Der Bayerische Landesbeauftragte
für den Datenschutz

# Internationale Datentransfers

## Orientierungshilfe

**Herausgeber:**

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18
Telefon: +49 89 21 26 72-0
E-Mail: poststelle@datenschutz-bayern.de
https://www.datenschutz-bayern.de

**Bearbeiterin:**

Dr. Constanze Groten

Version 1.0 | Stand: 1. Mai 2023

Diese Orientierungshilfe wird ausschließlich in elektronischer Form bereitgestellt. Sie kann im Internet auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018“ abgerufen werden.

Die PDF-Datei ist für den doppelseitigen Ausdruck optimiert.

# Vorwort

In seinem „Schrems II"-Urteil hat der Europäische Gerichtshof (EuGH) die datenschutzrechtlichen Anforderungen verdeutlicht, die an Datenübermittlungen in Drittländer zu stellen sind. Die Entscheidung hat einen Diskussionsprozess angestoßen, der noch nicht abgeschlossen ist. Auch auf den öffentlichen Sektor in Bayern hat die Entscheidung erhebliche Auswirkungen, nutzen doch zahlreiche bayerische öffentliche Stellen IT-Dienstleistungen zumeist US-amerikanischer Unternehmen, welche die einschlägigen datenschutzrechtlichen Anforderungen erfüllen müssen. Die Praxisrelevanz der Entscheidung zeigt sich nicht zuletzt daran, dass US-amerikanische Anbieter den Markt im Bereich Bürosoftware weithin dominieren.[1]

Die Schlüsselfragen, die sich in diesem Zusammenhang stellen, betreffen die grundsätzliche Zulässigkeit von Datenübermittlungen in Drittstaaten sowie die dafür möglicherweise notwendigen technisch-organisatorischen Vorkehrungen. Die vorliegende Orientierungshilfe erläutert die Voraussetzungen für eine Übermittlung personenbezogener Daten in ein Drittland anhand der aktuell bestehenden rechtlichen Rahmenbedingungen und stellt dabei die wesentlichen Konstellationen („Übermittlungsinstrumente") der Art. 44 ff. Datenschutz-Grundverordnung (DSGVO) vor. Auf die Datenübermittlung an internationale Organisationen, auf die die Art. 44 ff. DSGVO ebenfalls Anwendung finden, geht die vorliegende Orientierungshilfe aufgrund der geringen Praxisrelevanz für bayerische öffentliche Stellen hingegen nicht näher ein. Ein zusätzliches Augenmerk liegt auf den Anforderungen an die Rechenschaftspflicht des Datenexporteurs. Veranschaulicht mit zahlreichen Praxistipps und Fallbeispielen, bietet diese Orientierungshilfe somit eingehende Auslegungs- und Anwendungshilfen für die bayerischen öffentlichen Stellen.

Datenexporteure und ihre Vertragspartner sollten berücksichtigen, dass sich die Rechtsprechung und die Positionen der Datenschutz-Aufsichtsbehörden zu Fragen der Art. 44 ff. DSGVO in zügiger Geschwindigkeit fortentwickeln. Sie sollten daher stets auf neue Entscheidungen und Veröffentlichungen achten.

In Bezug auf Verwaltungsbereiche, die in den Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz[2] fallen, gelten die Art. 44 ff. DSGVO nicht. Der bayerische Gesetzgeber hat Kapitel V DSGVO, dem die Vorschriften angehören, nicht in seine Anwendbarkeitserklärung eingeschlossen (vgl. Art. 2 Satz 1, Art. 28 Abs. 2 Bayerisches Datenschutzge-

[1] So nehmen Schwartmann/Burckhardt: „Schrems II" als Sackgasse für die Datenwirtschaft?, ZD 2021, S. 235, 237, für 2020 einen Marktanteil von 96 % an.

[2] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4. Mai 2016, S. 89, ber. ABl. L 127 vom 23. Mai 2018, S. 9, und ABl. L 074 vom 4. März 2021, S. 36).

setz – BayDSG). Allerdings bestehen fachgesetzliche Vorgaben, beispielsweise in Art. 58 Polizeiaufgabengesetz (PAG) sowie in §§ 77d ff. Gesetz über die internationale Rechtshilfe in Strafsachen (IRG). Auf diese Regelungen geht die vorliegende Orientierungshilfe nicht ein.

Wenn Sie Rückfragen oder Verbesserungsvorschläge haben, nutzen Sie bitte das dafür eingerichtete Postfach **orientierungshilfen@datenschutz-bayern.de**.

# Inhaltsverzeichnis

# Normtexte und Erwägungsgründe

## Datenschutz-Grundverordnung

### Art. 4
### Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:
[…]
11. „Einwilligung" der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise· und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

[…].

### Art. 44
### Allgemeine Grundsätze der Datenübermittlung

[1]Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten aus dem betreffenden Drittland oder der betreffenden internationalen Organisation an ein anderes Drittland oder eine andere internationale Organisation. [2]Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

### Art. 45
### Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

(1) [1]Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. [2]Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung.

(2) Bei der Prüfung der Angemessenheit des gebotenen Schutzniveaus berücksichtigt die Kommission insbesondere das Folgende:
a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Land bzw. bei der betreffenden internationalen Organisation geltenden einschlägigen Rechtsvorschriften sowohl allgemeiner als auch sektoraler Art – auch

in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht sowie Zugang der Behörden zu personenbezogenen Daten – sowie die Anwendung dieser Rechtsvorschriften, Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weiterübermittlung personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, die Rechtsprechung sowie wirksame und durchsetzbare Rechte der betroffenen Person und wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden,

b) die Existenz und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Durchsetzungsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten zuständig sind, und

c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtsverbindlichen Übereinkünften oder Instrumenten sowie aus der Teilnahme des Drittlands oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben.

(3) [1]Nach der Beurteilung der Angemessenheit des Schutzniveaus kann die Kommission im Wege eines Durchführungsrechtsaktes beschließen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels bieten. [2]In dem Durchführungsrechtsakt ist ein Mechanismus für eine regelmäßige Überprüfung, die mindestens alle vier Jahre erfolgt, vorzusehen, bei der allen maßgeblichen Entwicklungen in dem Drittland oder bei der internationalen Organisation Rechnung getragen wird. [3]Im Durchführungsrechtsakt werden der territoriale und der sektorale Anwendungsbereich sowie gegebenenfalls die in Absatz 2 Buchstabe b des vorliegenden Artikels genannte Aufsichtsbehörde bzw. genannten Aufsichtsbehörden angegeben. [4]Der Durchführungsrechtsakt wird gemäß dem in Artikel 93 Absatz 2 genannten Prüfverfahren erlassen.

(4) Die Kommission überwacht fortlaufend die Entwicklungen in Drittländern und bei internationalen Organisationen, die die Wirkungsweise der nach Absatz 3 des vorliegenden Artikels erlassenen Beschlüsse und der nach Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassenen Feststellungen beeinträchtigen könnten.

(5) [1]Die Kommission widerruft, ändert oder setzt die in Absatz 3 des vorliegenden Artikels genannten Beschlüsse im Wege von Durchführungsrechtsakten aus, soweit dies nötig ist und ohne rückwirkende Kraft, soweit entsprechende Informationen – insbesondere im Anschluss an die in Absatz 3 des vorliegenden Artikels genannte Überprüfung – dahingehend vorliegen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifischer Sektor in einem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels mehr gewährleistet. [2]Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen. [3]In hinreichend begründeten

Fällen äußerster Dringlichkeit erlässt die Kommission gemäß dem in Artikel 93 Absatz 3 genannten Verfahren sofort geltende Durchführungsrechtsakte.

[…].

### Art. 46 DSGVO
### Datenübermittlung vorbehaltlich geeigneter Garantien

(1) Falls kein Beschluss nach Artikel 45 Absatz 3 vorliegt, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

(2) Die in Absatz 1 genannten geeigneten Garantien können, ohne dass hierzu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre, bestehen in

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

[…]

c) Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen werden,

[…]

e) genehmigten Verhaltensregeln gemäß Artikel 40 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, oder

f) einem genehmigten Zertifizierungsmechanismus gemäß Artikel 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.

[…]

### Art. 49
### DSGVO Ausnahmen für bestimmte Fälle

(1) [1]Falls weder ein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 vorliegt noch geeignete Garantien nach Artikel 46, einschließlich verbindlicher interner Datenschutzvorschriften, bestehen, ist eine Übermittlung oder eine Reihe von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur unter einer der folgenden Bedingungen zulässig:

a) die betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde,

[…]

### Normtexte

d) die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig,

[…]

f) die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben,

g) die Übermittlung erfolgt aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im Recht der Union oder der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

[…]

(2) [1]Datenübermittlungen gemäß Absatz 1 Unterabsatz 1 Buchstabe g dürfen nicht die Gesamtheit oder ganze Kategorien der im Register enthaltenen personenbezogenen Daten umfassen. [2]Wenn das Register der Einsichtnahme durch Personen mit berechtigtem Interesse dient, darf die Übermittlung nur auf Anfrage dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.

(3) Absatz 1 Unterabsatz 1 Buchstaben a, b und c und sowie Absatz 1 Unterabsatz 2 gelten nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen.

(4) Das öffentliche Interesse im Sinne des Absatzes 1 Unterabsatz 1 Buchstabe d muss im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, anerkannt sein.

[…]

### Erwägungsgrund 6

[1]Rasche technologische Entwicklungen und die Globalisierung haben den Datenschutz vor neue Herausforderungen gestellt. [2]Das Ausmaß der Erhebung und des Austauschs personenbezogener Daten hat eindrucksvoll zugenommen. [3]Die Technik macht es möglich, dass private Unternehmen und Behörden im Rahmen ihrer Tätigkeiten in einem noch nie dagewesenen Umfang auf personenbezogene Daten zurückgreifen. [4]Zunehmend machen auch natürliche Personen Informationen öffentlich weltweit zugänglich. [5]Die Technik hat das wirtschaftliche und gesellschaftliche Leben verändert und dürfte den Verkehr personenbezogener Daten innerhalb der Union sowie die Datenübermittlung an Drittländer und internationale Organisationen noch weiter erleichtern, wobei ein hohes Datenschutzniveau zu gewährleisten ist.

### Erwägungsgrund 101

[1]Der Fluss personenbezogener Daten aus Drittländern und internationalen Organisationen und in Drittländer und internationale Organisationen ist für die Ausweitung des internationalen Handels und der internationalen Zusammenarbeit notwendig. [2]Durch die Zunahme dieser Datenströme sind neue Herausforderungen und Anforderungen in Bezug auf den Schutz

personenbezogener Daten entstanden. [3]Das durch diese Verordnung unionsweit gewährleistete Schutzniveau für natürliche Personen sollte jedoch bei der Übermittlung personenbezogener Daten aus der Union an Verantwortliche, Auftragsverarbeiter oder andere Empfänger in Drittländern oder an internationale Organisationen nicht untergraben werden, und zwar auch dann nicht, wenn aus einem Drittland oder von einer internationalen Organisation personenbezogene Daten an Verantwortliche oder Auftragsverarbeiter in demselben oder einem anderen Drittland oder an dieselbe oder eine andere internationale Organisation weiterübermittelt werden. [4]In jedem Fall sind derartige Datenübermittlungen an Drittländer und internationale Organisationen nur unter strikter Einhaltung dieser Verordnung zulässig. [5]Eine Datenübermittlung könnte nur stattfinden, wenn die in dieser Verordnung festgelegten Bedingungen zur Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen vorbehaltlich der übrigen Bestimmungen dieser Verordnung von dem Verantwortlichen oder dem Auftragsverarbeiter erfüllt werden.

### Erwägungsgrund 108

[1]Bei Fehlen eines Angemessenheitsbeschlusses sollte der Verantwortliche oder der Auftragsverarbeiter als Ausgleich für den in einem Drittland bestehenden Mangel an Datenschutz geeignete Garantien für den Schutz der betroffenen Person vorsehen. [2]Diese geeigneten Garantien können darin bestehen, dass auf verbindliche interne Datenschutzvorschriften, von der Kommission oder von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln oder von einer Aufsichtsbehörde genehmigte Vertragsklauseln zurückgegriffen wird. [3]Diese Garantien sollten sicherstellen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen auf eine der Verarbeitung innerhalb der Union angemessene Art und Weise beachtet werden; dies gilt auch hinsichtlich der Verfügbarkeit von durchsetzbaren Rechten der betroffenen Person und von wirksamen Rechtsbehelfen einschließlich des Rechts auf wirksame verwaltungsrechtliche oder gerichtliche Rechtsbehelfe sowie des Rechts auf Geltendmachung von Schadenersatzansprüchen in der Union oder in einem Drittland. [4]Sie sollten sich insbesondere auf die Einhaltung der allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten, die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen beziehen. [5]Datenübermittlungen dürfen auch von Behörden oder öffentlichen Stellen an Behörden oder öffentliche Stellen in Drittländern oder an internationale Organisationen mit entsprechenden Pflichten oder Aufgaben vorgenommen werden, auch auf der Grundlage von Bestimmungen, die in Verwaltungsvereinbarungen – wie beispielsweise einer gemeinsamen Absichtserklärung –, mit denen den betroffenen Personen durchsetzbare und wirksame Rechte eingeräumt werden, aufzunehmen sind. [6]Die Genehmigung der zuständigen Aufsichtsbehörde sollte erlangt werden, wenn die Garantien in nicht rechtsverbindlichen Verwaltungsvereinbarungen vorgesehen sind.

### Erwägungsgrund 111

[1]Datenübermittlungen sollten unter bestimmten Voraussetzungen zulässig sein, nämlich wenn die betroffene Person ihre ausdrückliche Einwilligung erteilt hat, wenn die Übermittlung gelegentlich erfolgt und im Rahmen eines Vertrags oder zur Geltendmachung von Rechtsansprüchen, sei es vor Gericht oder auf dem Verwaltungswege oder in außergerichtlichen Ver-

fahren, wozu auch Verfahren vor Regulierungsbehörden zählen, erforderlich ist. [2]Die Übermittlung sollte zudem möglich sein, wenn sie zur Wahrung eines im Unionsrecht oder im Recht eines Mitgliedstaats festgelegten wichtigen öffentlichen Interesses erforderlich ist oder wenn sie aus einem durch Rechtsvorschriften vorgesehenen Register erfolgt, das von der Öffentlichkeit oder Personen mit berechtigtem Interesse eingesehen werden kann. [3]In letzterem Fall sollte sich eine solche Übermittlung nicht auf die Gesamtheit oder ganze Kategorien der im Register enthaltenen personenbezogenen Daten erstrecken dürfen. [4]Ist das betreffende Register zur Einsichtnahme durch Personen mit berechtigtem Interesse bestimmt, sollte die Übermittlung nur auf Anfrage dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind, wobei den Interessen und Grundrechten der betroffenen Person in vollem Umfang Rechnung zu tragen ist.

### Erwägungsgrund 112

[1]Diese Ausnahmen sollten insbesondere für Datenübermittlungen gelten, die aus wichtigen Gründen des öffentlichen Interesses erforderlich sind, beispielsweise für den internationalen Datenaustausch zwischen Wettbewerbs-, Steuer- oder Zollbehörden, zwischen Finanzaufsichtsbehörden oder zwischen für Angelegenheiten der sozialen Sicherheit oder für die öffentliche Gesundheit zuständigen Diensten, etwa im Falle der Umgebungsuntersuchung bei ansteckenden Krankheiten oder zur Verringerung und/oder Beseitigung des Dopings im Sport. [2]Die Übermittlung personenbezogener Daten sollte ebenfalls als rechtmäßig angesehen werden, wenn sie erforderlich ist, um ein Interesse, das für die lebenswichtigen Interessen – einschließlich der körperlichen Unversehrtheit oder des Lebens – der betroffenen Person oder einer anderen Person wesentlich ist, zu schützen und die betroffene Person außerstande ist, ihre Einwilligung zu geben. [3]Liegt kein Angemessenheitsbeschluss vor, so können im Unionsrecht oder im Recht der Mitgliedstaaten aus wichtigen Gründen des öffentlichen Interesses ausdrücklich Beschränkungen der Übermittlung bestimmter Kategorien von Daten an Drittländer oder internationale Organisationen vorgesehen werden. [4]Die Mitgliedstaaten sollten solche Bestimmungen der Kommission mitteilen. [5]Jede Übermittlung personenbezogener Daten einer betroffenen Person, die aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu erteilen, an eine internationale humanitäre Organisation, die erfolgt, um eine nach den Genfer Konventionen obliegende Aufgabe auszuführen oder um dem in bewaffneten Konflikten anwendbaren humanitären Völkerrecht nachzukommen, könnte als aus einem wichtigen Grund im öffentlichen Interesse notwendig oder als im lebenswichtigen Interesse der betroffenen Person liegend erachtet werden.

# I. Ausgangslage

## 1. Schrems II und seine Folgen

Der EuGH erklärte mit seinem Grundsatzurteil vom 16. Juli 2020 in der Rechtssache der irischen Data Protection Commissioner gegen **Maximilian Schrems und Facebook Ireland Limited**[3] den Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild (**Privacy Shield**) gebotenen Schutzes[4] für ungültig. Dieser Angemessenheitsbeschluss zum EU-US Privacy Shield hatte bis zur Entscheidung des EuGH vier Jahre lang als Grundlage für Datentransfers aus der Europäischen Union (EU) an entsprechend zertifizierte US-Unternehmen gedient. 1

Nach der Feststellung des EuGH **reicht der EU-US Privacy Shield nicht aus**, um das von Art. 45 Abs. 2 DSGVO durch Art. 7, 8 und 47 Charta der Grundrechte der Europäischen Union (GRCh) **geforderte Schutzniveau zu gewährleisten**. Der EuGH begründet seine Entscheidung zum einen mit dem Argument, dass die entsprechenden Rechtsgrundlagen (insbesondere **Section 702 Foreign Intelligence Surveillance Act of 1978 – FISA**[5] **–** sowie **Executive Order 12.333**[6]) keinerlei Einschränkungen für US-geheimdienstliche Überwachungsprogramme wie PRISM oder UPSTREAM[7] vorsähen und somit nicht dem **Erfordernis der Verhältnismäßigkeit** genügten. Eine Beschränkung auf das zwingend erforderliche Maß sei daher nicht möglich.[8] Zum anderen mangele es an **wirksamen Rechtsbehelfen**, da den von den Überwachungsprogrammen betroffenen Personen keine Rechte eingeräumt würden, die gegenüber den US-amerikanischen Behörden gerichtlich durchgesetzt werden könnten. Die von diesen geschaffene Ombudsperson sei zwar von den Nachrichtendiensten unabhängig, aber nicht ermächtigt, ihnen gegenüber verbindliche Entscheidungen zu treffen. Damit eröffnet der Ombudsmechanismus keinen den Anforderungen des Art. 47 GRCh genügenden Rechtsweg.[9] 2

3 EuGH, Urteil vom 16. Juli 2020, C-311/18.

4 ABl. Nr. L 207 vom 1. August 2016, S. 1.

5 Zugleich 50 United States Code §§ 1881, 1881a; eingeführt durch FISA Amendments Act of 2008 vom 10. Juli 2008, H.R. 6304, Publ. L. No. 110–261, 122 Stat. 2437; Internet: https://www.govinfo.gov/content/pkg/STATUTE-122/pdf/STATUTE-122-Pg2436.pdf. Zuletzt verlängert bis 31. Dezember 2023 durch FISA Amendments Reauthorization Act of 2017 vom 18. Januar 2018, Publ. L. No. 115–118, 132 Stat. 3; Internet: https://www.congress.gov/115/plaws/publ118/PLAW-115publ118.pdf.

