Verarbeitung personenbezogener Daten in Drittländern

Version 1.3 | Auf Basis der EU-Datenschutz-Grundverordnung post Schrems II

bitkom

Inhalt

Abbildungen und Tabellen

Herausgeber
Bitkom e. V.
Albrechtstraße 10
10117 Berlin
Tel.: 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Rebekka Weiß, LL.M.
Leiterin Vertrauen & Sicherheit
T 030 27576-161
r.weiss@bitkom.org

Verantwortliches Bitkom-Gremium
AK Datenschutz

Gestaltung
Anna Stolz

Titelbild
© 12521104 – istock.com

Vorwort

»Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer« war die vierte Publikation des Bitkom-Arbeitskreises Datenschutz und stammt bereits aus dem Jahr 2005.

Der Arbeitskreis Datenschutz besteht aus Expertinnen und Experten der Bitkom-Mitgliedsfirmen und befasst sich mit aktuellen Themen und datenschutzspezifischen Aspekten der Informations- und Kommunikationstechnik. Ein Profil des Arbeitskreises kann hier abgerufen werden: ↗ https://www.bitkom.org/Bitkom/Organisation/Gremien/Datenschutz.html

Die Version 1.1 des Leitfadens wurde im Sommer 2016 auf Basis des noch geltenden Rechts der EU-Datenschutzrichtlinie 95/46 und des Bundesdatenschutzgesetzes sowie unter Berücksichtigung der Rechtsprechung zu Safe Harbor erstellt. Sie diente als Orientierung für die Übergangsphase bis zur endgültigen Anwendung der EU-Datenschutz-Grundverordnung.

Die darauffolgende Version 1.2 wurde im Sommer 2017 auf Basis der EU-Datenschutz-Grundverordnung, die seit 25. Mai 2018 Anwendung findet, erstellt und im Sommer 2022 in der hier vorliegenden Version 1.3. aktualisiert. Die Version 1.3 berücksichtigt die Auswirkungen des am 16.07.2020 ergangenen EuGH-Urteils »Schrems II« (C-311/18), in dem der Angemessenheitsbeschluss (EU)2016/1250 der Europäischen Kommission vom 12. Juli 2016 zum US-EU Privacy Shield Framework – die Übermittlung personenbezogener Daten in die USA betreffend – für ungültig erklärt wurde. Das Urteil bringt unterdessen nicht nur für Datentransfers in die USA, sondern im Allgemeinen für die Verarbeitung personenbezogener Daten in Drittländern erhebliche Auswirkungen mit sich.[1]

Für die Aktualisierung zur Version 1.3 danken wir insbesondere:

- Arnd Böken, Graf von Westphalen Rechtsanwälte
- Dr. Paul Voigt, Taylor Wessing
- Dr. Jörg Friedrichs, Deutsche Telekom
- Frank Ingenrieth, Selbstregulierung Informationswirtschaft e.V.
- Dr. Christian Weitzel, Harder Rechtsanwälte
- Zeljko Matas, Bristol-Myers Squibb
- Linus Klingberg, Deutsche Bahn
- Dr. Christoph Bausewein, CrowdStrike
- Markus Zechel, migosens

1 Der Bitkom AK Datenschutz hat parallel zu dem hier vorliegenden Leitfaden ein Transfer Impact Assessment Tool entwickelt, das die Datentransfers unter Berücksichtigung des Schrems II-Urteils für Unternehmen strukturiert und diese prüfbar macht und die Einbeziehung zusätzlicher Schutzmaßnahmen zur Absicherung der Transfers vereinfacht.

Zu den ursprünglichen Versionen des Leitfadens hatten maßgeblich beigetragen: Anne Bernzen, Jonas von Dall Armi, Dr. Sibylle Gierschmann, LL. M., Ulrike Schroth, Regina Wacker-Dengler, Wolfgang Braun, Helmut Glaser, Alexander Heimel, Stefan Lerbs, Ralf Maruhn, Manfred Monreal, Mirko Schmidt, Barbara Schmitz, Florian Thoma.

Berlin, Juni 2022

Als weitere Publikationen des Bitkom Arbeitskreises Datenschutz sind erhältlich:

- ↗ Grafik Datenschutzkonforme Datenverarbeitung nach der EU-Datenschutz-Grundverordnung. Stand 2017.
- ↗ FAQ – Was muss ich wissen zur EU-Datenschutz Grundverordnung?
- ↗ Das Safe-Harbor-Urteil des EuGH und die Folgen. Fragen und Antworten.
- ↗ Mustervertragsanlage Auftragsverarbeitung und begleitende Hinweise. Stand 2017.
- ↗ Joint Controllership in der EU-Datenschutz-Grundverordnung. Checkliste. Stand 2017.
- ↗ Leitfaden Risk Assessment und Datenschutz-Folgenabschätzung. Stand 2017.
- ↗ Das Verarbeitungsverzeichnis (Version 4.0). Stand 2017.
- ↗ Informationspflichten nach der DS-GVO. Stand 2019.
- ↗ Datenschutzverletzung und Meldung im Kontext des »Hafnium Hacks«. Stand 2021

Executive Summary

Allgemein

- Der Transfer von personenbezogenen Daten ist durch die Rechtsprechung des EuGH in der Rechtssache C-311/18 - Schrems II) signifikant erschwert worden. So haben Verantwortliche – ohne Ausnahmen für kleine und mittelständische Unternehmen oder Vereine – vor jedem Transfer, d. h. der Nutzung von z. B. mit Drittlandtransfers einhergehenden Cloud-Diensten, die Pflicht durch geeignete Informationen zu prüfen und zu dokumentieren, dass im Zielland des Transfers das durch die DS-GVO vorgeschriebene Schutzniveau gewahrt ist.

- Datentransfers in alle Länder außerhalb des Europäischen Wirtschaftsraums (EWR) sind nur dann zulässig, wenn ein angemessenes Schutzniveau für die betroffenen Daten gewährleistet ist. Diesbezüglich ist wichtig zu wissen, dass die Europäische Kommission eine Reihe von Ländern überprüft und als sichere Häfen, was den Datenschutz nach der DS-GVO anbelangt, qualifiziert hat.

- Zu beachten ist, dass sich die jeweiligen Angemessenheitsbeschlüsse der Europäischen Kommission nach Art. 45 Abs. 3 DS-GVO in ihrer inhaltlichen Reichweite von Land zu Land unterscheiden können. So erfasst z. B. die Adäquanzentscheidung für Kanada nur solche Datenverarbeitungen, die dem kanadischen Bundesrecht unterfallen.

  Hinweis: Sollte ein Angemessenheitsbeschluss der Europäischen Kommission für das Zielland des Datentransfers vorliegen, kann ohne weiteren Aufwand der Transfer begonnen werden. In Abwesenheit eines Angemessenheitsbeschlusses bedarf es weiterer Maßnahmen, die im Folgenden dargestellt werden und zwingend beachtet werden müssen.

- Für alle übrigen Länder bedarf es für einen Datentransfer verbindliche, behördlich genehmigte Datenschutzregeln (sog. Binding Corporate Rules – BCR), den Abschluss von der jeweils zuständigen Aufsichtsbehörde genehmigter Vertragsklauseln, den dem Regelungsgehalt nach unverändertem Abschluss von sog. Standardvertragsklauseln, die von der Europäischen Kommission herausgegeben werden oder z. B. der Einwilligung des Betroffenen. Neuerdings können auch genehmigte Verhaltensregeln (Codes of Conduct – CoC) angewendet werden, die aktuell aber erst in der Entstehung sind und daher noch eher untergeordnete Bedeutung haben. Perspektivisch werden sie aber etwa Verbandsmitgliedern Datentransfers, vorbehaltlich der Erfüllung bestimmter Anforderungen, ermöglichen.

- **Einbeziehung des Auftragsverarbeiters:** Sollte kein Angemessenheitsbeschluss der Europäischen Kommission für das Zielland des Datentransfers vorliegen, empfiehlt es sich, auf den Auftragsverarbeiter zuzugehen und nach Informationen zur Durchführung eines Transfer Impact Assessment (TIA) zu suchen. Optimalerweise hat der Auftragsverarbeiter seinerseits bereits eine Analyse des Datenschutzniveaus im Zielland im Lichte der EuGH-Rechtsprechung und der lokal geltenden Überwachungsgesetze durchgeführt, die Sie sich in einer eigenen Prüfung zu eigen machen können. Im Allgemeinen hat der Auftragsverarbeiter für seinen Verantwortungsbereich eigene Dokumentationspflichten (Art. 30 DS-GVO).

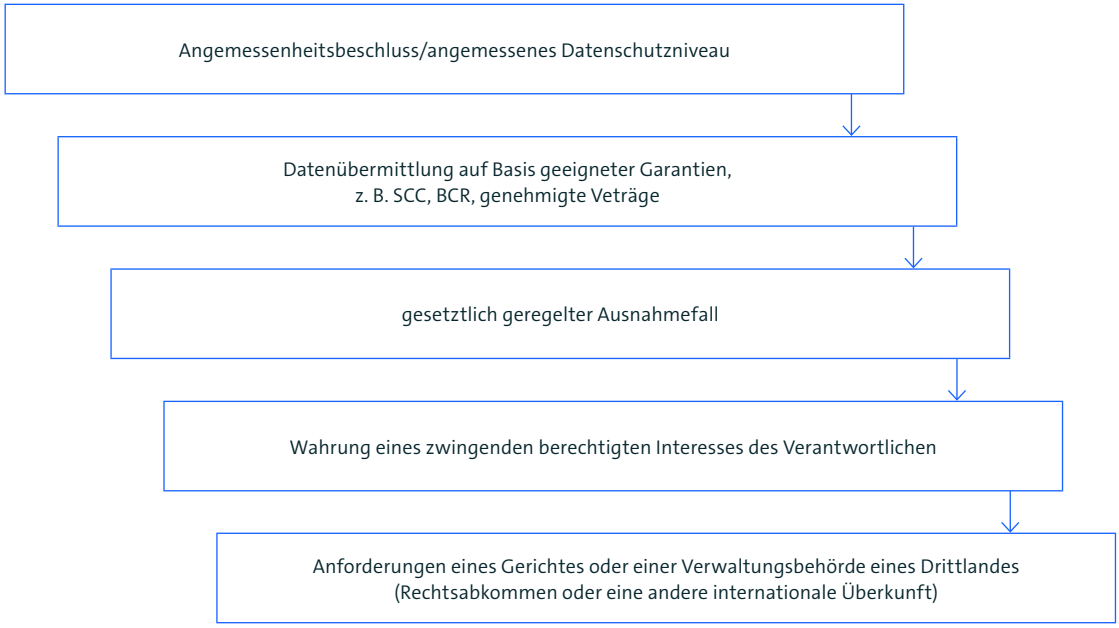

Abbildung 1: Überblick der Übermittlungstatbestände

Systematik der Übermittlungstatbestände

<table>
<tr><td colspan="7">Übermittlung in Drittstaaten nach der DS-GVO (Art. 44–49)</td></tr>
<tr><td rowspan="11">Drittstaaten mit Angemessenheitsbeschluss Art. 45</td><td colspan="6">Drittstaaten ohne Angemessenheitsbeschluss</td></tr>
<tr><td colspan="5">Datenübermittlung bei geeigneten Garantien Art. 46</td><td>Ausnahmetatbestände nach Art. 49 mit subsidiärem Charakter</td></tr>
<tr><td rowspan="10">Nur für konzerninterne Datenübertragung:

BCR Art. 47 (Abs. 1b)</td><td rowspan="10">Abschluss der unveränderten Standard- datenschutz-klauseln KOM (Abs. 1c)

Stets nur in Verbindung mit Einzelfallprüfung, ob die Gesetze im Empfängerland den Pflichten aus den Standardvertrags-Klauseln entgegenstehen</td><td rowspan="10">Abschluss der unveränderten Standard-datenschutz-klauseln DS-Aufsicht (Abs. 1d)</td><td rowspan="10">Genehmigte Verhaltensregeln (Code of Conduct) n. Art. 40 (Abs. 1e)</td><td rowspan="10">Zertifizierung n. Art. 42 (Abs. 1f)</td><td>Einwilligung (Abs. 1a)</td></tr>
<tr><td>Vertrag oder vorvertragliche Maßnahmen mit dem Betroffenen o. im Interesse der betroffenen Person abgeschlossener Vertrag (Abs. 1b und c)</td></tr>
<tr><td>Übermittlung aus wichtigen Gründen des öffentlichen Interesses (Abs. 1d)</td></tr>
<tr><td>Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Abs. 1e)</td></tr>
<tr><td>Schutz lebenswichtiger Interessen (Abs. 1f)</td></tr>
<tr><td>Übermittlung aus einem Register (Abs. 1g)</td></tr>
<tr><td colspan="6">Übermittlung zur Wahrung zwingend berechtigter Interessen des Verantwortlichen erforderlich Abs. 1</td></tr>
</table>

Tabelle 1: Systematik der Übermittlungstatbestände

Die Übermittlung personenbezogener Daten begleitet täglich die Anbahnung und Abwicklung der Geschäfte zahlreicher Unternehmen. Ebenso wie die Geschäfte macht auch die Datenübermittlung dabei schon lange nicht mehr an den Landesgrenzen Deutschlands halt, sondern erfolgt häufig grenzübergreifend zwischen europäischen Staaten oder international. Durch die ständig zunehmende Mobilität und die Globalisierung des Welthandels gewinnt dieser grenzübergreifende Datenaustausch stetig an Bedeutung. Gefördert wird dieser Trend durch die zunehmende Digitalisierung und den Einsatz von Cloud-Diensten. Dies betrifft nicht nur den

1 Einführung: Die Übermittlung personenbezogener Daten

Austausch von Daten zwischen Vertragspartnern, sondern auch den Austausch und die Weitergabe im Unternehmensverbund. In internationalen Konzernen werden z. B. häufig Personaldaten zwischen den Konzerntöchtern und der Konzernholding bzw. zwischen den Tochtergesellschaften ausgetauscht. Durch die Vernetzung der Produktions- und Handelsbeziehungen bleiben personenbezogene Daten nicht nur im Unternehmen bzw. Konzern, sondern werden auch an ausländische Geschäftspartner oder internationale Datenbanken übermittelt. Auch für Unternehmen, die allein in Deutschland und der EU tätig sind, sind die Regelungen zum Datentransfer wichtig, wenn sie Dienstleister für ihre Website oder als E-Mail Provider einsetzen, eine Kundendatenbank oder ein Bewerberportal verwenden und Dienstleister mit Sitz außerhalb Europas hieran mitwirken.

