Datenschutz- und Datennutzungsverträge

Vertragsmuster, Klauseln, Erläuterungen

Bearbeitet von
Herausgegeben von Dr. Flemming Moos, Bearbeitet von Prof. Dr. Ralf B. Abel, Marian Arning, Silvia C. Bauer, Dr. Ulrich Baumgartner, Thorsten Feldmann, Dr. Axel Bussche, Dr. Detlev Gabel, Dr. Till Gerhardt, Stephan Hansen-Oest, Frank Henkel, Britta Hinzpeter, Julian Höppner, Dr. Thomas Jansen, Dr. Wulf Kamlah, Dr. Markus Lang, Dr. Sebastian Meyer, Lukas Neff, Jamie Nowak, Leif Rohwedder, Tobias Rothkegel, Dr. Daniel Rücker, Adrian Schneider, Felix Sperling-Fröhlich, Dr. Martin Soppe, Dr. Frank Weberndörfer, Dr. Mirko Wieczorek, und Christoph Zieger

2. neu bearbeitete und erweiterte Auflage 2018. Buch mit CD-ROM. Rund 1344 S. Gebunden
ISBN 978 3 504 56100 0

Recht > Handelsrecht, Wirtschaftsrecht > Telekommunikationsrecht, Postrecht, IT-Recht > Datenschutz, Postrecht

schnell und portofrei erhältlich bei

beck-shop.de
DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung beck-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

Leseprobe zu

Moos

Datenschutz- und Datennutzungsverträge

Vertragsmuster, Klauseln, Erläuterungen

inkl. CD

2018, 1344 Seiten, gebunden, Formularbuch, 17 x 24cm

ISBN 978-3-504-56100-0

129,00 €

§ 36
Datenschutzklausel zum EU-U.S.-Privacy Shield

A. Einleitung 1
B. Datenschutzklausel zum EU-U.S.-Privacy Shield 8
I. Muster 8
II. Erläuterungen 9
1. Vorbemerkung 9
2. Zertifizierungspflicht (Ziffer 1) 10
a) Ratio 11
b) Beantragung der Zertifizierung (Ziffer 1.1) 12
c) Erneuerung der Zertifizierung (Ziffer 1.2) 14
d) Vorlagepflicht (Ziffer 1.3) 15
e) Mitteilung von Änderungen (Ziffer 1.4) 18
3. Mitteilungspflichten (Ziffer 2) 19
a) Ratio 20
b) Informationspflicht über Ermittlungsverfahren (Ziffer 2.1) 21
c) Kooperationsgebot (Ziffer 2.2) 22
d) Abwendungspflicht (Ziffer 2.3) 23
e) Informationspflicht bei Beschwerden (Ziffer 2.4) 24
4. Rechtsfolgen des Verlusts der Zertifizierung (Ziffer 3) 25
a) Ratio 26
b) Schadensersatz (Ziffer 3.1) 27
c) Kündigungsrecht (Ziffer 3.2) 28
5. Entfall der Wirkung des Privacy Shields (Ziffer 4) 30
a) Ratio 31
b) Entfall der Angemessenheitsfeststellung (Ziffer 4.1) 32
c) Ersetzung durch neuen Mechanismus (Ziffer 4.2) 33

Literatur: *Gola/Klug*, Die Entwicklung des Datenschutzrechts im ersten Halbjahr 2017, NJW 2017, 2593; *Grau/Granetzky*, EU-US-Privacy Shield – Wie sieht die Zukunft des transatlantischen Datenverkehrs aus?, NZA 2016, 405; *Heumann*, From Safe Harbor to Privacy Shield: the Future of transatlantic Data Transfer and its Implications, PinG 03.16, 106; *Hoffmann*, „Privacy Shield": Kein ausreichender Datenschutz im unsicheren Hafen USA, cep-Studie, April 2016; *Kühling/Buchner*, DSGVO, 2017; *Lejeune*, Der EU-US Privacy Shield: eine neue Grundlage zum Datenaustausch mit den USA, ITRB 9/2016, 201; *v. Lewinski*, Privacy Shield – Notdeich nach dem Pearl Harbor für den transatlantischen Datentransfer, EuR 2016, 405; *Moos/Schefzig*, „Safe Harbor" hat Schiffbruch erlitten, CR 2015, 625; *Neuber*, Ein Privacy Shield für alle, K&R 9/2016, Editorial; *Niklas/Faas*, Arbeitnehmerdatenschutz: EU-US Privacy Shield – Ende der Rechtsunsicherheit bei Datentransfers in die USA?, ArbRAktuell 2016, 473; *Schreiber/Kohm*, Rechtssicherer Datentransfer unter dem EU-US-Privacy Shield? Der transatlantische Datentransfer in der Unternehmenspraxis, ZD 2016, 255; *Weichert*, EU-US-Privacy-Shield – Ist der transatlantische Datentransfer nun grundrechtskonform? Eine erste Bestandsaufnahme, ZD 2016, 209; *Weiß*, Nach dem Ende von Safe Harbor: Das EU-U.S.-Privacy Shield, RDV 2016, 135; *Wybitul/Ströbel/Ruess*, Übermittlung personenbezogener Daten in Drittländer, ZD 2017, 503

