shield den **Angemessenheitsanforderungen des europäischen Datenschutzrechts** nicht genügt.[24]

3 Spezialregelungen für Beschäftigtendaten

Während die allgemeinen Regelungen des Privacy Shield vor Unverbindlichkeit strotzen, scheint der Transfer von Beschäftigtendaten[25] stringenter und konkreter normiert zu sein.[26] In den USA bestehen keine Institutionen, die analog zur FTC oder zum DOT (im Bereich der Verbraucherdatenverarbeitung) eine **Kontrollkompetenz im Beschäftigtenbereich** haben. Soweit ersichtlich, soll die FTC nicht bei der Privacy-Shield-Kontrolle im Beschäftigtenbereich eingesetzt werden.

Unter den Zusatzgrundsätzen heißt es unter der Überschrift **Selbstzertifizierung** unter 6 lit. c: „Wenn die Organisation wünscht, dass ihr die Vorteile des Datenschutzschilds auch bei Personaldaten zuteilwerden, die zur Verwendung im Rahmen von Beschäftigungsverhältnissen aus der EU übermittelt werden, so ist dies möglich, wenn eine in den Grundsätzen oder in einem künftigen Anhang zu den Grundsätzen aufgeführte gesetzliche Aufsichtsbehörde befugt ist, Beschwerden gegen die

[22] EU-Kommissions-Beschluss (Fn. 2) ErwGr 43 bis 60, L207/9-12.
[23] EU-Kommissions-Beschluss (Fn. 2) Schiedsmodell, D. und E., L 207/45 f.
[24] Börding CR 2016, 440; Weichert ZD 2016, 217; Prantl DuD 2016, 351; Däubler (Fn. 8), Rn. 504d; Grau/Granetzny NZA 2016, 405; Schreiber/Krohm ZD 2016, 255; Schantz in Schantz/Wolff (Fn. 8), Rn. 770; kritisch auch Ritzmann/Hänig K&R Beilage 1 zu Heft 9/2016, 43; a. A. rein formal argumentierend Thomale in Auernhammer, DSGVO BDSG, 5. Aufl. 2017, § 4b BDSG Rn. 20; sehr allgemein Nolan NZA 2016, 46.
[25] Das Privacy Shield verwendet den Begriff „Personaldaten“ statt dem der „Beschäftigtendaten“
[26] EU-Kommissions-Beschluss (Fn. 2) Anhang II Zusatzgrundsätze III.9. „Personaldaten“, L 207,59 f.

Organisation aufgrund der Verarbeitung von entgegenzunehmen. Darüber hinaus muss die Organisation darauf in ihrem Selbstzertifizierungsantrag hinweisen und sich bereit erklären, gemäß den Zusatzgrundsätzen „Personaldaten“ und „Rolle der Datenschutzbehörden“, soweit anwendbar, mit der (den) Datenschutzbehörde(n) in der EU zusammenzuarbeiten und den Empfehlungen dieser Behörden nachzukommen. Außerdem muss die Organisation dem Ministerium ihre Datenschutzbestimmungen für sowie Angaben dazu übermitteln, wo die Datenschutzbestimmungen von den betroffenen Mitarbeitern eingesehen werden können.“[27] Mit dem Begriff „Organisation“ wird das Daten importierende US-Unternehmen bezeichnet. Der Begriff „Personaldaten“ bezeichnet Beschäftigtendaten. Mit dem Begriff „Ministerium“ wird das US-Handelsministerium (Department of Commerce) bezeichnet. Dieses ist aber nicht für die Datenschutzaufsicht im Beschäftigtenbereich zuständig, sondern nur für die Veröffentlichung der Selbstzertifizierung sowie der Datenschutzbestimmungen.

Übermittelt werden dürfen Daten aus Beschäftigungsverhältnissen gemäß dem Privacy Shield nur an selbstzertifizierte Organisationen, die mit dem Arbeitergeber **ökonomisch verbunden oder als Dienstleister** tätig sind.

Die Regelungen zum Beschäftigtendatenschutz bleiben trotz ihrer scheinbaren Klarheit interpretierbar: So heißt es zunächst unter 9.a. i., dass „vor der Übermittlung die Rechtsvorschriften des EU-Mitgliedsstaats, aus dem sie stammen“, gelten. Dies verpflichtet den Datenexporteur in Europa, nicht den Importeur. Dann heißt es weiter: „Sämtliche nach diesen Rechtsvorschriften geltenden Bedingungen und Beschränkungen der Übermittlung müssen beachtet werden“, ohne dass der Adressat genannt wird. Dieser Halbsatz muss sich aber, wenn er einen eigenständigen Sinn und Regelungsinhalt haben soll, auch auf dem **Importeur** beziehen: Dieser muss die vom **nationalen Arbeits- und Datenschutzrecht** vorgegebenen Verarbeitungsbedingungen beachten. Klar wird dies aus der Formulierung nicht.

Eine Differenzierung zwischen **Auftragsverarbeitung** und verantwortlicher Verarbeitung durch das US-Unternehmen erfolgt bei der Regulierung des Privacy Shields zu den Beschäftigtendaten nicht, wenngleich mit dem Wirksamwerden der DSGVO, anders als bisher unter der Geltung der EG-DSRl, diese rechtliche Unterscheidung auch bei einem Datentransfer in ein Drittland relevant bleibt.