Die Regelungen zum Datenexport sind in den letzten Jahren komplizierter geworden. Durch das Schrems II Urteil des EuGH vom 16.7.2020 haben sich die Anforderungen deutlich erhöht. Die Datenschutzbehörden versenden Fragebögen an Unternehmen, um Datenübermittlungen zu überprüfen. Die Anforderungen sollten jedoch von jedem Unternehmen ernst genommen werden. Eine Datenübermittlung, die nicht den gesetzlichen Voraussetzungen genügt, kann als Ordnungswidrigkeit qualifiziert und mit empfindlichen Bußgeldern geahndet sowie von Betroffenenseite Schadenersatzansprüche nach sich ziehen.

Vor diesem Hintergrund will die Bitkom-Publikation »Verarbeitung personenbezogener Daten in Drittländern« eine praktische Hilfestellung für den täglichen Gebrauch beim Transfer von Daten bieten. Neben einer kurzen Darstellung des Rechtsrahmens für Datentransfers (Kapitel 2) wird die Datenverarbeitung in Drittstaaten mit angemessenem Datenschutzniveau (Kapitel 3) und ohne angemessenem Datenschutzniveau (Kapitel 4)[2] aufgeführt. Die verschiedenen Konstellationen werden jeweils mit einem kurzen Fallbeispiel illustriert. Abgerundet wird der Leitfaden schließlich durch ergänzende Materialien (Kapitel 6), Links und Literaturhinweise.

Bitte beachten Sie: Der Leitfaden kann angesichts der komplexen Materie keinen Anspruch auf Vollständigkeit erheben. Zudem ist die dargestellte Materie der fortlaufenden Entwicklung des Rechts und der Technik unterworfen. Letztlich versteht sich dieser Leitfaden daher als Einführung in die Problematik und bereitet beispielhaft Handlungsmöglichkeiten auf. Die Einbindung professioneller unternehmensinterner oder externer Berater wird dadurch jedoch nicht obsolet und der Leitfaden ersetzt keine Rechtsberatung.

2 ausführliche Erläuterungen zu den Folgen des Schrems II Urteils des EuGH finden sich im Bitkom Konzeptpapier für Drittstaatentransfers: ↗ https://www.bitkom.org/sites/default/files/2021-02/20210218_konzeptpapier-drittstaatentransfers-nach-schrems-ii.pdf

2 Rechtsrahmen

2.1 Anwendungsbereich Datenschutz-Grundverordnung

Die Datenschutzgrundverordnung (DS-GVO)(EU) 2016/679 des Europäischen Parlaments und des Rates und die Datenschutzrichtlinie (EU) 2016/680 wurden am 27. April 2016 verabschiedet und gelten seit dem 25. Mai 2018. Die DS-GVO schuf ein weitgehend einheitliches Datenschutzrecht innerhalb der gesamten Europäischen Union. Als Verordnung gilt sie unmittelbar, d. h. sie braucht nicht durch nationale Gesetze umgesetzt zu werden. Dies bedeutet, dass die Datenverarbeitung in anderen EU-Ländern genauso zu behandeln ist wie innerhalb Deutschlands. Auch für die EWR-Staaten Norwegen, Island, Liechtenstein ist die Angemessenheit des Datenschutzniveaus anerkannt. Diese Länder sind bezüglich der Datenübermittlung daher mit Ländern innerhalb der EU gleichzusetzen. Es gibt jedoch Konstellationen, in denen die Datenschutzgrundverordnung ggf. auch über den Wirkungsbereich der EU und einiger EWR-Länder hinaus Anwendung finden kann, z. B. im Rahmen der Nutzung von Cloud-Dienstleistungen. Hier gilt es zu prüfen, inwieweit die jeweilige (beabsichtigte) Verarbeitung in den Wirkungsbereich des Art. 3 DS-GVO fällt.

Der Text der DS-GVO ist ↗ hier abrufbar, in allen Amtssprachen der EU.

Die DS-GVO gilt grundsätzlich für alle Behörden der EU-Mitgliedsstaaten und für sämtliche Unternehmen der Privatwirtschaft, die eine Niederlassung innerhalb der Europäischen Union haben. Für Unternehmen ohne Niederlassung in der Union gilt sie unter bestimmten Voraussetzungen (siehe hierzu Abschnitt 2.4). Die Datenschutzrichtlinie gilt für den Polizei- und Justizbereich und bedarf eines nationalen Umsetzungsgesetzes.

Voraussetzung der Geltung ist weiter, dass personenbezogene Daten ganz oder teilweise automatisiert verarbeitet werden. Für die nicht-automatisierte Verarbeitung personenbezogener Daten gilt die DS-GVO, wenn die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 1).

2.2 Räumlicher Anwendungsbereich der DS-GVO[3]

Der DS-GVO liegen zwei Prinzipien zu Grunde: das »Niederlassungsprinzip« und das »Marktortprinzip« (Art. 3 DS-GVO).

Die Verordnung gilt für die Datenverarbeitung im Rahmen der Tätigkeit einer Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der EU. Es ist dabei unerheblich, ob die Verarbeitung in der EU stattfindet oder nicht. Eine Niederlassung ist jede feste Einrichtung, von der aus eine Tätigkeit ausgeübt wird, beispielsweise von einem gemieteten Büro aus, selbst wenn die Tätigkeit nur geringfügig ist (vgl. EuGH, Urteil vom 1.10.2015, Weltimmo, C-230/14).

> **Beispiel:** Unternehmen Inc. (U) mit Sitz in New York hat ein Büro in Berlin. Die Kundendatenbank der deutschen Filiale ist auf Servern des Unternehmens in den USA gespeichert. Die DS-GVO gilt gemäß Art. 3 Abs. 1.

Nach dem Marktortprinzip (Art. 3 Abs. 2) gilt die DS-GVO auch dann, wenn der Verantwortliche oder Auftragsverarbeiter keine Niederlassung in der Union hat, sofern Daten betroffener Personen, die sich in der Union befinden, verarbeitet werden, wenn

- den Personen Waren oder Dienstleistungen angeboten werden, auch wenn sie keine Zahlung zu leisten haben oder
- das Verhalten dieser Personen in der EU beobachtet wird.

> **Beispiel:** Unternehmen (A) mit Sitz in China und ohne Niederlassung in Europa bietet Waren an, die auch an Käufer in Deutschland geliefert werden. Für die Datenverarbeitung gilt die DS-GVO, Art. 3 Abs. 2.

Diese Regelung gilt auch für Angebote, die unentgeltlich sind.

3 Weiterführend EDSA: Leitlinie 3 / 2018 zum räumlichen Anwendungsbereich der DS-GVO (Artikel 3)

> **Beispiel:** Unternehmen (F) mit Sitz in Kalifornien betreibt ein soziales Netzwerk. Das Angebot ist kostenlos, es richtet sich auch an Nutzer aus Deutschland. Die DS-GVO gilt hier.

Für die Anwendbarkeit der DS-GVO reicht es schon aus, dass das Verhalten von Nutzern aus Europa beobachtet werden soll. Da bereits das Verwenden von Cookies auf Websites der Verhaltensbeobachtung dient, ist der räumliche Anwendungsbereich der DS-GVO sehr weit. Es genügt häufig schon, eine Website anzubieten, wenn sich diese auch an einen Nutzer aus der EU richtet.

2.3 Voraussetzungen der Datenverarbeitungen

Für die Verarbeitung personenbezogener Daten gilt als allgemeiner Grundsatz ein sogenanntes Verbot mit Erlaubnisvorbehalt. Hier besteht ein gesetzliches Regel-Ausnahme-Verhältnis, die Verarbeitung personenbezogener Daten ist regelmäßig unzulässig, soweit sie nicht ausnahmsweise erlaubt ist.

Grundsätze für die Verarbeitung personenbezogener Daten

Die DS-GVO gibt folgende Grundsätze für die Verarbeitung von personenbezogenen Daten vor (Art. 5 Abs. 1 DS-GVO):

a. Rechtmäßigkeit Verarbeitung nach Treu und Glauben, Transparenz
b. Zweckbindung
c. Datenminimierung
d. Richtigkeit
e. Speicherbegrenzung (zeitliche Begrenzung der Speicherung)
f. Integrität und Vertraulichkeit

Der Verantwortliche muss die Einhaltung dieser Grundsätze nachweisen können (»Rechenschaftspflicht«, Art. 5 Abs. 2 DS-GVO).

2.3.1 Erlaubnistatbestände

Die Verarbeitung von personenbezogenen Daten ist nur dann rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen aus Art. 6 Abs. 1 DS-GVO erfüllt ist:

a. Die betroffene Person hat ihre Einwilligung zu der Verarbeitung für einen oder mehrere bestimmte Zwecke gegeben.

b. Die Verarbeitung ist für die Erfüllung eines Vertrages, dessen Vertragspartei der Betroffene ist, erforderlich oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage des Betroffenen erfolgen.

c. Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen erforderlich; die Rechtspflicht kann sich aus dem EU-Recht oder dem Recht der Mitgliedsstaaten ergeben, dem der Betroffene unterliegt.

d. Die Verarbeitung ist erforderlich, um lebenswichtige Interessen des Betroffenen oder einer anderen natürlichen Person zu schützen.

e. Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

f. Die Verarbeitung ist zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern die Interessen oder Rechte und Freiheiten des Betroffenen nicht überwiegen.

Für die Privatwirtschaft sind vor allem die Erlaubnistatbestände der Einwilligung, der Vertragserfüllung, der Erfüllung einer rechtlichen Verpflichtung sowie der Wahrung berechtigter Interessen von besonderer Bedeutung.

2.4 Spezielle Datenschutzgesetze

Im öffentlichen Sektor sind die wichtigsten Bereiche, die durch Spezialgesetze geregelt werden, der Schutz der öffentlichen Sicherheit, die Strafverfolgung sowie der Bereich der Nachrichtendienste. Für diese Sektoren gilt die DS-GVO nicht. Für den Bereich der Strafverfolgung und der Strafvollstreckung einschließlich des Schutzes der öffentlichen Sicherheit, gibt es die Richtlinie (EU) 2016/680, die insbesondere durch das im DSAnpUG-EU neu gefasste BDSG (Teil 3, §§ 45 ff.) transformiert wurde. Im Bereich der Nachrichtendienste hat die EU keine Gesetzgebungskompetenz. Hier sind allein die Mitgliedsstaaten zuständig. Auch hier nimmt das DSAnpUG-EU Änderungen an einer Vielzahl von Spezialgesetzen vor, z. B. das Gesetz über den Militärischen Abschirmdienst, das Gesetz über den Bundesnachrichtendienst, das Sicherheitsüberprüfungsgesetz und das sogenannte Artikel-10-Gesetz. Gerade solche Gesetze in Drittländern sind es, die im Fokus des Schrems II Urteils stehen und somit die »hohe« Hürde darstellen, um geeignete Garantien und Maßnahmen zu ermitteln, die eine rechtskonforme Übermittlung von personenbezogenen Daten in Drittländer ohne gleichwertiges Datenschutzniveau ermöglichen.

Für die Wirtschaft sind die wichtigsten Bereiche, die durch Spezialgesetze geregelt werden, die Datenverarbeitung im Internet und bei der Telekommunikation, die durch das Telekommunikation-Telemedien-Datenschutzgesetz geregelt werden. Der EU-Gesetzgeber behandelt im Moment die ePrivacy-Verordnung (Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation COM (2017) 10), die diese Datenverarbeitung EU-weit einheitlich regelt. Zum Zeitpunkt dieser Veröffentlichung sind die Verhandlungen auf EU-Ebene noch nicht abgeschlossen.

Ein weiterer wichtiger Spezialbereich ist der Datenschutz im Beschäftigungsverhältnis, der weiter durch Gesetze der Mitgliedsstaaten geregelt werden kann.

3 Datenverarbeitung in einem Drittland mit angemessenem Datenschutzniveau

Die DS-GVO geht im Grundsatz davon aus, dass die Übermittlung von Daten an ausländische Stellen außerhalb der EU/EWR rechtmäßig nur dann erfolgen kann, wenn im Drittland ein angemessenes Datenschutzniveau gewährleistet ist.