A. Einleitung

1 Das in Folge der **„Safe Harbor"-Entscheidung** des EuGH[1] zwischen der EU und den USA abgestimmte „EU-U.S.-Privacy Shield"[2] (im Folgenden: „Privacy Shield") dient dazu, Datenflüsse aus der EU in die USA durch ein **Zertifizierungsverfahren** im Hinblick auf die Einhaltung eines bestimmten datenschutzrechtlichen Mindestschutzniveaus abzusichern[3]. Rechtsgrundlage solcher Datenübermittlungen in die USA ist ein **Angemessenheitsbeschluss** der EU-Kommission nach Art. 25 Abs. 6 DSRL, wonach bei Einhaltung der Vorgaben des Privacy Shields beim Datenempfänger in den

1 EuGH v. 6.10.2015 – C-362/14 – *Schrems*, ZD 2015, 549.
2 Zum Text des Abkommens: https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg.
3 *Weiß*, RDV 2016, 135 (136).

USA ein angemessenes Datenschutzniveau existiert, so dass die Drittstaatenübermittlung keiner gesonderten Genehmigung bedarf[4].

Gegenwärtig sind unter dem Privacy Shield-Framework 2.592 Unternehmen und andere Organisationen zertifiziert[5]. Die Liste gibt Auskunft über die Art der Daten, die das amerikanische Unternehmen erhebt, und den Zeitpunkt der letzten sowie der kommenden Zertifizierung. Die Zertifizierung muss alljährlich erneuert werden[6]. Zudem enthält die Liste Angaben zur Privacy Policy und Kontaktdaten des Unternehmens zur Meldung von Verstößen. Die Internetseite des U.S. Handelsministeriums listet auch die Unternehmen, die nicht mehr Privacy Shield zertifiziert sind[7]. 2

Der Privacy Shield bietet europäischen Unternehmen zumindest aktuell (die weitere Bewertung des Datenschutzniveaus auf U.S-Seite insbesondere durch regelmäßig zu wiederholende Überprüfungen durch die Kommission nach Art. 45 DSGVO gemeinsam mit dem US-amerikanischen Handelsministerium bleibt abzuwarten[8]) eine **gewisse Sicherheit** im Hinblick auf die Zulässigkeit von Datentransfers in die USA[9]. Im Oktober 2017 hat die EU-Kommission im Rahmen ihrer ersten jährlichen Prüfung festgestellt, dass der Privacy Shield grundsätzlich einen angemessen Schutz von personenbezogenen Daten bietet. Gleichzeitig hat die Kommission der US-Regierung in ihrem Prüfbericht einige Empfehlungen zur verbesserten Implementierung ausgesprochen[10]. Auch die Artikel 29-Datenschutzgruppe hat nunmehr einen Prüfbericht hinsichtlich der Belastbarkeit des Privacy Shields veröffentlicht, in dem zahlreiche Verbesserungen gefordert wurden (etwa hinsichtlich eines konstatierten Mangels an Informationen über die Prinzipien des Privacy Shields, in Bezug auf einen effektiveren Selbstzertifizierungsmechanismus sowie die Notwendigkeit, einen unabhängigen Ombudsmann zu installieren)[11]. 3

Die Effektivität des Datenschutzes auf US-Seite wird gerade angesichts der tiefgehenden Eingriffsbefugnisse der US-Geheimdienste[12] und teilweise besorgniserregender Äußerungen von politischer Seite[13] bezweifelt. Die Zugriffe der US-Geheimdienste wurden mittlerweile (nach den ***Snowden*-Enthüllungen**[14]) auf abschließend aufgeführte Zwecke wie z.B. Terrorismusbekämpfung, Spionageabwehr, Verhinderung der Verbreitung von Massenvernichtungswaffen, Gefahrenabwehr, Bedrohung amerikanischer oder verbündeter Streitkräfte, aber auch Bekämpfung internationaler Kriminalität oder Bedrohung der Cybersicherheit beschränkt[15]. 4

4 Der Privacy Shield bleibt gemäß Art. 45 Abs. 9 DSGVO grundsätzlich auch unter der DSGVO in Kraft, solange der zugrundeliegende Angemessenheitsbeschluss nicht von der EU-Kommission geändert, ersetzt oder aufgehoben wird; hierzu *Wybitul*/*Ströbel*/*Ruess*, ZD 2017, 503 (505); zur Ausgestaltung des Angemessenheitsbeschlusses vgl. *Lejeune*, ITRB 9/2016, 201 (203).