Unklarheit besteht auch bei 9.b.i. Dort ist vorgesehen, dass eine **Zweckbindung** der Daten durch das US-Unternehmen aufgehoben werden darf, wenn den Grundsätzen der Informationspflicht und Wahlmöglichkeit entsprochen wurde. Damit wird nicht nur auf die Grundsätze II 1. mit sehr weitgehenden Informationspflichten verwiesen, sondern auch auf II.2 (Wahlmöglichkeit), wonach generell nur ein „Opt-out“ vorgesehen ist und nur für sensible Daten (gem. Art. 9 Abs. 1 DSGVO) „die ausdrückliche Zustimmung („Opt-in“) der betroffenen Personen, wenn diese Daten i) an Dritte weitergegeben oder ii) für einen anderen als den ursprünglichen Erhebungszweck“ verwendet werden sollen. Dies bedeutet, dass nicht-sensitive Daten von Beschäftigten in den USA z. B. für Zwecke des US-Unternehmens, z. B. für Organisationsprüfungen des Mutterunternehmens, genutzt werden dürften, wenn die Betroffenen über ein Widerspruchsrecht informiert wurden und keinen Widerspruch eingelegt haben. Hinsichtlich der sensitiven Daten (im Privacy Shield als „sensible Daten“ bezeichnet) wird gemäß Grundsätze III.1.a. (entsprechend dem Katalog des Art. 9 Abs. 2 DSGVO) auf ein „Opt-in“

[27] EU-Kommissions-Beschluss (Fn. 2) Anhang II Zusatzgrundsätze III 6, L207/55.

verzichtet, wenn dies u. a. „v. zur Erfüllung der arbeitsrechtlichen Pflichten der Organisation notwendig ist“. Unter Grundsätze III. 9. b. i. S. 4 heißt es dann: „Macht ein Beschäftigter von seinem Recht Gebrauch, die Erlaubnis zu versagen, darf das keine Minderung seiner Berufschancen und keine Sanktionen gegen ihn zur Folge haben.“

Die Regelungen des Privacy Shield begründen **kein Konzernprivileg**. Ein solches Privileg ist auch weder in der EG-DSRl noch in der DSGVO in Bezug auf die Zulässigkeit der Verarbeitung vorgesehen. Wenn von „arbeitsrechtlichen Pflichten“ des US-Unternehmens die Rede ist, dann setzt dies einen Arbeitsvertrag mit diesem – evtl. ergänzend mit einem Vertrag mit dem europäischen Arbeitgeber – voraus. Ob für diesen Fall dann ein Widerspruchsrecht besteht, ist fraglich. Das Widerspruchsrecht besteht in jedem Fall, wenn ein Arbeitsvertrag ausschließlich mit dem europäischen Arbeitgeber besteht und z. B. ein US-Mutterunternehmen zweckändernd medizinische Auswertungen durchführen möchte.

Da es hinsichtlich der Auftragsverarbeitung im Privacy Shield keine inhaltlich relevanten Sonderregelungen gibt,[28] gelten ausschließlich die materiell-rechtlichen Regelungen nach europäischem Recht, die eine **Zweckänderung des Auftragsverarbeiters** ausschließen. Dies bedeutet, dass auch die Zweckänderungsregelungen unter 9.b.i. für diesen nicht gelten.

Unter b. ii. wird darauf hingewiesen, dass die **EU-Mitgliedstaaten ihre Regelungsbefugnis** dahingehend nutzen können, dass „die Nutzung der Daten für andere Zwecke … ausgeschlossen werden kann; solche Bedingungen müssen eingehalten werden.“ Insofern bestünde, wenn das politisch gewollt wäre, eine nationale Regelungsmöglichkeit, z. B. in einem Beschäftigtendatenschutzgesetz, für den deutschen Gesetzgeber.

Gemäß dem Privacy Shield „ist den individuellen **Datenschutzbedürfnissen der Arbeitnehmer** angemessen Rechnung“ zu tragen. Diese Formulierung, soll sie einen eigenständigen Wert haben, kann nur in Bezug auf den einzelnen Beschäftigten gelten. Worin dieses Rechnung-Tragen bestehen kann, bleibt unklar. Erwähnt werden Zugriffsbeschränkungen oder eine Pseudonymisierung bzgl. seiner Daten fordern (b. iii.).

Einschränkungen bzgl. der **Betroffenenrechte** sind anlässlich von Beförderungen, Ernennungen und ähnlichen Personalentscheidungen vorgesehen (b. iv.). Wieder ist unklar, was damit gemeint wird, so dass die Gefahr besteht, dass dies als Einfallstor für beliebige Einschränkungen der Betroffenenrechten genutzt wird. Der äußerste Rahmen für derartige Einschränkungen wird künftig durch Art. 23 DSGVO gesetzt, der als Begründung „den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen sowie „die Durchsetzung zivilrechtlicher Ansprüche“ nennt (Abs. 1 lit. i u. j). Da dies aber im Privacy Shield nicht spezifiziert wird, muss diese Regelungen als „unangemessen“ im Hinblick auf das europäische Recht angesehen werden (Art. 45 Abs. 1 DSGVO), so dass sie nicht zur Legitimation der Beschränkung von Betroffenenrechten herangezogen werden kann. Dem Auskunftsrecht kann direkt durch den US-amerikanischen Importeur oder durch den EU-Arbeitgebers entsprochen werden (c.).

Im Privacy Shield ist die **Rechtsdurchsetzung** (d.) für Beschäftigte spezifisch geregelt: Als rechtlich verantwortlich wird nicht der US-Datenimporteur behandelt, dies bleibt der EU-Arbeitgeber als

[28] EU-Kommissions-Beschluss (Fn. 2) Anhang II Zusatzgrundsätze III 10 lit. a, L 207/60.

Exporteur. Ein Betroffener kann sich daher an den Datenschutzbeauftragten des Arbeitgebers wenden und im Beschwerdefall an die für diesen zuständige Aufsichtsbehörde, selbst wenn die Entscheidung über die Weiterverarbeitung durch den US-amerikanischen Importeur getroffen wurde. Zitat Privacy Shield (d. i. S. 4): „So lässt sich am ehesten klären, wie die einander überschneidenden Bestimmungen des Arbeitsrechts, der Tarifverträge und des Datenschutzrechts miteinander in Einklang zu bringen sind." Das US-Unternehmen hat also „gegebenenfalls bei Untersuchungen der in der EU jeweils zuständigen Behörden mitzuwirken und deren Empfehlungen zu befolgen" (d. ii.).[29]

