Translations proofread by EDPB Members.
This language version has not yet been proofread.

Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten

Version 2.0

Angenommen am 18. Juni 2021

Versionsverlauf

Version 2.0	18. Juni 2021	Annahme der Leitlinien nach öffentlicher Konsultation
Version 1.0	10. November 2020	Annahme der Empfehlungen zur öffentlichen Konsultation

Zusammenfassung

Mit der Datenschutz-Grundverordnung (DSGVO) verfolgt die Europäische Union zwei Ziele: die Erleichterung des freien Verkehrs personenbezogener Daten in der Union bei gleichzeitigem Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere ihres Rechts auf den Schutz personenbezogener Daten.

In seinem jüngst ergangenen Urteil in der Rechtssache C-311/18 (Schrems II) erinnert uns der Gerichtshof der Europäischen Union (Gerichtshof) daran, dass der im Europäischen Wirtschaftsraum (EWR) geltende Schutz für personenbezogene Daten auch überall dort gewährleistet sein muss, wohin die Daten übermittelt werden. Wenn personenbezogene Daten in ein Drittland übermittelt werden, darf dies nicht dazu führen, dass das für sie geltende Schutzniveau hinter dem im EWR gewährten zurückbleibt oder verwässert wird. Der Gerichtshof hat dazu klargestellt, dass das Schutzniveau im Drittland nicht mit dem im EWR identisch, aber der Sache nach gleichwertig sein muss. Der Gerichtshof hat auch bestätigt, dass Standardvertragsklauseln als Übermittlungsinstrument dienen können, das auf vertraglichem Wege ein der Sache nach gleichwertiges Schutzniveau für in Drittländer übermittelte Daten gewährleistet.

Die Anwendung von Standardvertragsklauseln und anderen in Artikel 46 DSGVO genannten Übermittlungsinstrumenten erfolgt nicht in einem rechtlichen Vakuum. Der Gerichtshof hat ausgeführt, dass es einem Verantwortlichen oder Auftragsverarbeiter, der als Datenexporteur handelt, obliegt, in jedem Einzelfall – soweit angemessen, in Zusammenarbeit mit dem Datenimporteur im Drittland – zu prüfen, ob das Recht oder die Praxis des Drittlands die Effektivität der Garantien, die in den in Artikel 46 DSGVO genannten Übermittlungsinstrumenten enthalten sind, beeinträchtigt. In solchen Fällen lässt der Gerichtshof dem Verantwortlichen die Möglichkeit offen, zusätzliche Maßnahmen (auch ergänzende Maßnahmen genannt) zu ergreifen, um die Rechtsschutzlücken zu schließen und die Einhaltung des unionsrechtlichen Schutzniveaus zu gewährleisten. Der Gerichtshof macht keinerlei Vorgaben bezüglich der Art solcher Maßnahmen. Allerdings betont der Gerichtshof, dass die Datenexporteure in jedem Einzelfall die passenden Maßnahmen ermitteln müssen. Dies ergibt sich aus dem Grundsatz der Rechenschaftspflicht in Artikel 5 Absatz 2 DSGVO, der bestimmt, dass die Verantwortung für die Einhaltung der Grundsätze der DSGVO bei der Verarbeitung personenbezogener Daten bei den Verantwortlichen liegt, die die Einhaltung der DSGVO nachweisen können müssen.

Diese vom Europäischen Datenschutzausschuss (EDSA) erlassenen Empfehlungen sollen Datenexporteuren (ob Verantwortliche oder Auftragsverarbeiter, private oder staatliche Stellen, die im Anwendungsbereich der DSGVO personenbezogene Daten verarbeiten) bei der komplexen Aufgabe, die Datenschutzsituation in einem Drittland zu beurteilen und erforderlichenfalls geeignete zusätzliche Maßnahmen festzulegen, als Hilfe dienen. Die EDSA-Empfehlungen erläutern die von den Datenexporteuren zu befolgenden Schritte, informieren über potenzielle Informationsquellen und geben Beispiele für in Betracht kommende zusätzliche Maßnahmen.

Im **ersten Schritt** muss der Datenexporteur **seine Datenübermittlungen kennen**. Es kann recht kompliziert sein, alle Übermittlungen personenbezogener Daten in Drittländer zu erfassen. Man muss aber genau wissen, wohin die personenbezogenen Daten gehen, um sicherstellen zu können, dass diese, wo auch immer sie verarbeitet werden, der Sache nach ein gleichwertiges Schutzniveau genießen. Der Datenexporteur muss auch überprüfen, dass die von ihm übermittelten Daten für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sowie auf das notwendige Maß beschränkt sind.