5 Zuletzt überprüft am 8.1.2018. Die jeweils aktuelle Liste lässt sich unter https://www.privacyshield.gov/list einsehen.

6 *Lejeune*, ITRB 9/2016, 201 (207); *Neuber*, K&R 9/2016, Editorial.

7 Vgl. *Weichert*, ZD 2016, 209 (211).

8 Skeptisch insoweit: EDPS Opinion on the EU-U. S. Privacy Shield draft adequacy decision, Opinion 4/2016 v. 30.5.2016.

9 Vgl. zur Verbindlichkeit des Angemessenheitsbeschlusses *Schreiber*/*Kohm*, ZD 2016, 255 (257 f.).

10 S. die Pressemitteilung v. 18.10.2017: „EU-US-Datenschutzschild: Datenschutzschild funktioniert laut erster Bestandsaufnahme ordnungsgemäß, ist aber in der Praxis verbesserungswürdig", http://europa.eu/rapid/press-release_IP-17-3966_de.htm.

11 Art.-29-Gruppe, EU-U.S. Privacy Shield – First annual Joint Review, 28.11.2017, WP255.

12 *Hoffmann*, „Privacy Shield": Kein ausreichender Datenschutz im unsicheren Hafen USA, April 2016, S. 40-43, https://konzepte-online.de/wp-content/uploads/2016/04/cepStudie_Datentransfer_in_die_USA.pdf; *Grau*/*Granetzny*, NZA 2016, 405 (406).

13 https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united.

14 Vgl. *Heumann*, PinG 03.16, 106 f.

15 Kühling/Buchner/*Schröder*, Art. 45 DSGVO Rz. 41; *Weichert*, ZD 2016, 209 (212).

Die Wirksamkeit der Entscheidung der Kommission vom 12. Juli 2016[16] im Hinblick auf das angemessene Schutzniveau durch die Einführung des EU-U.S. Privacy Shields wird zudem gegenwärtig vor dem EuGH geprüft. Unklar sind auch noch mögliche Implikationen des durch den irischen High Court initiierten **Vorlageverfahrens vom 3. Oktober 2017** zur Wirksamkeit von durch die Kommission vorgelegten Standardvertragsklauseln.

5 Nichtsdestotrotz ist angesichts der **immensen Bedeutung transatlantischer Datenflüsse** gerade im Bereich der Auftragsverarbeitung (etwa bei der Nutzung von Cloud-Services)[17] ein dauerhaftes Verbot dieser Datenübermittlungen nicht zu erwarten. Insoweit ergibt es unter den gegenwärtigen Bedingungen Sinn, im Falle der beabsichtigten Nutzung eines U.S.-amerikanischen Dienstleisters etwaige Datenübermittlungen durch Abschluss eines Vertrages abzusichern, in dem idealiter die Möglichkeit eines eventuellen Folgevertrages bereits abgebildet ist.

6 Die Prinzipien und Garantien, die mit dem Privacy Shield in materiell-rechtlicher Hinsicht einhergehen, sind über verschiedene Dokumente verstreut[18] und teilweise in ihrer Konsistenz verbesserungswürdig[19]. Trotz aller zum Teil sicherlich berechtigter Kritik an der Durchsetzbarkeit der darin enthaltenen Gewährleistungen[20] stellt der Privacy Shield mittlerweile einen der wichtigsten juristischen Stützpfeiler transatlantischer Datenübertragungen dar. Sofern Unternehmen andere rechtliche Grundlagen wie **BCR's** oder durch die Kommission erlassene **Standarddatenschutzklauseln**[21] vermeiden möchten, ist die Aufnahme einer „Privacy-Shield-Klausel" beispielsweise in einen **Auftragsverarbeitungsvertrag** empfehlenswert. Einen praktischen Leitfaden in deutscher Sprache hält dabei die Europäische Kommission auf ihrer Website bereit[22].

7 Die folgende Musterklausel enthält ausschließlich Bestimmungen im Hinblick auf die Zertifizierung unter dem Privacy Shield. Üblicherweise wird diese Klausel ihre Heimstatt innerhalb eines umfangreicheren Vertragswerks (etwa eines Auftragsverarbeitungsvertrags[23]) finden. Auf dessen Spezifika wird im Folgenden jedoch nicht eingegangen.

16 EU-Kommission, Entscheidung C(2016) 4176 final v. 12.7.2016, im Internet abrufbar unter: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.
17 Vgl. zur Bedeutung in den Jahren 2000 bis 2015 *Niklas*/*Faas*, ArbRAktuell 2016, 473.
18 Vgl. *v. Lewinski*, EuR 2016, 405 (412).
19 Art. 29 Working Party, Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision v. 13.4.2016 (WP 238), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.
20 Vgl. hierzu beispielhaft *Gola*/*Klug*, NJW 2017, 2593 (2596) sowie *Hoffmann*, „Privacy Shield": Kein ausreichender Datenschutz im unsicheren Hafen USA, cep-Studie, April 2016.
21 Vgl. allgemein zu diesen verschiedenen Möglichkeiten das Kurzpapier Nr. 4 der Datenschutzkonferenz (DSK) zur Datenübermittlung in Drittländer (Stand: 11.7.2017); *Moos*/*Schefzig*, CR 2015, 625 (631 f.).
22 EU-Kommission, Leitfaden zum EU-US-Datenschutzschild, http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_de.pdf.
23 Siehe hierzu die Muster in Teil 2, §§ 7–9.