Was sich äußerst verbindlich liest, wird durch **Erwägungsgrund 40 des EU-Kommissions-Beschlusses** relativiert. Zwar wird zunächst bekräftigt, dass „eine Zusammenarbeit mit den Datenschutzbehörden zwingend vorgeschrieben ist", wenn eine Organisation Beschäftigtendaten verarbeitet. Dann heißt es aber weiter: „Als Alternative dazu kommen eine unabhängige alternative Streitbeilegung oder im Privatsektor entwickelte Datenschutzprogramme, welche die Datenschutzgrundsätze inkorporieren, in Betracht. Letztere müssen entsprechend den Anforderungen des Grundsatzes des Rechtsschutzes, der Durchsetzung und der Haftung wirksame Durchsetzungsmechanismen vorsehen. Die Organisationen sind verpflichtet, bei Problemen mit der Einhaltung für Abhilfe zu sorgen. Zudem müssen sie angeben, dass sie den Ermittlungs- und Durchsetzungsbefugnissen der FTC, des Verkehrsministeriums oder einer anderen autorisierten staatlichen Stelle der USA unterliegen."[30] Worauf sich diese Passage bezieht, bleibt dem interessierten Leser unklar. Und welche rechtliche Verbindlichkeit diesem Erwägungsgrund des Beschlusses beigemessen werden soll, ist noch unklarer. Soweit ersichtlich, wird diese „Alternative" in der Praxis nicht wahrgenommen, wohl auch nicht, weil niemandem klar sein dürfte, wie diese umgesetzt werden soll. Es ist aber nicht auszuschließen, dass dieser Erwägungsgrund genutzt wird, um einer Zusammenarbeitspflicht mit den Datenschutzbehörden zu entkommen.

Eine Sonderregelung hat das Privacy Shield im Hinblick auf Beschäftigtendaten bei „**operativen Erfordernissen**" wie dem Buchen von Flügen, Hotelzimmer oder dem Abschluss von Versicherungen, doch müssen auch hier die Grundsätze der Informationspflicht und der Wahlmöglichkeit eingehalten werden.[31] Danach kann „die Übertragung personenbezogener Daten einer geringen Zahl von Arbeitnehmern an die die Verarbeitung Verantwortliche ohne Anwendung des Auskunftsgrundsatzes oder Abschluss eines Vertrags mit dem als für die Verarbeitung Verantwortlicher tätigen Dritten erfolgen, … vorausgesetzt, die dem Datenschutzschild angehörende Organisation hat die Grundsätze der Informationspflicht und der Wahlmöglichkeit eingehalten".

4 Zugriffsmöglichkeiten von US-Behörden

Bezüglich des Schutzes von Beschäftigtendaten bestehen gewaltige rechtliche Defizite, wenn diese Daten für behördliche Zwecke angefordert und verwendet werden.[32] In diesen Fällen gilt für die US-Behörden und US-Unternehmen das allgemeine Regelwerk des Privacy Shields. Dies bedeutet, dass der Zugriff von Geheimdiensten de facto unbegrenzt und weitgehend kontrollfrei erfolgt.[33] Als einzige Maßnahme ist vorgesehen, dass sich die US-Organisationen verpflichten können, „freiwillig in regelmäßigen Abständen **Transparenzberichte** über die Anzahl der Anträge von Behörden auf

[29] Weichert ZD 2016, 210.
[30] EU-Kommissions-Beschluss (Fn. 2), ErwGr 40, L 207/8, 9.
[31] EU-Kommissions-Beschluss (Fn. 2) Anhang II Zusatzgrundsätze III.9. e., L 207,60.
[32] Schantz in Schantz/Wolff (Fn. 8), Rn. 770.
[33] Weichert ZD 2016, 216

Datenzugriff aus Gründen der Strafverfolgung oder nationalen Sicherheit“ zu veröffentlichen. Steht dem aber US-Recht entgegen, so kann selbst die statistische Veröffentlichung ausgeschlossen sein (Grundsätze 16. a.).

Die datenschutzrechtliche Achillesferse des Privacy Shields besteht beim Umgang mit Beschäftigtendaten in deren potenzieller Nutzung durch US-Behörden, der kein hinreichendes gesetzliches Korrektiv entgegengesetzt ist.[34] Die in den Dokumenten zum Privacy Shield ausführlich behandelte Presidential Policy Directive (PPD) 28 macht keine verbindlichen Vorgaben zur Beachtung des Verhältnismäßigkeitsgrundsatzes und verhindert schon vom Wortlaut her keine grenzenlosen **Massendatensammlungen**.[35] Entgegen dem europäischen Ansatz, der jede Form der Datenverarbeitung unter Gesetzesvorbehalt stellt, schließen die US-Regelungen insbesondere die Datenerfassung und die Datennutzung aus und konzentrieren sich auf die Speicherung und die Weitergabe. Zwar werden viele möglichen **Rechtsbehelfe** erwähnt; keiner von diesen gewährleistet aber effektiven Rechtsschutz vor einem unabhängigen Gericht in einem öffentlichen Verfahren[36], wie es nicht nur in Art. 6 Abs. 1, Art. 8 EMRK, sondern selbst in den Art. 14 Abs. 1, Art. 17 des Internationalen Paktes über bürgerliche und politische Rechte von 1966 vorgesehen ist. Daran änderte auch der Judicial Redress Act nichts, der zudem weiterhin Ausländer gegenüber US-Bürgern hinsichtlich des Rechtsschutzes diskriminiert.[37] Im Hinblick auf die geheimdienstlichen Einsichtsrechte wird erst recht jedes rechtsstaatliche Maß an Bestimmtheit, Transparenz und individuelle Abwehrmöglichkeit unterschritten.[38] Selbst die – anders als im Erstentwurf der Shield-Dokumente – letztlich zugesicherte Unabhängigkeit der **Ombudsperson** ist nicht ansatzweise prozessual abgesichert.[39] Im Safe-Harbor-Urteil hat der EuGH darauf hingewiesen, dass es gerade der unkontrollierte und übermäßige Behördenzugriff auf personenbezogene Daten ohne Rechtsschutzmöglichkeiten ist, der den Wesensgehalt der Grundrechte aus der Grundrechte-Charta verletzt.[40]

Angesichts dieser wenig ermutigenden Analyse ist es nur eine Frage der Zeit, wann das der Kommissions-Beschluss zum Privacy Shield **aufgehoben** wird.