Dieses Schutzniveau ist u. a. dann gewährleistet,

- wenn die Angemessenheit des Niveaus der Datenschutzgesetzgebung eines Landes, Gebiets oder Sektors von der EU-Kommission anerkannt ist, Art. 45.

3.1 Beurteilung der Angemessenheit

Die Feststellung der Angemessenheit erfolgt in einem förmlichen Verfahren durch die EU-Kommission (Art. 45 DS-GVO). Dieses hat sich gegenüber der Datenschutzrichtlinie 95/46/EG nicht geändert, allerdings sind die Vorschriften in vielerlei Hinsicht detaillierter:

- **Die Prüfungskriterien für Angemessenheitsentscheidungen wurden erweitert:** Die DS-GVO normiert die Prüfungskriterien für Angemessenheitsbeschlüsse, die die EU-Kommission beachten muss (Art. 45 Abs. 2) wie z. B. die Rechtsstaatlichkeit, Achtung der Menschenrechte und Grundfreiheiten, wirksamer gerichtlicher Rechtsschutz und die Existenz von unabhängigen Aufsichtsbehörden. Darüber hinaus ergibt sich aus der Schrems I-Entscheidung des EuGH, dass für die Prüfung eines angemessenen Schutzniveaus u. a. auch die nationalen Vorschriften und die Praxis der Sicherheits- und Strafverfolgungsbehörden bezüglich des Zugriffs auf personenbezogene Daten aus Gründen der öffentlichen Sicherheit in Betracht gezogen werden müssen.

- **Angemessenheit nicht nur für ein Drittland, sondern auch für ein Gebiet oder ein oder mehrere spezifische Sektoren in dem Drittland:** Gem. Art. 45 Abs. 3 kann sich eine Angemessenheitsentscheidung auch auf ein Gebiet (z. B. Länder mit Föderalstruktur wie den USA)[4] oder ein oder mehrere spezifische Sektoren beziehen (z. B. privater Sektor oder bestimmte Wirtschaftszweige). Dies war in der RL 95/46 EG bisher nicht vorgesehen.

Hinweis: Die Angemessenheit des Datenschutzniveaus bedeutet dabei nicht zwingend, dass die Verhältnisse gleichartig oder gleichwertig sind.

4 EU-Kommission, FAQ on Commission's adequacy finding on the Canadian Personal Information Protection and electronic Documents Act, question: »Does the Commission Decision also cover provincial legislation«, ↗ http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/third-countries-faq/ index_en.htm.

3.2 Angemessenheitsbeschlüsse[5]

- Die DS-GVO normiert die Prüfungskriterien für Angemessenheitsbeschlüsse, die die EU-Kommission beachten muss (Art. 45 Abs. 2 DS-GVO) wie z. B. die Rechtsstaatlichkeit, Achtung der Menschenrechte und Grundfreiheiten, wirksamer gerichtlicher Rechtsschutz und die Existenz von unabhängigen Aufsichtsbehörden. Darüber hinaus ergibt sich aus der Schrems I-Entscheidung des EuGH , dass für die Prüfung eines angemessenen Schutzniveaus u. a. auch die nationalen Vorschriften und die Praxis der Sicherheits- und Strafverfolgungsbehörden bezüglich des Zugriffs auf personenbezogenen Daten aus Gründen der öffentlichen Sicherheit in Betracht gezogen werden müssen.

Hinweis: In der ↗ EU-Mitteilung (2017) 7 hatte die EU-Kommission angekündigt, dass sie sich – nach der Vereinbarung des in diesem Zeitpunkt noch gültigen EU-US Privacy Shields – mit den Regelungen zu Datentransfers in weitere Staaten außerhalb der EU beschäftigen werde. Geprüft worden ist, ob zum Beispiel andere Länder wie Japan oder Südkorea über ähnlich hohe Datenschutzstandards verfügen wie die EU. Diese Länder haben im Jahr 2017 neue Datenschutzgesetze erlassen und den Schutz der Privatsphäre damit gestärkt.

Nachdem die EU-Kommission am 05.09.2018 auf Antrag Japans das Verfahren zur Annahme ihrer Angemessenheitsfeststellung eingeleitet hat, ist am 23.09.2018 ein Angemessenheitsbeschluss ergangen. Darin hat die Kommission festgestellt, dass Japan als Drittland mit seinen inländischen Rechtsvorschriften oder internationalen Verpflichtungen für personenbezogene Daten ein vergleichbares Schutzniveau bietet wie die Europäische Union. Als Konsequenz aus der Angemessenheitsentscheidung profitiert die EU von einem ungehinderten Verkehr personenbezogener Daten nach und aus Japan sowie von einem privilegierten Zugang zu seinem Markt.

Am 16. Juni 2021 leitete die Kommission das Verfahren zum Erlass eines Angemessenheitsbeschlusses für die Übermittlung personenbezogener Daten nach Südkorea im Rahmen der Datenschutz-Grundverordnung ein, das im Dezember 2021 auch positiv abgeschlossen wurde.

Am 28.06.2021 hat die EU-Kommission außerdem den Angemessenheitsbeschluss zum Vereinigten Königreich angenommen. Datenübermittlungen für die vom Vereinigten Königreich praktizierte Einwanderungskontrolle sind allerdings vom sachlichen Geltungsbereich des im Rahmen der DS-GVO angenommenen Angemessenheitsbeschlusses ausgenommen.

Für die Geltung der Angemessenheitsentscheidungen gibt es grundsätzlich keine Zeitbegrenzung, die Beschlüsse werden aber in regelmäßigen Abständen – zunächst nach 2 Jahren und dann alle 4 Jahre – überprüft. Die Angemessenheitsentscheidung für das Vereinte Königreich ist

5 Übersicht und Erläuterungen finden sich z. B. auch hier:
↗ https://datenschutz.hessen.de/datenschutz/internationales/angemessenheitsbeschl%C3%BCsse

jedoch zunächst auf vier Jahre befristet und endet am 27.06.2025, sofern nicht eine Verlängerung beschlossen wird. Zudem besteht die Möglichkeit, den Angemessenheitsbeschluss vorzeitig auszusetzen. Eine solche Aussetzung dürfte maßgeblich davon abhängen, wie die britische Regierung das lokale Datenschutzrecht reformiert.

Ein angemessenes Datenschutzniveau wurde von der EU-Kommission in einer förmlichen Entscheidung für folgende Länder festgestellt:

- Argentinien (2003/490/EC)
- Andorra (2010/625/EU)
- Guernsey (2003/821/EC)
- Isle of Man (2004/411/EC)
- Jersey (2008/393/EC)
- Kanada (2002/2/EC)[6]
- Neuseeland (2013/65/EU)
- Israel (2011/61/EU)
- Schweiz (2000/518/EC)
- Färöer Inseln (2010/146/EU)
- Uruguay (2012/484/EU)
- Japan (2019/419/EU)
- Vereinigtes Königreich (C(2021) 4800)[7]
- Republik Korea (Südkorea) (C(2021) 9316)[8]

Weitere Informationen zu den Entscheidungen der Kommission können auf der ↗ EU-Datenschutz-Homepage abgerufen werden.

> **Beispiel:** Unternehmer D mit Sitz in Deutschland übermittelt z. B. Kundendaten an das Unternehmen A mit einem angemessenen Datenschutzniveau (z. B. Schweiz, Guernsey, Argentinien, Kanada, etc.).

Angemessenheitsbeschlüsse, die die Kommission gem. Art. 25 Abs. 6 der RL 95/46 EG getroffen hat oder neue Angemessenheitsbeschlüsse auf Basis der DS-GVO bleiben in Kraft, solange bis sie durch einen Beschluss der EU-Kommission geändert, ersetzt oder aufgehoben werden. Sie unterliegen der fortwährenden Überwachung der EU-Kommission (Prüfung mindestens alle 4 Jahre), die ein Prüfverfahren einleiten muss, wenn ihr Informationen vorliegen, dass kein angemessenes Datenschutzniveau vorliegt.

6 Beschränkt auf solche Datenverarbeitungen, die dem Personal Information Protection and Electronic Documents Act (PIPEDA) unterfallen

7 Übersicht und Erläuterungen zu einigen Beschränkungen (insb. Verfallsklausel) und Besonderheiten der UK-Adäquanz: ↗ https://ec.europa.eu/commission/presscorner/detail/de/ip_21_3183

8 ↗ https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf

4 Datenverarbeitung in Drittstaaten ohne angemessenes Datenschutzniveau

4.1 Garantien – Einführung

Bei Fehlen eines Angemessenheitsbeschlusses können geeignete Garantien für den Schutz der Betroffenen den im Drittland bestehenden Mangel an Datenschutz ausgleichen. Hierbei unter- scheidet Art. 46 zwischen genehmigungsfreien Garantien (Abs. 2) und genehmigungspflichtigen Garantien (Abs. 3).

Garantien ohne besondere Genehmigung der Aufsichtsbehörden können bestehen in:

a. einem rechtlich bindenden und durchsetzbaren **Dokument zwischen den Behörden oder öffentlichen Stellen**,

b. verbindlichen internen **Datenschutzvorschriften gemäß Art. 47**,

c. **Standarddatenschutzklauseln**, die von **der Kommission** gemäß dem Prüfverfahren nach Art. 93 Abs. 2 erlassen werden,

d. **von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln**, die von der Kommission gemäß dem Prüfverfahren nach Art. 93 Abs. 2 genehmigt wurden,

e. genehmigten **Verhaltensregeln gemäß Art. 40** zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverar beiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, oder

f. einem genehmigten **Zertifizierungsmechanismus gemäß Art. 42** zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen.

Zu den Garantien, die gem. Art. 46 Abs. 3 dem Vorbehalt der Genehmigung der zuständigen Aufsichtsbehörde unterliegen, gehören

a. **Vertragsklauseln**, die zwischen dem Verantwortlichen oder dem Auftragsverarbeiter und dem Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger der personenbezogenen Daten im Drittland oder der internationalen Organisation vereinbart wurden, und

b. **Bestimmungen**, die **in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen** aufzunehmen sind und durchsetzbare und wirksame Rechte für die betroffenen Personen einschließen.

Zweck der Garantien ist die angemessene Beachtung der Datenschutzvorschriften und Rechte der betroffenen Personen.

4.2 Standarddatenschutzklauseln, Art. 46 Abs. 2 lit. c und d DS-GVO

Gem. Art. 46 Abs. 2 können Datenübermittlungen an ein Drittland auch auf Standarddatenschutzklauseln der Kommission (lit. c) oder der Aufsichtsbehörde (lit. d) gestützt werden. Die DS-GVO sieht zusätzlich vor, dass auch Aufsichtsbehörden Standarddatenschutzklauseln entwickeln können, welche von der Kommission im Rahmen eines Prüfverfahrens genehmigt werden müssen.

Basierend auf Art. 45 Abs. 3 DS-GVO hatte die Kommission Standardvertragsklauseln für unterschiedliche Fallkonstellationen verabschiedet:

- Standardvertragsklauseln für die Datenübermittlung zwischen für die Verarbeitung Verantwortlichen (Controller-Controller-Transfer)
  - Set I aus der Entscheidung 2001/497/EG vom 15. Juni 2001
  - Set II (sog. alternative Standardvertragsklauseln) aus der Entscheidung 2004/915/EG vom 27. Dezember 2004 zu Änderungen der Entscheidung 2001/497/EG
- Standardvertragsklauseln für die Datenübermittlung zwischen für die Verarbeitung Verantwortlichen und nach deren Weisung handelnden Auftragsverarbeitern (Controller-Processor-Transfer):
  - (aktueller) Beschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates

Im Juni 2021 veröffentlichte die EU-Kommission neue Standardvertragsklauseln für Übermittlungen personenbezogener Daten in Drittländer. Diese sollen zum einen die Entwicklungen der vergangenen Jahre in der digitalen Wirtschaft sowie die zunehmende Komplexität der Verarbeitungsvorgänge berücksichtigen und ersetzen die bisherigen Standarddatenschutzklauseln aus den Jahren 2001, 2004 und 2010.

Hinweis: Während Art. 26 Abs. 4 der RL 95/46/EG von Standardvertragsklauseln spricht, bezeichnet die DS-GVO in Art. 46 Abs. 2 sowie im EG 108 die von der Kommission oder einer Aufsichtsbehörde vorgegebenen Garantien zum Ausgleich für den in einem Drittland bestehenden Mangel an Datenschutz nunmehr als Standarddatenschutzklauseln.

Es handelt sich bei den neuen Standarddatenschutzklauseln um:

- ↗ Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer[9]
- ↗ Standardvertragsklauseln für Verantwortliche und Auftragsverarbeiter in der EU / im EWR

Darüber hinaus trägt die Verabschiedung der neuen Standarddatenschutzklauseln den neuen rechtlichen Entwicklungen Rechnung, die aus der Entscheidung des EuGH vom 16.07.2020 (»Schrems II«) resultieren. Der EuGH erklärte in jenem Urteil den EU-US Privacy Shield-Beschluss für ungültig, der bis dahin den Transfer von personenbezogenen Daten von der EU in die USA ermöglichte.

Die am 04.06.2021 verabschiedeten Standarddatenschutzklauseln ersetzen somit die vorherigen Standardvertragsklauseln.