B. Datenschutzklausel zum EU-U.S.-Privacy Shield

I. Muster

M 36.1 EU-U.S.-Privacy Shield-Klausel

8

EU-U.S.-Privacy Shield-Klausel

1. Zertifizierungspflicht unter dem EU-U.S.-Privacy Shield[24]

*1.1 Der Auftragnehmer ist verpflichtet, die Zertifizierung der zuständigen Behörde im Hinblick auf die Einhaltung der Anforderungen des EU-U.S.-Privacy Shields (im Folgenden: „**Privacy Shield**") zu beantragen und sämtliche hierfür geforderten Voraussetzungen zu erfüllen. Diese Zertifizierung muss mindestens die Datenkategorien … umfassen.*

1.2 Der Auftragnehmer ist darüber hinaus verpflichtet, bis zum Abschluss der in diesem Vertrag vorgesehenen Datenübermittlungen die Zertifizierung in den erforderlichen regelmäßigen Intervallen erneut zu beantragen, um die Zertifizierung lückenlos sicherzustellen.

1.3 Der Auftragnehmer ist verpflichtet, die erlangte Privacy Shield-Zertifizierung und einen Nachweis, dass die vom Übermittlungsvertrag umfassten Daten auch von der Zertifizierung abgedeckt sind, dem Auftraggeber ohne gesonderte Aufforderung vorzulegen. Das Gleiche gilt bezüglich erneuerter Privacy Shield-Zertifizierungen.

1.4 Der Auftragnehmer ist darüber hinaus verpflichtet, jede Änderung seines Zertifikats, insbesondere des Umfangs der umfassten Datenkategorien, dem Auftraggeber unverzüglich anzuzeigen.

2. Mitteilungspflichten[25]

2.1 Der Auftragnehmer ist verpflichtet, für den Fall, dass ihm Ermittlungen der für die Zertifizierung zuständigen Behörde bekannt werden, den Auftraggeber unverzüglich hierüber zu informieren.

2.2 Der Auftragnehmer ist in diesem Fall verpflichtet, mit der ermittelnden Behörde soweit gesetzlich vorgesehen umfassend zu kooperieren, wobei im Rahmen des rechtlich Zulässigen die Betriebs- und Geschäftsgeheimnisse des Auftraggebers zu wahren sind.

2.3 Er ist ferner verpflichtet, sämtliche ihm zumutbaren Maßnahmen durchzuführen, um den Verlust der Zertifizierung abzuwenden.

2.4 Der Auftragnehmer ist überdies verpflichtet, den Auftraggeber in Kenntnis zu setzen, wenn betroffene Personen gegen ihn wegen tatsächlicher oder behaupteter Datenschutzverstöße Rechtsbehelfe vor staatlichen Stellen oder im Rahmen eines Schiedsverfahrens geltend machen.

3. Rechtsfolgen eines Verlusts der Zertifizierung[26]

3.1 Für den Fall, dass von der zuständigen Stelle die Zertifizierung wegen eines Verstoßes gegen datenschutzrechtliche Anforderungen entzogen wird, ist der Auftragnehmer dem Auftraggeber zum Ersatz des ihm entstandenen Schadens verpflichtet. Dies gilt nicht, wenn den Auftragnehmer an dem Datenschutzverstoß kein Verschulden trifft.

3.2 Dem Auftraggeber steht überdies für den Fall des Verlusts der Zertifizierung ein fristloses Sonderkündigungsrechts des Vertrags … zu.

24 Zu den Erläuterungen siehe Rz. 11 ff.
25 Zu den Erläuterungen siehe Rz. 20 ff.
26 Zu den Erläuterungen siehe Rz. 26 ff.

4. Folgen einer Unwirksamkeit des Privacy Shields[27]

4.1 Für den Fall, dass die Angemessenheitsfeststellung zugunsten des „Privacy Shields" durch die EU-Kommission entfällt, z.B. weil der entsprechende Angemessenheitsbeschluss aufgehoben oder für ungültig erklärt wird, verpflichten sich beide Parteien, an einer Lösung mitzuwirken, welche den sodann geltenden datenschutzrechtlichen Voraussetzungen an eine Datenübermittlung in die USA gerecht wird.

4.2 Dies schließt ein Bemühen um eine vergleichbare Zertifizierung oder eine Mitwirkung in einem ähnlichen Verfahren für den Fall ein, dass der „Privacy Shield" durch einen anderen Mechanismus ersetzt wird und dessen Angemessenheit durch einen Beschluss der EU-Kommission verbindlich festgestellt ist.