6 Internet: https://www.archives.gov/federal-register/codification/executive-order/12333.html.

7 Dazu Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, 2014, S. 7 f., Internet: https://www.pclob.gov/Oversight.

8 EuGH, Urteil vom 16. Juli 2020, C-311/18, Rn. 171 ff.

9 EuGH, Urteil vom 16. Juli 2020, C-311/18, Rn. 186 ff.

## I. Ausgangslage

**3** Da der EuGH in seiner Entscheidung keine Übergangsfrist vorsah, führte dies dazu, dass Übermittlungen in Drittländer auf Grundlage des EU-US Privacy Shields **mit sofortiger Wirkung unzulässig** wurden. Die Praxisrelevanz dieses Teils des EuGH-Urteils dürfte allerdings eher überschaubar sein: Zum einen hatten sich nur rund 5.300 Unternehmen, wenn auch darunter große IT-Dienstleister, nach dem EU-US-Privacy-Shield selbst zertifiziert, das heißt gegenüber dem US-Handelsministerium zur Einhaltung der niedergelegten datenschutzrechtlichen Grundsätze freiwillig selbstverpflichtet. Zum anderen hatten diese ihre Datenverarbeitungen mit EU-Unternehmen zusätzlich auf **Standardvertragsklauseln** gestützt, die sich seit jeher bei Unternehmen größerer Beliebtheit erfreuten.[10]

**4** Diese waren ebenfalls Gegenstand der Entscheidung. Der den Standardvertragsklauseln zugrunde liegende Beschluss der EU-Kommission[11] hielt der Prüfung des EuGH allerdings grundsätzlich stand. Der EuGH machte jedoch deutlich, dass der in Art. 46 Abs. 2 Buchst. c DSGVO vorgesehene vertragliche Mechanismus auf der Eigenverantwortlichkeit des in der Union ansässigen Verantwortlichen beruhe, der **in jedem Einzelfall die Gleichwertigkeit des Schutzniveaus im Drittland überprüfen** und gegebenenfalls **zusätzliche Maßnahmen** ergreifen müsse, um die Einhaltung des Schutzniveaus zu gewährleisten.[12] Der Abschluss von Standarddatenschutzklauseln zwischen Datenexporteur und Datenimporteur allein reiche folglich nicht in jedem Fall aus, um dem in Art. 46 Abs. 2 DSGVO geregelten Erfordernis der „geeigneten Garantien" Genüge zu tun.[13] Damit wurde die Datenübermittlung in Drittländer auf Grundlage von Standarddatenschutzklauseln im Einzelfall unter schwer erfüllbare Bedingungen gestellt.

**5** Die Kommission reagierte auf das Urteil des EuGH, indem sie am 12. November 2020 die Entwurfsfassung eines neuen Durchführungsbeschlusses zu Standardvertragsklauseln veröffentlichte.[14] Innerhalb der vierwöchigen Konsultationsfrist gingen zahlreiche Rückmeldungen ein, die sich in der am 4. Juni 2021 beschlossenen finalen Fassung der Standardvertragsklauseln niederschlugen.[15] Der Durchführungsbeschluss über die **neuen Standardvertragsklauseln** im Sinne von Art. 46 Abs. 2 Buchst. c DSGVO trat gemäß Art. 4 Abs. 1 des Durchführungsbeschlusses (EU) 2021/914 der Kommission vom 4. Juni 2021 am

[10] Jungkind/Raspé/Schramm, Risikoanalyse und zusätzliche Maßnahmen – Konzerninterner US-Datentransfer nach „Schrems II", NZG 2020, S. 1056 (1057).

[11] Beschluss 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (ABl. L 39 vom 12. Februar 2010, S. 5) in der durch den Durchführungsbeschluss (EU) 2016/2297 der Kommission vom 16. Dezember 2016 geänderten Fassung (ABl. L 344 vom 17. Dezember 2016, S. 100).

[12] EuGH, Urteil vom 16. Juli 2020, C-311/18, Rn. 134.

[13] EuGH, Urteil vom 16. Juli 2020, C-311/18, Rn. 128.

[14] Internet: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Datenschutz-Standardvertragsklauseln-fur-die-Ubermittlung-personenbezogener-Daten-in-Nicht-EU-Lander-Durchfuhrungsrechtsakt-_de.

[15] Durchführungsbeschluss (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 (ABl. L 199 vom 7. Juni 2021, S. 31); Baumgartner/Hansch/Roth: Die neuen Standardvertragsklauseln der EU-Kommission für Datenübermittlungen in Drittstaaten, ZD 2021, S. 608.

27. Juni 2021 in Kraft; der Durchführungsbeschluss über die bisherigen Standardvertragsklauseln wurde nach einer Übergangsphase gemäß Art. 4 Abs. 2 und 3 des Durchführungsbeschlusses (EU) 2021/914 der Kommission vom 4. Juni 2021 mit Wirkung vom 27. September 2021 aufgehoben. Seit diesem Zeitpunkt sind bei Neuverträgen die neuen Standardvertragsklauseln zu verwenden; Altverträge mussten spätestens bis zum 27. Dezember 2022 auf die neuen Standardvertragsklauseln umgestellt werden. Zeitgleich mit den neuen Standardvertragsklauseln beschloss die EU-Kommission zudem **Standardvertragsklauseln für EU-Auftragsverarbeitungen** im Sinne von Art. 28 Abs. 7 DSGVO, die jedoch nicht die Anforderungen an eine Übermittlung personenbezogener Daten in Drittländer nach Maßgabe des Kapitels V DSGVO erfüllen.[16]

6 Parallel zur Erarbeitung der neuen Standardvertragsklauseln erstellte der Europäische Datenschutzausschuss (EDSA) **Empfehlungen** zur praktischen Umsetzung der vom EuGH im „Schrems II"-Urteil vorgegebenen Prüfungen und Maßnahmen, deren finale Fassung am 18. Juni 2021 angenommen wurde.[17]

7 Damit entsprechen die EU-Institutionen dem Ziel der Datenschutz-Grundverordnung, das hohe Schutzniveau für personenbezogene Daten in den Mitgliedstaaten der EU sowie des Europäischen Wirtschaftsraums (EWR) auch bei der Übermittlung personenbezogener Daten aus Ländern der EU und des EWR an Drittländer zu gewährleisten (vgl. auch Erwägungsgründe 6 und 101 DSGVO).

8 Faktisch könnte dies als Versuch gewertet werden, der Datenschutz-Grundverordnung mittels dieser Vorgaben dort Geltung zu verschaffen, wo ihr räumlicher Geltungsbereich ansonsten an seine Grenzen stoßen würde. Mit anderen Worten: Man ist bemüht, das unionale Schutzniveau auf Rechtsordnungen von Drittländern auszuweiten. Eine gewisse Ausstrahlungswirkung auf die betreffenden Drittländer haben bereits die Regelungen der Art. 44 ff. DSGVO selbst,[18] wie sie auch das „Untergrabungsverbot" des Art. 44 Satz 2 DSGVO festschreibt. Auch wenn diese Vorschrift als bloßer Programmsatz und reine Auslegungsregel ohne eigenständigen Regelungsanspruch zu verstehen sein soll,[19] gründet sie unmittelbar auf der in Art. 8 Abs. 1 GRCh ausdrücklich vorgesehenen Pflicht zum Schutz personenbezogener Daten und soll auch bei einer Übermittlung in ein Drittland den von der Datenschutz-Grundverordnung garantierten Mindeststandard gewährleisten.[20] Dieses Selbstverständnis der Datenschutz-Grundverordnung wird wohl auch das „Schrems II"-Urteil inspiriert haben.

16 Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates (ABl. L 199 vom 7. Juni 2021, S. 18).

17 EDSA, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Version 2.0, Stand 6/2021, Internet: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de.

18 Klug, in: Gola/Heckmann, Datenschutz-Grundverordnung, 3. Aufl. 2022, Art. 44 Rn. 1.

19 Schröder, in: Kühling/Buchner, DSGVO/BDSG, 3. Aufl. 2020, Art. 44 DSGVO Rn. 23.

20 Zerdick, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 44 Rn. 16.

## 2. Konsequenzen bei der Auswahl von Betriebsmitteln

**9** Die Datenschutzkonformität ist bei – oftmals ohnehin austauschbaren – Betriebsmitteln ein wesentliches Auswahlkriterium. Viele Betriebsmittel haben Drittstaatentransfers „im Gepäck", manchmal gilt dies auch bloß für einzelne (gerade ökonomisch scheinbar attraktivere) Varianten. Bayerische öffentliche Stellen müssen sich an das geltende Recht halten; sie müssen rechtlich unzulässige Drittstaatentransfers unterlassen und sollten rechtlich zweifelhafte Drittstaatentransfers vermeiden, also etwa solche, bei denen Unklarheiten über rechtliche Rahmenbedingungen im Drittstaat (Rn. 62 ff.) oder die Hinlänglichkeit zusätzlicher Maßnahmen (Rn. 71 ff.) bestehen. Eine bayerische öffentliche Stelle muss hinsichtlich ihrer Verarbeitungen die Rechenschaftspflicht in Bezug auf die Rechtmäßigkeit erfüllen (Art. 5 Abs. 2 in Verbindung mit Abs. 1 Buchst. a DSGVO). In diesem Rahmen muss sie einen positiven Nachweis führen; unklare Sachverhalte und Zweifel bei der Rechtsanwendung gehen dabei zu ihren Lasten.

# II. Zwei-Stufen-Prüfung

Sofern personenbezogene Daten an Empfänger in Drittländern übermittelt werden sollen, ist eine **zweistufige Zulässigkeitsprüfung** vorzunehmen: Gemäß Art. 44 Satz 1 DSGVO ist eine Datenübermittlung in ein Drittland nur dann zulässig, wenn **alle „sonstigen Bestimmungen dieser Verordnung" (1. Prüfungsstufe)** und **gleichzeitig die in Kapitel V niedergelegten Bedingungen (2. Prüfungsstufe)** eingehalten werden. 10

Auf einer **ersten Stufe** müssen – wie bei jeder Datenverarbeitung – zunächst die **allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten** der Art. 5 ff. DSGVO beachtet werden. So müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Insbesondere muss eine Rechtsgrundlage die jeweilige Verarbeitung legitimieren (Art. 5 Abs. 1 Buchst. a Var. 1, Art. 6 Abs. 1, Art. 9 Abs. 1, 2 DSGVO); kommt es zu einer Zweckänderung, muss auch diese gesetzmäßig sein (Art. 5 Abs. 1 Buchst. b, Art. 6 Abs. 4 DSGVO). Außerdem sind die übrigen Verarbeitungsgrundsätze (vgl. Art. 5 Abs. 1 DSGVO) zu berücksichtigen. 11

**Praxistipp** (und Warnhinweis): Die Prüfung der Art. 44 ff. DSGVO enthebt bayerische öffentliche Stellen – trotz des damit verbundenen Aufwands – nicht der Aufgabe, die nach dem Fachrecht oder dem allgemeinen bayerischen Datenschutzrecht in Betracht kommenden Verarbeitungsbefugnisse und – soweit erforderlich – Zweckänderungsregeln zu prüfen. 12

Soweit der Datentransfer im Kontext einer Auftragsverarbeitung steht, sind insbesondere die Vorgaben aus Art. 28 DSGVO einzuhalten.[21] 13

Zusätzlich sind **auf der zweiten Stufe** die **Zulässigkeitsvoraussetzungen für die Übermittlung personenbezogener Daten in ein Drittland** gemäß den Art. 44 ff. DSGVO zu würdigen, sofern ein Drittlandtransfer im Sinne der Datenschutz-Grundverordnung vorliegt. 14

Die Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO bezieht sich auf beide Prüfungsstufen. Das ist bei der Dokumentation zu berücksichtigen (näher hierzu unter Rn. 123 ff.). 15

[21] Vgl. zur Auftragsverarbeitung: Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Stand 9/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Auftragsverarbeitung".

# III. Vorprüfung

## 1. Datenübermittlung in ein Drittland

### a) Begriff des Drittlands

**16** Der Begriff „Drittland" ist zunächst synonym mit dem Begriff „Drittstaat" und bezeichnet alle Länder, die **weder der Europäischen Union noch dem Europäischen Wirtschaftsraum** angehören. Der EWR umfasst neben den EU-Mitgliedstaaten die Länder Island, Liechtenstein und Norwegen.

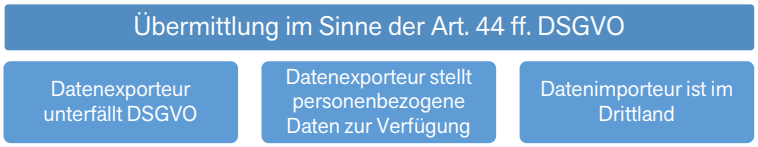
**17** Auch wenn der Wortlaut des Art. 44 Satz 1 DSGVO („an ein Drittland") andere Rückschlüsse zulassen mag, gilt hinsichtlich des Begriffs „Empfänger" die Definition des Art. 4 Nr. 9 DSGVO, so dass „Übermittlung" als jede Offenlegung personenbezogener Daten **gegenüber einem Empfänger** in einem Drittland zu verstehen ist; das Drittland muss also nicht selbst Empfänger oder Übermittler der personenbezogenen Daten sein.[22]

**18** Zudem setzen die Art. 44 ff. DSGVO nicht eine „Übermittlung an einen Dritten" voraus, so dass die Vorschriften folglich auch bei einer Offenlegung von personenbezogenen Daten an einen Auftragsverarbeiter in einem Drittland greifen, der nach der Datenschutz-Grundverordnung kein Dritter ist (vgl. Art. 4 Nr. 10 DSGVO).[23]

### b) Kriterien für eine Drittlandübermittlung

**19** Bei der Auslegung der Terminologie der „Übermittlung an ein Drittland" bieten die **„Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR"** [24] des EDSA eine Hilfestellung, deren finale Fassung am 14. Februar 2023 verabschiedet wurde.

**20** In den „Guidelines" stellt der EDSA folgende grundlegende Anforderungen an eine Übermittlung im Sinne der Art. 44 ff. DSGVO, die kumulativ erfüllt sein müssen:




22 Pauly, in: Paal/Pauly, DSGVO/BDSG, 3. Aufl. 2021, Art. 44 DSGVO Rn. 4.

23 Pauly, in: Paal/Pauly, DSGVO/BDSG, 3. Aufl. 2021, Art. 44 DSGVO Rn. 3.

24 EDSA, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, Version 2.0, Stand 2/2023, Internet: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en.

Zunächst hebt der EDSA hervor, dass die Vorgaben zum Drittlandtransfer auch dann Anwendung finden, wenn **der in einem Drittland ansässige Verantwortliche oder Auftragsverarbeiter**, für den die Datenschutz-Grundverordnung aufgrund des Marktortprinzips nach Art. 3 Abs. 2 DSGVO zur Anwendung gelangt, Daten in „sein" oder in ein anderes Drittland übermittelt, die Datenübermittlung also – geographisch gesehen – nicht „aus der EU heraus" erfolgt.[25] 21

Zudem muss nach Auslegung des EDSA für die Anwendbarkeit der Art. 44 ff. DSGVO die Offenlegung der Daten auf Export- wie auch auf Importseite **jeweils zwischen Verantwortlichen oder Auftragsverarbeitern** erfolgen; die Übermittlung kann folglich nicht nur von einem Verantwortlichen, sondern auch von einem Auftragsverarbeiter durchgeführt werden. Somit liegt kein Fall der Art. 44 ff. DSGVO vor, wenn die in der EU oder im EWR befindliche betroffene Person selbst auf ihre eigene Initiative hin Daten direkt gegenüber einem Empfänger im Drittland offenlegt.[26] Gleiches gilt für die Konstellation, dass ein Beschäftigter eines Verantwortlichen auf einer Dienstreise in ein Drittland personenbezogene Daten auf seinem Notebook verarbeitet, weil die Datenübermittlung innerhalb desselben Verantwortlichen erfolgt.[27] Eine Drittlandübermittlung ist hingegen dann anzunehmen, wenn der europäische Auftragsverarbeiter personenbezogene Daten an „seinen" Verantwortlichen in einem Drittland rückübermittelt oder er personenbezogene Daten mit seiner in einem Drittland ansässigen Muttergesellschaft teilt, da Unternehmen derselben Unternehmensgruppe als gesonderte Verantwortliche oder Auftragsverarbeiter bewertet werden können.[28] 22

Des Weiteren sind die Vorgaben der Art. 44 ff. DSGVO nach Ansicht des EDSA auch dann zu beachten, wenn **der im Drittland ansässige Datenimporteur** aufgrund des Marktortprinzips bereits in den Anwendungsbereich der Datenschutz-Grundverordnung fällt. Dieser Klarstellung des EDSA muss gerade im Hinblick auf die Tatsache, dass die aktuellen Standardvertragsklauseln diese Konstellation nicht abdecken (siehe Rn. 85), Rechnung getragen werden.[29] 23

Schließlich gelten die Voraussetzungen für die Datenübermittlung aus der EU in ein Drittland gemäß Art. 44 Satz 1 Halbsatz 2 DSGVO und Erwägungsgrund 101 Satz 3 DSGVO ebenso für die **Weiterübermittlung durch den Datenimporteur** innerhalb des Drittlands oder in ein weiteres Drittland. In dieser Konstellation versucht die EU also, den Anwendungsbereich der Datenschutz-Grundverordnung noch weiter zu verlängern. 24

25

[25] EDSA, Guidelines 05/2021 (Fn. 24), Rn. 13 f.

[26] EDSA, Guidelines 05/2021 (Fn. 24), Rn. 18. Die Guidelines scheinen jedoch nicht den Fall zu berücksichtigen, dass die betroffene Person selbst durch einen in der Europäischen Union belegenen Verantwortlichen dazu gebracht wird, ihre Daten ohne Umweg über diese Stelle ins Drittland zu exportieren. Dies spricht in Ansehung des Art. 44 Satz 2 DSGVO dafür, dass die Art. 44 ff. DSGVO auch in diesem Fall zumindest entsprechend anwendbar sind, um das durch die Datenschutz-Grundverordnung gewährleistete Schutzniveau nicht zu untergraben.

[27] EDSA, Guidelines 05/2021 (Fn. 24), Rn. 20.

[28] EDSA, Guidelines 05/2021 (Fn. 24), Rn. 19, 21.

[29] EDSA, Guidelines 05/2021 (Fn. 24), Rn. 22.

### III. Vorprüfung

**Praxistipp:** Oft ist die Tatsache, dass ein Drittlandtransfer vorliegt, nicht auf den ersten Blick ersichtlich. Bayerische öffentliche Stellen sind häufig unbewusst einem solchen Übermittlungsszenario ausgesetzt, zum Beispiel bei der Verwendung eines E-Mail-Dienstes oder eines Konferenztools, aber auch im Falle einer Fernwartung oder der Verwendung von Cloud-Diensten. Bestehende wie neu abzuschließende Verträge sind daher insbesondere auch auf das Vorliegen von Drittlandtransfers zu prüfen.

**26** Die „Guidelines" beantworten allerdings immer noch nicht eindeutig die Frage, wann ein Datenimporteur im Drittland „ist". Denkbare Lesarten wären der **Ort der Niederlassung des Datenimporteurs** sowie der Ort der Datenverarbeitung – respektive der Standort des Servers und anderer relevanter IT-Systeme.[30] Da Letzterer für Vertragspartner oftmals insbesondere aufgrund der fortschreitenden Virtualisierung schwer lokalisierbar sein dürfte, ist erstere Auffassung vorzugwürdig, zumal auch der Wortlaut der „Guidelines" in diese Richtung deutet („the importer is geographically in a third country"[31]).

**27** **Praxistipp:** Häufig sehen sich verantwortliche bayerische öffentliche Stellen mit der Argumentation von Auftragsverarbeitern mit Sitz in einem Drittland konfrontiert, es liege kein Drittlandtransfer vor, da die Datenverarbeitung ausschließlich auf einem in der EU oder dem EWR gelegenen Server erfolge. Solange sich allerdings nicht mit Sicherheit ausschließen lässt, dass der Auftragsverarbeiter auf die auf dem Server oder auf anderen relevanten IT-Systemen (z. B. Netzkomponenten) gespeicherten Daten zugreift (so bei einem Remote-Zugriff), ist wegen des Sitzes des Auftragsverarbeiters im Drittland ein Drittlandtransfer gegeben.

**28** Der in Art. 44 ff. DSGVO verwendete Begriff der Übermittlung ist nach Art. 4 Nr. 2 DSGVO eine Form der Offenlegung. Eine Übermittlung in ein Drittland liegt vor, wenn Daten dorthin **übertragen** werden; eine Übermittlung kann aber auch dadurch bewirkt werden, dass gespeicherte Daten für Stellen im Drittstaat **zugänglich gemacht** werden, beispielsweise durch die Gewährung von Zugriffsrechten. Dabei kommt es darauf an, dass die Daten nach der Übermittlung im Drittland verarbeitet werden können, und nicht darauf, dass tatsächlich ein Abruf der Daten erfolgt.[32] Zu einer Übermittlung in ein Drittland kommt es nicht notwendig, wenn personenbezogene Daten an einen im Geltungsbereich der Datenschutz-Grundverordnung niedergelassenen Cloud-Provider übermittelt werden, der eine internationale Cloud-Infrastruktur nutzt, vorausgesetzt, dieser Provider erklärt ausdrücklich, dass keinerlei Verarbeitung in Drittländern stattfindet.[33] Kurzum: Eine Niederlassung in der EU oder im EWR in Kombination mit einer Datenverarbeitung innerhalb der EU oder des EWR an einem **europäischen Standort der relevanten IT-Systeme (Server, Netzkomponenten usw.)** verhindert daher üblicherweise die Anwendung der Art. 44 ff. DSGVO.

[30] Voigt, Leitlinien des Europäischen Datenschutzausschusses zu internationalen Datentransfers, Datenschutz-Berater, Nr. 03/2002, S. 90 (92).