Die bedeutsamste Neuerung: Neben der Vereinbarung der Standarddatenschutzklauseln ist der Abschluss eines Vertrages zur Auftragsverarbeitung bzw. Data Processing Agreements (DPA) nun nicht mehr erforderlich, da die Anforderungen des Art. 28 Abs. 3 DS-GVO Bestandteil der Standardvertragsklauseln sind. Das ist bei Vertragsabschlüssen dringend zu beachten! Sonst droht eine Auslegung des DPA als Änderung der Standarddatenschutzklauseln, die jedoch nur Wirkung entfalten, wenn sie unverändert abgeschlossen werden.

Wichtige Änderung: kein separater Auftragsverarbeitungsvertrag mehr erforderlich neben Standarddatenschutzklauseln

Die Beschlüsse der EU-Kommission zu den bisherigen Standardvertragsklauseln verlieren zum 27.09.2021 ihre Wirkung. Für neue Verträge zur Übermittlung personenbezogener Daten in Drittstaaten dürfen ab diesem Zeitpunkt nur noch die neuen Standardvertragsklauseln verwendet werden. Bereits bestehende Verträge auf Basis der bisherigen Standardvertragsklauseln müssen bis zum 27.12.2022 auf die neuen Standardvertragsklauseln umgestellt werden.

9 Darüber hinaus wurden am 04.06.2021 auch unverbindliche ↗ Standardvertragsklauseln für EU-interne Datentransfers zwischen Verantwortlichen und Auftragsverarbeitern gem. Art. 28 DS-GVO veröffentlicht.

4.2.1 Die besondere praktische Bedeutung der Standarddatenschutzklauseln seit »Schrems II«

Nachdem der EuGH im Oktober 2015 die bis dahin angewendete Safe-Harbor-Entscheidung der Europäischen Kommission für ungültig erklärt hatte, hatte die EU-Kommission am 12. Juli 2016 den »EU-US Datenschutzschild« (engl. »Privacy Shield«) förmlich angenommen. Mit dem Privacy Shield bestand bis Juli 2020 eine Grundlage für den kommerziellen Austausch von personenbezogenen Daten zwischen der Europäischen Union und den Vereinigten Staaten. Mit der Entscheidung des EuGH vom 16.07.2020 (»Schrems II«) ist das Privacy Shield jedoch für ungültig erklärt worden.

Übermittlungen personenbezogener Daten in die USA sind seitdem auf der Grundlage des Privacy Shield unzulässig und mussten daher auf andere Rechtsgrundlagen umgestellt oder unverzüglich eingestellt werden.

Auch wenn das Schrems II Urteil des EUGH vornehmlich auf Datenübermittlungen in die USA Bezug nimmt, so findet das Urteil auch Anwendung auf alle Drittländer, für die kein gültiger Angemessenheitsbeschluss der Europäischen Kommission vorliegt. Das bedeutet auch, dass sofern Daten in Drittländer auf der Grundlage von Standarddatenschutzklauseln übermittelt werden sollen, Unternehmen bewerten müssen, ob die Rechte der betroffenen Personen im Drittland ein gleichwertiges Schutzniveau wie in der EU genießen. Sofern das nicht der Fall ist, ist zu prüfen, ob zusätzliche Maßnahmen zur Sicherstellung eines im Wesentlichen gleichwertigen Schutzniveaus ergriffen werden können. Dabei sind rechtliche, technische oder organisatorische Maßnahmen denkbar. Die tatsächliche Wirksamkeit solcher Maßnahmen darf jedoch nicht durch die Rechtsordnung des Drittlandes beeinträchtigt werden.

Auch wenn das Urteil des EuGH unmittelbar nur auf Standarddatenschutzklauseln Bezug nimmt, gelten die Anforderungen entsprechend auch bei der Nutzung von verbindlichen internen Datenschutzvorschriften gemäß Art. 47 DS-GVO (BCR). Auch hier haben Unternehmen fortan zu prüfen, ob im Drittland ein gleichwertiges Schutzniveau vorherrscht oder ob gegebenenfalls zusätzliche Maßnahmen ergriffen werden können, um das angemessene Schutzniveau zu erreichen.

4.2.2 Praktische Tipps zur Verwendung der Standarddatenschutzklauseln

4.2.2.1 Unveränderte Nutzung

Hinweis: In anderen EU-Staaten (z. B. AT, HR, CY, EE, FR, IS, LV, LT, LU, MT, RO, SI, ES) konnte bisher unter der Datenschutzrichtlinie eine Genehmigung auch im Fall von Standardvertragsklauseln erforderlich sein. Dies ist nach der DS-GVO in allen EU-Staaten nun nicht mehr erforderlich.

Bei der Verwendung von Standarddatenschutzklauseln ist darauf zu achten, dass die vorgegebenen Klauseln von den Vertragspartnern in ihrer Substanz nicht verändert oder durch Nebenabreden anderweitig eingeschränkt werden dürfen. Ergänzungen sind nur im Rahmen sog. geschäftlicher Klauseln zulässig, soweit die betreffenden Standarddatenschutzklauseln eine solche Ergänzung zulassen und solange diese nicht direkt oder indirekt im Widerspruch zu den Standarddatenschutzklauseln stehen oder Grundrechte oder Grundfreiheiten der betroffenen Personen verletzen. Im Fall einer unzulässigen Änderung verlieren die Klauseln ihren privilegierten Status als Standarddatenschutzklauseln im Sinne des Art. 46 Abs. 2 DS-GVO und unterliegen sodann als »einfache« Vertragsklauseln der Genehmigungspflicht. Erfolgt die Übermittlung hingegen auf Basis von (unveränderten) Standarddatenschutzklauseln bedarf es nach deutschem Datenschutzrecht keiner Genehmigung durch die Aufsichtsbehörde, da die Kommission im Rahmen des Prüfverfahrens nach Art. 93 Abs. 2 DS-GVO (bzw. nach Art. 26 Abs. 4 i. V.m. Art. 31 Abs. 2 der RL 95/46 EG) ja bereits die Feststellung getroffen hat, dass die Standarddatenschutzklauseln ausreichende Garantien zum Schutz der Persönlichkeitsrechte der Betroffenen enthalten. Allerdings können Aufsichtsbehörden die Vorlage der vereinbarten Standarddatenschutzklauseln verlangen.

4.2.2.2 Einzelfallprüfung des angemessenen Datenschutzniveaus

Verantwortliche für die Datenübermittlung in Drittstaaten unter Berücksichtigung der oben beschriebenen Ausnahmen können bis zum 27.12.2022 bestehende Verträge inkl. der alten Standarddatenschutzklauseln nutzen. Dies alleine reicht nach der EuGH-Rechtsprechung allerdings nur noch selten aus. Unternehmen haben vielmehr vor jeder Übermittlung zusätzlich zu prüfen, ob im Drittland die Rechte der Betroffenen in gleicher Weise geschützt werden können, wie in der EU nach Maßgabe der DS-GVO. Dies betrifft insbesondere den Aspekt der Zugriffsmöglichkeiten von Behörden auf die exportierenden Daten.

Beispiel USA: Datenimporteure in den USA können in bestimmten Konstellationen, z. B. wenn der Datenimporteur in den Anwendungsbereich der FISA 702 fällt und die Voraussetzungen im Einzelfall gegeben sind, aufgrund von Zugriffsmöglichkeiten der amerikanischen Ermittlungsbehörden dieses Schutzniveau nicht bieten, weshalb beim Einsatz der Standarddatenschutzklauseln für die Datenübermittlung in die USA stets zu prüfen ist, ob und welche weiteren technischen und organisatorischen Maßnahmen vertraglich vereinbart sind und umgesetzt werden können, wenn die Parteien zu dem Ergebnis kommen, das die bisher eingesetzten Transfer-Tools keinen hinreichenden

Schutz bieten (auch die EDPB Guidelines sprechen insofern stets von »supplementary measures«).
Zu empfehlen ist eine mehrstufige Prüfung, die alle Aspekte der Datenübermittlung ins Auge fasst:

- Ist der **Übertragungsweg** ausreichend vor Zugriffen Dritter geschützt? Gibt es z. B. Vorschriften, die Geheimdiensten einen Zugriff auf die Leitungen oder Kommunikationsgeräte ermöglichen (wie in Deutschland mit der sogenannten »Quellen-TKÜ«) und sind die Rechtsschutzmöglichkeiten hiergegen zureichend oder unzureichend?
- Welche Risiken bei der **Speicherung** beim jeweiligen Empfänger bestehen? Ist der durch seine Branche z. B. besonderen gesetzlichen Übertragungs- oder Einsichtspflichten ausgesetzt, die bei anderen Datenempfängern im Land so nicht bestehen?
- Falls Risiken bestehen: Gibt es zumutbare Alternativen, bei denen diese Risiken nicht bestehen?

Kommen Verantwortliche bei ihrer Prüfung zu dem Ergebnis, dass bestehende Standarddatenschutzklauseln für das jeweilige Drittland nicht ausreichen und das geforderte Schutzniveau verfehlt wird, ist eine Übermittlung noch nicht ausgeschlossen. Allerdings müssen dann weitere Garantien geboten und Schutzmaßnahmen ergriffen werden. Denkbar sind etwa Verschlüsselungen sowie Anonymisierung oder Pseudo-nymisierung der personenbezogenen Daten. Hilfreich sind insoweit die Empfehlungen des Europäischen Datenschutzausschusses vom 18. Juni 2021.

Bei der Verwendung der neuen Standardvertragsklauseln ist in jedem Fall eine Analyse des Datenschutzniveaus für das Empfängerland erforderlich. Das sogenannte Transfer Impact Assessment (TIA) berücksichtigt unter anderem die relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten) sowie die geltenden Beschränkungen und Garantien.

4.3 Verbindliche interne Datenschutzvorschriften (»Binding Corporate Rules«)

4.3.1 Einleitung

Der europäische Gesetzgeber hat »verbindliche interne Datenschutzvorschriften«, so die offizielle deutschsprachige Bezeichnung für »Binding Corporate Rules«, explizit in den Kreis der »geeigneten Garantien« zur Absicherung von Datenverarbeitungen in Ländern ohne angemessenes Schutzniveau aufgenommen, Art. 46 Abs. 2 lit. b DS-GVO. »Geeignete Garantien« sollen eine Kompensation dafür schaffen, dass personenbezogene Daten in einem Land verarbeitet werden, das über kein (festgestelltes) adäquates Datenschutzniveau verfügt, ErwG. 108. Ziel ist die weitestgehende Gewährleistung, dass personenbezogene Daten auch dort gemäß den Prinzipien der DS-GVO verarbeitet werden und Betroffene ihre gesetzlich normierten Rechte durchsetzen können.

> **Beachten!**
>
> »Geeignete Garantien« bezwecken – nur – einen Ausgleich für den Transfer von personenbezogenen Daten in »unsichere Drittländer«. Deshalb müssen bei der Verarbeitung der personenbezogenen Daten stets – auch – die allgemeinen Anforderungen an eine rechtskonforme Datenverarbeitung erfüllt werden. Dies stellt ErwG. 48 in Satz 2 klar! Eine Verarbeitung personenbezogener Daten bedarf daher stets einer sie legitimierenden Grundlage im Sinne von Art. 6 Abs. 1 DS-GVO und auch bei konzerninternen Auftragsverarbeitungen ist immer ein Vertrag gemäß Art. 28 DS-GVO zu schließen (siehe hierzu auch 5.4).

Die DS-GVO hat weitestgehend die von der Art. 29-Datenschutzgruppe (Datenschutzgruppe) entwickelten inhaltlichen Anforderungen an BCR übernommen, die diese im Laufe der letzten zwanzig Jahre in mehreren Arbeitspapieren (Working Paper, kurz »WP« genannt und durchlaufend nummeriert) veröffentlicht hat. Rechtsdogmatisch betrachtet sind BCR weder ein Vertrag noch Verhaltensregeln, sondern ein Instrument der »Selbstkontrolle der Wirtschaft« (WP 12).

BCR sind dadurch gekennzeichnet, dass sie verbindlich bzw. rechtlich durchsetzbar, unternehmensintern und für internationale Datentransfers bestimmt sind (WP 74). Zentrales Element ist die einseitige Selbstverpflichtungserklärung der Unternehmungsleitung, die Grundsätze des europäischen Datenschutzrechts bei Verarbeitungen außerhalb der Europäischen Union zu beachten. Die Selbstverpflichtungserklärung ist aber auch ein gewisses Manko, weil sie als einseitige Willenserklärung nicht in allen Rechtsordnungen als rechtsverbindlich angesehen wird (WP 74). Dieses Akzeptanzproblem dürfte sich durch die ausdrückliche Aufnahme in der DS-GVO zumindest für die Mitgliedstaaten der EU erledigt haben. Während Standardvertragsklauseln einmalig Übermittlungen an individuelle Empfänger absichern, stellen BCR eine dauerhafte Absicherung für unzählige Übermittlungen an einen oder mehrere Empfänger dar. Aus diesen Besonderheiten leiten sich spezielle Anforderungen (siehe 4.5.3) ab, die interessierte Nutzer erfüllen müssen.

4.3.2 Begriffe

Verbindliche interne Datenschutzvorschriften sind gemäß der Legaldefinition in Art. 4 Nr. 20 DS-GVO »Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern«.