5 Alternativen

Genügt das Privacy Shield nicht den Angemessenheitsanforderungen des europäischen Rechts, so stellt sich die Frage, welche Alternativen hierzu bestehen.

Rein formal könnte man auf die Idee kommen, dass der Arbeitgeber von seinen Beschäftigten zur Datenübermittlung in die USA deren **Einwilligung** einholt (Art. 49 Abs. 1 lit. a DSGVO). Es ist inzwischen geklärt, dass Einwilligungen im Arbeitsverhältnis grundsätzlich zulässig sind.[41] Die Rahmenbedingungen hierfür werden explizit in § 26 Abs. 2 BDSG-neu geregelt. Allerdings scheidet dieses Instrument hier aus mehreren Gründen aus. Voraussetzung für die Gültigkeit einer Einwilligung ist nämlich die

[34] Börding CR 2016, 434, 437.
[35] Weichert ZD 2016, 212.
[36] Ausführlich dazu Weichert in ZD 2016, 213 f., 216 f.
[37] Börding CR 2016, 435 f.
[38] Börding CR 2016, 437 f.
[39] Börding CR 2016, 439; vgl. Weichert ZD 2016, 213, 216.
[40] EuGH (Fn. 1), Rn. 94, 95, NJW 3157.
[41] BAG U. v. 11.12.2014, 8 AZR 1010/13, NJW-Spezial 11/2015, 339.

Freiwilligkeit der Einwilligung, die höchstens bei rechtlichen und wirtschaftlichen Vorteilen für die Betroffenen angenommen werden kann. Außerdem muss es jederzeit und ohne Nachteile möglich sein, eine einmal erteilte Einwilligung zu widerrufen. Beide Voraussetzungen sind bei einer Verarbeitung in den USA, insbesondere in Konzernzusammenhängen, in der Regel nicht gegeben: Die Vorteile liegen einseitig beim Arbeitgeber; der Nachteil ist die gesteigerte Gefährdung durch Weiterverarbeitungen und Zweckentfremdungen, etwa durch US-Behörden. Eine Widerrufbarkeit und individuelle Rückholbarkeit der Verarbeitung nach Europa würde die beabsichtigten Vorteile für den Arbeitgeber zunichtemachen,[42], ganz davon abgesehen, dass eine Alternative zur Verarbeitung in den USA faktisch meist gar nicht vorhanden ist. Dies wäre aber Voraussetzung dafür, dass eine Einwilligung auch tatsächlich widerrufbar wäre.

Auf den Art. 49 Abs. 1 lit. c DSGVO kann sich der Arbeitgeber auch nicht berufen. Dieser erlaubt Transfers, die „für die **Erfüllung eines Vertrags** zwischen der betroffenen Person und dem Verantwortlichen … erforderlich“ sind. Eine solche Erforderlichkeit besteht bei klassischen Arbeitsverträgen mit einem Arbeitgeber in Deutschland nicht, da die Verarbeitung auch in Europa stattfinden kann.[43]

Zur Legitimation von Drittlands-Datentransfers sieht die DSGVO, wie schon bisher die EG-DSRl, in Art. 46 Abs. 2 lit. c **Standardvertragsklauseln** und in Art. 47 verbindliche interne Datenschutzvorschriften (**Binding Corporate Rules** – BCRs) vor.[44] Problematisch bleibt aber insofern, dass die Standardverträge wie auch die meisten BCRs vor dem Urteil des EuGH vom 06.10.2015 genehmigt wurden und die dort gemachten Vorgaben nicht inhaltlich berücksichtigt sind. Das Problem des behördlichen Datenzugriffs auf Unternehmensdaten wird darin regelmäßig überhaupt nicht thematisiert, geschweige denn adressiert, so dass von deren Rechtswidrigkeit ausgegangen werden muss. Nach den Standardvertragsklauseln muss der Datenimporteur erklären, dass er seines Wissens nach keinen Gesetzen unterliegt, die ihm die Verfolgung der vom Exporteur auferlegten vertraglichen Pflichten unmöglich machen.[45] Solche Gesetze gibt es aber in den USA. Es ist davon auszugehen, dass auch die bisherigen Kommissionsgenehmigungen von Standardverträgen mittelfristig vom EuGH aufgehoben werden. Dennoch bieten Verträge auf Basis der Standardvertragsklauseln immer noch einen besseren Schutz als die undurchsichtigen und unverbindlichen Regelungen des Privacy Shields.

Als Alternative hatte das Netzwerk Datenschutzexpertise schon kurz nach dem EuGH-Urteil zu Safe Harbor einen Vorschlag für einen zwischen EU-Unternehmen und US-Unternehmen abzuschließenden **Export-Import-Vertrag** erarbeitet und veröffentlicht.[46] Hierbei handelt es sich um eine Weiterentwicklung der von der Kommission genehmigten Standardvertragsklauseln unter Berücksichtigung des Safe-Harbor-Urteils des EuGH.

Der Grundansatz für dieses Vertragsmuster besteht darin, dass die **Verantwortlichkeit des Datenexporteurs** nach dem Export bestehen bleibt und der Importeur sich diesem gegenüber zur

[42] Grau/Granetzny NZA 2016, 407; ähnlich Nolan NZA 2016, 45.
[43] Dazu Grau/Granetzny NZA 2016, 409; Arbeitspapier der Art.-29-Arbeitgruppe (WP) 114 v. 25.11.2005, S. 13; offener Nolan NZA 2016, 45.
[44] Däubler (Fn. 8), Rn. 507g ff.
[45] Grau /Granetzny NZA 2016, 408.
[46] Weichert/Schuler, Export-Import-Standardvertrag, http://www.netzwerk-datenschutzexpertise.de/sites/default/files/entwurf_2016_01_exportimportvertrag_08.pdf; diess. Ein „Export-Import-Standardvertrag“ für Drittlands-Datentransfer, DuD 2016, 386.