II. Erläuterungen

1. Vorbemerkung

9 Das vorliegende Muster beinhaltet Klauseln allein zur Umsetzung des Privacy Shields und nicht zur Übermittlung von Daten in die USA. Im Einzelfall kann die Vereinbarung weiterer Klauseln erforderlich sein. So ist der Abschluss eines Auftragsverarbeitungsvertrages[28] i.S.v. Art. 28 Abs. 3 DSGVO neben der Privacy Shield-Klausel zwingend erforderlich, wenn der Auftragnehmer Daten weisungsgebunden im Auftrag des Auftraggebers verarbeitet. Unternehmen müssen zudem die Vorschriften der DSGVO und der nationalen Datenschutzgesetze einhalten.

Die folgenden Klauseln sollen sicherstellen, dass eine Übermittlung von Daten an Unternehmen in den USA auf der „**zweiten Stufe**", also jenseits der Frage nach der datenschutzrechtlichen Ermächtigungsgrundlage aus dem Katalog des Art. 6 Abs. 1 DSGVO, zulässig ist.

2. Zertifizierungspflicht (Ziffer 1)

10 **M 36.1.1 Zertifizierungspflicht**

1. Zertifizierungspflicht unter dem EU-U.S.-Privacy Shield

1.1 Der Auftragnehmer ist verpflichtet, die Zertifizierung der zuständigen Behörde im Hinblick auf die Einhaltung der Anforderungen des EU-U.S.-Privacy Shields (im Folgenden: „Privacy Shield") zu beantragen und sämtliche hierfür geforderten Voraussetzungen zu erfüllen. Diese Zertifizierung muss mindestens die Datenkategorien … umfassen.

1.2 Der Auftragnehmer ist darüber hinaus verpflichtet, bis zum Abschluss der in diesem Vertrag vorgesehenen Datenübermittlungen die Zertifizierung in den erforderlichen regelmäßigen Intervallen erneut zu beantragen, um die Zertifizierung lückenlos sicherzustellen.

1.3 Der Auftragnehmer ist verpflichtet, die erlangte Privacy Shield-Zertifizierung und einen Nachweis, dass die vom Übermittlungsvertrag umfassten Daten auch von der Zertifizierung abgedeckt sind, dem Auftraggeber ohne gesonderte Aufforderung vorzulegen. Das Gleiche gilt bezüglich erneuerter Privacy Shield-Zertifizierungen.

1.4 Der Auftragnehmer ist darüber hinaus verpflichtet, jede Änderung seines Zertifikats, insbesondere des Umfangs der umfassten Datenkategorien, dem Auftraggeber unverzüglich anzuzeigen.

a) Ratio

11 Die Regelung legt den **zeitlichen und inhaltlichen Umfang** der Zertifizierungspflicht fest.

27 Zu den Erläuterungen siehe Rz. 31 ff.

28 Siehe hierzu die Muster in Teil 2, §§ 7–9.

b) Beantragung der Zertifizierung (Ziffer 1.1)

Die Zertifizierung muss aktuell beim **US-amerikanischen Handelsministerium** (Department of Commerce – DoC) beantragt werden. Die im Musterformular vorgesehene Formulierung stellt gleichwohl mittels einer allgemeineren Formulierung auf die jeweilige Zuständigkeit ab, um erforderliche Vertragsänderungen aufgrund geänderter staatlicher Zuständigkeiten zu vermeiden. 12

Bezüglich der Datenkategorien unterscheidet der Privacy Shield im Hinblick auf die Zertifizierung lediglich zwischen **Personaldaten** („Human Resources Data") und **anderen Daten**. Auftragnehmer müssen, wollen sie Personaldaten verarbeiten, dies nicht nur bei der Beantragung eines Privacy Shield-Zertifikats angeben, sondern sich damit auch der europäischen Datenschutzaufsicht und dem Recht des datenexportierenden europäischen Auftraggebers unterwerfen[29]. Von einem Zertifikat können dabei beide Kategorien umfasst sein.

Im Falle von Übermittlungen an einen Verantwortlichen in den USA fungiert der Datenexporteur seinerseits ebenfalls als Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO und hat sicherzustellen, dass die zu übermittelnden Daten auch vom Zertifikat umfasst sind. Andernfalls fehlt es insoweit an einer Grundlage für die Datenübermittlung.