Damit hat sich der Gesetzgeber vom Konzept der »unternehmensinternen« Regeln verabschiedet und BCR zu »internen« Regeln für Unternehmen gemacht, die ggfs. keine gemeinsame steuernde »Unternehmensführung« haben.

4.3.3 Anforderungen

Art. 47 DS-GVO enthält eine lange Liste von Anforderungen, die BCR erfüllen müssen. Viele der Anforderungen sind vage formuliert und lassen Raum zur Interpretation. Bei der Auslegung der Anforderungen werden die Aufsichtsbehörden auf ihre in den letzten Jahren veröffentlichten Arbeitspapiere zurückgreifen, in denen teilweise sehr präzise Aussagen zur Verwirklichung einzelner Anforderungen gemacht wurden. Das WP 256 enthält Aussagen darüber, welche Anforderungen in den BCR zu erfüllen sind und wo man weitere Informationen zu den Anforderungen finden kann. Die Darstellung versucht hierzu einen Überblick zu geben.

Anforderung	In BCR zu erfüllen?	Anmerkung
Abs. 1 lit. a BCR sind für alle betreffenden Mitglieder der Unternehmensgruppe bzw. Gruppe von Unternehmen verbindlich und werden durchgesetzt, und zwar auch für ihre Beschäftigten,	Ja	WP 256 Punkt 1.1 und 1.2
Abs. 1 lit. b Betroffenenrechte haben drittbegünstigende Wirkung	Ja	WP 256 Punkt 1.3
Abs. 2 lit. a Struktur und Kontaktdaten der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und jedes ihrer Mitglieder;	Ja	WP 256 Punkt 6.2
Abs. 2 lit. b die betreffenden Datenübermittlungen oder Reihen von Datenübermittlungen einschließlich der betreffenden Arten personenbezogener Daten, Art und Zweck der Datenverarbeitung, Art der betroffenen Personen und das betreffende Drittland beziehungsweise die betreffenden Drittländer;	Ja	WP 256 Punkt 4.1
Abs. 2 lit. c interne und externe Rechtsverbindlichkeit der betreffenden internen Datenschutzvorschriften;	Ja	WP 256 Punkt 1.1 und 1.2
Abs. 2 lit. d die Anwendung der allgemeinen Datenschutzgrundsätze, insbesondere Zweckbindung, Datenminimierung, begrenzte Speicherfristen, Datenqualität, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Rechtsgrundlage für die Verarbeitung, Verarbeitung besonderer Kategorien von personenbezogenen Daten, Maßnahmen zur Sicherstellung der Datensicherheit und Anforderungen für die Weiterübermittlung an nicht an diese internen Datenschutzvorschriften gebundenen Stellen;	Ja	WP 256 Punkt 6.1
Abs. 2 lit. e die Rechte der betroffenen Personen in Bezug auf die Verarbeitung und die diesen offenstehenden Mittel zur Wahrnehmung dieser Rechte einschließlich des Rechts, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung nach Art. 22 unterworfen zu werden sowie des in Art. 79 niedergelegten Rechts auf Beschwerde bei der zuständigen Aufsichtsbehörde bzw. auf Einlegung eines Rechtsbehelfs bei den zuständigen Gerichten der Mitgliedstaaten und im Falle einer Verletzung der verbindlichen internen Datenschutzvorschriften Wiedergutmachung und gegebenenfalls Schadenersatz zu erhalten;	Ja	WP 256 Punkt 1.3
Abs. 2 lit. f die von dem in einem Mitgliedstaat niedergelassenen Verantwortlichen oder Auftragsverarbeiter übernommene Haftung für etwaige Verstöße eines nicht in der Union niedergelassenen betreffenden Mitglieds der Unternehmensgruppe gegen die verbindlichen internen Datenschutzvorschriften; der Verantwortliche oder der Auftragsverarbeiter ist nur dann teilweise oder vollständig von dieser Haftung befreit, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, dem betreffenden Mitglied nicht zur Last gelegt werden kann;	Ja	WP 256 Punkt 1.6
Abs. 2 lit. g die Art und Weise, wie die betroffenen Personen über die Bestimmungen der Art. 13 und 14 hinaus über die verbindlichen internen Datenschutzvorschriften und insbesondere über die unter den Buchstaben d), e) und f) genannten Aspekte informiert werden;	Ja	WP 256 Punkt 1.7 Die Mitgliedstaaten können bei der Nutzung von BCR für Beschäftigtendaten besonde re Transparenzanforderungen aufstellen, Art 88 Abs.2 DS-GVO.

Anforderung	In BCR zu erfüllen?	Anmerkung
Abs. 2 lit. h die Aufgaben jedes gemäß Art. 37 benannten Datenschutzbeauftragten oder jeder anderen Person oder Einrichtung, die mit der Überwachung der Einhaltung der verbindlichen internen Datenschutzvorschriften in der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben sowie mit der Überwachung der Schulungsmaßnahmen und dem Umgang mit Beschwerden befasst ist;	Ja	WP 153 Punkt 2.4
Abs. 2 lit. i die Beschwerdeverfahren;	Ja	WP 153 Punkt 2.2
Abs. 2 lit. j die innerhalb der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, bestehenden Verfahren zur Überprüfung der Einhaltung der verbindlichen internen Datenschutzvorschriften. Derartige Verfahren beinhalten Datenschutzüberprüfungen und Verfahren zur Gewährleistung von Abhilfemaßnahmen zum Schutz der Rechte der betroffenen Person. Die Ergebnisse derartiger Überprüfungen sollten der in Buchstabe h) genannten Person oder Einrichtung sowie dem Verwaltungsrat des herrschenden Unternehmens einer Unternehmensgruppe oder der Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, mitgeteilt werden und sollten der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden;	Ja	WP 153 Punkt 2.3
Abs. 2 lit. k die Verfahren für die Meldung und Erfassung von Änderungen der Vorschriften und ihre Meldung an die Aufsichtsbehörde;	Ja	WP 153 Punkt 5.1
Abs. 2 lit. l die Verfahren für die Zusammenarbeit mit der Aufsichtsbehörde, die die Befolgung der Vorschriften durch sämtliche Mitglieder der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, gewährleisten, insbesondere durch Offenlegung der Ergebnisse von Überprüfungen der unter Buchstabe j) genannten Maßnahmen gegenüber der Aufsichtsbehörde;	Ja	WP 153 Punkt 3.1
Abs. 2 lit. m die Meldeverfahren zur Unterrichtung der zuständigen Aufsichtsbehörde über jegliche für ein Mitglied der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem Drittland geltenden rechtlichen Bestimmungen, die sich nachteilig auf die Garantien auswirken könnten, die die verbindlichen internen Datenschutzvorschriften bieten;	Ja	WP 256 Punkt 6.3
Abs. 2 lit. n geeignete Datenschutzschulungen für Personal mit ständigem oder regelmäßigem Zugang zu personenbezogenen Daten.	Ja	WP 256 Punkt 2.1

Tabelle 2: Anforderungen

Überlegung!

Diese von der Datenschutzgruppe über viele Jahre entwickelten und aufgestellten Anforderungen beruhen auf der Prämisse, dass sie für einen Unternehmensverbund mit einer zentralen und steuernden Stelle gelten. Durch die Erweiterung der Nutzergruppe und die teilweise fehlende Akzeptanz von BCR in einigen Rechtsordnungen, kann es eine Überlegung für Interessierte sein, ihre BCR als multilateralen Vertrag auszugestalten.

Tipp!

Die Arbeitspapiere der Datenschutzgruppe sind auch nach dem 25. Mai 2018 gültig und enthalten viele interessante Erläuterungen. Besonders hinzuweisen ist auf die WP 74 und WP 108 sowie auf das WP 155, das eine FAQ-Liste zu BCRs enthält. Diese wird bei Bedarf aktualisiert; letztmalig im Februar 2017(rev.05).

4.3.4 Genehmigungsverfahren

BCR sind von der zuständigen Aufsichtsbehörde nach dem Kohärenzverfahren zu genehmigen, Art. 57 Abs. 1 lit. s, Art. 47 Abs. 1 i. V.m. Art. 64 Abs. 1 lit. f DS-GVO. Hierdurch soll gewährleistet werden, dass die europäischen Aufsichtsbehörden aufgrund eines gemeinsamen Verständnisses eine von allen getragene Entscheidung herbeiführen und so einen Beitrag zur einheitlichen Anwendung der DS-GVO leisten.

Das DSAnpUG-EU hat in § 19 Abs. 1 BDSG (2018) festgelegt, dass die Behörde die federführende Behörde ist, in deren Land der Verantwortliche oder der Auftragsverarbeiter seine Hauptniederlassung hat. In Anlehnung an die europarechtlichen Vorgaben ist in § 18 BDSG (2018) das Verfahren der Zusammenarbeit der Behörden des Bundes und der Länder dezidiert geregelt worden.

Der Gesetzgeber hat der bisherigen Praxis ein Ende bereitet, nach der einzelne oder – im Falle des Verfahrens der gegenseitigen Anerkennung – drei nationale Aufsichtsbehörden aufgrund ihres individuellen Verständnisses eine Entscheidung über die Rechtmäßigkeit der vorgelegten BCR getroffen haben. Die Erfahrung mit den oftmals sehr langen Genehmigungsverfahren hat dazu geführt, dass es nunmehr gesetzliche Fristen gibt, die das Verfahren beschleunigen wer- den. Positiv ist in diesem Zusammenhang auch zu werten, dass das Schweigen einer in das Genehmigungsverfahren eingebundenen Aufsichtsbehörde als Zustimmung gewertet wird, Art. 64 Abs. 3 DS-GVO.

Werden von den Aufsichtsbehörden genehmigte BCR als Absicherung für Drittlandtransfers genutzt, bedarf es keiner weiteren »besonderen Genehmigung einer Aufsichtsbehörde«, Art. 46 Abs. 2 1. Halbsatz DS-GVO. Damit hat der europäische Gesetzgeber einer von einigen Aufsichtsbehörden gepflegten Praxis jede Grundlage entzogen und so einen aktiven Beitrag zur harmonisierten Datenschutzpraxis geleistet.

4.3.5 »Alt-BCR«

Art. 46 Abs. 5 DS-GVO stellt klar, dass die von Aufsichtsbehörden auf der Grundlage von Art. 26 Abs. 2 RL 95/46 EG erteilten Genehmigungen so lange gültig bleiben, bis sie aufgehoben werden. Somit sind genehmigte (Alt-) BCR grundsätzlich auch nach dem 25. Mai 2018 gültig und können zur Absicherung von internationalen Datentransfers genutzt werden.

(Alt-)BCR spiegeln allerdings die datenschutzrechtliche Situation unter Geltung der RL 95/46 EG bzw. der darauf erlassenen nationalen Datenschutzgesetze wider. Durch Art. 47 DS-GVO wurden einige neue Bestandteile von BCR festgelegt, die bei einer Aktualisierung bestehender BCR zu berücksichtigen sind. Die Anforderungen an BCR unter der DS-GVO sind in WP 256 zusammengestellt. Werden der zuständigen Aufsichtsbehörde

die geänderten BCR vorgelegt, stellt dies eine Änderungsmeldung gemäß Art. 47 Abs. 2 lit. k DS-GVO und nicht einen Antrag auf Genehmigung von (neuen) BCR dar.

Die Wertungen des EuGH-Urteils »Schrems II« finden auch auf andere Garantien nach Artikel 46 DS-GVO, wie die Vereinbarung von BCR, Anwendung. Werden auf Grundlage von BCR personenbezogene Daten in die USA und andere Drittstaaten übermittelt, deren Datenschutzniveau nicht vergleichbar mit dem der EU ist, müssen auch für Datenübermittlungen auf der Grundlage von BCR ergänzende Garantien vereinbart werden. Sofern die Rechte der betroffenen Personen im Drittland kein gleichwertiges Schutzniveau genießen, sind Unternehmen somit verpflichtet, Schutzmaßnahmen, wie etwas Anonymisierung oder Pseudonymisierung von Daten, zu ergreifen.

Die vom EDSA genehmigten BCR sind unter diesem ↗ Link aufgeführt.

4.4 Individuelle Vertragsklauseln, Art. 46 Abs. 3 lit. a DS-GVO

Der Datenexporteur, der sowohl Verantwortlicher oder Auftragsverarbeiter sein kann, kann mit dem im Drittland ansässigen Verantwortlichen, Auftragsverarbeiter oder Empfänger einen individuellen, d. h. selbst formulierten Vertrag zum Datenschutz schließen, welcher von der zuständigen Aufsichtsbehörde – bei Post- und Telekommunikationsunternehmen durch den/die Bundesbeauftragte(n) für den Datenschutz und die Informationsfreiheit (BfDI) – genehmigt werden muss. Diese Möglichkeit der Umsetzung angemessener Garantien kannte bereits die RL 95/46 EG in Art. 26 Abs. 2.

4.5 Genehmigte Verhaltensregeln («Codes of Conduct«) oder Zertifizierung

Mit der Datenschutz-Grundverordnung wurden zwei neue Typen von geeigneten Garantien eingeführt.