Einhaltung des europäischen Datenschutzrechtes verpflichtet und ihm gegenüber zudem informationspflichtig bleibt. Dies hat zur Folge, dass der Importeur vertraglich u. a. zur Beachtung der Grundsätze der Zweckbindung und der Verhältnismäßigkeit sowie zur Beachtung der Betroffenenrechte verpflichtet wird. Diese Verträge haben drittschützende Wirkung. Betroffene können also ihre Rechte gegenüber dem Exporteur geltend machen und diesem gegenüber eine unabhängige Datenschutzkontrolle über die für diesen zuständige Datenschutzaufsichtsbehörde initiieren sowie ihm gegenüber in Europa Rechtsschutz erhalten. Insofern bestehen Parallelen zur der Sonderregelung des Privacy Shield zu Beschäftigtendaten (s. o. 3). Der relevante Unterschied zum Privacy Shield besteht darin, dass für den Fall des Verstoßes gegen Vertragspflichten **wirksame Sanktionen** vorgesehen sind. Gem. Art. 6 des Export-Import-Vertrags werden vertragliche Haftungs- und Schadenersatzansprüche bei Verletzungen des Datenschutzes statuiert. Vorgesehen ist weiterhin die Aussetzung des weiteren Datenexports sowie bei einer Prognose weiterer wesentlicher Vertragsverstöße die vollständige Einstellung des weiteren Datenexportes.

Durch diese Regelungen werden auch die nach europäischem Recht nicht konformen **Datenbeschaffungen von US-Behörden** erfasst sowie **Informationsverweigerungen** des Importeurs, die mit US-Recht (sog. gag-orders[47]) begründet werden. Zwar lassen sich damit die Folgen unzulässiger Datenverarbeitungen nicht vollständig beseitigen. Dies wird aber auch nicht von der DSGVO gemäß den Art. 44 ff. gefordert.

Die Regelungen des Export-Import-Vertragsmusters lassen sich **generell für Datenexporte** in die USA nutzen. Sie können als Gestaltungsbaustein für Binding Corporate Rules gemäß Art. 47 DSGVO verwendet werden (Art. 46 Abs. 2 lit. b DSGVO), für Verhaltensregeln nach Art. 40 DSGVO (Art. 46 Abs. 2 lit. e DSGVO) sowie für zukünftig mögliche Zertifizierungen nach Art. 42 Abs. 2 DSGVO, mit denen geeignete Garantien für Drittlandsdatentransfers geboten werden (Art. 46 Abs. 2 lit. f). In jedem Fall kann sich an dem Muster ein individueller Vertrag zwischen Exporteur und Importeur orientieren, der von der zuständigen Aufsichtsbehörden gem. Art. 46 Abs. 3 DSGVO zu genehmigen ist.[48]

Ein Export-Import-Vertrag kann auch als Grundlage für eine **Kollektivvereinbarung** nach Art. 88 Abs. 1 DSGVO dienen, in der eine Datenverarbeitung in den USA erlaubt wird. Arbeitgeber sind gem. § 87 Abs. 1 Nr. 6 BetrVG zur Mitbestimmung verpflichtet, wenn ein IT-Verfahren geeignet ist, „das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“.[49] Diese Voraussetzungen sind bei Datenübermittlungen ins Drittausland gegeben. Gemäß § 80 Abs. 1 Nr. 1 BetrVG hat nicht nur der Arbeitgeber, sondern auch der Betriebsrat die Pflicht, auf die Einhaltung des Beschäftigtendatenschutzrechtes hinzuwirken und dies zu kontrollieren.[50]

6 Empfehlungen

Rein formal gesehen scheint das Privacy Shield für den Bereich der Beschäftigtendatenverarbeitung Schutzmechanismen zu bieten: So sollen Betroffene und Betriebsrat über die Aufsichtsbehörde des

[47] Dabei handelt es sich um „behördliche Redeverbote“, also für das US-Unternehmen rechtlich verbindliche Anordnungen, die Anfrage durch sowie die Datenweiterleitung an die US-Behörde gegenüber dem Betroffenen oder Dritten offenzulegen.
[48] Zur Niederlassungsproblematik bei Art. 46 Abs. 3 Däubler (Fn. 8), Rn. 507a.
[49] Däubler (Fn. 8), Rn. 710 ff.
[50] Däubler (Fn. 8), Rn. 630 ff.

Daten-Exporteurs, also i. d. R. des Arbeitgebers, sowie über die Arbeitsgerichte vor Ort eine gewisse Chance haben, ihre Datenschutzrechte durchzusetzen. Es ist aber zu vermuten, dass diese Chance nur auf dem Papier steht. Es ist nämlich sehr wahrscheinlich, dass die US-Unternehmen, die sich gemäß dem Privacy Shield für „Human Resources" selbst zertifiziert haben, dies als reinen Formalismus behandeln. Erfahrungen mit dem Zertifizierungsprozess von Safe Harbor legen den Schluss nahe, dass viele US-Unternehmen nicht, wie in der DSGVO vorgesehen, ein umfassendes Datenschutzmanagement etablieren, das die Einhaltung der materiellen Datenschutzregelungen, die Umsetzung der Betroffenenrechte und die organisatorischen Vorkehrungen, etwa über die Durchführung von Datenschutz-Folgeabschätzungen, gewährleistet. Ein **Erfahrungsbericht der Kommission**, der gemäß Art. 4 Abs. 4 des Kommissions-Beschlusses zum Privacy Shield binnen eines Jahres vorgelegt werden soll und hierüber Auskunft geben könnte, wurde für September 2017 angekündigt.

Betriebsräte und Beschäftigte, die die Rechtmäßigkeit der Verarbeitung der Beschäftigtendaten kontrollieren wollen, sollten zunächst prüfen, ob die Daten in den USA oder in einem sonstigen Drittland verarbeitet werden. Sie sollten zudem die vom Ort der Verarbeitung unabhängige Zulässigkeitsgrundlage für die Datenverarbeitung erfragen. Zu beidem ist der Arbeitgeber als Verantwortlicher auskunftspflichtig.