[31] EDSA, Guidelines 05/2021 (Fn. 24), Rn. 22, sowie Example 11 für den Fall des Remote-Zugriffs.

[32] Beck, in: Wolff/Brink, BeckOK Datenschutzrecht, Stand 11/2021, Art. 44 DSGVO Rn. 15; Schröder, in: Kühling/Buchner, DSGVO/BDSG, 3. Aufl. 2020, Art. 44 DSGVO Rn. 16.

[33] EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 13.

## c) Zugriffsmöglichkeiten durch öffentliche Stellen in Drittländern

Diese Hypothese kann jedoch nicht vorbehaltlos **im Hinblick auf den europäischen Niederlassungs- und Serverstandort eines US-amerikanischen Cloud-Providers** mit Hauptsitz in den USA **gelten**: Zum einen fallen in den räumlichen Anwendungsbereich von **Section 702 FISA** auch Daten von Nicht-US-Bürgern, die von US-Telekommunikationsunternehmen sowie US-Anbietern von Computerspeicher- und -verarbeitungsleistungen einschließlich ihrer EU-Tochterunternehmen auf EU-Servern gespeichert werden.[34] Zum anderen verpflichtet der sogenannte **CLOUD Act** (Clarifying Lawful Overseas Use of Data Act)[35] US-Anbieter von Kommunikations- und Cloud-Dienstleistungen zur Preisgabe von Kundendaten an US-Behörden, unabhängig davon, wo die Daten gespeichert werden.[36] **29**

Insofern ist davon auszugehen, dass Tochtergesellschaften von US-Unternehmen trotz ihres Sitzes in der EU aufgrund der extraterritorialen Wirkung von US-Rechtsvorschriften Zugriffsersuchen ihrer Muttergesellschaft oder auch von US-Behörden direkt ausgesetzt und sogar zur Offenlegung von personenbezogenen Daten verpflichtet sein können. Der potentielle Datenzugriff oder das potentielle Herausgabeverlangen schaffen ein latentes, jederzeit realisierbares Risiko für eine Datenübermittlung in die USA, die nicht den Anforderungen der Art. 44 ff. DSGVO genügt. Um den Schutzzweck der Art. 44 ff. DSGVO auch in diesen Fällen zu erfüllen, könnten die Vorschriften über den Drittlandtransfer bereits im Verhältnis zur EU-Tochtergesellschaft angewendet werden.[37] Diese Betrachtungsweise lässt aber außer Acht, dass sich die EU-Tochtergesellschaft gegen eine solche Herausgabeaufforderung möglicherweise auch zur Wehr setzen könnte. Entscheidend ist vielmehr eine Einzelfallbetrachtung.[38] **30**

Falls diese Einzelfallbetrachtung ergeben sollte, dass – beispielsweise mangels technischer Zugriffsmöglichkeit – sich ein Zugriff auf die oder eine Offenlegung der Daten nicht unmittelbar realisiert, so dass bei der Übermittlung an die EU-Tochtergesellschaft noch kein Drittlandtransfer gegeben ist, muss die Gefahr eines Zugriffs, eines Herausgabeverlangens oder einer Offenlegung stattdessen im Rahmen des Art. 28 Abs. 1 DSGVO Berücksichtigung finden. Danach dürfen Verantwortliche nur mit Auftragsverarbeitern arbeiten, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der Datenschutz-Grundverordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Solche Garantien bestünden bei einem Auftragsverarbeiter, auf den Section 702 FISA Anwendung finden kann, aber im Hinblick auf die Bestimmungen von Kapitel V DSGVO gerade nicht von vornherein. Deshalb wird ein Verantwortlicher, der nicht selbst Daten in ein Drittland übermit- **31**

[34] Vladeck, Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse vom 15. November 2021, S.10, Internet: https://www.datenschutzkonferenz-online.de/weitere_dokumente.html.

[35] Internet: https://www.congress.gov/bill/115th-congress/house-bill/4943/text.

[36] Gausling, Offenlegung von Daten auf Basis des CLOUD Act, MMR 2018, S. 578 (579 f.).

[37] So auch Vergabekammer Baden-Württemberg, Beschluss vom 13. Juli 2022, 1 VK 23/22, Rn. 62.

[38] Gegen die Annahme eines Drittlandtransfers bei Auftragsverarbeitern, die der Gesetzgebung eines Drittlands unterliegen können, mittlerweile auch eindeutig EDSA, Guidelines 05/2021 (Fn. 24), Example 12.

telt, sondern mit einem Auftragsverarbeiter arbeitet, der den Rechtsvorschriften von Drittstaaten mit extraterritorialer Wirkung unterliegt, diese Tatsache schon aufgrund von Art. 28 Abs. 1 DSGVO vor Beauftragung des Auftragsverarbeiters berücksichtigen und sicherstellen müssen, dass dieser die geforderten Garantien zur Umsetzung geeigneter Sicherheitsmaßnahmen bietet (vgl. hierzu auch Rn. 38 ff.).

32 **Praxistipp:** Um festzustellen, ob ein Drittlandtransfer im Sinne der Datenschutz-Grundverordnung vorliegt, sollte stets geprüft werden, wo der Empfänger niedergelassen ist, aber auch, wo er seinen Hauptsitz hat und an welchem Standort konkret die Datenverarbeitung erfolgt. In erster Linie finden die Vorschriften zum Drittlandtransfer dann Anwendung, wenn der Empfänger außerhalb der EU bzw. des EWR ansässig ist. Aufgrund von Bestimmungen, wie denjenigen des CLOUD Act oder von Section 702 FISA, sind sie aber – zumindest mittelbar – auch dann zu beachten, wenn Empfänger etwa die in der EU ansässige Tochtergesellschaft eines US-Konzerns ist.

## d) Überblick Drittlandszenarien

33 Die nachfolgende Tabelle fasst wichtige Konstellationen mit Drittstaatenbezug zusammen und ordnet sie hinsichtlich der Anwendbarkeit von Art. 44 ff. DSGVO ein:

| Konstellation | Art. 44 ff. DSGVO anwendbar | Art. 44 ff. DSGVO nicht anwendbar | Erläuterung siehe |
|---|---|---|---|
| bayer. öff. Stelle überträgt Daten an einen Verantwortlichen/Auftragsverarbeiter in der EU/dem EWR | | ● | Rn. 16 |
| bayer. öff. Stelle überträgt Daten an einen Verantwortlichen/Auftragsverarbeiter in einem Drittland | ● | | Rn. 16, 20 |
| Auftragsverarbeiter einer bayer. öff. Stelle in einem Drittland rückübermittelt Daten an die bayer. öff. Stelle | | ● | Rn. 20 |
| bayer. öff. Stelle verschafft einem Verantwortlichen/Auftragsverarbeiter in einem Drittland Zugang zu Daten | ● | | Rn. 28 |
| (Unter-)Auftragsverarbeiter einer bayer. öff. Stelle in der EU/ im EWR überträgt Daten an einen Unterauftragsverarbeiter in einem Drittland | ● | | Rn. 22 |
| (Unter-)Auftragsverarbeiter einer bayer. öff. Stelle in einem Drittland überträgt Daten an einen Unterauftragsverarbeiter in demselben Drittland | ● | | Rn. 24 |
| (Unter-)Auftragsverarbeiter einer bayer. öff. Stelle in einem Drittland überträgt Daten an einen Unterauftragsverarbeiter in einem anderen Drittland | ● | | Rn. 24 |
| bayer. öff. Stelle veranlasst eine betroffene Person, Daten an einen Auftragsverarbeiter in einem Drittland offenzulegen, und lässt die Daten dort verarbeiten | ● | | Fn. 26 |

| Konstellation | Art. 44 ff. DSGVO anwendbar | Art. 44 ff. DSGVO nicht anwendbar | Erläuterung siehe |
|---|---|---|---|
| Beschäftigte einer bayer. öff. Stellen verarbeiten personenbezogene Daten auf dem Dienst-Notebook während einer Dienstreise in einem Drittland | | ● | Rn. 22 |
| (Unter-)Auftragsverarbeiter einer bayer. öff. Stelle in der EU/ im EWR teilt Daten mit seiner Muttergesellschaft (Unterauftragsverarbeiter) in einem Drittland | ● | | Rn. 22 |
| (Unter-)Auftragsverarbeiter einer bayer. öff. Stelle in der EU/ im EWR unterliegt den Rechtsvorschriften eines Drittlandes | | ● | Rn. 29 ff. |

# 2. Normadressat der Art. 44 ff. DSGVO

## a) Datenexporteur als Normadressat

Vor dem Einstieg in die Prüfung der Art. 44 ff. DSGVO ist die nicht unerhebliche Frage zu beantworten, wer eigentlich **Normadressat** dieser Vorschriften ist und daher ihre Anforderungen einzuhalten hat.[39] Grundsätzlich sind dies die nach Art. 4 Nr. 7 DSGVO Verantwortlichen sowie Auftragsverarbeiter nach Art. 4 Nr. 8 DSGVO.[40] Denkbar wäre folglich, dass alle an der Verarbeitung Beteiligten die für die Datenübermittlung in ein Drittland geltenden Vorschriften einzuhalten haben. Dies hätte zur Folge, dass der Verantwortliche dann beispielsweise mit dem in einem Drittland ansässigen Unterauftragsverarbeiter in einer Vertragsbeziehung stehen müsste, um die Anforderungen der Art. 44 ff. DSGVO wirksam erfüllen zu können. Dem widerspricht jedoch der Wortlaut des Art. 46 Abs. 3 Buchst. a DSGVO, der als Variante vorsieht, dass der Auftragsverarbeiter mit dem Auftragsverarbeiter im Drittland Vertragsklauseln mit den entsprechenden geeigneten Garantien vereinbart. Müsste der Verantwortliche stets als Normadressat der Art. 44 ff. DSGVO behandelt werden, wäre diese Konstellation nie möglich. **34**

Auch die übrige Systematik der Datenschutz-Grundverordnung lässt nicht darauf schließen, dass die Art. 44 ff. DSGVO neben einem Auftragsverarbeiter als Datenexporteur immer auch den Verantwortlichen adressieren: Im Rahmen des in diesem Fall abzuschließenden Auftragsverarbeitungsvertrags wird bereits über Art. 28 Abs. 3 Buchst. a DSGVO sichergestellt, dass ein etwaiger Auftragsverarbeiter personenbezogene Daten weisungsgebunden zu verarbeiten und die Vorschriften zum Drittlandtransfer zu beachten hat. Die Erfüllung des Regelungszwecks der Datenschutz-Grundverordnung, ein gleichbleibend hohes Datenschutzniveau zu garantieren, ist also auch in einer längeren „Verarbeiterkette" sichergestellt, ohne zusätzlich den Verantwortlichen mitverpflichten zu müssen. Schließlich ist auch dem Wortlaut **35**

[39] Vgl. ausführlich zu dieser Frage: Golland, Datenschutzrechtliche Anforderungen an internationale Datentransfers, NJW 2020, S. 2593 (2595 f.).

[40] Klug, in: Gola/Heckmann, Datenschutz-Grundverordnung, 3. Aufl. 2022, Art. 44 DSGVO Rn. 1.

von Satz 5 des Erwägungsgrunds 101 DSGVO, wonach die Bedingungen von Drittlandtransfers vom „Verantwortlichen oder dem Auftragsverarbeiter erfüllt werden", zu entnehmen, dass nicht alle Beteiligten als Normadressaten der Art. 44 ff. DSGVO zu verstehen sind.

**36** Dass demzufolge **nur der Datenexporteur**, also der Verantwortliche oder (Unter-)Auftragsverarbeiter, der die Datenübermittlung in das Drittland unmittelbar durchführt, konkret die Gleichwertigkeit des Schutzniveaus überprüfen muss, belegen mittlerweile auch die **Standardvertragsklauseln** der Europäischen Kommission für die Drittlandübermittlung, die in Modul 3 die Konstellation der Übermittlung durch Auftragsverarbeiter an (Unter-)Auftragsverarbeiter behandeln und damit gerade vermeiden wollen, dass der Verantwortliche mit dem in einem Drittland ansässigen Unterauftragsverarbeiter einen gesonderten Vertrag abschließen muss (näher hierzu unter Rn. 87).

**Beispiel 1:** Ein Landratsamt möchte zur Datenspeicherung die Cloud-Dienste eines Anbieters mit Sitz in Singapur verwenden. Sofern das Landratsamt nicht selbst einen Vertrag mit dem entsprechenden Dienstleister schließt, sondern mit einem in der EU ansässigen Auftragsverarbeiter, der die Daten an den Cloud-Anbieter in Singapur als Unterauftragsverarbeiter übermittelt, ist das Landratsamt nicht als Datenexporteur zu betrachten. Stattdessen muss der Auftragsverarbeiter das Datenschutzniveau prüfen und mit dem Unterauftragsverarbeiter den Abschluss von Standardvertragsklauseln und gegebenenfalls die wirksame Umsetzung zusätzlicher Maßnahmen vereinbaren.

## b) Prüfpflichten des Verantwortlichen

**37** Auch wenn nur der datenexportierende Auftragsverarbeiter die direkten Anforderungen der Art. 44 ff. DSGVO einzuhalten hat, kann der Verantwortliche durch Beauftragung eines Auftragsverarbeiters wegen seiner Rechenschaftspflicht nicht gänzlich eine Prüfung in Bezug auf die Erfüllung der Vorgaben der Art. 44 ff. DSGVO durch den Auftragsverarbeiter umgehen. Schließlich bezieht sich die Rechenschaftspflicht des Verantwortlichen gemäß Art. 5 Abs. 2 DSGVO auch auf den Verarbeitungsgrundsatz „Rechtmäßigkeit" gemäß Art. 5 Abs. 1 Buchst. a DSGVO (vgl. hierzu Rn. 123). Zudem wird der Auftragsverarbeiter gemäß Art. 28 Abs. 3 Satz 1 Buchst. a DSGVO **stets auf Weisung des Verantwortlichen** auch in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland tätig.[41] Die Einschaltung eines Auftragsverarbeiters wirkt sich auf die Verantwortlichkeit somit grundsätzlich nicht aus, wenngleich der Auftragsverarbeiter im Falle eines weisungswidrigen Drittlandtransfers gemäß Art. 28 Abs. 10 DSGVO selbst als Verantwortlicher gilt. Der Verantwortliche kann sich seinen datenschutzrechtlichen Pflichten und Verantwortlichkeiten **nicht durch die Auslagerung seiner Datenverarbeitung entziehen**. Er bleibt vielmehr auch im Fall der Auftragsverarbeitung, selbst wenn sie einen Drittlandtransfer umfasst, Adressat der datenschutzrechtlichen Betroffenenrechte.[42]

[41] Vgl. hierzu auch Klausel 7.8 Buchst. a im Anhang des Durchführungsbeschlusses (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates, C/2021/3701 (ABl. L 199 vom 7. Juni 2021, S. 18).

[42] Vgl. Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Stand 9/2019, S. 11.

Deshalb darf der Verantwortliche gemäß Art. 28 Abs. 1 DSGVO, Erwägungsgrund 81 DSGVO nur solche Auftragsverarbeiter mit einer Verarbeitungstätigkeit betrauen, die – insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen – hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen – auch im Hinblick auf die Sicherheit der Verarbeitung – getroffen werden, die den Anforderungen der Datenschutz-Grundverordnung genügen. Dem Verantwortlichen obliegt gemäß Art. 28 Abs. 1 DSGVO also eine **Auswahlverantwortung** bezüglich des Auftragsverarbeiters (vgl. hierzu bereits Rn. 31), die vom Verantwortlichen zwar keine regelmäßige Überprüfung verlangt, ihm aber eine gewisse **Kontrollpflicht** auferlegt, da nach Art. 28 Abs. 1 DSGVO eine Zusammenarbeit mit Auftragsverarbeitern ab dem Zeitpunkt nicht mehr gestattet ist, ab dem entsprechende Garantien nicht mehr gewährleistet sind.[43] **38**

Gerade in Fällen, in denen eine Norm eines Drittstaats die abstrakte Gefahr einer nach EU-Recht unzulässigen Übermittlung personenbezogener Daten aus der EU in einen Drittstaat durch einen Auftragsverarbeiter mit Sitz in der EU begründet, sind nach einem Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) an **diese Zuverlässigkeitsprüfung** besonders hohe Anforderungen zu stellen, die dieser Gefahr Rechnung tragen.[44] Der Verantwortliche sollte daher insbesondere folgende Punkte berücksichtigen: **39**

- Extraterritoriale Anwendbarkeit und tatsächliche Anwendung des Drittland-Rechts, das die Pflichten aus dem Auftragsverarbeitungsvertrag beeinträchtigen könnte;
- Risiko der Anweisung zur Datenübermittlung in das Drittland durch Drittlands-Muttergesellschaft, auch vor dem Hintergrund möglicher Sanktionen durch Drittland und EU;
- Gestaltung des Auftragsverarbeitungsvertrags im Hinblick auf etwaige Drittlands-Übermittlungen: Werden diese ausgeschlossen bzw. für diesen Fall – realisierbar erscheinende – Zusicherungen abgegeben?
- Geeignetheit der ergriffenen technischen und organisatorischen Maßnahmen für den Ausschluss eines unzulässigen Drittlandtransfers?

Sollte der Verantwortliche nach dieser Prüfung zu der Bewertung kommen, dass der Auftragsverarbeiter keine hinreichenden Garantien gemäß Art. 28 Abs. 1 DSGVO bietet, muss er selbst technische und organisatorische Maßnahmen ergreifen, um die festgestellten Defizite auszugleichen und so die Risiken einer unzulässigen Drittlandsübermittlung zu vermeiden. Diese Maßnahmen können sich an den „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten“ des EDSA orientieren, auch wenn diese für den unmittelbaren Drittlandtransfer konzipiert und daher gegebenenfalls nur entsprechend anwendbar sind (vgl. dazu ausführlich unter Rn. 56 ff.). **40**

[43] Hartung, in: Kühling/Buchner, DSGVO/BDSG, 3. Aufl. 2020, Art. 28 DSGVO Rn. 60.

[44] DSK, Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten, Beschluss vom 31. Januar 2023, Internet: https://www.datenschutz-bayern.de, Rubrik: „Konferenzen“.

**Beispiel 2:** Eine bayerische Schule möchte ein cloudbasiertes Office-Produkt einsetzen, das eine Datenübermittlung in die USA mit sich bringt. Um die Anforderungen der Art. 44 ff. DSGVO erfüllen zu können, beauftragt sie einen IT-Dienstleister mit Sitz in Deutschland, die betreffenden personenbezogenen Daten vor dem Drittlandtransfer angemessen zu verschlüsseln und dann zu exportieren. Zwar ist der IT-Dienstleister als Datenexporteur zu betrachten; ihn treffen daher die konkreten Prüfpflichten des Kapitels V DSGVO. Die Schule muss jedoch trotzdem ihrer Rechenschaftspflicht als Verantwortlicher genügen und die Zuverlässigkeit des Auftragsverarbeiters auch im Hinblick auf den Drittlandtransfer anhand der oben dargestellten Kriterien überprüfen. Dies gilt insbesondere für den Fall, dass auf den IT-Dienstleister als Tochterunternehmen einer Drittlands-Muttergesellschaft drittstaatliches Recht Anwendung finden kann. Prüfung sowie Prüfungsergebnis sind von der Schule entsprechend zu dokumentieren.