4.5.1 Generelles

Betrachtet man Verhaltensregeln oder auch Zertifizierungen in der Gesamtschau bestehender Rechtfertigungsmöglichkeiten, so sollten sich die inhaltlichen Anforderungen an den bestehenden Schutzniveaus orientieren. Je nach Umsetzung ist es zwar denkbar, dass die neuen Rechtfertigungsgründe einen effektiveren Schutz bieten. Dies wird indessen der zu erwartenden, höheren Operationalisier- und Durchsetzbarkeit geschuldet sein. Im Übrigen ist zu beachten, wie hoch die Anforderungen an eine Anerkennung nach Art. 40 sowie Art. 42 DS-GVO sind.

4.5.2 Genehmigte Verhaltensregeln

Art. 46 Abs. 2 lit. e DS-GVO nennt genehmigte Verhaltensregeln nach Art. 40 DS-GVO als geeignete Garantien, wenn sie zusammen gehen mit rechtlich durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland, diese Garantien auch anzuwenden – inklusive der Betroffenenrechte. Wie die Durchsetzbarkeit der geeigneten Garantien sicherzustellen ist, lässt die DS-GVO offen. Art. 40 Abs. 3 DS-GVO spricht nur allgemein von vertraglichen oder sonstigen rechtlich bindenden Instrumenten. Es bedarf also neben den durch die Aufsichtsbehörden genehmigten Verhaltensregeln eines Aktes des Unternehmens, der eine Durchsetzung der Garantien im Drittland für Betroffene ermöglicht. Dieser Akt kann – je nach inhaltlicher Ausgestaltung der Verhaltensregel – auch bereits die Unterzeichnung der Verhaltensregel durch ein Unternehmen sein. Die Einhaltung muss für die Betroffenen rechtlich durchsetzbar sein – dazu muss es wirksame Rechtsbehelfe geben (wie gerichtliche Rechtsbehelfe sowie das Recht auf Geltendmachung von Schadenersatzansprüchen).

4.5.2.1 Hintergrund

Verhaltensregeln sind nur anerkennungsfähig, wenn diese aus Sicht der Aufsichtsbehörden zur ordnungsgemäßen Anwendung der DS-GVO beitragen, z. B. durch eine Präzisierung der Anwendung der DS-GVO. Handelt es sich um Verhaltensregeln, die in mehr als einem Mitgliedsstaat Anwendung finden sollen, ist zwingend ein positives Votum des Europäischen Datenschutzausschusses vor Anerkennung der zuständigen (nationalen) Aufsichtsbehörde einzuholen. Ergänzend müssen Verhaltensregeln vorsehen, dass eine unabhängige und ebenfalls durch die zuständige Aufsichtsbehörde anerkannte Aufsichtsstelle (»Monitoring Body«) die Einhaltung der Verhaltensregeln durch jene überwacht, die sich den Verhaltensregeln unterworfen haben und sich letztlich auf die Rechtswirkungen der Verhaltensregeln berufen möchten.

Hierdurch ergibt sich bereits, dass Verhaltensregeln kein Selbstzweck sind. Verhaltensregeln im Sinne der DS-GVO sind als glaubwürdige und seriöse Ergänzung zur staatlichen Aufsicht zu verstehen. So hat die unabhängige Aufsichtsstelle zwingend ein Beschwerdeverfahren vorzusehen. Die unabhängige Aufsichtsstelle ist zudem mit hinreichenden Sanktionsmöglichkeiten auszustatten und ist gegenüber der Datenschutzaufsicht selbst berichtspflichtig. Hierdurch besteht nicht nur die Möglichkeit durch die staatliche Aufsicht korrigierend einzugreifen. Vielmehr wird hierdurch auch eine hohe Qualität dieses ergänzenden Instruments sichergestellt; schließlich sehen sich auch die unabhängigen Aufsichtsstellen im Falle unzureichender Pflichterfüllung erheblichen Bußgeldern ausgesetzt.

4.5.2.2 Konkrete Auswirkungen

Es stellt sich daher die Frage, inwieweit die Anforderungen an Verhaltensregeln bezüglich der Umsetzungsakte im jeweiligen Drittland über das hinausgehen müssen, was zum Beispiel durch Standarddatenschutzklauseln oder Binding Corporate Rules gewährleistet wird. Weder Standarddatenschutzklauseln noch BCR werden etwaige Widersprüche zum nationalen Recht des Drittlandes auflösen können noch ggf. bestehende (gesetzliche) Rechtsbehelfe schaffen können. Binding Corporate Rules und Standarddatenschutzklauseln sind dabei zwar von den Aufsichtsbehörden abgesegnete Instrumente, sie bleiben aber eben auch Vereinbarungen.

Weitergehende, dem jeweiligen Rechtfertigungstatbestand inhärente und unabhängige Überprüfungsmechanismen sind für Standarddatenschutzklauseln oder BCR nicht vorgesehen; für diese Rechtfertigungsgründe obliegt es ausschließlich der staatlichen Aufsicht, die Einhaltung dieser Vorgaben zu kontrollieren.

4.5.2.3 Verhältnis zu anderen Rechtfertigungsgründen

Der Europäische Datenschutz-Ausschuss hat in seinen Leitlinien 04/2021 (Entwurf)[10] die Anforderungen an Verhaltensregeln als Rechtfertigungsgrund weiter ausgestaltet. Der Leitlinie ist zu entnehmen, dass der EDSA sich noch nicht auf ein einengendes Bild der Verhaltensregeln festlegen wollte. Im Umkehrschluss ergibt sich, dass der EDSA eine spezifische Ausgestaltung der Verhaltensregeln erwartet, die nicht nur eine Kopie bestehender BCR oder Standarddatenschutzklauseln ergänzt um eine Aufsichtsstelle sind.

Während BCR geeignet sind, gleichgelagerte Transfers innerhalb einer Unternehmensgruppe zu rechtfertigen, erlauben Verhaltensregeln dies auch über die Grenzen einer Unternehmensgruppe hinweg. Ein Umstand, aus dem auch der EDSA ein besonderes Interesse an Verhaltensregeln ableitet. Versteht man BCR nun zumindest teilweise doch als eine besondere Form der Verhaltensregeln, so ergeben sich relativ klare Potenziale der Rechtfertigung des Drittstaatentransfers durch Verhaltensregeln. Aufsetzend auf den Anforderungen der BCR sowie Standarddatenschutzklauseln werden an den Inhalt der Verhaltensregeln keine besonderen Anforderungen gestellt werden können. Vielmehr könnte argumentiert werden, dass sogar geringere Anforderungen ausreichen müssten, da dieses »Minus« durch die weiteren Sicherungsmechanismen der Verhaltensregeln – nämlich zwingende Überwachung durch eine Aufsichtsstelle – kompensiert würde.

Auch in Bezug auf die Standarddatenschutzklauseln schärfen die Leitlinien des EDSA die Vorstellung. Standarddatenschutzklauseln zwingen beide Parteien – nämlich Datenexporteur und Datenimporteur – in eine den Datentransfer ausgestaltende Vertragsbeziehung. Der EDSA betrachtet es jedoch als möglich, dass lediglich Datenimporteure sich einer Verhaltensregel unterwerfen.

Der EDSA betrachtet die Verhaltensregeln als reines Sicherungsinstrument für etwaige Transfers, insbesondere in der Operationalisierung geeigneter Garantien. Weitere Pflichten der DS-GVO stellt der EDSA als wichtig und zwingend fest, erlaubt deren Absicherung aber über parallele Mechanismen. Soweit Verhaltensregeln eine weitere, selbstständige Säule der Rechtsfertigungsgründe darstellen sollen, sollte dies bei der Entwicklung berücksichtigt werden.

10 ↗ EDPB Guidelines (Draft) 04/2021

4.5.2.4 Vorteile und Chancen

Verhaltensregeln bieten Verantwortlichen wie Auftragsverarbeitern in Branchen, in denen ein Datentransfer auch außerhalb der eigenen Unternehmensgruppe erforderlich ist, eine sinnvolle Datentransfer-Möglichkeit.

Verhaltensregeln können zudem als Maßstab realistischer (Mindest-)Standards in jeweiligen Branchen dienen und somit die europaweite Auslegung der DS-GVO frühzeitig und sachdienlich beeinflussen. Es ist daher nicht auszuschließen, dass staatliche Aufsichtsstellen das in Verhaltensregeln niedergelegte (Mindest-)Niveau bei allen Prüfungen als Referenz heranziehen.

4.5.2.5 Bisherige Erfahrungen und Initiativen

Die Anerkennung erster, insbesondere transnationaler Verhaltensregeln, erfolgte erst im Jahr 2021.[11] Dem durch den EDSA geführten Register anerkannter Verhaltensregeln können auch nationale Initiativen entnommen werden. Jedoch steht die Anerkennung teils noch unter der Bedingung, eine unabhängige und akkreditierte Aufsichtsstelle zu benennen.[12] Weitere Initiativen streben eine Anerkennung ihrer Verhaltensregel an.[13] Keiner der bisher anerkannten Verhaltensregeln qualifiziert sich als Rechtfertigungsgrund für den Transfer personenbezogener Daten. Nicht zuletzt, da zum Zeitpunkt ihrer Entwicklung die Veröffentlichung der Leitlinien zur Erstellung dieser speziellen Form von Verhaltensregeln[14] ausstand. Es bestehen bei mindestens einer anerkannten Verhaltensregel derzeit Bestrebungen, die Verhaltensregel den Leitlinien entsprechend weiterzuentwickeln.[15]

11 Positive Opinions des EDSA vom 19. Mai 2021: ↗ Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the »EU Data Protection Code of Conduct for Cloud Service Providers« submitted by Scope Europe | European Data Protection Board, abrufbar unter ↗ https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-162021-draft-decision-belgian-supervisory_en, sowie ↗ Opinion 17/2021 on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE) | European Data Protection Board, abrufbar unter ↗ https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-172021-draft-decision-french-supervisory_en.

12 ↗ https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en

13 So etwa Bitkom und GDD im Bereich der Pseudonymisierung - ↗ 20200825_mitteilung-und-status-quo-coc_pseudonymisierung.pdf (bitkom.org)

14 ↗ EDPB Guidelines (Draft) 04/2021

15 ↗ https://eucoc.cloud/3rdcountryinitiative

4.5.3 Zertifizierung

Nach Art. 46 Abs. 2 lit. f DS-GVO und Art. 42 Abs. 2 DS-GVO kann auch ein genehmigter Zertifizierungsmechanismus als geeignete Garantie dienen, wenn er zusammen geht mit rechtlich durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland, diese Garantien auch anzuwenden und die Betroffenenrechte einzuhalten. Es gelten bis auf Weiteres die gleichen Rahmenbedingungen wie für genehmigte Verhaltensregeln.

Sobald und soweit der EDSA einen Entwurf für Drittstaatentransfer rechtfertigende Zertifizierungen veröffentlicht, wären die dort genannten Ausführungen zu berücksichtigen.

Hinweis: Die Voraussetzungen für eine rechtmäßige Übermittlung im Inland gemäß Art. 6 sind auch bei einer Datenübermittlung in ein Drittland relevant, denn bei jeder Datenübermittlung ins Ausland muss neben der Frage nach den speziellen Voraussetzungen für die Übermittlung in ein bestimmtes Land zusätzlich geprüft werden, ob darüber hinaus auch die allgemeinen Voraussetzungen für eine Übermittlung vorliegen Erforderlich ist also eine ZWEI- STUFIGE PRÜFUNG.

4.5.3.1 Gesetzliche Ausnahmetatbestände (Artikel 49 DS-GVO)

Auch in Fällen, in denen für das betreffende Drittland kein angemessenes Datenschutzniveau festgestellt wurde und keine geeigneten Garantien (Art. 46) vorliegen, kann eine Datenübermittlung möglich sein (Art. 49). Die wichtigsten Anwendungsfälle des Art. 49, u. a. Übermittlung zur Vertragserfüllung und Einwilligung der Betroffenen, werden in diesem Abschnitt erläutert.

Die Diskussion über den Umfang des Anwendungsbereichs von Art. 49 DS-GVO scheint noch nicht abgeschlossen. Es ist daher über die nachfolgend beschriebenen Szenarien hinaus zu empfehlen, die Entwicklung des Anwendungsumfangs des Art. 49 DS-GVO weiter zu verfolgen.

4.5.3.2 Zur Vertragserfüllung notwendige Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau

Eine Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau ist ausnahmsweise zulässig, wenn zwischen dem Betroffenen und dem Verantwortlichen ein Vertrag abgeschlossen worden ist, für dessen Erfüllung die Datenübermittlung erforderlich ist.

Art. 49 Abs. 1 S. 1 lit. b. Das gilt auch dann, wenn die Übermittlung zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist.

Der praktische Anwendungsbereich dieser Zulässigkeitsalternative liegt neben dem internationalen Zahlungsverkehr und Kaufverträgen im Fernabsatz vor allem im Tourismusgewerbe. Die Durchführung von vertraglichen Vereinbarungen über internationale Beförderungsleistungen, Reservierungen von Mietwagen, Unterkünften oder Hotelzimmern in Drittländern wird so ermöglicht.

> **Beispiel:** Kunde (K) möchte, dass sein Reisebüro für ihn in Peking ein Hotelzimmer reserviert. Das Reisebüro kann sich für die Übermittlung der Daten des (K) an das Hotel in Peking auf Art. 49 Abs. 1 S. 1 lit b) berufen, da zur Durchführung bzw. Erfüllung des Vertrages zwischen Kunde (K) und dem Reisebüro die Weitergabe seiner Daten zwingend notwendig ist.