Darüber hinaus sollte in Erfahrung gebracht werden, wie der Arbeitgeber im Falle des Drittstaatentransfers das angemessene Datenschutzniveau herstellen will. Wird hierfür als Grundlage das Privacy Shield angegeben, so sollte anhand der Liste des Department of Commerce (DOC) geprüft werden, ob die Selbstzertifizierung noch gültig ist.[51] Für die Verarbeitung von Beschäftigtendaten ist eine spezielle Selbstzertifizierung nötig, die mit HR (human resources) gekennzeichnet ist. In einem weiteren Schritt sollten die **Datenschutzbestimmungen des Importeurs** eingesehen werden; der Zugang hierzu muss gemäß Zusatzgrundsatz 6. Selbstzertifizierung (lit. c letzter Satz) allgemein eröffnet werden; die dazu nötigen Informationen können beim US-Handelsministerium (DOC) eingeholt werden; die Kontaktdaten finden sich auf der Privacy Shield-Liste. Aufgrund der Erfahrungen mit Safe Harbor ist zu befürchten, dass es sich bei den „Datenschutzbestimmungen" des US-Unternehmens oft um die Übernahme von Musterformulierungen handelt, in die der Name des Unternehmens eingefügt wird, ohne dass das Konzept mit Leben gefüllt wurde. Deshalb hatten die Datenschutzbehörden bzgl. Safe Harbor schon 2010 gefordert, dass das die Daten exportierende europäische Unternehmen die Einhaltung der Zusagen verifizieren muss.[52] Einen derartigen Nachweis können Betriebsräte vom Arbeitgeber auch bzgl. des Privacy Shields einfordern.

Wird eine Anfrage oder Beschwerde innerhalb von 45 Tagen nicht beantwortet, sollte man sich an die für den Arbeitgeber zuständige **Datenschutzbehörde** wenden. Ist auf der Liste ein „alternativer" Weg zur Rechtsdurchsetzung angegeben, so kann man, muss aber nicht diesen Weg beschreiten. Endet dieser Weg nicht erfolgreich bzw. befriedigend, so kann und sollte ein arbeitsrechtliches Vorgehen erwogen werden.

[51] Im Netz abzurufen unter https://www.privacyshield.gov/list.

[52] Beschluss der obersten Aufsichtsbehörden vom 28./20.04.2010, Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen, https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2010/Pruefung_der_Selbst-Zertifizierung_des_Datenimporteuers/Beschluss_28_29_04_10neu.pdf.

Nach Berücksichtigung der vorstehenden Ausführungen muss man Betriebsräten davon abraten, im Rahmen von Mitbestimmungsprozessen nach § 87 Abs. 1 Nr. 6 BetrVG der Durchführung von Beschäftigtendatenübermittlungen auf Basis des Privacy Shields zuzustimmen. Sie sollten vielmehr im Rahmen der bei Auslandsübermittlungen zwingenden Mitbestimmung gegenüber dem Arbeitgeber darauf dringen, dass die Übermittlungen stattdessen auf der Basis eines eigenständigen Vertrags erfolgen. Lässt sich dies gegenüber dem Arbeitgeber nicht durchsetzen, so empfiehlt es sich, die (oben unter 3. dargestellten) Regelungen des Privacy Shields in der **Betriebsvereinbarung** ausdrücklich aufzunehmen und zu konkretisieren. Nur so wird dem Arbeitgeber und dem US-Unternehmen sowie sonstigen Beteiligten unmissverständlich bewusst, mit welchen Pflichten die Verarbeitung von Beschäftigtendaten verbunden ist.

Zu empfehlen ist außerdem – nicht zuletzt wegen der beim Privacy Shield bestehenden Rechtsunsicherheit – eine **Befristung der Gültigkeit** einer solchen Betriebsvereinbarung, z. B. auf die beim US-Unternehmen bestehende Gültigkeitsfrist der Selbstzertifizierung von maximal zwei Jahren. Danach sollten eine Evaluation der Erfahrungen und eine Neubewertung erfolgen. Denkbar ist auch die Aufnahme eines Passus, der bei mangelnder Bewährung des Privacy Shields die Verpflichtung zu einer vertraglichen Regelung oder zu einem Wechsel des Importeurs bei der Verarbeitung der Beschäftigtendaten ausspricht.

Von Arbeitgebern, US-Unternehmen und auch vielen Beratern wird behauptet, dass ein Datentransfer von Beschäftigtendaten datenschutzrechtlich unproblematisch sei, allein weil das die Daten importierende Unternehmen sich dem Privacy Shield angeschlossen habe. Dies trifft nicht zu, weil das Privacy Shield nicht den Vorgaben des europäischen Rechts genügt. Die Aussage basiert zumeist auf einem weiteren Fehlschluss: Die Berufung auf einen Angemessenheitsbeschluss hinsichtlich des Datenschutzniveaus beim Empfänger begründet noch nicht die Rechtmäßigkeit der konkreten Verarbeitung: Der Arbeitgeber und ebenso die datenverarbeitende Stelle in den USA müssen selbstverständlich sämtliche in Deutschland bzw. Europa geltenden Vorschriften des Arbeits- und des Datenschutzrechtes, also der DSGVO und sonstiger Regelungen, beachten, ebenso wie jede Stelle, die Daten ausschließlich in Europa verarbeitet. Die Rechtmäßigkeit einer Verarbeitung ist also **in zwei Schritten** zu prüfen: 1. Gibt es für die konkrete Verarbeitung eine hinreichende normative Legitimation? 2. Besteht im Empfängerland ein angemessenes Datenschutzniveau? Der Arbeitgeber wird also nicht davon entbunden, dem Betroffenen oder dem Betriebsrat darzulegen, weshalb eine konkrete Verarbeitung für die Durchführung des Arbeitsvertrags legitim, erforderlich und angemessen ist.[53]

7 Fazit

Das Kapitel des Privacy Shields sollte so schnell wie möglich geschlossen werden. Das EU-Parlament nahm am 06.04.2017 eine Entschließung an, in der angesichts neuer Entwicklungen unter der Trump-Regierung in den USA die Geschäftsgrundlage für das Privacy Shield in Frage gestellt wird.[54] In einem Schreiben an die EU-Kommission hat die Artikel-29-Arbeitsgruppe auf große Defizite beim Privacy

[53] Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD), EU-US Privacy Shield / Safe Harbor, https://www.datenschutz-bayern.de/faq/FAQ-SafeHarbor.html.
[54] Data Privacy Shield: MEPs alarmed at undermining of privacy safeguards in the US, http://www.europarl.europa.eu/news/de/press-room/20170329IPR69067/data-privacy-shield-meps-alarmed-at-undermining-of-privacy-safeguards-in-the-us.