## c) Verarbeitungskette

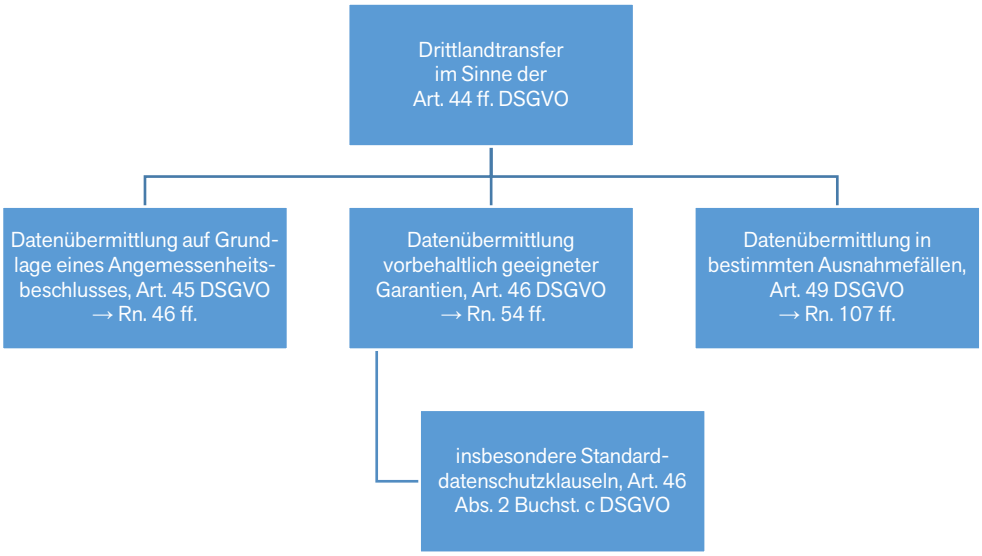
**41** Bei der Einbeziehung eines Unter-Auftragsverarbeiters oder mehrerer Unter-Auftragsverarbeiter in einer „Kette" müssen dem Verantwortlichen gemäß Art. 28 Abs. 4 DSGVO keine eigenen Überprüfungs- und Kontrollrechte gegenüber dem Unter-Auftragsverarbeiter eingeräumt werden. Hier reicht es stattdessen aus, wenn der Auftragsverarbeiter in der Lage ist, seinen Unter-Auftragsverarbeiter zu kontrollieren. Für die Verarbeitungskette bedeutet dies konkret, dass der Verantwortliche nur seinen Auftragsverarbeiter kontrollieren und in diesem Zusammenhang gegebenenfalls eine Plausibilitätsprüfung der Rechtmäßigkeit eines Drittlandtransfers durchführen muss, während er sich darüber hinaus vergewissern muss, dass sein Auftragsverarbeiter wiederum seiner Kontrollpflicht gegenüber den Unter-Auftragsverarbeitern nachkommt; die Vorgaben des Art. 28 Abs. 2 DSGVO sind dabei zu beachten. Die Unterauftragsverarbeitung ist nichtsdestotrotz gemäß Art. 29 DSGVO in erster Linie an die Weisungen des Verantwortlichen und nicht an die des Auftragsverarbeiters gebunden. [45]

**42** **Praxistipp:** Häufig wird die Konstellation anzutreffen sein, dass der Verantwortliche eine Verarbeitungskette „in Gang setzt", von der er – selbst in Unkenntnis der jeweiligen konkreten vertraglichen Regelungen – jedoch von Beginn an weiß, dass es am Ende der Verarbeitungskette zu einem unzulässigen Drittlandtransfer kommen wird, da beispielsweise ein bestimmtes Produkt, das diesen bekanntermaßen erfordert, zum Einsatz kommen soll. Auch wenn hier – den obigen Ausführungen gemäß – eigentlich der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten sämtlicher weiteren Auftragsverarbeiter haftet, wird man vor diesem Hintergrund bereits die Auftragsverarbeitung für unzulässig erachten müssen.

[45] Hartung, in: Kühling/Buchner, DSGVO/BDSG, 3. Aufl. 2020, Art. 28 DSGVO Rn. 86.

## 3. Übersicht über die möglichen Übermittlungsinstrumente

Sollte die Prüfung ergeben, dass ein Drittlandtransfer vorliegt, stehen im Wesentlichen die folgenden drei in Art. 44 ff. DSGVO vorgesehenen Übermittlungsinstrumente zur Verfügung: **43**




## 4. Erstellung eines Datenschutz-Sicherheitskonzepts

Unabhängig davon, ob der Verantwortliche selbst Datenexporteur ist oder nicht, sollte er **als vorbereitende Maßnahme** stets ein **Datenschutz-Sicherheitskonzept** im Rahmen seiner aus Art. 24 DSGVO resultierenden Pflichten erstellen. Das Datenschutz-Sicherheitskonzept sollte insbesondere auf die folgenden Fragen eingehen: **44**

- Welches **Produkt** sollte in welcher Konfiguration und in welcher IT-Umgebung eingesetzt werden?
- Welche **Kategorien personenbezogener Daten** sollen mit dem Produkt verarbeitet werden?
- Welche **nachteiligen Folgen** können sich daraus für die betroffenen Personen im Hinblick auf die Vertraulichkeit, Verfügbarkeit und Integrität ihrer personenbezogenen Daten ergeben? Wie sind diese Folgen und deren Eintrittswahrscheinlichkeiten zu bewerten, und mit welchen Maßnahmen ist ihnen gegebenenfalls zu begegnen?

Zur Beantwortung dieser Fragen kann zunächst auf den einschlägigen BSI-Standard zurückgegriffen werden.[46] Die weitere Bewertung nachteiliger Folgen für die Vertraulichkeit der personenbezogenen Daten wie auch der Implementierung von Maßnahmen zu ihrer Minimierung wird durch Art. 44 ff. DSGVO angeleitet. **45**

[46] Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 203-3. Risikoanalyse auf der Basis von IT-Grundschutz, Internet: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.html.

# IV. Vorliegen eines Angemessenheitsbeschlusses (Art. 45 DSGVO)

**46** Ein für alle Beteiligten vergleichsweise einfaches Transferinstrument stellt der **Angemessenheitsbeschluss** gemäß Art. 45 DSGVO dar. Einen solchen Beschluss erlässt die **Europäische Kommission**, indem sie nach Prüfung der Kriterien des Art. 45 Abs. 2 DSGVO feststellt, dass das betreffende Drittland ein **angemessenes Schutzniveau** bietet. Der Vorteil eines Angemessenheitsbeschlusses liegt vor allem darin, dass er **unmittelbare Wirkung** entfaltet und eine Datenübermittlung in dieses Drittland keiner aufsichtsbehördlichen Genehmigung (vgl. Art. 45 Abs. 1 Satz 2 DSGVO) oder sonstiger Schutzmaßnahmen bedarf. Allerdings kann ein Angemessenheitsbeschluss nicht nur durch die Kommission widerrufen, geändert oder ausgesetzt (vgl. Art. 45 Abs. 5 DSGVO), sondern auch durch den EuGH für ungültig erklärt werden; prominente Beispiele hierfür sind die Urteile in den Rechtssachen **Schrems**[47] und **Schrems II**[48] bezüglich Angemessenheitsbeschlüssen für die USA.

**47** Nach Erlass eines Angemessenheitsbeschlusses muss die Kommission gemäß Art. 45 Abs. 3 Satz 2 DSGVO in regelmäßigen Abständen prüfen, ob das Schutzniveau unverändert geblieben ist, und dabei sämtliche maßgeblichen Entwicklungen im Drittland berücksichtigen; letztere sind gemäß Art. 45 Abs. 4 DSGVO sogar fortlaufend zu überwachen.

**48** Angemessenheitsbeschlüsse oder vergleichbar wirkende Rechtsakte der EU-Kommission sind erlassen

für die folgenden europäischen Staaten und Gebiete:

- die Schweiz,[49]
- das Vereinigte Königreich,[50]

[47] EuGH, Urteil vom 6. Oktober 2015, C-362/14.

[48] EuGH, Urteil vom 16. Juli 2020, C-311/18.

[49] Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz (2000/518/EG, ABl. Nr. L 215 vom 25. August 2000, S. 1), geändert durch Durchführungsbeschluss (EU) 2016/2295 der Kommission vom 16. Dezember 2016 zur Änderung der Entscheidungen beziehungsweise Beschlüsse 2000/518/EG, 2002/2/EG, 2003/490/EG, 2003/821/EG, 2004/411/EG, 2008/393/EG, 2010/146/EU, 2010/625/EU, 2011/61/EU und Durchführungsbeschlüsse 2012/484/EU sowie 2013/65/EU über die Angemessenheit des Schutzes personenbezogener Daten in bestimmten Drittländern gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (ABl. Nr. L 344 vom 17. Dezember 2016, S. 83).

[50] Durchführungsbeschluss [unzutreffender amtlicher Titel: Durchführungsverordnung] (EU) 2021/1772 der Kommission vom 28. Juni 2021 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zur Angemessenheit des Schutzes personenbezogener Daten durch das Vereinigte Königreich (ABl. Nr. L 360 vom 11. Oktober 2021, S. 1).

- die nicht zu diesem gehörenden Inseln Guernsey,[51] Jersey[52] und Man,[53]
- Andorra,[54]
- die Färöer-Inseln;[55]

für die folgenden amerikanischen Staaten:

- Kanada,[56]
- Argentinien,[57]
- Uruguay;[58]

für die folgenden asiatischen Staaten:

- Israel,[59]
- Japan,[60]

[51] Entscheidung der Kommission vom 21. November 2003 über die Angemessenheit des Schutzes personenbezogener Daten in Guernsey (2003/821/EG, ABl. Nr. L 308 vom 25. November 2003, S. 27, geändert durch Durchführungsbeschluss (EU) 2016/2295 (Fn. 49).

[52] Entscheidung der Kommission vom 8. Mai 2008 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Jersey (2008/393/EG, ABl. L 138 vom 28. Mai 2008, S. 21, geändert durch Durchführungsbeschluss (EU) 2016/2295 (Fn. 49).

[53] Entscheidung der Kommission vom 28. April 2004 über die Angemessenheit des Schutzes personenbezogener Daten auf der Insel Man (2004/411/EG, ABl. Nr. L 151 vom 30. April 2004, S. 51, ber. ABl. L 208 vom 10. Juni 2004, S. 47), geändert durch Durchführungsbeschluss (EU) 2016/2295 (Fn. 49).

[54] Beschluss der Kommission vom 19. Oktober 2010 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Andorra (2010/625/EU, ABl. Nr. L 277 vom 21. Oktober 2010, S. 27), geändert durch Durchführungsbeschluss (EU) 2016/2295 (Fn. 49).

[55] Beschluss der Kommission vom 5. März 2010 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus, den das färöische Gesetz über die Verarbeitung personenbezogener Daten bietet (2010/146/EU, ABl. Nr. L 58 vom 9. März 2010, S. 17), geändert durch Durchführungsbeschluss (EU) 2016/2295 (Fn. 49).

[56] Entscheidung der Kommission vom 20. Dezember 2001 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet (2002/2/EG, ABl. Nr. L 2 vom 4. Januar 2002, S. 13), geändert durch Durchführungsbeschluss (EU) 2016/2295 (Fn. 49).

[57] Entscheidung der Kommission vom 30. Juni 2003 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Argentinien (2003/490/EG, ABl. Nr. L 168 vom 5. Juli 2003, S. 19), geändert durch Durchführungsbeschluss (EU) 2016/2295 (Fn. 49).

[58] Durchführungsbeschluss der Kommission vom 21. August 2012 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in der Republik Östlich des Uruguay im Hinblick auf die automatisierte Verarbeitung personenbezogener Daten (2012/484/EU, ABl. Nr. L 227 vom 23. August 2012, S. 11), geändert durch Durchführungsbeschluss (EU) 2016/2295 (Fn. 49).

[59] Beschluss der Kommission vom 31. Januar 2011 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus im Staat Israel im Hinblick auf die automatisierte Verarbeitung personenbezogener Daten (2011/61/EU, ABl. Nr. L 27 vom 1. Februar 2011, S. 39), geändert durch Durchführungsbeschluss (EU) 2016/2295 (Fn. 49).

[60] Durchführungsbeschluss (EU) 2019/419 der Kommission vom 23. Januar 2019 nach der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Japan im Rahmen des Gesetzes über den Schutz personenbezogener Informationen (ABl. Nr. L 76 vom 19. März 2019, S. 1).

– Republik Korea (Südkorea);[61]

außerdem für Neuseeland.[62]

**49** Die Angemessenheitsbeschlüsse bezüglich Kanada und Israel gelten jeweils **nur partiell** (vgl. Art. 45 Abs. 1 Satz 1 DSGVO): In Kanada fallen darunter nur private Unternehmen, die dem kanadischen Personal Information Protection and Electronic Documents Act unterliegen, d.h. die im Rahmen einer kommerziellen Tätigkeit personenbezogene Daten verarbeiten.[63] Im Fall von Israel bezieht sich der Angemessenheitsbeschluss lediglich auf automatisierte Verarbeitungen im Staat Israel im Sinne des Völkerrechts; ausgeschlossen sind folglich die Golanhöhen, der Gazastreifen und das Westjordanland einschließlich Ost-Jerusalem.[64]

**50** **Praxistipp:** Vor Übermittlung von personenbezogenen Daten an einen Empfänger außerhalb der EU bzw. des EWR sollte daher stets zunächst die aktuelle Liste der Angemessenheitsbeschlüsse der Europäischen Kommission geprüft werden.[65] Sofern für das Empfängerland ein Angemessenheitsbeschluss besteht, können die Daten ohne diesbezüglich weitere Prüfung übermittelt werden.

**51** Am 25. März 2022 gaben die Europäische Kommission und die USA bekannt, dass sie sich grundsätzlich auf einen neuen Transatlantischen Datenschutzrahmen (**Trans-Atlantic Data Privacy Framework**) geeinigt haben, der den transatlantischen Datenverkehr fördert und gleichzeitig den Bedenken des EuGH Rechnung trägt.[66] Darin verpflichten sich die USA zu Reformen, die den Schutz der Privatsphäre und der bürgerlichen Freiheiten stärken werden. Dem Transatlantischen Datenschutzrahmen waren mehr als einjährige Verhandlungen vorausgegangen.

[61] Durchführungsbeschluss (EU) 2022/254 der Kommission vom 17. Dezember 2021 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten durch die Republik Korea im Rahmen des koreanischen Gesetzes über den Schutz personenbezogener Daten (ABl. Nr. L 44 vom 24. Februar 2022, S. 1).

[62] Durchführungsbeschluss der Kommission vom 19. Dezember 2012 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Neuseeland (2013/65/EU, ABl. Nr. L 28 vom 30. Januar 2013, S. 12), geändert durch Durchführungsbeschluss (EU) 2016/2295 (Fn. 49).

[63] Art. 1 in Verbindung mit Erwägungsgrund 5 der Entscheidung 2002/2/EG der Kommission vom 20. Dezember 2001 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet, K(2001) 4539 (ABl. Nr. L 2 vom 4. Januar 2002, S. 13-16), geändert durch VO (EU) 2016/2295 der Kommission vom 16. Dezember 2016 (ABl. Nr. L 344 vom 17. Dezember 2016, S. 83).

[64] Erwägungsgrund 14 des Beschlusses 2011/61/EU der Kommission vom 31. Januar 2011 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus im Staat Israel im Hinblick auf die automatisierte Verarbeitung personenbezogener Daten, K(2011) 332 (ABl. Nr. L 27 vom 1. Februar 2011, S. 39-42), geändert durch VO (EU) 2016/2295 der Kommission vom 16. Dezember 2016 (ABl. Nr. L 344 vom 17. Dezember 2016, S. 83).

[65] Internet: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de.

[66] Vgl. Gemeinsame Erklärung der Europäischen Kommission und der Vereinigten Staaten zum Transatlantischen Datenschutzrahmen vom 25. März 2022, Internet: https://ec.europa.eu/commission/presscorner/detail/de/ip_22_2087.

Die intensive Zusammenarbeit wird nun fortgesetzt; dabei hat US-Präsident Biden am 7. Oktober 2022, wie angekündigt, die Selbstverpflichtungen in die Durchführungsverordnung (Executive Order) „Enhancing Safeguards for United States Signals Intelligence Activities“ überführt.[67] Diese sieht zum einen verbindliche Garantien vor, die den Zugriff auf Daten durch US-Geheimdienste auf das zum Schutz der nationalen Sicherheit erforderliche und angemessene Maß beschränken. Der Begriff der „Verhältnismäßigkeit“ hält damit Einzug in das US-amerikanische Recht, wobei damit nicht notwendigerweise auch dasselbe Verständnis des Begriffs beiderseits des Atlantiks verbunden ist. Zum anderen wird als Kontrollinstanz der „Civil Liberties Protection Officer“ („CLPO“) eingeführt, der jede neue nachrichtendienstliche Maßnahme bewerten muss. Überdies soll ein unabhängiger und unparteiischer Rechtsbehelfsmechanismus geschaffen werden, bei dem der CLPO auf einer ersten Stufe auch Beschwerden von Betroffenen über den Zugriff auf ihre Daten durch nationale US-Sicherheitsbehörden nachgehen und Abhilfemaßnahmen, wie zum Beispiel die Löschung von Daten, anordnen kann. Auf einer zweiten Stufe überprüft der neu errichtete „Data Protection Review Court“ („DPRC“) die Beschwerden von EU-Bürgern bezüglich Entscheidungen und Abhilfemaßnahmen auf der ersten Stufe. Seine Entscheidungen sind für die Sicherheitsbehörden bindend. Dass der von der Legislative erlassene FISA damit durch die Exekutive in seiner Wirkung beschränkt wird, ist gemäß der US-amerikanischen Verfassung – im Gegensatz zum deutschen Grundgesetz – im Übrigen kein Hinderungsgrund; Executive Orders haben die gleiche Wirkung wie Gesetze. Der Erlass der Executive Order, der zeigt, dass die USA die vom EuGH geäußerte Kritik offenbar ernst genommen haben, soll nun als Grundlage für die Bewertung der Kommission in ihrem künftigen Angemessenheitsbeschluss dienen. Dieser liegt seit dem 13. Dezember 2022 als Entwurf vor.[68] Dazu hat der EDSA am 28. Februar 2023 eine unverbindliche Stellungnahme abgeben;[69] zusätzlich muss ein Ausschuss, der sich aus Vertretern der EU-Mitgliedstaaten zusammensetzt, den Vorschlag mit qualifizierter Mehrheit billigen. Auch das EU-Parlament kann sich in einer formellen Stellungnahme äußern. Deshalb ist derzeit noch nicht absehbar, wann der neue Angemessenheitsbeschluss in Kraft treten kann (voraussichtlich nicht vor Sommer 2023).[70] **52**

**Praxistipp:** Da gerade Datenübermittlungen in die USA aufgrund der Vielzahl der dort ansässigen und für die bayerischen öffentlichen Stellen bedeutsamen Dienstleister von hoher Praxisrelevanz sind, ist es dringend anzuraten, die weiteren Entwicklungen aufmerksam zu verfolgen und den einschlägigen aufsichtsbehördlichen Empfehlungen zu folgen. Bis zum Erlass des Angemessenheitsbeschlusses ändert sich – trotz der neuen Entwicklungen in den USA – **53**

67 Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities vom 7. Oktober 2022, Internet: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/.

68 Vgl. Adequacy decision for the EU-US Data Privacy Framework, Internet: https://commission.europa.eu/document/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en.

69 EDSA, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, 28 February 2023, Internet: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_de.

70 Vgl. Äußerung des EU-Kommissars Didier Reynders bei einer Pressekonferenz am 30. März 2022, Internet: https://audiovisual.ec.europa.eu/en/video/I-222851; vgl. Questions & Answers: EU-U.S. Data Privacy Framework der Europäischen Kommission, Internet: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045.

für bayerische öffentliche Stellen zunächst nichts. Immerhin setzt die Inanspruchnahme des neuen Rechtsmittelmechanismus' auch voraus, dass die USA wiederum die EU-Mitgliedstaaten als „qualifizierte Staaten", die den US-Anforderungen an eine Rechtsstaatlichkeit genügen, formal anerkannt haben, was bislang noch nicht geschehen ist.