Ein Vertrag i.S.d. lit. b kann auch ein Arbeitsvertrag sein, so dass die Übermittlung von Arbeitnehmerdaten in ein Drittland auf Grund eines Arbeitsvertrages zulässig sein kann. Entscheidend für die Beurteilung der Zulässigkeit ist, ob die Übermittlung für die Durchführung bzw. Erfüllung der jeweiligen einzelnen Regelung des Arbeitsvertrags erforderlich ist. Dies ist für jeden Arbeitnehmer gesondert zu prüfen. Denkbar ist die Zulässigkeit der Datenübermittlung z. B., wenn der Mitarbeiter zu Auslandseinsätzen verpflichtet ist oder bei der Gewährung von Aktienbezugsrechten, die in einem Drittland verwaltet werden.

Etwas anders ist es bei der Konstellation, für die Art. 49 Abs. 1 S. 1 lit. c die Zulässigkeit einer Datenübermittlung begründen kann. Nach lit. c kann eine Übermittlung zulässig sein, die zur Erfüllung eines Vertrags notwendig ist, der zwar nicht vom Betroffenen selbst mit dem Verantwortlichen geschlossen wurde, aber im Interesse des Betroffenen zwischen dem Verantwortlichen und einem Dritten.

> **Beispiel:** Der Arbeitgeber übermittelt Daten eines Arbeitnehmers oder einer Arbeitnehmerin, für den oder die eine Mitarbeiterversicherung abgeschlossen hat, an eine ausländische Versicherungsgesellschaft. Häufig wird es sich bei der Anwendung von lit. c) um Verträge zugunsten Dritter i.S.d. § 328 BGB handeln.

4.5.4 Datenübermittlung auf der Grundlage einer Einwilligung

Wie bei der Datenübermittlung innerhalb Deutschlands oder innerhalb der EU/EWR kann auch eine Datenübermittlung in ein Drittland auf der Grundlage einer Einwilligung des Betroffenen zulässig sein, Art. 49 Abs. 1 S. 1 lit. a.

Für die Einwilligung in die Drittlandübermittlung von Daten gelten jedoch recht strenge Anforderungen.

Beim Datentransfer in ein Drittland kommt noch eine weitere Schwierigkeit hinzu. Denn nach Art. 49 Abs. 1 S. 1 lit. a ist der Betroffene (zusätzlich zu den oben aufgeführten Umständen der Datenübermittlung) umfassend über die Risiken der Übermittlung seiner Daten in ein Land ohne ausreichendes Datenschutzniveau zu informieren. Erforderlich ist also die Transparenz bezüglich der Schutzmaßnahmen bzw. Datenschutzgarantien bei der empfangenden Stelle oder im Empfängerland.

4.5.5 Datenübermittlung auf Grund zwingender berechtigter Interessen

Für eng umgrenzte Ausnahmefälle gestattet Art. 49 Abs. 1 S. 2 eine Übermittlung in einen Drittstaat ohne angemessenes Datenschutzniveau. Danach ist die Übermittlung zulässig, wenn sie nicht wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, die Interessen oder die Rechte und Freiheiten der betroffenen Personen nicht überwiegen und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat. Zusätzlich hat der Verantwortliche die Aufsichtsbehörde sowie die betroffenen Personen zu informieren. Die Beurteilung sowie die angemessenen Garantien sind in das Verarbeitungsverzeichnis nach Art. 30 aufzunehmen.

Der Anwendungsbereich dieser Ausnahmevorschrift ist sehr eng. In ErwG. 113 werden als Beispiele wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke genannt. Sofern eine Übermittlung auf diesen Ausnahmetatbestand gestützt werden soll, ist es dem Verantwortlichen anzuraten, schon vorab Kontakt zur zuständigen Aufsichtsbehörde aufzunehmen.

4.5.6 Datenübermittlung in ein Drittland auf Anweisung eines Gerichts oder einer Behörde

Anders als die RL 95/46 EG enthält die DS-GVO eine ausdrückliche Regelung der Fälle, in denen ein Gericht oder eine Behörde eines Drittlandes die Übermittlung personenbezogener Daten verlangt.

Art. 48 bestimmt, dass diese Urteile oder Verwaltungsentscheidungen in der EU nur dann anerkannt und befolgt werden dürfen, wenn sie auf ein Rechtshilfeabkommen oder eine andere internationale Übereinkunft zwischen dem Drittland und der EU oder dem Mitgliedsstaat gestützt sind. Das können bspw. das »Haager Übereinkommen über die Beweisaufnahme im Ausland in Zivil- oder Handelssachen« sein oder auch internationale Übereinkünfte im Bereich der Zusammenarbeit bei der Verbrechensbekämpfung und der Strafverfolgung.

Sofern das Gerichtsurteil oder die Verwaltungsentscheidung nicht auf ein Rechtshilfeabkommen oder eine sonstige internationale Übereinkunft gestützt werden kann, können sie die Datenübermittlung nicht rechtfertigen. Dann gelten die allgemeinen Grundsätze: Nur wenn eine gesetzliche Erlaubnis für eine Übermittlung vorliegt und im Empfängerland ein angemessenes Schutzniveau besteht oder eine Ausnahme nach Art. 49 gegeben ist, ist eine Übermittlung zulässig.

5 Begriffsbestimmungen, Materialien, Grafiken und Übersichten

5.1 Begriffsbestimmungen

Im Folgenden werden einige zentrale Begriffe des Datenschutzes kurz erläutert:

- **Auftragsverarbeitung/Auftragsverarbeiter**
  Eine Datenverarbeitung im Auftrag ist eine Datenverarbeitung personenbezogener Daten durch den Auftragsverarbeiter (Auftragnehmer) nach Weisung und im Auftrag des Verantwortlichen (Auftraggeber). Auftragsverarbeiter ist eine natürliche oder juristische Person, die Daten im Auftrag des Verantwortlichen verarbeitet, vgl. Art. 4 Nr. 8 DS-GVO.

- **Personenbezogene Daten**
  Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (die auch als die »betroffene Person« bezeichnet wird); juristische Personen des privaten Rechts (z. B. AG, GmbH) werden damit nicht erfasst. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung (z. B. Name), zu einer Kennnummer (z. B. Sozialversicherungsnummer, Steueridentifikationsnummer), zu Standortdaten, zu einer Online-Kennung (z. B. IP-Adresse oder Cookie-Kennung) oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann, vgl. Art. 4 Nr. 1 DS-GVO.

- Besondere Arten personenbezogener Daten
  Von den allgemeinen personenbezogenen Daten sind die besonderen Kategorien von Daten zu unterscheiden. Dies sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit sowie die Verarbeitung von genetischen Daten, biometrischen Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person, vgl. Art. 9 DS-GVO.

- **Betroffene Person / Betroffener**
  Jede natürliche Person, um deren personenbezogene Daten es geht und die davor zu schützen ist, dass sie durch die Verarbeitung in ihrem Recht auf Schutz personenbezogener Daten beeinträchtigt wird, vgl. Klammerzusatz in Definition von Art. 4 Nr. 1 DS-GVO.

- **Datenexporteur**
  Datenexporteur ist der für die Verarbeitung Verantwortliche, der personenbezogene Daten übermittelt.

- **Datenimporteur**
  Datenimporteur ist der für die Verarbeitung Verantwortliche, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten für die Verarbeitung entgegenzunehmen.

- **Dritter**
  Der Ausdruck »Dritter« bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten (Art. 4 Nr. 10 DS-GVO). Nicht unter den Begriff »Dritter« fallen rechtlich unselbstständige Zweigstellen eines Unternehmens (wie z. B. Filialen). Rechtlich selbstständige Einrichtungen – wie Betriebskrankenkassen – sind jedoch auch dann Dritte, wenn sie organisatorisch, räumlich oder personell mit der speichernden Stelle verbunden sind.

- **Drittland**
  Als Drittländer werden alle anderen Staaten außerhalb der EU/EWR bezeichnet (zu EWR siehe 2.1).

- **Einwilligung**
  Jede von der betroffenen Person freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung, in Form einer Erklärung oder einer sonsti-gen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, ist eine »Einwilligung«, vgl. Art. 4 Nr. 11 DS-GVO.

- **Empfänger**
  Empfänger ist jede Stelle, die Daten erhält. Als Stelle sind sowohl natürliche oder juristische Personen, Behörden oder andere Einrichtungen zu verstehen.

- **Unternehmen**
  Eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig wirtschaftlichen Tätigkeiten nachgehen, vgl. Art. 4 Nr. 18 DS-GVO. Damit ist der datenschutzrechtliche Unternehmensbegriff sehr weit und umfasst jedes Unternehmen unabhängig von Größe und Branche, so dass z. B. auch Freiberufler erfasst sind.

- **Unternehmensgruppe**
  Eine Gruppe, die aus einem herrschenden Unternehmen und den von diesen abhängigen Unternehmen besteht; vgl. Art. 4 Nr. 19 DS-GVO sowie Art. 37, 47 und 88 DS-GVO, wo die Definition eine Rolle spielt. Die Definition ist auf einen Unternehmensverbund beschränkt, wo ein Unternehmen einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann, z. B. aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen (ErwG. 37). Davon abzugrenzen sind andere Begriffsbestimmungen wie z. B. eine Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, die aufgrund der Selbständigkeit nicht vom Begriff erfasst sind.

- **Verarbeitung personenbezogener Daten**
  Verarbeitung ist jeder Vorgang, mit oder ohne Hilfe automatisierter Verfahren, im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung, vgl. Art. 4 Nr. 2 DS-GVO.

- **Verbindliche interne Datenschutzvorschriften (engl. Binding Corporate Rules, BCR)**
  Verbindliche interne Datenschutzvorschriften (engl. Binding Corporate Rules; BCR) sind Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats der Union niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern, vgl. Art. 4 Nr. 20 DS-GVO.

- **Verantwortlicher**
  Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, vgl. Art. 4 Nr. 7 DS-GVO.

- **Vertreter**
  Eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt, vgl. Art. 4 Nr. 17.
  Diese Definition ist nur für nicht in der Union niedergelassene Verantwortliche oder Auftragsverarbeiter relevant.

5.2 Übersicht über die rechtlichen Möglichkeiten der Übermittlung personenbezogener Daten in Drittländer

	»Art«	Geltungsbereich	Abschluss	Pb Daten	Aufsichtsbehörde	Bemerkungen
Einwilligung (Art. 49 Abs. 1 lit. a)	Einseitige, empfangsbedürftige Einwilligungserklärung	Individuell; zwischen betroffener Person und Verantwortlichen	Durch Abgabe der entsprechenden Willenserklärung seitens des Einwilligenden	Grundsätzlich die autorisierten pb Daten des Betroffenen; Umfang im Rahmen der gesetzlichen Möglichkeiten, der guten Sitten u. des vorgesehenen Zwecks	Keine Mitwirkung erforderlich	Die betroffene Person muss über die für sie möglicherweise bestehenden Risiken unterrichtet worden sein und sie muss ihre Einwilligung ausdrücklich abgegeben haben
Datenübermittlung ist zur Erfüllung des Vertrages o. zur Durchführung vorvertraglicher Maßnahmen erforderlich (Art. 49 Abs. 1 lit. b)	Vertrag o. vertragsähnliche Beziehung zwischen Verantwortlichen und betroffener Person	Individuell; zwischen betroffener Person und Verantwortlichen	Durch Abgabe der entsprechenden Willenserklärungen von der oder dem Verantwortlichen und der betroffenen Person	Grundsätzlich die pb Daten des Betroffenen, die für die Durchführung des Vertrages erforderlich sind	Keine Mitwirkung erforderlich	Vertragsbeispiele: Hotelreservierung im Ausland; Arbeitsvertrag mit ausländischem Arbeitgeber; Warenbestellung (auch online) im Ausland
Datenübermittlung ist zum Abschluss o. zur Erfüllung eines im Interesse der betroffenen Person geschlossenen Vertrags erforderlich (Art. 49 Abs. 1 lit. c)	Vertrag zwischen Verantwortlichen und einem Dritten	Individuell; zwischen Verantwortlichen und einem Dritten	Durch Abgabe der entsprechenden Willenserklärungen von dem oder der Verantwortlichen und Dritten	Grundsätzlich die pb Daten des Betroffenen, die für die Durchführung des Vertrages erforderlich sind	Keine Mitwirkung erforderlich	Vertragsbeispiele: Übermittlung Daten Arbeitnehmer für Mitarbeiterversicherung an ausländische Versicherungsgesellschaft
Andere Ausnahmen (Art. 49 Abs.1 lit d –f)	Anderer Ausnahmetatbestand	Begrenzt auf den Sachverhalt der Ausnahmeregelung	Prüfung erforderlich, ob die Voraussetzungen des Ausnahmetatbestands vorliegen	Mitarbeiter-, Kunden-, Nichtkunden, Interessenten und Lieferantendaten, soweit für die Übermittlung im Rahmen der Ausnahmeregelung erforderlich	Keine Mitwirkung erforderlich	z. B. Wahrung eines wichtigen öffentlichen Interesses; Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht; Wahrung lebenswichtiger Interessen