Datenkategorien lassen sich selbstverständlich noch deutlich breiter aufschlüsseln. Insofern finden sich für die Verarbeitung des US-amerikanischen Auftragnehmers von unterschiedlichen Datenkategorien und Verarbeitungssituationen (u.a. Reisedaten, Daten im Zusammenhang mit pharmazeutischen und medizinischen Produkten sowie öffentlich zugängliche Daten) Zulässigkeitsregelungen in den Zusatzprinzipien („**Supplementary Principles**") Nr 13–15 des Privacy Shields. Hinsichtlich der vertraglich manifestierten Zertifizierungspflicht reicht an dieser Stelle jedoch eine Unterscheidung zwischen **Personal- und Nicht-Personaldaten**. Die genaue Aufschlüsselung der verarbeiteten Datentypen sollte sich im Übrigen bereits im Auftragsverarbeitungsvertrag finden. 13

c) Erneuerung der Zertifizierung (Ziffer 1.2)

Die unter dem Privacy Shield zertifizierten Unternehmen müssen ihre „Mitgliedschaft" (genauer gesagt: die Zertifizierung) **jährlich erneuern**[30]. Erneuern sie diese nicht, können sie nicht mehr auf Grundlage des Privacy Shields personenbezogene Daten aus der EU verarbeiten. Eine entsprechende Pflicht sollte daher in eine Vertragsklausel einbezogen werden. Bezüglich des Erneuerungsintervalls wurde wiederum eine allgemeine Formulierung gewählt, um erforderliche Vertragsanpassungen wegen geänderter Intervallvorgaben zu vermeiden. 14

Im Einzelfall mag es sinnvoll sein, eine **Härtefallklausel** aufzunehmen, die Fälle statuiert, in denen eine Erneuerung der Zertifizierung vom Auftragnehmer nicht verlangt werden kann. Härtefälle könnten vorliegen, wenn die Erneuerung mit erheblichen Kosten verbunden ist oder eine Umstrukturierung des Unternehmens mit sich bringen würde, die dem Auftragnehmer nicht zugemutet werden kann.

d) Vorlagepflicht (Ziffer 1.3)

Die Auftraggeber sind datenschutzrechtlich für die Einhaltung der Vorschriften zur Übermittlung in Drittstaaten nach Kapitel V DSGVO verantwortlich, weshalb es sinnvoll ist, die obligatorische vorherige eigenständige Überprüfung im Hinblick auf die Zertifizierung des Auftragnehmers durch eine **Vorlagepflicht** zu erleichtern. 15

29 http://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2017_privacyshield_personaldaten_fin.pdf, S. 6 ff.

30 Leitfaden der Kommission zum EU-US-Datenschutzschild, http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_de.pdf.

16 Der Auftraggeber hat die Geeignetheit des Auftragnehmers im Hinblick auf die Privacy Shield-Zertifizierung vor Durchführung der Auftragsverarbeitung **dreischrittig** daraufhin zu überprüfen, ob der Auftragnehmer überhaupt über ein Zertifikat verfügt, dieses Zertifikat noch gültig ist und die betroffenen Daten von der Zertifizierung umfasst sind. Dies entbindet den Auftraggeber nicht zwingend von der Obliegenheit, stichprobenartig zu überprüfen, ob der Auftragnehmer die Vorgaben der Privacy Shield-Grundsätze auch tatsächlich einhält. Insbesondere sollte die öffentlich zugängliche Verlinkung zum Eintrag in der Privacy Shield-Liste regelmäßig eingesehen werden.

17 Um diese Überprüfung des Auftragnehmers nachweisen zu können, sollte der Auftraggeber die abgeprüften Schritte sorgfältig **dokumentieren**. Bei der Prüfung und der Dokumentation hilft eine vertragliche Vorlagepflicht der relevanten Informationen des Auftragnehmers. Der Auftragnehmer dürfte der Vorlagepflicht nach der jetzigen Ausgestaltung des Privacy Shields regelmäßig durch das Zusenden eines Hyperlinks zu seinem Eintrag in der öffentlich abrufbaren Privacy Shield-Liste genügen. Die Einträge dieser Liste enthalten nämlich Informationen dazu, ob die Zertifizierung eines Unternehmens aktiv oder inaktiv ist, welche Datenkategorien von der Zertifizierung umfasst sind und verlinken auf die Datenschutzrichtlinien der Unternehmen.

e) Mitteilung von Änderungen (Ziffer 1.4)

18 Der Auftragnehmer sollte darüber hinaus verpflichtet werden, etwaige **Änderungen bzgl. des Umfangs seiner Zertifizierung** dem Auftraggeber unverzüglich anzuzeigen, damit der Auftraggeber seine Datenübermittlungen anpassen kann.

3. Mitteilungspflichten (Ziffer 2)

19 **M 36.1.2 Mitteilungspflichten**

2. Mitteilungspflichten

2.1 Der Auftragnehmer ist verpflichtet, für den Fall, dass ihm Ermittlungen der für die Zertifizierung zuständigen Behörde bekannt werden, den Auftraggeber unverzüglich hierüber zu informieren.

2.2 Der Auftragnehmer ist in diesem Fall verpflichtet, mit der ermittelnden Behörde soweit gesetzlich vorgesehen umfassend zu kooperieren, wobei im Rahmen des rechtlich Zulässigen die Betriebs- und Geschäftsgeheimnisse des Auftraggebers zu wahren sind.