# V. Vorsehen geeigneter Garantien (Art. 46 DSGVO)

Art. 46 Abs. 1 DSGVO gestattet die Datenübermittlung an ein Drittland, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Da für einen Angemessenheitsbeschluss hohe Hürden zu überwinden sind, weshalb er nur für einige wenige Drittländer besteht, kommt den im Sinne von Art. 46 DSGVO geeigneten – vor allem vertraglichen – **Garantien eine wichtige Funktion** zu. Gemäß Erwägungsgrund 108 DSGVO sollten die Garantien „sicherstellen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen auf eine der Verarbeitung innerhalb der Union angemessene Art und Weise beachtet werden". Den Begriff „angemessen" hat der EuGH in seinem „Schrems II"-Urteil konkretisiert. Danach müssen „die geeigneten Garantien so beschaffen sein, dass sie für Personen, deren personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt werden – wie im Rahmen einer auf einen Angemessenheitsbeschluss gestützten Übermittlung –, **ein Schutzniveau gewährleisten, das dem in der Union garantierten Schutzniveau der Sache nach gleichwertig ist**."[71] **54**

Dabei reicht es nicht aus, eine der in Art. 46 Abs. 2 DSGVO genannten Garantien als Übermittlungsinstrument auszuwählen; vielmehr muss der Datenexporteur prüfen, ob die Rechtslage im Drittland dem Datenimporteur überhaupt die Einhaltung der etwaigen vertraglichen Verpflichtungen ermöglicht. Ist dies nicht der Fall, muss der Datenexporteur **zusätzliche Maßnahmen** ergreifen, die geeignet sind, die Einhaltung dieses Schutzniveaus zu gewährleisten.[72] Das spiegelt sich auch im Wortlaut von Art. 46 Abs. 2 DSGVO wider, wonach geeignete Garantien in einem der aufgelisteten Instrumente bestehen „können", aber nicht müssen. **55**

## 1. Sechs-Schritte-Prüfung gemäß EDSA

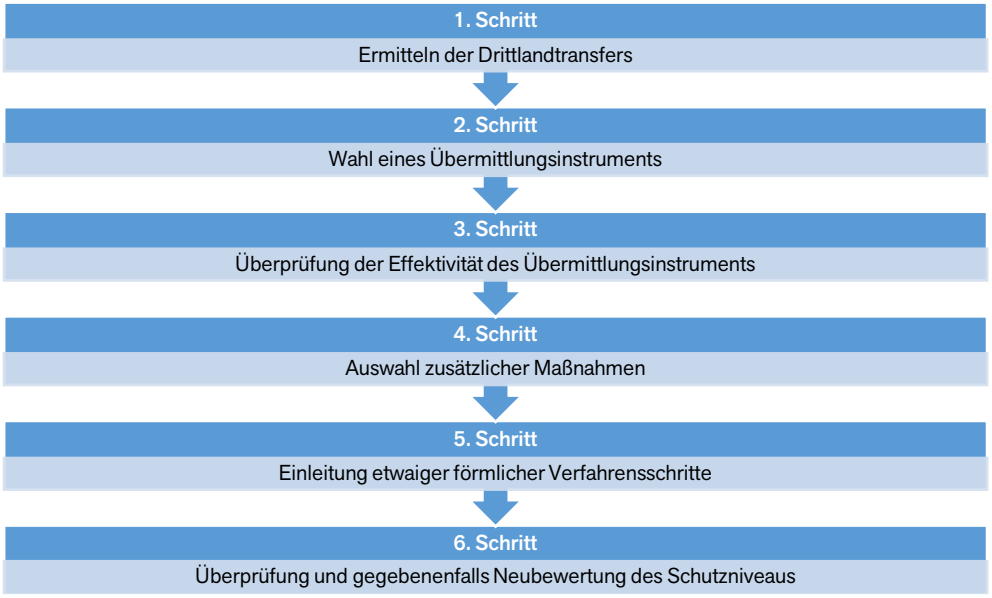
Für die Umsetzung der Vorgaben des „Schrems II"-Urteils für einen Drittlandtransfer hat der EDSA die „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten"[73] (**„Recommendations"**) beschlossen, die vor allem für eine auf Art. 46 DSGVO gestützte Datenübermittlung herangezogen werden sollten. Sie sehen eine Sechs-Schritte-Prüfung vor, um die Datenschutzsituation in einem Drittland zu beurteilen; außerdem erläutert der EDSA anhand von Beispielen, ob zusätzliche Maßnahmen etwaige Rechtsschutzlücken schließen können oder ob dies nicht möglich ist. **56**

71 EuGH, Urteil vom 16. Juli 2020, C-311/18, Rn. 96.

72 EuGH, Urteil vom 16. Juli 2020, C-311/18, Rn. 131 ff..

73 Siehe Fn. 17.

**57** Die sechs Schritte der Empfehlungen des EDSA lauten im Überblick wie folgt:




## a) Ermitteln der Datenübermittlungen

**58** Der Datenexporteur muss in einem **ersten Schritt** folglich die potentiellen Drittlandübermittlungen ermitteln und erfassen (**„know your transfers“**). Es muss also festgestellt werden,

- welche Kategorien personenbezogener Daten
- in welchem Umfang
- auf welchen Übermittlungswegen
- an welche Adressaten in Drittländern übermittelt werden und
- mit welchen technischen und organisatorischen Mitteln diese Übermittlungen gesichert werden.

**59** Hier kann insbesondere auf das Verzeichnis von Verarbeitungstätigkeiten, das der Verantwortliche oder Auftragsverarbeiter gemäß Art. 30 DSGVO führen muss, zurückgegriffen werden. Bei der Erfassung der Übermittlungen sind auch Weiterübermittlungen einzubeziehen, wenn zum Beispiel die für den Datenexporteur tätigen Auftragsverarbeiter außerhalb des EWR die personenbezogenen Daten, die sie vom Datenexporteur empfangen haben, an einen Unterauftragsverarbeiter in einem anderen oder im selben Drittland übermitteln. Denn für diesen Fall ist gemäß Art. 28 Abs. 2 DSGVO stets die vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen erforderlich.[74]

**60** Überdies muss der Datenexporteur beachten, dass die von ihm übermittelten Daten für die Verarbeitungszwecke angemessen und erheblich sowie auf das notwendige Maß beschränkt sind (Grundsatz der Datenminimierung, vgl. Art. 5 Abs. 1 Buchst. c DSGVO).[75]

[74] EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 10.
[75] EDSA, Empfehlungen 01/2020 (Fn.17), Rn. 8 ff.

## b) Wahl des Übermittlungsinstruments

In einem **zweiten Schritt** wählt der Datenexporteur eines der in Art. 44 ff. DSGVO aufgeführten Übermittlungsinstrumente. Falls für das betreffende Drittland ein Angemessenheitsbeschluss der Kommission gemäß Art. 45 DSGVO vorliegt, ist die Prüfung hiermit beendet (vgl. auch Rn. 46 ff.).[76] 61

## c) Prüfung der Wirksamkeit des gewählten Übermittlungsinstruments

Sofern der Datenexporteur sich für die Datenübermittlung mithilfe geeigneter Garantien gemäß Art. 46 DSGVO entschieden hat, muss er in einem **dritten Schritt** prüfen, ob die **Effektivität** des gewählten Übermittlungsinstruments möglicherweise durch die Rechtsvorschriften oder Praktiken der Behörden des Drittlands **beeinträchtigt** wird.[77] Entscheidend ist insofern das gesetzliche wie auch das tatsächlich „gelebte" Datenschutzniveau im Drittland. Diese Prüfung wird auch als **„Transfer Impact Assessment"** (Datentransfer-Folgenabschätzung, kurz „TIA") bezeichnet. Wenn der Datenexporteur zugleich der Verantwortliche ist, dient als Ausgangspunkt aller Überlegungen das Datenschutz-Sicherheitskonzept (vgl. Rn. 44 f.). Der Datenexporteur muss im Rahmen des Transfer Impact Assessment zunächst prüfen, ob seine Übermittlung **in den Anwendungsbereich von Rechtsvorschriften oder Praktiken** fällt, die die Wirksamkeit seines Übermittlungsinstruments beeinträchtigen können. Diese Beurteilung, die vor allem auf die öffentlich zugänglichen Rechtsvorschriften zu stützen ist, muss Angaben dazu enthalten, 62

- ob Behörden des Drittlands unter Berücksichtigung der Rechtsvorschriften, der Praxis und der gemeldeten Präzedenzfälle mit oder ohne Wissen des Datenimporteurs **um Zugriff auf die Daten ersuchen können** und
- ob sie aufgrund der ihnen zur Verfügung stehenden Rechtsvorschriften, rechtlichen Befugnisse, technischen, finanziellen und personellen Ressourcen und der gemeldeten Präzedenzfälle über den Datenimporteur oder über die Telekommunikationsanbieter oder Kommunikationskanäle **auf die Daten zugreifen können**.[78]

Welche Rechtsvorschriften und Praktiken einschlägig sind, wird auch von folgenden Faktoren abhängen, die zugleich bei der Folgenabschätzung helfen können:[79] 63

- **Art, Inhalt und Sensibilität der Daten:** Übertragene Daten, die „foreign intelligence" beinhalten, also Themen wie Verteidigung, Politik, Energieversorgung, Geldwäsche, sind für Behörden eines Drittlands besonders von Interesse und deshalb gegebenenfalls einem

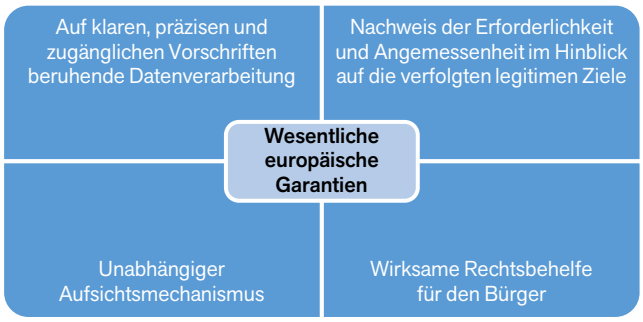
[76] EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 14 ff.
[77] EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 28 ff.
[78] EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 31.
[79] Vgl. Darstellung bei Jungkind/Raspé/Schramm, Risikoanalyse und zusätzliche Maßnahmen – Konzerninterner US-Datentransfer nach „Schrems II", NZG 2020, S. 1056, 1057 f. Dazu auch EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 33.

behördlichen Zugriff eher ausgesetzt als andere Daten. Sensible Daten wie Gesundheitsdaten dürfen nur unter strengen Voraussetzungen verarbeitet werden und müssen aus diesem Grund bei der Folgenabschätzung besonders berücksichtigt werden.

- **Umfang, Häufigkeit und Zweckbindung der Datenübermittlung:** Große Datensätze, häufige Übermittlungen sowie eine relativ offene Zweckbindung erhöhen die Wahrscheinlichkeit eines behördlichen Zugriffs im Drittland und sind daher auf ihre Notwendigkeit hin zu überprüfen.
- **Adressat des Datentransfers:** Gerade große Telekommunikationsunternehmen stehen regelmäßig im Fokus von Geheimdiensten. Daher ist Datenübermittlungen mit Hilfe von Cloud-Diensten oder externen E-Mail-Servern im Rahmen der Folgenabschätzung besondere Beachtung zu schenken.

**64** Dass sich die aus den Rechtsvorschriften und Praktiken ergebenden Verpflichtungen oder Befugnisse nachteilig auf die Verpflichtungen aus dem Übertragungsinstrument gemäß Art. 46 DSGVO auswirken oder damit unvereinbar sind, ist dann anzunehmen, wenn sie den **Wesensgehalt der Grundrechte und Grundfreiheiten der Charta der Grundrechte der Europäischen Union** nicht achten oder über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist, um eines der wichtigen Ziele zu wahren, die auch im Unionsrecht oder im Recht der Mitgliedstaaten anerkannt sind.[80]

**65** Der EDSA gibt mit weiteren Empfehlungen[81] eine Hilfestellung, welche die folgenden **vier wesentlichen europäischen Garantien** zugrundelegt und Orientierung bietet zum einen für die Beurteilung der Frage, ob der rechtliche Rahmen, der in einem Drittland für den Zugriff staatlicher Stellen auf personenbezogene Daten gilt, als gerechtfertigter Eingriff angesehen werden kann oder nicht.[82] Zum anderen gehen die Empfehlungen auf die Frage ein, ob die betreffenden behördlichen Befugnisse den Datenimporteur in nicht gerechtfertigter Weise daran hindern, seiner Verpflichtung zur Sicherstellung einer Gleichwertigkeit der Sache nach im Sinne der Datenschutz-Grundverordnung oder seinen Verpflichtungen im Rahmen des Übertragungsinstruments nachzukommen.[83]




80 EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 38.

81 EDSA, Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, Stand 11/2020, Internet: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_de.

82 EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 41.

83 EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 42.

Die wesentlichen europäischen Garantien dienen somit als **Maßstab für die Bewertung von Grundrechtseingriffen**, die im Rahmen internationaler Datenübermittlungen in Verbindung mit Überwachungsmaßnahmen eines Drittlands erfolgen. 66

Die Durchführung der Prüfung impliziert eine **rechtliche Bewertung** der für die Datenübermittlung relevanten Vorschriften im Drittland, was eine umfangreiche Kenntnis des dortigen Rechts erfordert. **Mögliche Informationsquellen** für die Beurteilung finden sich beispielsweise in Anhang 3 der „Empfehlungen"; so zählen dazu auch Transparenzberichte.[84] Eine etwaige Versicherung des Vertragspartners, dass „bislang ja nie etwas passiert sei", hat der Datenexporteur hingegen außer Acht zu lassen; eine reine Wahrscheinlichkeitsbetrachtung ist nicht angezeigt. 67

**Praxistipp:** Diese Prüfung wird häufig sehr komplex sein und den Datenexporteur vor erhebliche Schwierigkeiten stellen, die er ohne juristische Expertise aus dem jeweiligen Drittland kaum bewältigen kann. Daher kann es im Einzelfall empfehlenswert sein, bei der Prüfung in Schritt 3 **eine Beeinträchtigung der Effektivität der geeigneten Garantien anzunehmen** – zumal es fast immer „etwas"[85] geben wird, das die Wirksamkeit der angemessenen Sicherheitsvorkehrungen der Übermittlungsinstrumente beeinträchtigen könnte.[86] 68

Auch für den Fall, dass eine Übermittlung etwa **in den Anwendungsbereich von Section 702 des US-amerikanischen FISA oder von Executive Order 12.333** fällt, kann der Datenexporteur sogleich mit Schritt 4 fortfahren, da der EuGH bereits deren Unvereinbarkeit mit dem unionsrechtlichen Verhältnismäßigkeitsgrundsatz im Rahmen der Prüfung des Angemessenheitsbeschlusses zum EU-US Privacy Shield festgestellt hat. Daher kann nicht angenommen werden, dass beispielsweise der (bloße) Abschluss von Standardvertragsklauseln ein angemessenes Schutzniveau gemäß Art. 44 DSGVO für die betreffende Datenübermittlung gewährleistet.

Zum aktuellen Stand des US-Überwachungsrechts hat die DSK das von ihr in Auftrag gegebene **Gutachten des US-Rechtsexperten Stephen Vladeck** veröffentlicht.[87] Dieses kann allerdings nicht abschließend den persönlichen Anwendungsbereich von Section 702 FISA („Anbieter von elektronischer Kommunikation") klären, in den möglicherweise auch Banken, Fluggesellschaften, Hotels oder Versanddienstleister fallen. Zudem muss es – erwartungsgemäß – verneinen, dass zum Zeitpunkt der Fertigstellung des Gutachtens allen Betroffenen in der EU/im EWR gemäß US-amerikanischem Recht Rechtsbehelfe zur Verfügung stehen, die den Anforderungen des Art. 47 GRCh genügen. Eine Ausnahme hierzu stellt zum Beispiel der CLOUD Act dar, wonach die Unternehmen die behördliche Anfrage anfechten können, wenn die Forderung die Datenschutzrechte des Landes verletzt, in dem die Daten

84 EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 144 ff.

85 Vgl. die sehr offen gehaltene Formulierung „anything" in der englischen Fassung, EDSA, Recommendations 01/2020 (Fn. 17), Rn. 30, Internet: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

86 Vgl. Spies, EU-US-Privacy-Shield – eine schwierige Reparatur. Probleme bei den Verhandlungen und Schwierigkeiten mit der Risikoanalyse des EDSA, ZD 2021, S. 478 (479).

87 Internet: https://www.datenschutzkonferenz-online.de/weitere_dokumente.html.

gespeichert sind.[88] Zu dem Gutachten liegt bislang nur eine kurze Erstbewertung durch die DSK vor.[89]

Auf dieser Grundlage kann bis auf Weiteres nur empfohlen werden, bei Schritt 3 im Zweifelsfall die Beeinträchtigung der Wirksamkeit der geeigneten Garantien zu bejahen.

**69** Nur auf **Ausnahmefälle** wird die in Nr. 43.3 der EDSA-Empfehlungen geschilderte Konstellation zutreffen: Danach kann der Datenexporteur bei seiner Beurteilung zu dem Schluss kommen, die Übermittlung vorzunehmen, **ohne zusätzliche Maßnahmen zu ergreifen**, obwohl einschlägige Rechtsvorschriften möglicherweise problematisch sind und auf die konkrete Übermittlung anwendbar sein könnten. Voraussetzung ist, dass der Datenexporteur keinen Grund zur Annahme hat, dass diese auf seine übermittelten Daten und/oder auf den Datenimporteur angewandt werden. Diese Annahme muss er durch einen ausführlichen Bericht bezüglich der rechtlichen Würdigung der Rechtsvorschriften und der entsprechenden Praxis, wobei auch die am Bericht mitwirkenden Akteure, wie zum Beispiel Anwaltskanzleien, Berater oder interne Dienststellen, zu nennen sind, begründen und dokumentieren.[90]

**70** **Praxistipp:** Dies würde bedeuten, dass der Datenexporteur die zu übermittelnden Daten nach dem Gefährdungspotential für eine Datensammlung durch Geheimdienste und Sicherheitsbehörden einteilen und die Datenübermittlungen, die für Geheimdienste vermutlich irrelevant sind, von der Folgenabschätzung ausschließen könnte.[91]

Den Nachweis zu erbringen, dass die zu übermittelnden personenbezogenen Daten von vornherein nicht Gegenstand der betreffenden Zugriffsrechte von Geheimdiensten und Sicherheitsbehörden werden können, wird mit erheblichen Schwierigkeiten verbunden sein. Auch hier gilt, im Zweifelsfall eine Beeinträchtigung der Wirksamkeit der geeigneten Garantien zu bejahen.

## d) Auswahl und Anwendung zusätzlicher Maßnahmen

**71** Sofern sich durch die Prüfung im Rahmen von Schritt 3 ergibt, dass die Effektivität des Übermittlungsinstruments beeinträchtigt ist, wählt der Datenexporteur im **vierten Schritt zusätzliche Maßnahmen** aus, um für die übermittelten Daten ein **Schutzniveau zu erzielen, das dem unionsrechtlichen Standard gleichwertig** ist.[92] Auch hier gilt es für den Datenexporteur, die Effektivität der zusätzlichen Maßnahmen im Hinblick auf eine mögliche Beeinträchtigung durch die Rechtsvorschriften sowie die Praktiken im Drittland zu prüfen. Dabei muss die

[88] Vladeck, Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse vom 15. November 2021, S.14 f., Internet: https://www.datenschutzkonferenz-online.de/weitere_dokumente.html.

[89] DSK, Wesentliche Befunde des Gutachtens von Stephen I. Vladeck vom 15. November 2021 zur Rechtslage in den USA vom 25. Januar 2022, Internet: https://www.datenschutzkonferenz-online.de/weitere_dokumente.html.

[90] EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 43.3.

[91] Vgl. zu diesem risikobasierten Ansatz ausführlich Spies, EU-US-Privacy-Shield – eine schwierige Reparatur. Probleme bei den Verhandlungen und Schwierigkeiten mit der Risikoanalyse des EDSA, ZD 2021, S. 478 (480 f.).

[92] EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 50 ff.

zusätzliche Maßnahme genau die spezifischen Mängel beheben, die der Datenexporteur bei seiner Prüfung im dritten Schritt ermittelt hat.[93]

Die zusätzlichen Maßnahmen können **technischer, vertraglicher oder organisatorischer Natur** sein. Dabei sind sowohl **vertragliche als auch organisatorische Maßnahmen** nach Ansicht des EDSA **allein regelmäßig nicht ausreichend**, um ein angemessenes Schutzniveau sicherzustellen. Gerade wenn der Datenzugriff zu Überwachungszwecken erfolgt, können nur technische Maßnahmen den Zugriff staatlicher Stellen im Drittland auf personenbezogene Daten verhindern oder ineffektiv werden lassen.[94] Beispiele für technische, vertragliche und organisatorische Maßnahmen, die zusätzlich ergriffen werden können, sind in Anhang 2 der Empfehlungen aufgelistet.[95] Sofern der Datenexporteur zu dem Ergebnis kommt, dass **keinerlei zusätzliche Maßnahmen** im Rahmen der Datenübermittlung ein gleichwertiges Schutzniveau sicherstellen können, muss er die **Übermittlung vermeiden, aussetzen oder beenden**. 72

## aa) Zusätzliche technische Maßnahmen

Behörden in Drittländern können auf Daten zum einen während der Übermittlung durch Zugriff auf die Kommunikationsleitungen zugreifen, zum anderen, während sie sich im Besitz des vorgesehenen Datenempfängers befinden. Zur letztgenannten Konstellation sind auch die Fälle zu zählen, in denen der Datenempfänger angehalten wird, die gewünschten Daten an die Behörden herauszugeben. Für beide Fälle können technische Maßnahmen insbesondere in Form der **Verschlüsselung und Pseudonymisierung** geeignete zusätzliche Maßnahmen darstellen. An eine entsprechend ausreichend gesicherte **Verschlüsselung** sind nach Ansicht des EDSA folgende Anforderungen zu stellen:[96] 73

- **Angemessen starke Verschlüsselungsmethode:** Der Verschlüsselungsalgorithmus und seine Parametrisierung (z. B. Schlüssellänge, Verschlüsselungsstärke, Betriebsmodus) müssen angemessen sein und den spezifischen Zeitraum berücksichtigen, für den die Vertraulichkeit der verschlüsselten personenbezogenen Daten sicherzustellen ist.
- **Besonderer Schutz der Schlüssel:** Die Schlüssel müssen allein durch den Datenexporteur verwaltet und kontrolliert werden. Dadurch wird ein Zugriff auf unverschlüsselte Daten (Klardaten) durch unberechtigte Dritte mit Hilfe einer Ende-zu-Ende-Verschlüsselung ausgeschlossen. Zudem liefe eine zum Beispiel auf Section 702 FISA beruhende Verpflichtung des Datenimporteurs zur Herausgabe des kryptographischen Schlüssels ins Leere. Außerdem muss der Verschlüsselungsalgorithmus fehlerfrei durch ordnungsgemäß gepflegte Software implementiert sein, deren Konformität mit der Spezifikation des ausgewählten Algorithmus etwa durch Zertifizierung bestätigt wurde. Die Verschlüsselung muss – unter Berücksichtigung der zur Verfügung stehenden Ressourcen und technischen Möglichkeiten (z. B. Rechenleistung für Brute-Force-Angriffe) – Robustheit gegen eine eventuell durchgeführte Kryptoanalyse bieten. Ferner muss im Hinblick auf die

93 EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 75.
94 EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 53.
95 EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 74 ff.
96 EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 79 ff.