	»Art«	Geltungsbereich	Abschluss	Pb Daten	Aufsichtsbehörde	Bemerkungen
Drittländer mit durch die EU Kommission festgestelltem angemessenen Datenschutzniveau (Art. 45)	Entscheidung gemäß Art. 45 (EU-Kommissionsentscheidung)	Gilt für alle Empfänger im entscheidungsgegenständlichen Drittland	n. a.	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten- und Lieferantendaten	Keine Mitwirkung erforderlich	Die aktuellsten Kommissionsentscheidungen umfassen insbesondere Japan, die Republik Korea (Südkorea) und das Vereinigte Königreich-
Individuelle Vertragsklauseln (Art. 46 Abs. 3 lit. a)	Vertragliche, verbindliche Regelung zwischen den Parteien (auch mehrere, auch Unterauftragsnehmer) über den Umgang mit personenbezogenen Daten	Zwischen den Vertragsparteien (auch mehr als 2) z. B. Datenexporteur (Verantwortlicher, Auftragsverarbeiter) und Datenimporteur (Verantwortlicher, Auftragsverarbeiter)	Durch Abgabe der entsprechenden Willenserklärungen zwischen den vertragsschließenden Parteien	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten- und Lieferantendaten soweit sie Gegenstand des individuellen Datenschutzvertrages sein sollen	Genehmigung einzelner Datenübermittlungen oder bestimmter Arten von Übermittlungen pb Daten durch Aufsichtsbehörde gem. Art. 46 Abs. 3	Flexibel; (z. B. Anpassung an Besonderheiten einer bestimmten Branche), je nach Umfang auch zeitaufwendig, wesentliche Datenschutzgarantien der DS-GVO sowie für die betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe müssen eingeräumt werden.
Vertrag auf Basis der Standarddatenschutzklauseln für die Übermittlung personenbezogener Daten (auch an Auftragsverarbeiter) (Art. 46 Abs. 2 lit. c und lit. d)	Vertrag zwischen Datenexporteur und dem Datenimporteur auf Basis der EU-Kommisionsentscheidung zu den Standarddatenschutzklauseln oder den genehmigten Standarddatenschutzklauseln der Aufsichtsbehörden	Zwischen Datenimporteur(en) in einem Drittland und Exporteur(en) mit Sitz in der EU (bzw. außerhalb der EU bei Anwendung des datenschutzrechtlichen Marktortprinzips).	Durch Abgabe der entsprechenden Willenserklärung zwischen den vertragsschließenden Parteien.	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten- und Lieferantendaten soweit sie Gegenstand des individuellen Datenschutzvertrages sein sollen	Bei unverändertem Abschluss des Vertrages keine Genehmigung erforderlich	Etabliertes Verfahren auf vertraglicher Basis. Im Lichte der Schrems II Entscheidung sind ggf. zusätzliche Schutzmaßnahmen zu ergreifen und zu vereinbaren. Bei größeren Unternehmensverbünden ist zudem der Vertragsmanagementaufwand nicht unerheblich.
Binding Corporate Rules (»Verbindliche unternehmensinterne Vorschriften) (Art. 46 Abs. 2 lit.b iVM Art. 47)	Verbindliche Unternehmensregelungen für Teile oder die Gesamtheit eines multinationalen Unternehmensverbundes (Konzern) oder Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben (z. B. bestimmte Branche)	Die Teile des Konzerns, für die Unternehmensregelung (BCR) verbindlich sind	Verbindliche, interne Anweisung durch die führende Gesellschaft	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten- und Lieferantendaten soweit sie Gegenstand des individuellen Datenschutzvertrages sein sollen	Nach Abschluss keine (zusätzlichen) weiteren aufsichtsbehördlichen Genehmigungen notwendig	

	»Art«	Geltungsbereich	Abschluss	Pb Daten	Aufsichtsbehörde	Bemerkungen
Genehmigte Verhaltensregeln (Codes of Conduct) (Art. 46 Abs. 2 lit. e)	Vereinbarung Verantwortlichen oder Auftragsverarbeitern über verbindliche Verhaltensregeln zum Datenschutz	Datenverkehr pb Daten zwischen Datenexporteuren mit Sitz in der EU und an CoC teilnehmenden Unternehmen (Datenimporteur)	Beitritt der Unternehmen zu CoC durch rechtsverbindliche und durchsetzbare Verpflichtung zur Befolgung der in den Verhaltensregeln enthaltenen Garantien	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten- und Lieferantendaten im Rahmen der Registrierung	Nach Zustimmung der zuständigen Aufsichtsbehörde und Gültigkeitserklärung der EU-Kommission keine weiteren Genehmigungen notwendig	
Genehmigte Zertifizierungsmechanismen (Art. 46 Abs. 2 lit. f i. V.m Art.42)	Rechtsverbindliche und durchsetzbare Verpflichtungen zur Befolgung geeigneter Garantien durch den Verantwortlichen oder Auftragsvearbeiter	Datenverkehr pb Daten zwischen Datenexporteuren mit Sitz in der EU und der von Zertifizierungsstellen oder Aufsichtsbehörden zertifizierten Unternehmen (Datenimporteur)	Datenexporteure und -importeure wurden gem. den Zertifizierungskriterien durch die Zertifizierungsstellen oder durch die zuständige Aufsichtsbehörde zertifiziert	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten- und Lieferantendaten im Rahmen der Registrierung	Nach Zertifizierung keine weiteren Genehmigungen notwendig	
Nichts tun	Keine Regelung implementieren	n. a.	n. a.	n. a.	n. a.	Hohes Risiko für die Verantwortlichen (Bußgeld/ Haftstrafe) und das Unternehmen (Schadensersatz/Risiko der Untersagung der Geschäftstätigkeit des EDV-Betriebs/neg. Auswirkungen auf Image, Umsatz, Ertrag, Shareholder-Value

Tabelle 3: Übersicht über die rechtlichen Möglichkeiten der Übermittlung personenbezogener Daten in Drittländer

Quelle: AK Datenschutz | Stand September 2021

5.3 Möglichkeiten der Datenübermittlung

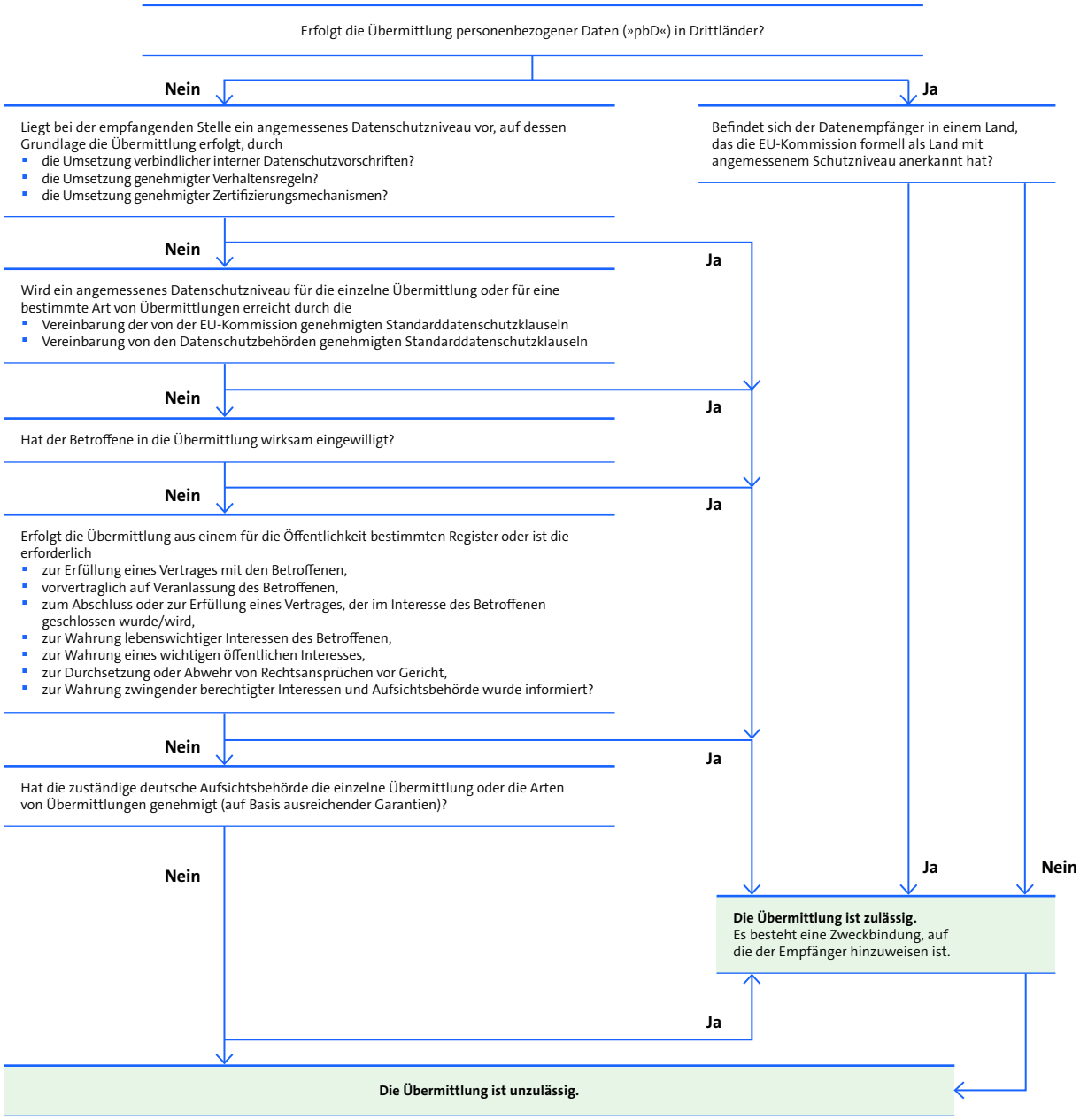

Abbildung 2: Möglichkeiten der Datenübermittlung

6 Weiterführende Links und Literatur

Urteile

EuGH, Urteil vom 24.11.2011, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado, C-468/10 und C-469/10, EU:C: 2011:777.

EuGH, Urteil vom 1.10.2015, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, EU:C:2015:639.

EuGH, Urteil vom 6.10.2015, Schrems v DPC Irland, C-362/24, EU:C:2015:650.

Irish High Court, Data Protection Commissioner v. Facebook Ireland Limited & Maximilian Schrems, Az. 2016/4809P.

La Quadrature du Net and others v Commission, Case T-738/16. Digital Rights Ireland v Commission, Case T-670/16.

EuGH, Urteil vom 16.07.2020, Data Protection Commissioner / Maximillian Schrems & Facebook Ireland, C-311/18.VG Wiesbaden: Einstweilige Untersagung der Nutzung eines Cookie-Dienstes auf der Webseite einer öffentlich-rechtlichen Hochschule, Beschluss vom 1.12.2021 – 6 L 738/21.WI

Aufsätze

Voigt, Paul, Neue Standardvertragsklauseln für internationale Datentransfers, CR 2021, 458ff.

Baumgartner/Hansch/Roth: Die neuen Standardvertragsklauseln der EU-Kommission für Datenübermittlungen in Drittstaaten, ZD 2021, 608

Leibold/Roth: Gelegentliche bzw. nicht wiederholte Datenverarbeitung? Auslegungsschwierigkeiten bei Art. 49 DS-GVO, ZD-Aktuell 2021, 05247

Conrad/Siara: Endlich Lösungen für die konzerninterne Drittlandübermittlung von Beschäftigtendaten? ZD 2021, 471

Wittmann/Haidenthaler: IT-Compliance in der Cloud – Rechtssicherheit durch Codes of Conduct?, MMR 2022, 8

Datenschutzaufsichtsbehörden

↗ Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer vom 04.06.2021

↗ Gemeinsame Stellungnahme 2/2021 des EDSA und des EDSB zum Durchführungsbeschluss der Europäischen Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer

↗ Empfehlungen des Europäischen Datenschutzausschusses (EDSA) für ergänzende Schutzmaßnahmen beim Transfer personenbezogener Daten in Drittländer außerhalb der EU und des EWR vom 18.06.2021

↗ https://www.datenschutzkonferenz-online.de/media/pm/2021_pm_neue_scc.pdf

↗ Leitlinien des Europäischen Datenschutzausschusses (EDSA) 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679

Leitlinien des EDSA 4/2021 zu genehmigten Verhaltensregeln als geeignete Garantien für Datenübermittlungen ↗ https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-Internationales/Internationaler_Datentransfer.html

↗ »Perspektiven des internationalen Datentransfers und die Notwendigkeit harmonisierender Datenschutzvorschriften«, Vortrag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit Prof. Ulrich Kelber vom 10.02.2022

Weitere hilfreiche Links

↗ DLA Piper: Data Protection Laws of the Worlds.

↗ Baker & McKenzie: Global Data Privacy & Security Handbook.

Greenleaf, Graham, Global Tables of Data Privacy Laws and Bills (7th Ed, January 2021) (February 11, 2021). (2021) 169 Privacy Laws & Business International Report. 6-19, Kostenloser Download unter: ↗ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3836261

↗ Bitkom Positionspapier: EDPB Guidelines Data protection by Design & by Default

↗ Bitkom Positionspapier: EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

↗ Bitkom Positionspapier: Position SCCs for third country data transfer

↗ Bitkom Positionspapier: Verbändebrief zum Erhalt des internationalen Datentransfers nach Schrems II

↗ Orientierungshilfe: Was jetzt in Sachen internationaler Datentransfer?

Bitkom vertritt mehr als 2.000 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bitkom e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org

bitkom