2.3 Er ist ferner verpflichtet, sämtliche ihm zumutbaren Maßnahmen durchzuführen, um den Verlust der Zertifizierung abzuwenden.

2.4 Der Auftragnehmer ist überdies verpflichtet, den Auftraggeber in Kenntnis zu setzen, wenn betroffene Personen gegen ihn wegen tatsächlicher oder behaupteter Datenschutzverstöße Rechtsbehelfe vor staatlichen Stellen oder im Rahmen eines Schiedsverfahrens geltend machen.

a) Ratio

20 Ziffer 2 regelt bestimmte **Informationspflichten** des Auftragnehmers in Bezug auf die **Zertifizierung** unter dem Privacy Shield.

b) Informationspflicht über Ermittlungsverfahren (Ziffer 2.1)

21 Die Parteien einer Auftragsverarbeitung unter dem Privacy Shield sollten **Mitteilungspflichten** über Ermittlungsverfahren gegen den Auftragnehmer vertraglich regeln, um den Auftraggeber in die Lage zu versetzen, dem Auftragnehmer dabei zu helfen, die Ermittlung abzuwenden und selbst präventive Vorkehrungen wie die Suche nach einem alternativen Auftragnehmer einzuleiten. Selbst im Falle ver-

öffentlichter Verfahren der Federal Trade Commission oder eines US-Gerichts kann dem Auftraggeber jedenfalls nicht zugemutet werden, erst durch eine solche Veröffentlichung von Ermittlungen gegen den Auftragnehmer zu erfahren. Die Bedeutung der Formulierung „unverzüglich" orientiert sich an der Definition des **§ 121 Abs. 1 Satz 1 BGB** (**ohne schuldhaftes Zögern**), auch wenn ein Vertrag mit einem US-amerikanischen Auftragnehmer ohne eine explizite Bezugnahme auf das BGB freilich nicht von dieser Definition ausgehen kann. Ein ähnliches Verständnis wird gleichwohl auch im Rahmen einer Vertragsauslegung angenommen werden können.

c) Kooperationsgebot (Ziffer 2.2)

Ziffer 2.2 sollte allgemein gehalten werden und Ermittlungen aller Behörden, d.h. **europäischer und amerikanischer**, beinhalten. Der Rahmen des rechtlich Zulässigen richtet sich nach dem jeweils anwendbaren Recht. 22

d) Abwendungspflicht (Ziffer 2.3)

Die Klausel sieht auch eine **Abwendungsverpflichtung** des Auftragnehmers vor, deren Erfüllung bereits im Hinblick auf etwaige Schadensersatzansprüche des Auftraggebers generell im Interesse des Auftragnehmers sein sollte. 23

e) Informationspflicht bei Beschwerden (Ziffer 2.4)

Betroffene Personen können **Beschwerden** auch direkt an den Auftragnehmer richten. Daneben können sie gerichtlich vorgehen oder eine unabhängige Stelle für alternative Streitbeilegung anrufen, sofern sich der Auftragnehmer für die alternative Streitbeilegung entschieden hat. In solchen Fällen besteht für den Auftraggeber ebenfalls das Risiko, dass der Auftragnehmer „ausfällt", so dass auch diese Konstellation präventiv vertraglich mit einer Mitteilungspflicht versehen werden sollte. 24

4. Rechtsfolgen des Verlusts der Zertifizierung (Ziffer 3)

M 36.1.3 Rechtsfolgen eines Verlusts der Zertifizierung 25

3. Rechtsfolgen eines Verlusts der Zertifizierung

3.1 Für den Fall, dass von der zuständigen Stelle die Zertifizierung wegen eines Verstoßes gegen datenschutzrechtliche Anforderungen entzogen wird, ist der Auftragnehmer dem Auftraggeber zum Ersatz des ihm entstandenen Schadens verpflichtet. Dies gilt nicht, wenn den Auftragnehmer an dem Datenschutzverstoß kein Verschulden trifft.

3.2 Dem Auftraggeber steht überdies für den Fall des Verlusts der Zertifizierung ein fristloses Sonderkündigungsrechts des Vertrags … zu.

a) Ratio

Die Regelung statuiert **Rechte des Auftraggebers** für den Fall, dass der Auftragnehmer die **Zertifizierung unter dem Privacy Shield** verliert. 26

b) Schadensersatz (Ziffer 3.1)

Unternehmen, die die Grundsätze des Privacy Shields fortgesetzt missachten, werden vom US-amerikanischen Handelsministerium von der Privacy Shield-Liste gestrichen. Im Einzelfall mag es (praxisnah jedoch zumeist eher an anderer Stelle des Vertragswerks in einer allgemeineren Klausel) sach- 27

gerecht sein, das **anwendbare Recht für Schadensfälle sowie den Gerichtsstand** vertraglich zu regeln. Andernfalls bestünde die Gefahr, dass ein in Deutschland niedergelassener Auftraggeber seinen Schaden am Sitz des Auftragnehmers in den USA einklagen müsste. Die amerikanischen Gerichte müssten ggf. Verstöße nach der DSGVO oder anderem europäischem oder nationalem Recht prüfen.

c) Kündigungsrecht (Ziffer 3.2)

28 Für den Fall, dass der Auftragnehmer das Privacy Shield-Zertifikat verliert, ist es interessengerecht, dass dem Auftraggeber ein **außerordentliches, fristloses Kündigungsrecht** vertraglich zugestanden wird.