Schlüssel, deren Generierung und Einsatz ein angemessener Schutz durch technische und organisatorische Maßnahmen gegen unbefugte Zugriffe, gegen unbefugte Veränderungen sowie gegen Störung der erforderlichen Verfügbarkeit bestehen.

– **Stand der Technik:** Das eingesetzte Verschlüsselungsverfahren muss grundsätzlich dem Stand der Technik entsprechen. Die Wirksamkeit der Verschlüsselung als datenschutzrechtliche Schutzmaßnahme muss durch bedarfsgerechte Überprüfungen durchgängig gewährleistet sein.

**Beispiel 3:** Eine Gemeinde nutzt einen Anbieter in einem Drittland zur Speicherung von Daten zu Backup-Zwecken. Falls die Daten vor der Übermittlung nach dem Stand der Technik stark verschlüsselt wurden und die Kontrolle über die Schlüssel allein bei der Gemeinde liegt, so dass der Anbieter weder Zugriff auf die unverschlüsselten Daten noch auf den Schlüssel hat, stellt die vorgenommene Verschlüsselung – die Position des EDSA zugrunde gelegt – eine effektive zusätzliche Maßnahme dar.

Wenn aber der Datenimporteur, beispielsweise ein Cloud-Service-Anbieter als Auftragsverarbeiter, Zugang zu unverschlüsselten Daten benötigt, um die Daten auftragsgemäß für den Datenexporteur zu verarbeiten, die Daten aber nicht pseudonymisiert sind oder nicht pseudonymisiert werden können und zugleich die den Behörden des Drittlands eingeräumte Befugnis, auf die betreffenden übermittelten Daten zuzugreifen, über das hinausgeht, was in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist, ist nach dem heutigen Stand der Technik keine wirksame technische Maßnahme vorstellbar, die eine Datenschutzverletzung verhindern könnte. Dies gilt auch für Transportverschlüsselungen und Data-at-Rest-Verschlüsselungen, selbst wenn sie kombiniert angewandt werden.

**74** Eine ausreichend sicher gestaltete **Pseudonymisierung** kann laut EDSA insbesondere unter den folgenden Voraussetzungen in Betracht kommen:[97]

– **Angemessen starke Pseudonymisierungsmethode:** Personenbezogene Daten werden so verarbeitet, dass sie ohne Hinzuziehung zusätzlicher Informationen weder einer spezifischen betroffenen Person zugeordnet noch dazu verwendet werden können, die betroffene Person in einer größeren Gruppe zu identifizieren. Zudem darf ein Abgleich mit sämtlichen Informationen, die Dritten zur Verfügung stehen, nicht dazu führen, dass die pseudonymisierten Daten identifizierten oder identifizierbaren natürlichen Personen zugeordnet werden können.

– **Besonderer Schutz der Zuordnungsregeln:** Die Zuordnung der pseudonymisierten Daten zu Identitätsinformationen („Zuordnungsregeln", z. B. Datentabelle oder Formel) und damit die Re-Identifizierung darf nur durch den Datenexporteur möglich sein. Zudem müssen die Zuordnungsregeln grundsätzlich innerhalb der EU gehalten und einem angemessenen Schutz durch technische und organisatorische Maßnahmen gegen unbefugte Zugriffe, gegen unbefugte Veränderungen sowie gegen Störung der erforderlichen Verfügbarkeit unterliegen.

– **Stand der Technik:** Das eingesetzte Pseudonymisierungsverfahren muss dem Stand der Technik entsprechen. Die Wirksamkeit der Pseudonymisierung als datenschutzrechtliche

[97] EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 79 ff.

Schutzmaßnahme muss durchgängig gewährleistet sein, was durch bedarfsgerechte Überprüfung stetig sicherzustellen ist.

**Beispiel 4:** Für die Nutzung des Office-Produkts aus Beispiel 2 müssen für die Schülerinnen und Schüler E-Mail-Accounts angelegt werden. Dafür verwendet die Schule nicht die Klarnamen der Schülerinnen und Schüler, sondern Pseudonyme, die an den Produktanbieter im Drittland übermittelt werden. Sofern der Anbieter die Daten nicht mehr identifizierbaren Personen zuordnen kann und er keine Möglichkeit zur De-Pseudonymisierung hat, stellt die vorgenommene Pseudonymisierung nach Ansicht des EDSA eine effektive zusätzliche Maßnahme dar.

Der Datenexporteur muss in beiden Fällen den **Nachweis** erbringen, dass eine **Aufhebung der Verschlüsselung und/oder Pseudonymisierung** bei dem ausländischen Vertragspartner durch Behörden seines Heimatstaats **ausgeschlossen** werden kann. Welche Kompensationsmaßnahmen im Einzelnen notwendig und ausreichend sind, ist in erster Linie aus technisch-organisatorischer Sicht zu bewerten. 75

**Beispiel 5:** Ein Staatstheater möchte Einblick in die kulturellen Interessen seiner Besucherinnen und Besucher erhalten und nutzt deshalb auf seiner Website ein Webanalyse-Tool eines US-Anbieters, das bei jedem Websitebesuch Daten über die Nutzerinnen und Nutzer der Website sammelt. Dabei setzt das Webanalyse-Tool Cookies, die Client IDs und User IDs enthalten, die auf dem Endgerät bzw. dem Browser abgelegt werden. Client IDs und User IDs werden an Cloud-Rechenzentren des Anbieters in den USA übermittelt; es besteht also eine direkte Verbindung zwischen dem Gerät der Nutzerinnen und Nutzer und dem US-Anbieter (sog. Client-seitiges Tracking).

Beide IDs sind Online-Kennungen und dienen der eindeutigen Identifizierbarkeit natürlicher Personen. Wenn die Nutzerinnen und Nutzer etwa über IDs oder Kennungen bestimmbar gemacht werden, liegt keine Pseudonymisierung im Sinne einer zusätzlichen technischen Maßnahme vor. Denn hier werden die Daten nicht pseudonymisiert, um die identifizierbaren Daten zu verschleiern oder zu löschen, so dass die betroffenen Personen nicht mehr adressiert werden können, sondern IDs und Kennungen werden dazu verwendet, die einzelnen Individuen unterscheidbar und adressierbar zu machen.

**Praxistipp:** Möglicherweise bietet Server-seitiges Tracking eine datenschutzkonforme Alternative, bei der die Informationen über Seitenaufrufe und Interaktionen zunächst an einen Server-Tag-Manager gesendet werden. Hier besteht keine direkte Verbindung zwischen dem Gerät der Nutzerinnen und Nutzer und dem Anbieter. Dieser erhält nur Daten, die vom Server vorab festgelegt worden sind. Nur der Server der Website kann die Daten und Interaktionen der Nutzerinnen und Nutzer auslesen. 76

Bei **Videokonferenz-Systemen** ist zu beachten, dass bei der – mit ihnen zwingend verbundenen – Übertragung von Bild- und Tondaten nach aktuellem Kenntnisstand eine **ausreichend starke Verschlüsselung und/oder Pseudonymisierung derzeit technisch noch nicht ohne Funktionseinschränkungen möglich** ist. Somit können Verschlüsselungsmechanismen bei Videokonferenz-Systemen in nicht wenigen Konstellationen keine ausreichenden Kompensationsmaßnahmen darstellen, um Unzulänglichkeiten bei der Wirksamkeit etwaig vereinbarter Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 Buchst. c DSGVO zu überwinden. 77

## bb) Zusätzliche vertragliche Maßnahmen

**78** Da vertragliche Maßnahmen aufgrund ihrer zivilrechtlichen Natur die Behörden eines Drittlands im Allgemeinen nicht binden können, weil diese nicht Partei der geschlossenen Verträge sind (**Wirkung nur „inter partes“**), müssen sie in der Regel **mit technischen und organisatorischen Maßnahmen kombiniert** werden, um das erforderliche Datenschutzniveau sicherzustellen. Insbesondere bei Datenübermittlungen in die USA können rein vertragliche Maßnahmen nach Ansicht des EDSA nicht die Anwendung von im Drittland geltenden Rechtsvorschriften verhindern, so dass zwingend eine Kombination mit technischen Maßnahmen erfolgen muss. Beispielsweise folgende zusätzliche vertragliche Maßnahmen sind nach Ansicht des EDSA denkbar:[98]

- **Verpflichtung zur Verwendung spezifischer technischer Maßnahmen:** In Fällen, in denen der Datenexporteur erkannt hat, dass zusätzliche technische Maßnahmen ergriffen werden müssen, kann diese Klausel sicherstellen, dass sich der Datenimporteur verpflichtet, die notwendigen spezifischen technischen Maßnahmen zu ergreifen.

- **Transparenzklauseln:** Der Datenimporteur könnte verpflichtet werden, den Datenexporteur bei der Beurteilung des Schutzniveaus im Drittland zu unterstützen, indem er dem Datenexporteur – soweit möglich – entsprechende Informationen zur Verfügung stellt, beispielsweise die einschlägigen Vorschriften, Berichte oder Statistiken über behördliche Zugriffe auf vergleichbare personenbezogene Daten oder auch Angaben über entsprechende behördliche Anfragen bei ihm selbst. Darüber hinaus kann der Datenimporteur verpflichtet werden, Änderungen bezüglich dieser Angaben dem Datenexporteur binnen einer bestimmten Frist mitzuteilen. Diese Klauseln können dem Datenexporteur auch bei der Erfüllung seiner Dokumentationspflichten helfen. Zudem sind Klauseln möglich, mit denen der Datenimporteur beispielsweise bestätigt, dass er nicht absichtlich über Hintertüren („back doors“) einen Zugriff auf personenbezogene Daten ermöglicht oder dass er aufgrund nationalen Rechts nicht verpflichtet ist, „back doors“ zu schaffen. Falls dem Datenimporteur entsprechende Rechtsvorschriften des Drittlandes aber eine solche Information untersagen sollten, läuft die Klausel ins Leere. Dies gilt auch für die Vereinbarung sogenannter „Warrant Canary“-Erklärungen, kryptographisch signierter Mitteilungen des Datenimporteurs, die den Datenexporteur darüber informieren sollen, dass dem Datenimporteur bis zu einem bestimmten Zeitpunkt kein Ersuchen um Offenlegung personenbezogener Daten zugegangen ist.

- **Verpflichtung zum Ergreifen bestimmter Maßnahmen:** Der Datenimporteur könnte sich verpflichten, eine etwaige behördliche Anordnung zur Datenoffenlegung zu prüfen und gegebenenfalls dagegen vorzugehen – möglichst schon im Wege des einstweiligen Rechtschutzes. Effektiv in diesem Zusammenhang wäre zudem die Verpflichtung des Datenimporteurs, die Daten nicht offenlegen zu dürfen, bis ein Gericht abschließend über die Sache entschieden hat.

**79** Diese Empfehlungen des EDSA – wie auch natürlich die Anforderungen des EuGH – spiegeln sich in den neuen Standardvertragsklauseln wider.

[98] EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 98 ff.

### cc) Zusätzliche organisatorische Maßnahmen

Die zusätzlichen organisatorischen Maßnahmen können in **internen Strategien, Organisationsmethoden oder Standards** bestehen, die die Datenexporteure nicht nur bei sich selbst anwenden, sondern auch den Datenimporteuren auferlegen können. Nach Ansicht des EDSA kann der Datenexporteur beispielsweise folgende organisatorische Maßnahmen ergreifen:[99] 80

- **Interne Grundsätze für Übermittlungen:** Der Datenimporteur könnte verpflichtet werden, die mit behördlichen Ersuchen befassten Mitarbeiterinnen und Mitarbeiter regelmäßig zu schulen und die Schulungsinhalte entsprechend der Entwicklung im Drittland regelmäßig zu aktualisieren. Aber auch der Datenexporteur kann etwa mittels der Pflicht zur frühzeitigen Beiziehung des Datenschutzbeauftragten bei Drittlandtransfers zusätzliche organisatorische Maßnahmen implementieren.
- **Maßnahmen zur Datenminimierung:** Mithilfe der Datenminimierung kann von vornherein das Risiko, personenbezogene Daten der Gefahr unbefugter Zugriffe auszusetzen, reduziert werden.

**Beispiel 6:** Eine Schule wählt für Supportdienste für ihre Website einen IT-Dienstleister in einem Drittland. Dieser kann regelmäßig seine Dienstleistung auch dann erbringen, wenn ihm nur eingeschränkter Zugriff auf die Daten gewährt wird.

### e) Einleitung aller förmlichen Verfahrensschritte

In einem **fünften Schritt** leitet der Datenexporteur alle förmlichen Verfahrensschritte ein, die die zusätzlichen Maßnahmen gegebenenfalls erfordern. Dazu zählen beispielsweise **Genehmigungen** durch die Datenschutz-Aufsichtsbehörden, die erforderlich wären, wenn der Datenexporteur als zusätzliche Maßnahme die Standard-Datenschutzklauseln wesentlich abändern – und nicht lediglich ergänzen – möchte.[100] 81

### f) Überprüfung und Neubewertung des Schutzniveaus

Abschließend muss der Datenexporteur in einem **sechsten Schritt** das Datenschutzniveau im Drittland **in geeigneten Abständen überprüfen, neu bewerten und laufend überwachen** in Bezug auf mögliche Beeinträchtigungen des Schutzniveaus. Die Rechenschaftspflicht besteht also dauerhaft fort.[101] 82

[99] EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 128 ff.
[100] EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 59 ff.
[101] EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 67 ff.

## 2. Standarddatenschutzklauseln (Art. 46 Abs. 2 Buchst. c DSGVO)

**83** **Hauptanwendungsfall** für geeignete Garantien – und daher an erster Stelle behandelt – dürften Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 Buchst. c DSGVO sein, insbesondere die von der Europäischen Kommission per Beschluss vorformulierten **Standardvertragsklauseln** für die Drittlandübermittlung (**„standard contractual clauses“**, im Folgenden abgekürzt mit **„SCC“**).[102] Es handelt sich dabei um förmlich beschlossene **Musterverträge**, die zwischen einem oder mehreren Datenexporteuren und einem oder mehreren davon zu unterscheidenden Datenimporteuren abzuschließen sind.

### a) Anwendungsbereich

**84** Gemäß Art. 1 Abs. 1 des Durchführungsbeschlusses (EU) 2021/914 gelten die SCC für Datenübermittlungen zwischen einem **in der EU ansässigen Datenexporteur** und einem **Datenimporteur mit Sitz außerhalb des EWR**. Nach Erwägungsgrund 3 des Durchführungsbeschlusses (EU) 2021/914 ist Datenexporteur derjenige Verantwortliche oder (Unter-)Auftragsverarbeiter, der personenbezogene Daten in ein Drittland übermittelt. Datenimporteur ist danach der die personenbezogenen Daten annehmende Verantwortliche oder (Unter-) Auftragsverarbeiter. Die Rollen des Datenexporteurs und des Datenimporteurs werden damit im jeweiligen (Vertrags-) Verhältnis einzeln betrachtet und definiert. Ist in einem Verhältnis keiner der Akteure als Datenexporteur – mangels einer Datenübermittlung ins Drittland – zu werten, sind die SCC in diesem Vertragsverhältnis nicht anwendbar. Möglicherweise kommt stattdessen die Anwendung der Standardvertragsklauseln für EU-Auftragsverarbeitung in Betracht (vgl. Rn. 97 ff.).

**85** Überdies darf der **Datenimporteur nicht bereits gemäß Art. 3 Abs. 2 DSGVO in den territorialen Anwendungsbereich der Datenschutz-Grundverordnung** fallen. Damit soll vermieden werden, dass die aus der Datenschutz-Grundverordnung resultierenden Verpflichtungen „verdoppelt“ werden.[103] Diese Einschränkung hat jedoch zur Folge, dass die SCC in der Konstellation, dass auf den im Drittland ansässigen Datenimporteur aufgrund des Marktortprinzips die Datenschutz-Grundverordnung Anwendung findet, nicht als geeignete Garantien im Sinne des Art. 46 Abs. 1 DSGVO dienen können. Laut EDSA sollen für diesen Fall neue Standardvertragsklauseln entwickelt werden, die nur auf die ansonsten „fehlenden“ Elemente eingehen (sozusagen als „SCC light“), wie beispielsweise die Maßnahmen, die im Falle von Divergenzen zwischen Rechtsvorschriften eines Drittlandes und der Datenschutz-Grundverordnung sowie bei einem rechtsverbindlichen Ersuchen von Drittländern um Offenlegung von Daten zu ergreifen sind.[104]

[102] Durchführungsbeschluss (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, C/2021/3972 (ABl. L 199 vom 7. Juni 2021, S. 31).

[103] EDSA, Guidelines 05/2021 (Fn. 24), Rn. 29.

[104] So EDSA, Guidelines 05/2021 (Fn. 24), Rn. 29.

**Praxistipp:** Da dem Datenexporteur im Einzelfall die Beurteilung schwer fallen dürfte, ob der Datenimporteur die Voraussetzungen von Art. 3 Abs. 2 DSGVO erfüllt, ist es bis zum Beschluss der vom EDSA vorgeschlagenen „SCC light" sinnvoll, im Zweifelsfall die „normalen" SCC anzuwenden, um die Anforderungen der Art. 44 ff. DSGVO erfüllen zu können. 86

## b) Struktur der Standardvertragsklauseln

Die SCC verfolgen einen **modularen Ansatz**, der mit allgemeinen Klauseln kombiniert ist, um die verschiedenen Datenübermittlungsszenarien abbilden zu können.[105] Sie selbst stellen also noch keinen vollständigen und fertigen Vertrag dar. Die insgesamt **18 Klauseln** bestehen zum einen aus den allgemeinen Klauseln, die auf alle Konstellationen angewandt werden können, wie beispielsweise die Klauseln 1 bis 7, zum anderen aus Klauseln, die Regelungen für ein, zwei, drei oder alle vier Module enthalten, wie zum Beispiel die Klauseln 8 und 9. Folgende Module sind verfügbar: 87

- **Modul 1:** Übermittlung von **Verantwortlichen an Verantwortliche.** Diese Konstellation war bereits in den früheren Standardvertragsklauseln geregelt. Für den Fall von Datenübermittlungen zwischen mehreren gemeinsam verantwortlichen Parteien ist weiterhin ein separater Vertrag gemäß Art. 26 Abs. 2 DSGVO abzuschließen, dessen Regelungen nicht im Widerspruch zu den SCC stehen dürfen.
- **Modul 2:** Übermittlung von **Verantwortlichen an Auftragsverarbeiter.** Die Vereinbarung von Modul 2 soll regelmäßig den bislang erforderlichen zusätzlichen Vertrag gemäß Art. 28 Abs. 3 DSGVO ersetzen.[106] Um dies zu erreichen, ist auf entsprechend genaue und transparente Angaben in den Anhängen zu den SCC zu achten.[107]
- **Modul 3:** Übermittlung von **Auftragsverarbeitern an Auftragsverarbeiter.** Damit enthalten die SCC erstmals Regelungen für diese sehr praxisrelevante Konstellation, für die bislang ein gesonderter Vertrag zwischen dem in der EU ansässigen Verantwortlichen und dem in einem Drittland ansässigen Unterauftragsverarbeiter notwendig war. Auch hier erfüllen die SCC die Anforderungen an einen Vertrag zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO.
- **Modul 4:** Übermittlung von **Auftragsverarbeitern an Verantwortliche.** Die Konstellation, dass ein in der EU ansässiger Auftragsverarbeiter an einen Verantwortlichen mit Sitz in einem Drittland Daten (zurück)übermittelt, dürfte in der Praxis des öffentlichen Sektors allerdings eher selten vorkommen.

[105] Vgl. Erwägungsgrund 10 des Durchführungsbeschlusses (EU) 2021/914.

[106] Vgl. Erwägungsgrund 9 des Durchführungsbeschlusses (EU) 2021/914.