Shield, auch hinsichtlich „human resources data“ hingewiesen.[55] Dafür sorgen möglicherweise auch Bestrebungen, die darauf hinauslaufen, dass der Kommissions-Beschluss gerichtlich aufgehoben wird. Die irische Datenschutzgruppe Digital Rights Ireland (DRI) hat schon am 16.09.2016 beim Gericht der Europäischen Union (EuG) gegen den Kommissions-Beschluss Nichtigkeitsklage eingereicht.[56] Die dadurch bestehende Rechtsunsicherheit für alle Beteiligten sollte dadurch beseitigt werden, dass entweder auf eine Datenverarbeitung in den USA verzichtet wird oder für den Transfer dorthin eine **rechtskonforme vertragliche Basis** geschaffen wird.

Unabhängig von den bestehenden Bestrebungen, das Privacy Shield zu kippen, ist es auch an der Zeit, **arbeitsgerichtlich überprüfen** zu lassen, inwieweit das Privacy Shield den europäischen rechtlichen Vorgaben entspricht. Die Internationalisierung der Beschäftigtendatenverarbeitung geht voran. Hier nehmen US-Unternehmen Spitzenpositionen bei dem Empfang und der Verarbeitung europäischer Beschäftigtendaten ein. Der durch das Privacy Shield vorgegebene Standard setzt Maßstäbe für jede Form der Beschäftigtendatenverarbeitung in Drittländern, entspricht jedoch in keiner Weise den europäischen Vorgaben. Eine solch unangemessene Pseudolösung sollte nicht ohne Widerspruch hingenommen werden.

[55] Mitteilung für die Presse 13 June 2017, Preparation of the Privacy Shield annual Joint Review.
[56] Rechtssache T-670/16, http://curia.europa.eu/juris/document/document.jsf?text=&docid=185146&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=114465.

Anlage 1 – Inhaltsverzeichnis des EU-Kommissions-Beschlusses zum Privacy Shield

ABl. EU v. 1.8.2016, L 207/

Anlage 2 – Historische und rechtliche Hintergründe

Die Diskussion über den Datenaustausch mit den USA ist eine never-ending Story mit wechselndem Licht und Schatten. Das Licht setzen zunächst unsere **Grundrechte** und die Verfassung. Art. 8 Abs. 1 der Europäischen Konvention für Menschenrechte (EMRK) aus dem Jahr 1950 garantiert jeder Person das „Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz". Inzwischen ist von den für die EMRK zuständigen Gremien, insbesondere vom Europäischen Gerichtshof für Menschenrechte (EGMR) anerkannt, dass damit auch ein Schutz der persönlichen Daten verbunden ist.[57] Dies gilt auch im Hinblick auf das Verhältnis eines Arbeitsgebers zu seinen Beschäftigten.[58] Dieser Schutz ist in Deutschland seit dem Volkszählungsurteil des Bundesverfassungsgerichts (BVerfG) vom 15.12.1983 als „Recht auf informationelle Selbstbestimmung" verfassungsrechtlich anerkannt.[59]

Auf europäischer Ebene hat das Grundrecht auf Datenschutz durch die Europäische **Grundrechte-Charta** von 2009 (GRCh) umfassende Anerkennung gefunden. Art. 7 GRCh schützt das Recht auf Vertraulichkeit der Kommunikation. Art. 8 GRCh hat folgenden Wortlaut: „(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht."

Dieser Schutz soll nicht nur innerhalb eines Staates bzw. innerhalb der Europäischen Union (EU) gelten, sondern auch bei **grenzüberschreitenden Datenflüssen**. Da die jeweiligen lokalen Gesetzgeber keinen direkten Einfluss auf die Wahrung des Datenschutzes im Drittausland, also beim Empfänger eines grenzüberschreitenden Datentransfers, haben, wurde schon 1981 in der Europäischen Datenschutzkonvention versucht, einen einheitlichen Datenschutzstandard festzulegen und in Art. 12 Abs. 2 bestimmt, dass bei Gültigkeit der Konvention im Empfängerland der Datenschutz für einen grenzüberschreitenden Transfer kein Hindernis darstellen darf. Dieses Grundprinzip wurde 1995 von der **Europäischen Datenschutzrichtlinie** (EG-DSRl) übernommen, die hohe Datenschutzstandards von den EU-Mitgliedsstaaten verlangt und in Art. 1 Abs. 2 festgelegt, dass zwischen den Mitgliedstaaten (also im Binnenmarkt) der Datenverkehr aus Datenschutzgründen nicht eingeschränkt wird. Gemäß Art. 25 Abs. 1 EG-DSRl ist die Übermittlung in Drittstaaten zulässig, wenn „dieses Drittland ein angemessenes Schutzniveau gewährleistet". Festgestellt werden kann dies gem. Art. 25 Abs. 6 EG-DSRl durch die EU-Kommission.