Zwar sind Situationen denkbar, bei denen kurzfristig eine andere Rechtfertigungsmöglichkeit für die Datenübermittlung in die USA gewählt werden kann, vor allem durch Verwendung von **Standarddatenschutzklauseln der EU-Kommission**. In der Regel bedeutet der Verlust der Zertifizierung aber, dass die Auftragsverarbeitung im Hinblick auf die Drittstaatenübermittlung ihre Rechtfertigungsgrundlage verliert und dementsprechend sofort zu beenden und zu unterlassen ist. Die wirtschaftlichen Folgen für den Auftraggeber können nur sinnvoll durch ein Sonderkündigungsrecht abgefangen werden.

29 Im Einzelfall könnten noch weitere Regelungen aufgenommen werden, die beispielsweise regeln, wie im Falle der außerordentlichen Kündigung mit **bereits übermittelten und gespeicherten Daten** umzugehen ist, wenn diese nicht bereits in anderen Klauseln aufgenommen worden sind.

5. Entfall der Wirkung des Privacy Shields (Ziffer 4)

30 **M 36.1.4 Folgen einer Unwirksamkeit des Privacy Shields**

4. Folgen einer Unwirksamkeit des Privacy Shields

4.1 Für den Fall, dass die Angemessenheitsfeststellung der EU-Kommission zugunsten des „Privacy Shields" entfällt, z.B. weil der entsprechende Angemessenheitsbeschluss aufgehoben oder für ungültig erklärt wird, verpflichten sich beide Parteien, an einer Lösung mitzuwirken, welche den sodann geltenden datenschutzrechtlichen Voraussetzungen an eine Datenübermittlung in die USA gerecht wird.

4.2 Dies schließt ein Bemühen um eine vergleichbare Zertifizierung oder eine Mitwirkung in einem ähnlichen Verfahren für den Fall ein, dass der „Privacy Shield" durch einen anderen Mechanismus ersetzt wird und dessen Angemessenheit durch einen Beschluss der EU-Kommission verbindlich festgestellt ist.

a) Ratio

31 Die Vorschrift dient dazu, sicherzustellen, dass eine Datenverarbeitung zwischen den Parteien weiterhin möglich sein soll, wenn die **Legitimationswirkung** des Privacy Shields zur Erfüllung der Anforderungen von Kap. V DSGVO **entfallen** sollte.

b) Entfall der Angemessenheitsfeststellung (Ziffer 4.1)

32 Um die vertragliche Beziehung auch einer längerfristigen Zusammenarbeit zugänglich zu machen, ist es sinnvoll, etwaigen Änderungen in der datenschutzrechtlichen Ausgestaltung von Datentransfers aus der Europäischen Union in die USA durch eine **dynamische Klausel** zu begegnen. Es ist keineswegs sicher, dass der Privacy Shield einer gerichtlichen Kontrolle des EuGH auch dauerhaft standhält. Die Parteien sollten diese Ungewissheit in den Klauseln abbilden.

Vor diesem Hintergrund normiert Ziffer 4.1 eine zweiseitige Verpflichtung der Parteien, an einer Lösung mitzuwirken, die die Datenübermittlung an den Empfänger in den USA weiterhin legitimieren

kann. In der Praxis wäre hier insbesondere an den Abschluss eines Vertrages auf Basis der EU-Standarddatenschutzklauseln[31] zu denken.

c) Ersetzung durch neuen Mechanismus (Ziffer 4.2)

33 Der Verweis auf eine ggf. auch unter einem Folgemechanismus bestehende Zertifizierungsobliegenheit sollte unter dem Gesichtspunkt aufgenommen werden, dass die Erforderlichkeit einer Mitwirkung des betroffenen Unternehmens in den USA auch unter einem eventuell **anderen oder überarbeiteten Zertifizierungsverfahren** nicht unwahrscheinlich ist. In diesem Fall müssten die Parteien zwar ohnehin ihre Klausel im Hinblick auf die Datenübermittlung ersetzen; sachgerecht ist es dabei jedoch, eine **Pflicht zur Mitwirkung** an dem dann festgelegten Verfahren bereits jetzt festzuschreiben.

31 Siehe hierzu die Muster in Teil 5, §§ 26–28.