[107] Baumgartner/Hansch/Roth, Die neuen Standardvertragsklauseln der EU-Kommission für Datenübermittlungen in Drittstaaten, ZD 2021, S. 608 (611).

88 Darüber hinaus finden sich in der Anlage zu den SCC **drei Anhänge**, die ebenfalls Vertragsbestandteil sind und von den Parteien individualisiert werden müssen:

- **Anhang I:** Liste der Parteien und Beschreibung der Datenübermittlungen;
- **Anhang II:** Beschreibung der vom Datenimporteur ergriffenen technischen und organisatorischen Maßnahmen;
- **Anhang III:** Liste der Unterauftragsverarbeiter.

89 Es ist gemäß der Erläuterung zur Anlage der SCC zwar nicht zwingend erforderlich, für jede Datenübermittlung oder Kategorie von Datenübermittlung und bzw. oder für jedes Vertragsverhältnis getrennte Anlagen auszufüllen; allerdings müssen die diesbezüglichen Informationen jeweils klar voneinander unterschieden werden können und transparent dargestellt werden.

90 **Praxistipp:** Die Angaben in den Anhängen sind somit recht konkret zu formulieren. Andererseits sollten allzu detaillierte Beschreibungen vermieden werden, um sich häufige Aktualisierungen zu ersparen.

91 Die SCC eignen sich gemäß Erwägungsgrund 10 des Durchführungsbeschlusses (EU) 2021/914 auch für Mehrparteienverhältnisse und ermöglichen den Beitritt weiterer Verantwortlicher und Auftragsverarbeiter während der gesamten Laufzeit des Vertrags, was die früheren Standardvertragsklauseln nicht vorsahen.

## c) Zentrale Regelungen

92 Ein kurzer Überblick im Folgenden soll die zentralen Regelungen der SCC vorstellen:

- **Klausel 2:** Wie schon in Erwägungsgrund 3 des Durchführungsbeschlusses (EU) 2021/914 festgehalten, ist es möglich, die SCC in einen umfangreicheren Vertrag aufzunehmen und um weitere Klauseln oder zusätzliche Garantien zu erweitern, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den SCC stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

  **Praxistipp:** Hier wird es zur Herstellung größtmöglicher Transparenz ratsam sein, zusätzliche Regelungen erkennbar vom Text der Standardvertragsklauseln abzusetzen. Damit diese aber nicht der vorherigen Genehmigung der Aufsichtsbehörde bedürfen (vgl. Art. 46 Abs. 3 Buchst. a DSGVO), sollte man bei der Abänderung der SCC Vorsicht walten lassen. Wenn Zweifel bestehen, ob durch die Änderungen oder Ergänzungen nicht doch die Rechtsposition des Datenexporteurs und/oder mittelbar auch die der betroffenen Person geschwächt wird, ist hiervon Abstand zu nehmen. Für die betroffenen Personen rein vorteilhafte Änderungen oder Ergänzungen bleiben hingegen genehmigungsfrei.

- **Klausel 3:** Damit werden betroffene Personen in die Lage versetzt, zahlreiche Klauseln der SCC als Drittbegünstigte gegenüber dem Datenexporteur und/oder dem Datenimporteur geltend zu machen.

- **Klausel 5:** Diese Klausel regelt die vorrangige Geltung der SCC gegenüber sonstigen zwischen den Vertragsparteien bereits bestehenden Regelungen. Im Falle eines Widerspruchs verlieren diese sonstigen Regelungen aber nicht ihre Geltung; vielmehr können die SCC gemäß Klausel 2 dann nicht mehr als geeignete Garantien dienen.
- **Klausel 7:** Die sog. Koppelungsklausel („docking clause") ermöglicht den Beitritt neuer Parteien durch Ausfüllen und Unterzeichnen von Anhang I nach Zustimmung der bisherigen Vertragsparteien.
- **Klausel 8:** Die in Art. 5 Abs. 1 DSGVO verankerten Grundsätze für die Verarbeitung personenbezogener Daten sowie die Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO werden als vertragliche Pflichten vereinbart.
- **Klausel 9:** Hier wird die Einbeziehung weiterer Unterauftragsverarbeiter geregelt, für die entweder die Möglichkeit einer vorherigen gesonderten oder die einer allgemeinen schriftlichen Genehmigung besteht. Damit orientiert sich die Klausel eng an den Vorgaben des Art. 28 Abs. 2 und 4 DSGVO.
- **Klausel 12:** Die Haftungsklausel sieht eine unbeschränkte Haftung im Innenverhältnis zwischen den Vertragsparteien vor. Deshalb wird sich in der Praxis häufig die Frage stellen, ob eine weitgehende Haftungsbeschränkung im Innenverhältnis, wie sie gerade marktstarke Anbieter oft vorgeben, eine unzulässige Abänderung der SCC darstellt. Sofern damit aber kein Nachteil für die betroffenen Personen verbunden ist, könnte dies gemäß der Wertung der Klausel 2 Buchst. a für die Zulässigkeit einer solchen Haftungsbeschränkung sprechen.[108]

## d) Transfer Impact Assessment im Rahmen der Standardvertragsklauseln

In den **Klauseln 14 und 15** der SCC, die für alle Übermittlungskonstellationen gleichermaßen gelten, finden sich **„zusätzliche Maßnahmen" vertraglicher Natur**, die die Einhaltung des Schutzniveaus gewährleisten sollen, wie es der EuGH in seinem „Schrems II"-Urteil gefordert hatte. Diese müssen im Fall der USA aber zwingend mit technischen Maßnahmen kombiniert werden. **93**

Zunächst enthält Klausel 14 Buchst. a die Zusicherung der Parteien, dass die Rechtsvorschriften und Gepflogenheiten im Drittland den Datenimporteur nicht an der Erfüllung seiner aus den SCC resultierenden Pflichten hindern. Darauf folgt in Klausel 14 Buchst. b die Erklärung der Parteien, dass neben den für die Übermittlung relevanten Rechtsvorschriften auch die **Gepflogenheiten** des Drittlands berücksichtigt werden. Hinter dem Begriff „Gepflogenheiten" verbirgt sich, wie aus Fußnote 12 zu Klausel 14 hervorgeht, eine **Erleichterung** bezüglich der Prüfpflichten der Parteien, da in die Beurteilung des Schutzniveaus im Drittland nun auch einschlägige und dokumentierte praktische Erfahrungen mit behördlichen Auskunftsersuchen und Zugriffen fließen können. Damit lassen die SCC – vermutlich stärker als die Empfehlungen des EDSA – Raum für eine **risikobasierte Gesamtbeurteilung**. Allerdings sind **94**

[108] Baumgartner/Hansch/Roth, Die neuen Standardvertragsklauseln der EU-Kommission für Datenübermittlungen in Drittstaaten, ZD 2021, S. 608 (612).

diese subjektiven Beobachtungen durch öffentlich verfügbare Informationen über behördliche Vorgehensweisen innerhalb desselben Wirtschaftszweiges und über die Anwendung der Rechtsvorschriften in der Praxis zu belegen. Eine **umfassende Dokumentationspflicht** der Beurteilung folgt aus Klausel 14 Buchst. d, eine neue formale Verpflichtung, die die Datenschutz-Grundverordnung in dieser Form nicht vorsieht. Klausel 14 Buchst. e und f enthalten Regelungen für den Fall, dass sich Rechtslage oder Gepflogenheiten ändern. Falls es zu einem behördlichen Zugriff auf die Daten kommen sollte, finden die Bestimmungen der Klausel 15 Anwendung.

95 **Praxistipp:** Bis auf Weiteres akzeptiert der Bayerische Landesbeauftragte für den Datenschutz unter den oben unter Rn. 94 dargelegten Anforderungen diesen subjektiven, risikobasierten Ansatz, der den SCC zu entnehmen ist und den auch die FAQ der EU-Kommission zu den SCC stützen.[109] Es ist daher nicht erforderlich, den rein objektiven Ansatz, den die EDSA-Empfehlungen zunächst vermuten ließen und der vor allem eine abstrakte Betrachtung der Gesetze im Drittland zu verlangen scheint, im Rahmen der SCC zu verfolgen.

96 Die sich aus der Rechtsprechung des EuGH ergebenden Anforderungen an die Durchführung eines Transfer Impact Assessment haben somit nun Eingang in die SCC gefunden; sie bilden dort das Kernstück. Klausel 14 ist jedoch nicht isoliert zu betrachten, sondern stets im Kontext mit den detaillierten Vorgaben des EDSA in seinen Empfehlungen.[110] Deshalb hat sich nichts an der Situation geändert, dass der Datenexporteur – auch bei Verwendung der neuen SCC – jeweils **im Einzelfall die Rechtslage und -praxis des Drittlands prüfen** und gegebenenfalls zusätzliche Schutzmaßnahmen ergreifen oder, wenn dies nicht gelingt, von der Übermittlung Abstand nehmen muss. Damit verbietet es sich, sich mit dem Abschluss der SCC allein, quasi „für die Schublade", zu begnügen.

Die Verwendung der SCC bedeutet für die Vertragsparteien damit folgende Schritte:

- Auswahl der passenden Klauseln,
- Ausfüllen der Anhänge und
- Durchführung des Transfer Impact Assessment.

**Beispiel 7:** Ein US-Anbieter von Office-Produkten unterwirft alle Datenflüsse den neuen SCC. Er ermöglicht seinen in der EU ansässigen Kunden aus dem öffentlichen Sektor zugleich, all ihre Daten innerhalb der EU zu verarbeiten und zu speichern. Zudem implementiert er eine Datenverschlüsselung sowohl für die Verarbeitung als auch für eine möglicherweise doch notwendige Übermittlung und für den Ruhezustand.

Mit diesen Maßnahmen ist ein wichtiger Schritt in Richtung Datenschutz getan; allerdings löst diese Vorgehensweise nicht die Problematik einer möglichen Herausgabeverpflichtung des US-Dienstleisters gemäß CLOUD Act oder FISA. Hier kann nur eine Pseudonymisierung und bzw. oder eine ausreichend sichere Verschlüsselung weiterhelfen, wobei der Kunde alle wesentlichen Schlüssel selbst verwaltet und einen Zugriff auf diese aus dem Geltungsbereich

[109] Vgl. EU-Kommission, Questions and Answers for the two sets of Standard Contractual Clauses vom 25. Mai 2022, S. 21 f., Internet: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

[110] Vgl. EU-Kommission, Questions and Answers for the two sets of Standard Contractual Clauses vom 25. Mai 2022, S. 22.

des FISA bzw. des Cloud Acts ausschließt. Ob diese Technik tatsächlich auf alle Prozesse angewandt werden kann, muss stets im Einzelfall geprüft werden.

## e) Standardvertragsklauseln für EU-Auftragsverarbeitung gemäß Art. 28 Abs. 7 DSGVO

Für den Fall, dass **im Verhältnis zwischen Verantwortlichem und Auftragsverarbeiter keine personenbezogenen Daten in Drittländer übermittelt** werden, sondern erst in demjenigen zwischen Auftragsverarbeiter und Unterauftragsverarbeiter, können die mit dem Durchführungsbeschluss der EU-Kommission (EU) 2021/915 (und nicht (EU) 2021/914) veröffentlichten **Standardvertragsklauseln für die EU-Auftragsverarbeitung**[111] eingesetzt werden. 97

Der Verantwortliche wird bei Verwendung der Standardvertragsklauseln für die EU-Auftragsverarbeitung hinsichtlich des Einsatzes eines Unterauftragsverarbeiters durch den Auftragsverarbeiter, einschließlich möglichem Drittlandtransfer, mittels der Klauseln 7.7 und 7.8 wie folgt abgesichert: 98

- Für die (Unter-)Vergabe der Verarbeitungsvorgänge durch den Auftragsverarbeiter an den Unterauftragsverarbeiter bedarf es einer vorherigen gesonderten schriftlichen Genehmigung des Verantwortlichen auf informierten Antrag des Auftragsverarbeiters. Optional kann der Verantwortliche dem Auftragsverarbeiter eine allgemeine Genehmigung hierfür erteilen. In diesem Fall hat der Verantwortliche ein Einspruchsrecht bei etwaigen Änderungen der Unterauftragsverarbeitungsverhältnisse.
- Die Unterbeauftragung muss im Wege eines Vertrages erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter selbst entsprechend den Klauseln und gemäß der Datenschutz-Grundverordnung unterliegt.
- Der Auftragsverarbeiter hat dem Verantwortlichen auf dessen Verlangen eine Kopie dieses Vertrages und etwaiger späterer Änderungen zur Verfügung zu stellen.
- Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt.
- Der Verantwortliche erklärt sich damit einverstanden, dass Auftragsverarbeiter und Unterauftragsverarbeiter die Einhaltung der Anforderungen der Art. 44 ff. DSGVO ihm gegen-

[111] Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates, C/2021/3701 (ABl. L 199 vom 7. Juni 2021, S. 18).

über dadurch sicherstellen können, dass sie wiederum die mit dem Durchführungsbeschluss (EU) 2021/914 erlassenen SCC (Modul 3) vereinbaren (vgl. Klausel 7.8 Buchst. b).[112]

99 **Beispiel 8:** Um die Einhaltung von Art. 28 Abs. 3 und 4 DSGVO sicherzustellen, ist im Falle des Beispiels 1 dem Landratsamt anzuraten, mit dem in der EU ansässigen Auftragsverarbeiter einen Vertrag unter Verwendung der Standardvertragsklauseln für die EU-Auftragsverarbeitung abzuschließen. Der Auftragsverarbeiter wiederum schließt dann mit dem Cloud-Anbieter in Singapur einen Vertrag unter Verwendung der SCC als geeignete Garantie im Sinne des Art. 46 Abs. 1 DSGVO ab.

## 3. Rechtlich bindende und durchsetzbare Dokumente zwischen den Behörden oder öffentlichen Stellen (Art. 46 Abs. 2 Buchst. a DSGVO)

100 Eine der gemäß Art. 46 Abs. 2 DSGVO möglichen Garantien, die für bayerische öffentliche Stellen grundsätzlich neben der Verwendung von SCC in Frage kommen können, sind **rechtlich bindende und durchsetzbare Dokumente** zwischen den Behörden oder öffentlichen Stellen eines Mitgliedstaates und denen eines Drittlandes **für Datenübermittlungen zwischen Behörden oder öffentlichen Stellen**. Diese bedürfen zwar **keiner vorherigen Beteiligung** der Datenschutz-Aufsichtsbehörden oder der Europäischen Kommission, spielen aber in der Praxis für bayerische öffentliche Stellen vermutlich eine eher untergeordnete Rolle, da dort weit häufiger Datentransfers an privatwirtschaftliche Unternehmen statt an Behörden oder öffentliche Stellen in Drittländern anzutreffen sein werden. Der EDSA hat hierzu Leitlinien erstellt, die nähere Ausführungen zu den Anforderungen an Verwaltungsvereinbarungen im Sinne von Art. 46 Abs. 2 Buchst. a DSGVO enthalten.[113]

101 Rechtsverbindlichkeit und Durchsetzbarkeit liegen dabei nur dann vor, wenn die betroffenen Personen die Möglichkeit haben, die ihnen in dem Dokument gewährleisteten Rechte durchzusetzen. Ihnen muss das Dokument laut Erwägungsgrund 108 DSGVO somit **wirksame verwaltungsrechtliche oder gerichtliche Rechtsbehelfe sowie das Recht auf Geltendmachung von Schadensersatzansprüchen** einräumen. Unter „verwaltungsrechtlichen Rechtsbehelfen" ist auch das Recht auf Anrufung einer Datenschutz-Aufsichtsbehörde zu verstehen.[114] Solche Dokumente müssen rechtlich bindend und durchsetzbar sein. Daher können im Rahmen dieser Bestimmung internationale Verträge, öffentlich-rechtliche Verträge oder unmittelbar anwendbare Verwaltungsvereinbarungen herangezogen werden.[115]

[112] Vgl. für weitere ausführliche Informationen zu den Rechten und Pflichten des Verantwortlichen und des Auftragsverarbeiters: Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Stand 9/2019.

[113] EDSA, Leitlinien 2/2020 zu Artikel 46 Absatz 2 Buchstabe a und Absatz 3 Buchstabe b der Verordnung (EU) 2016/679 für die Übermittlung personenbezogener Daten zwischen Behörden und öffentlichen Stellen im EWR und Behörden und öffentlichen Stellen außerhalb des EWR, Version 2.0, Stand 12/2020, Internet: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_de.

[114] Lange/Filip, in: Wolff/Brink, BeckOK Datenschutzrecht, Stand 11/2021, Art. 46 DSGVO Rn. 21.

[115] EDSA, Leitlinien 2/2020 (Fn. 113), Rn. 65.

Verwaltungsvereinbarungen ohne rechtsverbindlichen Charakter eignen sich hingegen nicht. Für diese kann aber Art. 46 Abs. 3 Buchst. b DSGVO greifen. Sie bedürfen dann allerdings vorab einer Genehmigung durch die zuständige Datenschutz-Aufsichtsbehörde.

## 4. Genehmigte Verhaltensregeln (Art. 46 Abs. 2 Buchst. e DSGVO)

Zur Legitimierung von Datenübermittlungen in Drittländer stehen als Garantieinstrument zudem **die genehmigten Verhaltensregeln** gemäß Art. 46 Abs. 2 Buchst. e DSGVO zur Verfügung. Diese müssen sowohl **von der zuständigen Aufsichtsbehörde genehmigt** als auch **von der Europäischen Kommission für in der EU allgemein gültig** erklärt worden sein (Art. 40 Abs. 3 in Verbindung mit Abs. 5 und 9 DSGVO). Zusätzlich wird das Vorliegen **rechtsverbindlicher und durchsetzbarer Verpflichtungen** des Verantwortlichen oder des Auftragsverarbeiters im Drittland vorausgesetzt; die Rechte der Betroffenen müssen gewahrt werden. **102**

Wenn Verhaltensregeln Drittstaatentransfers datenschutzrechtlich legitimieren sollen, müssen sie somit **strengere Voraussetzungen** erfüllen als die „generellen" Verhaltensregeln gemäß Art. 40 Abs. 5 DSGVO. Für die entsprechende Anerkennung als Übermittlungsinstrument hat der EDSA wiederum Richtlinien veröffentlicht.[116] **103**

2021 wurden zwei Verhaltensregeln von der belgischen bzw. der französischen Datenschutz-Aufsichtsbehörde anerkannt, der „EU Data Protection Code of Conduct for Cloud Service Providers" (**„EU Cloud CoC"**) sowie der „Data Protection Code of Conduct for Cloud Infrastructure Service Providers" (**„CISPE CoC"**). Diese Verhaltensregeln enthalten praktische Leitlinien und spezifische Anforderungen gemäß Art. 28 DSGVO für in der EU ansässige Verarbeiter, die diesen Verhaltensregeln unterliegen. Jedoch dürfen sie **mangels Allgemeingültigkeitserklärung** durch die EU-Kommission gerade nicht im Zusammenhang mit internationalen Übermittlungen personenbezogener Daten verwendet werden. Die Verarbeitung muss hier regelmäßig insbesondere mithilfe der SCC ergänzend abgesichert werden.[117] **104**

## 5. Genehmigter Zertifizierungsmechanismus (Art. 46 Abs. 2 Buchst. f DSGVO)

Schließlich können nach Art. 46 Abs. 2 Buchst. f DSGVO auch **genehmigte Zertifizierungsmechanismen** gemäß Art. 42 DSGVO geeignete Garantien für genehmigungsfreie Datenübermittlungen darstellen. Dies setzt voraus, dass die daran teilnehmenden Verantwortlichen **105**

[116] EDSA, Guidelines 04/2021 on Codes of Conduct as tools for transfers, Version 2.0, Stand 2/2022, Internet: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_de.

[117] Vgl. zu dieser Thematik ausführlich: Wittmann/Haidenthaler, IT-Compliance in der Cloud – Rechtssicherheit durch Codes of Conduct?, MMR 2022, S. 8 (11).

und Auftragsverarbeiter in Drittländern **rechtsverbindliche und durchsetzbare Verpflichtungen** zur Befolgung der geeigneten Garantien einschließlich der Rechte betroffener Personen eingehen. Gemäß Art. 42 Abs. 5 DSGVO muss eine **akkreditierte Zertifizierungsstelle** gemäß Art. 43 DSGVO oder die zuständige **Datenschutz-Aufsichtsbehörde** die Zertifizierungskriterien genehmigen; bei Bedarf muss das Kohärenzverfahren gemäß Art. 63 ff. DSGVO durchgeführt werden. Auch hierzu hat der EDSA Richtlinien verabschiedet.[118]

106 **Praxistipp:** Die Wertung des EuGH zum angemessenen Schutzniveau ist demnach nicht nur auf die SCC, sondern auch auf die übrigen Garantien gemäß Art. 46 DSGVO anzuwenden. Erleichterungen bei der Legitimierung von Drittlandtransfers gibt es bei diesen Garantien im Vergleich zu den SCC somit nicht.