Eine solche Feststellung durch die EU-Kommission erfolgte mit Beschluss vom 26.07.2000 in Bezug auf die USA, wenn sich das jeweilige US-Unternehmen im Rahmen des dort festgehaltenen **Safe-Harbor-Regelwerks** im Rahmen einer Selbstverpflichtung zur Beachtung bestimmter Datenschutzgrundsätze bekennt.[60] Eine solche Selbstverpflichtung hatten 2015 ca. 4.400 US-Unternehmen abgegeben, darunter auch sämtliche großen IT-Unternehmen in den USA (Google, Facebook, Microsoft, Amazon, Salesforce). Eine derartige Selbstzertifizierung erfolgte auch von vielen US-Mutterunternehmen mit

[57] Ausführlich dazu Siemen, Datenschutz als europäisches Grundrecht, 2005, S. 51 ff.
[58] EGMR U. v. 05.09.2017, Az. 61496/08, Barbulescu v. Romania.
[59] BVerfG U. v. 15.12.1983 – 1 BvR 209/83 u. a., NJW 1984, 419 ff.
[60] Entscheidung 2000/520/EG, ABl. EG v. 25.08.2000, L 215/7.

Töchtern in der EU in Bezug auf die Verarbeitung von Beschäftigtendaten. Dank Safe Harbor war so der Datentransfer von der EU in die USA aus Datenschutzgründen faktisch nicht beschränkt.

Anlässlich einer Beschwerde gegen Datentransfers bei Facebook und einer Vorlage durch den Irish High Court entschied der **EuGH mit Urteil v. 06.10.2015**, dass der Safe-Harbor-Rechtsrahmen gegen Art. 7, 8 und 47 GRCh verstößt und deshalb die Safe-Harbor-Entscheidung der EU-Kommission aufgehoben wird.[61] Dabei stellte der EuGH fest, dass die Kommission die Angemessenheit des Datenschutzes im Rahmen von Safe Harbor gar nicht überprüft hatte. Insbesondere schützte dieses Regelwerk nicht vor übermäßigen Zugriffen vor US-Behörden und -Geheimdiensten. Im Sommer 2013 war durch die Enthüllungen des Whistleblowers Edward Snowden bekannt geworden, dass insbesondere der US-Geheimdienst NSA (National Security Agency) massenhaft u. a. auf europäische Daten zugreift. Der EuGH stellte fest, dass Safe Harbor diesen Datenzugriff nicht „auf das absolut Notwendige beschränkt". Die Aufhebung der Safe-Harbor-Entscheidung der EU-Kommission erfolgte wegen einer Verletzung, teilweise sogar des „Wesensgehalts" der in der Grundrechte-Charta verbürgten Grundrechte. Das Urteil des EuGH postulierte, dass den Datenschutzbehörden ein Prüfrecht bzgl. Kommissionsentscheidungen über die Angemessenheit des Niveaus im Drittland zusteht, die Aufhebung aber durch den EuGH, evtl. ausgelöst durch eine Klage der Aufsichtsbehörde, erfolgen muss.

Es ist schon seit vielen Jahren klar, dass in den USA generell kein den europäischen Standards **entsprechendes Datenschutzniveau** besteht.[62], weshalb z. B. Safe Harbor von den deutschen Datenschutzbehörden 2010 in Frage gestellt wurde. Das generelle Fehlen eines adäquaten Datenschutzes in den USA wurde mit dem EuGH-Urteil höchstrichterlich bestätigt.

Dieses Fehlen eines adäquaten Datenschutzes in den USA ist nicht selbstverständlich, zumal der moderne Datenschutz **wesentliche Wurzeln in den USA** hat, etwa die Veröffentlichung der US-Juristen Warren/Brandeis aus dem Jahr 1890 „The Right to Privacy"[63] oder von Alan F. Westin im Jahr 1967 „Privacy and Freedom". Schon 1967 erklärte der US-Supreme Court in der Katz-Entscheidung, dass jeder US-Bürger den Anspruch darauf habe, dass seine „reasonable expectations of privacy" beachtet werden.[64]

Seitdem ist aber die **Datenschutzentwicklung in den USA** nur noch stockend vorangekommen. Die Anerkennung eines Grundrechts auf Datenschutz, gar als Menschenrecht, erfolgte nicht. Eine rechtliche Bindung von Privaten hieran besteht, anders als in Europa, nicht. Die gesetzlichen Regelungen sind unvollständig und garantieren keinen umfassenden individuellen Rechtsschutz. Der im europäischen Recht zentrale Zweckbindungsgrundsatz existiert im US-Recht nicht. Vielmehr wird über die „Third Party Doctrin" bei Daten, die den persönlichen Kreis verlassen haben, gerade keine Nutzungsbegrenzung anerkannt.[65] Generell gilt im Hinblick auf die behördliche Nutzung von Daten, insbesondere durch Sicherheitsbehörden und Geheimdienste, dass diese Vorrang hat gegenüber freiheitlich begründeten Schutzbedürfnissen der Betroffenen.

[61] EuGH (Fn. 1).
[62] Weichert, RDV 2012, 113; Däubler, Gläserne Belegschaften? (Fn. 8), Rn. 504'; Schantz in Schantz/Wolff (Fn. 8), Rn. 767.
[63] Deutsche Übersetzung in DuD 2012, 755.
[64] Katz v. United States 389 U.S. 347 (1967).
[65] Börding CR 2016, 437.

Abkürzungen

ABl.	Amtsblatt
Abs.	Absatz
Art.	Artikel
Aufl.	Auflage
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
CR	Computer und Recht (Zeitschrift)
DOC	Department of Commerce (US-Handelsministerium)
DOT	Department of Transport (US-Verkehrsministerium)
DSGVO	Europäische Datenschutz-Grundverordnung
DuD	Datenschutz und Datensicherheit (Zeitschrift)
EG	Europäische Gemeinschaften
EG-DSRl	Europäische Datenschutzrichtlinie
EMRK	Europäische Menschenrechts-Konvention
ErwGr	Erwägungsgrund
EU	Europäische Union
EuGH	Europäische Gerichtshof
f/f.	fort-/folgende
FTC	Federal Trade Commission
K&R	Kommunikation und Recht (Zeitschrift)
JZ	Juristenzeitung
NJW	Neue Juristische Wochenschrift
NZA	Neue Zeitschrift für Arbeitsrecht
PPD	Presidential Policy Directive
Rn.	Randnummer (im Inhaltsverzeichnis Erwägungsgrund)
U.	Urteil
US/A, U.S./A	United States /of America
v.	von
WP	Working Paper
ZD	Zeitschrift für Datenschutz