[118] EDSA, Guidelines 07/2022 on certification as a tool for transfers, Version 2.0, Stand 2/2023, Internet: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072022-certification-tool-transfers_de.

# VI. Ausnahmen für bestimmte Fälle (Art. 49 DSGVO)

Für den Fall, dass für ein Drittland weder ein Angemessenheitsbeschluss der Europäischen Kommission noch geeignete Garantien vorliegen, kann die Übermittlung personenbezogener Daten möglicherweise auf einen der **abschließend geregelten Ausnahmetatbestände** des Art. 49 DSGVO gestützt werden. Da in dieser Konstellation ungewiss ist, ob die Daten nach der Übermittlung auf dem von der Datenschutz-Grundverordnung garantierten Niveau geschützt werden, und das Risiko daher hoch ist, dass kein adäquater Schutz besteht, sind die Ausnahmetatbestände des Art. 49 Abs. 1 DSGVO **restriktiv auszulegen und anzuwenden**.[119] Dazu muss im Einzelfall insbesondere die Erforderlichkeit der Datenübermittlung genau geprüft werden.[120] Dementsprechend betonte der EDSA in einer ersten Stellungnahme zum „Schrems II"-Urteil, dass die Ausnahmen gemäß Art. 49 DSGVO in der Praxis nicht „zur Regel" werden dürften, sondern auf bestimmte Situationen beschränkt bleiben müssten, wobei jeder Datenexporteur sicherstellen müsste, dass die Übermittlung der strengen Notwendigkeitsprüfung entspricht.[121] Nur so kann gewährleistet werden, dass der dem ungehinderten Datenverkehr gegenüber dem Schutz der personenbezogenen Daten ausnahmsweise gewährte Vorrang nicht überspannt wird. 107

**Praxistipp:** Bevor ein Drittlandtransfer auf einen der Ausnahmetatbestände des Art. 49 DSGVO gestützt wird, ist dringend angeraten zu prüfen, ob nicht eines der anderen Übermittlungsinstrumente, vor allem die SCC, in Betracht kommen. 108

Für bayerische öffentliche Stellen können insbesondere die folgenden Ausnahmetatbestände von Bedeutung sein: 109

## 1. Einwilligung (Art. 49 Abs. 1 UAbs. 1 Buchst. a DSGVO)

Gemäß Art. 49 Abs. 1 UAbs. 1 Buchst. a DSGVO ist die Übermittlung an ein Drittland zulässig, wenn die betroffene Person in die vorgeschlagene Datenübermittlung **ausdrücklich eingewilligt** hat, nachdem sie über die für sie **bestehenden möglichen Risiken** derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien **unterrichtet** wurde. 110

[119] Lange/Filip, in: Wolff/Brink, BeckOK Datenschutzrecht, Stand 11/2021, Art. 49 DSGVO Vorbemerkung.

[120] Schantz, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 49 DSGVO Rn. 10.

[121] EDSA, Häufig gestellte Fragen zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 – Data Protection Commissioner gegen Facebook Ireland Ltd und Maximilian Schrems; Stand 7/2020, S. 5, Internet: https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_de.

### VI. Ausnahmen für bestimmte Fälle

**111** Der Begriff der Einwilligung per se ist in Art. 4 Nr. 11 DSGVO gesetzlich definiert. Danach ist eine Einwilligung „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist".

**112** Damit verlangt eine wirksame Einwilligung gemäß Art. 49 Abs. 1 UAbs. 1 Buchst. a DSGVO insbesondere die Erfüllung folgender **zwei Voraussetzungen**:

- eine verschärfte Informationspflicht in Form der **Unterrichtung über bestehende mögliche Risiken**, also insbesondere darüber, dass kein angemessenes Datenschutzniveau gegeben ist und Betroffenenrechte gegebenenfalls nicht durchgesetzt werden können;
- eine **ausdrückliche** Einwilligung, und damit mehr, als für eine Einwilligung gemäß Art. 4 Nr. 11 DSGVO erforderlich ist. Mithin reichen weder Stillschweigen, Opt-Out (beispielsweise durch ein vorangekreuztes Kästchen bei Formularen im Internet) und Untätigkeit noch konkludentes Handeln als Einwilligung aus.[122]

**113** Erwägungsgrund 111 DSGVO bestimmt für einige Tatbestände des Art. 49 Abs. 1 UAbs. 1 DSGVO, dass diese nur **im Falle von gelegentlichen Datenübermittlungen** greifen; für die ausdrückliche Einwilligung ist diese Einschränkung nicht vorgesehen. Dennoch muss nach Ansicht des EDSA die Ausnahme der ausdrücklichen Einwilligung so ausgelegt werden, dass „nicht gegen das Wesen einer Ausnahmeregelung verstoßen wird, nämlich dass es sich dabei um eine Ausnahme von der Regel handelt, dass personenbezogene Daten nur dann an ein Drittland übermittelt werden dürfen, wenn dieses Drittland ein angemessenes Datenschutzniveau bietet oder alternativ dazu geeignete Garantien zur Anwendung gebracht werden."[123]

**114** Daher kommt der Ausnahmetatbestand der Einwilligung **für die wiederholte, massenhafte oder routinemäßige Übermittlung personenbezogener Daten regelmäßig nicht in Betracht**.[124] Dann ist es nämlich nicht mehr gerechtfertigt, auf geeignete Garantien gemäß Art. 46 DSGVO zu verzichten, deren Vereinbarung in Fällen einer punktuellen Datenübermittlung einen unverhältnismäßigen Aufwand bedeuten mag.[125]

**115** Bayerische öffentliche Stellen werden **nur in eng begrenzten Ausnahmefällen** eine Datenübermittlung in ein Drittland auf eine Einwilligung stützen können:

– Gemäß Art. 49 Abs. 3 DSGVO ist die auf eine Einwilligung gestützte Übermittlung von vornherein für Tätigkeiten ausgeschlossen, die **Behörden in Ausübung ihrer hoheitlichen Befugnisse** durchführen.

[122] Pauly, in: Paal/Pauly, DSGVO/BDSG, 3. Aufl. 2021, Art. 49 DSGVO Rn. 7.

[123] EDSA, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, Stand 5/2018, S. 5, Internet: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_de.

[124] EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, Stand 5/2020, Fn. 47, Internet: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_de.

[125] Schantz, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 49 DSGVO Rn. 7.

**Beispiel 9:** Ein kommunales Krankenhaus möchte zur Besetzung einer Tarifbeschäftigtenstelle ein Vorstellungsgespräch mittels Nutzung eines Videokonferenztools durchführen, das eine Datenübermittlung in die USA mit sich bringt. Die Möglichkeit einer Einwilligung des betroffenen Bewerbers ist hier nicht von vornherein gemäß Art. 49 Abs. 3 DSGVO ausgeschlossen, da die öffentliche Stelle in der vorliegenden Konstellation nicht in Ausübung ihrer hoheitlichen Befugnisse, sondern als (potentielle) Arbeitgeberin handelt.

- Aufgrund ihrer **jederzeitigen Widerrufbarkeit**, über die gemäß Art. 7 Abs. 3 Satz 3 DSGVO informiert werden muss, eignet sich die Einwilligung nur in begrenztem Maße als Rechtsgrundlage für den Drittlandtransfer, auch wenn der Widerruf die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt (vgl. Art. 7 Abs. 3 Satz 2 DSGVO).

- Außerdem liegen gerade im Rahmen eines Beschäftigungsverhältnisses **Zweifel an der Freiwilligkeit** der Einwilligung nahe; diese muss in jedem Einzelfall geprüft werden.

  **Beispiel 10:** In dem in Beispiel 9 geschilderten Fall bietet das kommunale Krankenhaus dem Bewerber keine datenschutzkonforme Alternative zum Vorstellungsgespräch an. Dies führt zu einem faktischen „Benutzungszwang" für das Videokonferenztool, der die Freiwilligkeit einer erteilten Einwilligung ausschließen kann.[126] Bewerberinnen und Bewerber wären praktisch gezwungen, in die Übermittlung personenbezogener Daten einzuwilligen, um überhaupt am Bewerbungsverfahren weiter teilnehmen zu können. In diesem Fall müsste daher eine datenschutzkonforme Alternative für die Durchführung des Vorstellungsgesprächs angeboten werden.

- Ferner erscheint die Einwilligung aufgrund einer möglicherweise **unvollständigen oder intransparenten Darstellung** der möglichen Risiken des Drittlandtransfers nur bedingt praktikabel – dies auch deshalb, weil die Einwilligung gemäß Art. 49 Abs. 1 UAbs. 1 Buchst. a DSGVO für den bestimmten Fall erfolgen muss, was die Möglichkeit von Pauschaleinwilligungen in Drittlandübermittlungen ausschließt.

## 2. Erforderlichkeit für die Erfüllung eines Vertrags (Art. 49 Abs. 1 UAbs. 1 Buchst. b DSGVO)

**Regelmäßig keine geeignete Rechtsgrundlage** für eine Drittlandübermittlung – wenn auch oft bemüht und deshalb hier vorgestellt – ist Art. 49 Abs. 1 UAbs. 1 Buchst. b DSGVO, wonach die Datenübermittlung in ein Drittland zulässig ist, wenn sie **für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen** oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person **erforderlich** ist. Eine **Nützlichkeit** der Datenübermittlung **reicht hierbei nicht aus**. Zudem muss die Übermittlung in einem direkten und objektiven Zusammenhang zum Zweck des Vertrags stehen. **116**

[126] Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung, Stand 9/2021, Rn. 68, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Einwilligung".

**Beispiel 11:** Eine Kommune möchte eine Bürosoftware einsetzen, die eine Übermittlung personenbezogener Daten der Mitarbeiterinnen und Mitarbeiter der Kommune in die USA mit sich bringt. Ein „direkter und objektiver Zusammenhang" der Datenübermittlung mit dem Arbeitsvertrag wird in der Regel nicht anzunehmen sein, es sei denn, die Nutzung der Software ist – wie beispielsweise bei Produkttestern – ausnahmsweise selbst Gegenstand der geschuldeten Tätigkeit. In diesem Fall müsste zusätzlich aber noch die Erforderlichkeit der Datenübermittlung in die USA dargelegt werden.[127]

## 3. Wichtige Gründe des öffentlichen Interesses (Art. 49 Abs. 1 UAbs. 1 Buchst. d DSGVO)

**117** Die Übermittlung kann auch gemäß Art. 49 Abs. 1 UAbs. 1 Buchst. d DSGVO zulässig sein, wenn sie aus **wichtigen Gründen des öffentlichen Interesses** notwendig ist. Wie aus Erwägungsgrund 112 DSGVO hervorgeht, meint der Verordnungsgeber hiermit insbesondere Datentransfers im Rahmen der **internationalen behördlichen Zusammenarbeit**, etwa zwischen Wettbewerbs-, Steuer- oder Zollbehörden. Bei dieser Ausnahme ist Art. 49 Abs. 4 DSGVO zu beachten, wonach das öffentliche Interesse **im Recht des Mitgliedstaats**, dem der Verantwortliche unterliegt, **oder im Unionsrecht anerkannt** sein muss. Folglich können öffentliche Interessen von Drittstaaten eine Übermittlung allein nicht rechtfertigen; ansonsten könnte der Drittstaat per unilateraler politischer Entscheidung bestimmen, wann eine Übermittlung zulässig ist.[128]

## 4. Schutz lebenswichtiger Interessen (Art. 49 Abs. 1 UAbs. 1 Buchst. f DSGVO)

**118** Art. 49 Abs. 1 UAbs. 1 Buchst. f DSGVO gestattet eine Übermittlung, wenn sie **zum Schutz lebenswichtiger Interessen** der betroffenen Person oder anderer Personen erforderlich ist, sofern die betroffene Person aus physischen oder rechtlichen Gründen zur Erteilung der Einwilligung außerstande ist. Laut Erwägungsgrund 112 Satz 2 DSGVO zählen zu den lebenswichtigen Interessen insbesondere die **körperliche Unversehrtheit und das Leben**. In der Praxis ist hier an Situationen zu denken, in denen sich die betroffene oder eine andere Person in einem lebensbedrohlichen Zustand befindet und zugleich bewusstlos und deshalb außerstande ist, eine Einwilligung abzugeben, es zur Rettung aber erforderlich ist, Daten der betroffenen Person etwa an Ärztinnen und Ärzte in einem Drittland zu übermitteln.[129]

[127] Vgl. zu diesem Beispiel Schwartmann/Burckhardt, „Schrems II" als Sackgasse für die Datenwirtschaft?, ZD 2021, S. 235 (236).

[128] Schantz, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 49 DSGVO Rn. 35.

[129] Lange/Filip, in: Wolff/Brink, BeckOK Datenschutzrecht, Stand 11/2021, Art. 49 DSGVO Rn. 39.

An der Erforderlichkeit fehlte es allerdings bei der Übermittlung medizinischer Daten in Drittländer, die nicht unmittelbar der Behandlung der betroffenen Person, sondern beispielsweise der allgemeinen medizinischen Forschung dienen.[130] 119

Dieser Ausnahmetatbestand kann sich gegebenenfalls mit dem des Buchst. d überschneiden. 120

## 5. Übermittlung aus einem Register (Art. 49 Abs. 1 UAbs. 1 Buchst. g DSGVO)

Ein weiterer möglicher Ausnahmefall, von dem bayerische öffentliche Stellen Gebrauch machen können, ist gemäß Art. 49 Abs. 1 UAbs. 1 Buchst. g DSGVO die **Übermittlung aus einem Register**, das nach Unions- oder mitgliedstaatlichem Recht **zur Information der Öffentlichkeit bestimmt** ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, **zur Einsichtnahme offensteht**. Dies setzt aber unter anderem voraus, dass die im Unionsrecht oder im Recht der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall erfüllt sind. Die Einsichtnahme in das fragliche Register muss entweder für die allgemeinen Öffentlichkeit ohne Erfüllung weiterer Voraussetzungen möglich sein – in Deutschland wäre dies etwa das Handels- oder Vereinsregister – oder für jede Person, die ein berechtigtes Interesse nachweisen kann, wie in Deutschland etwa beim Grundbuch.[131] Zudem beschränkt Art. 49 Abs. 2 Satz 1 DSGVO die Übermittlung: Die Gesamtheit oder ganze Kategorien der im Register enthaltenen personenbezogenen Daten dürfen nicht übermittelt werden. 121

Weiterhin darf die Übermittlung gemäß Art. 49 Abs. 2 Satz 2 DSGVO, wenn das Register zur Einsichtnahme ein berechtigtes Interesse voraussetzt, nur auf Anfrage dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind. Dies soll sowohl die Übermittlung des gesamten Registers als auch die zweckentfremdende Nutzung der in dem Register enthaltenen Daten verhindern.[132] 122

[130] Klug, in: Gola/Heckmann, Datenschutz-Grundverordnung, 3. Aufl. 2022, Art. 49 DSGVO Rn. 11.

[131] EDSA, Leitlinien 2/2018 (Fn. 123), S. 16.

[132] Lange/Filip, in: Wolff/Brink, BeckOK Datenschutzrecht, Stand 11/2021, Art. 49 DSGVO Rn. 43.

# VII. Rechenschaftspflicht (Art. 5 Abs. 2, Art. 28 Abs. 3 Buchst. h DSGVO)

**123** Das Recht auf Datenschutz erfordert **aktives Handeln** des Datenexporteurs. Dass er das Recht auf Datenschutz stets einhält und die Rechtmäßigkeit der Verarbeitung der Daten gemäß Art. 5 Abs. 1 Buchst. a DSGVO gewährleistet, indem er rechtliche, technische und organisatorische Maßnahmen ergreift, die die Wirksamkeit des Rechts sicherstellen, muss er den betroffenen Personen und den Datenschutz-Aufsichtsbehörden gegenüber **nachweisen** können.[133] Dieser **Grundsatz der Rechenschaftspflicht** ist in Art. 5 Abs. 2 DSGVO für den Verantwortlichen verankert; damit er die Rechenschaftspflicht bei einem Auftragsverhältnis erfüllen kann, gilt für den Auftragsverarbeiter gegenüber seinem Verantwortlichen Art. 28 Abs. 3 Buchst. h DSGVO, wonach er diesem alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung zu stellen hat. Der Grundsatz der Rechenschaftspflicht muss auch bei Datenübermittlungen in Drittländer beachtet werden. Zur Rechtmäßigkeit der Datenübermittlung in Drittländer gehört die Einhaltung der Art. 44 ff. DSGVO. Im Rahmen der Rechenschaftspflicht muss ein Datenexporteur, der Datentransfers in Drittländer durchführen möchte, **auch dokumentieren, dass er die durch die Art. 44 ff. DSGVO geforderte Prüfung vorgenommen** hat. Sofern der Datenexporteur ein (Unter-)Auftragsverarbeiter ist, ist dem Verantwortlichen anzuraten, auf eine detaillierte Dokumentation durch den (Unter-)Auftragsverarbeiter schon aus Gründen der Rechenschaftspflicht, welcher er selbst unterliegt, zu achten (vgl. auch Rn. 37 ff.).

**124** Die Nachweispflicht des Verantwortlichen für die Einhaltung der Vorgaben der Datenschutz-Grundverordnung gemäß Art. 5 Abs. 2 DSGVO begründet seine Darlegungs- und Beweislast und führt damit zu einer **Beweislastumkehr**: Nicht die betroffene Person oder die Datenschutz-Aufsichtsbehörde müssen eine Verletzung der Datenschutz-Grundverordnung nachweisen; vielmehr muss der Verantwortliche nachweisen, dass die Verarbeitung rechtmäßig im Sinne der Datenschutz-Grundverordnung ist.[134]

**125** Gerade im Hinblick auf einen auf Art. 46 DSGVO gestützten Drittlandtransfer fordert die Rechenschaftspflicht vom Datenexporteur, dass er **seine Überlegungen sowie die Gesamtbeurteilung** der für seine Übermittlung geltenden Rechtsvorschriften und Praktiken des Drittlands seines Datenimporteurs **mit der gebotenen Sorgfalt durchführen und sorgfältig dokumentieren** muss.[135] Dies gilt auch für die **Bewertung der zusätzlichen Maßnahmen**.[136] Für die Datenschutz-Aufsichtsbehörden werden diese Überlegungen so kontrollierbar. Praktische Erwägungen für den Drittlandtransfer spielen bei der Prüfung der Rechtmäßigkeit im Übrigen keine Rolle.

[133] EuGH, Urteil vom 11. November 2020, C-61/19 (Orange România SA/ANSPDCP), Rn. 42.

[134] Heberlein, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 5 Rn. 32. Vgl. dazu auch jüngst BVerwG, Urteil vom 2. März 2022, 6 C 7/20, Rn. 49 ff.

[135] EDSA, Empfehlungen 01/2020 (Fn. 17), Rn. 48.

[136] EDSA, Empfehlungen 01/2020 (Fn. 17), S. 5 und Rn. 7.

Was die Beachtung von Art. 44 ff. DSGVO angeht, sind für die Erfüllung der Rechenschaftspflicht gegenüber der Aufsichtsbehörde insbesondere Dokumentationen relevant, die zu diesem Zwecke erstellt wurden. Verantwortliche und Auftragsverarbeiter können daher nicht erwarten, dass ihnen die Datenschutz-Aufsichtsbehörde die Erfüllung der Rechenschaftspflicht abnimmt; sie können insbesondere nicht erwarten, dass die Datenschutz-Aufsichtsbehörde die Zulässigkeit durchgeführter Drittstaatentransfers würdigt, wenn keine oder keine ausreichenden Dokumentationen vorgelegt werden können. **126**

Bei Drittstaatentransfers – ausgenommen sind Videokonferenz-Systeme – akzeptiert der Bayerische Landesbeauftragte für den Datenschutz unter den oben unter Rn. 44 ff. dargelegten Anforderungen bis auf Weiteres grundsätzlich auch Dokumentationen zur Erfüllung der Rechenschaftspflicht, die auf eine Prüfung der tatsächlichen Wirksamkeit von Klauselwerken (siehe oben Rn. 62 ff.) verzichten. Vorausgesetzt ist dabei, **127**

- dass das vereinbarte Klauselwerk nach den Vorgaben unter Rn. 83 ff. auf den aktuellen Standardvertragsklauseln beruht und von diesen nicht abweicht, sowie
- dass der Datenexporteur nach den Vorgaben unter Rn. 73 ff., 88 und 93 eine ausreichend sicher gestaltete Verschlüsselung und/oder Pseudonymisierung vorsieht und anwendet.

# VIII. Prüfungsschema für internationale Datentransfers