Der **zweite Schritt** ist die **Überprüfung des gewählten Übermittlungsinstruments**: Ist es in Kapitel V DSGVO aufgeführt? Wenn die Europäische Kommission bereits in einem Angemessenheitsbeschluss gemäß Artikel 45 DSGVO oder in einer aufgrund der Vorgängerbestimmung (Richtlinie 95/46) ergangenen und noch gültigen Entscheidung erklärt hat, dass das Drittland, das Gebiet oder der Sektor, wohin die Übermittlung erfolgt, ein angemessenes Schutzniveau bietet, muss der Datenexporteur

nichts weiter tun, als zu überwachen, dass der Angemessenheitsbeschluss weiterhin gilt. Gibt es keinen Angemessenheitsbeschluss, muss der Datenexporteur von einem der in Artikel 46 DSGVO aufgeführten Übermittlungsinstrumente Gebrauch machen. Nur in einigen Fällen kann sich der Datenexporteur, sofern er die erforderlichen Voraussetzungen erfüllt, auf eine der in Artikel 49 DSGVO vorgesehenen Ausnahmen stützen. Ausnahmen dürfen jedoch in der Praxis nicht zur „Regel" werden, sondern müssen auf bestimmte Situationen beschränkt werden.

Der **dritte Schritt** ist die **Beurteilung** der Frage, ob die Effektivität der geeigneten Garantien, die die vom Datenexporteur gewählten Übermittlungsinstrumente bieten, im Kontext der vorgesehenen Übermittlung möglicherweise durch die Rechtsvorschriften oder Praktiken des Drittlands beeinträchtigt werden. Die Beurteilung des Datenexporteurs sollte sich in allererster Linie auf die Rechtsvorschriften des Drittlands konzentrieren, die für seine Datenübermittlung relevant sind, und auf das von ihm gewählte Übermittlungsinstrument gemäß Artikel 46 DSGVO. Auch anhand der Praktiken der Behörden des Drittlandes können Sie prüfen, ob die im Übermittlungsinstrument enthaltenen Garantien in der Praxis den wirksamen Schutz der übermittelten personenbezogenen Daten gewährleisten können. Eine Prüfung dieser Praktiken ist für die Beurteilung durch den Datenexporteur besonders relevant, wenn

(i.) die Rechtsvorschriften in dem Drittland zwar formal den EU-Standards entsprechen, in der Praxis aber offensichtlich nicht angewandt/eingehalten werden;

(ii.) es Praktiken gibt, die mit den Verpflichtungen des Übertragungsinstruments unvereinbar sind, wenn einschlägige Rechtsvorschriften in dem Drittland fehlen;

(iii.) die vom Datenexporteur übermittelten Daten und/oder der Datenimporteur unter problematische Rechtsvorschriften fallen (wenn also die vertragliche Garantie des Übermittlungsinstruments, dass ein der Sache nach gleichwertiges Schutzniveau gewährleistet ist, und die EU-Standards in Bezug auf Grundrechte, Notwendigkeit und Verhältnismäßigkeit nicht eingehalten werden).

In den ersten beiden Fällen ist der Datenexporteur gehalten, die Übermittlung auszusetzen oder angemessene ergänzende Maßnahmen zu ergreifen, wenn er die Übermittlung fortsetzen möchten.

Im dritten Fall kann sich der Datenexporteur in Anbetracht von Ungewissheiten im Zusammenhang mit der potenziellen Anwendung problematischer Rechtsvorschriften auf seine Übermittlung für eine Aussetzung der Übermittlung bzw. deren Durchführung nach zusätzlichen Maßnahmen entscheiden; alternativ kann er beschließen, die Übermittlung ohne Durchführung zusätzlicher Maßnahmen vorzunehmen, wenn er der Auffassung und in der Lage ist, nachzuweisen und zu dokumentieren, dass er keinen Grund zu der Annahme haben, dass die einschlägigen und problematischen Rechtsvorschriften in der Praxis so ausgelegt und/oder angewandt werden, dass sie seine übermittelten Daten und seinen Datenimporteur abdecken.

Was die Beurteilung der Rechtslage in Bezug auf Überwachungszwecken dienende Datenzugriffe staatlicher Stellen angeht, wird auf die Empfehlungen des EDSA zu den „Wesentlichen europäischen Garantien" verwiesen.

Der Datenexporteur sollte diese Beurteilung mit der gebotenen Sorgfalt durchführen und sie sorgfältig dokumentieren. Seine zuständigen Aufsichts- und/oder Justizbehörden können dies verlangen und ihn für jede Entscheidung, die er auf dieser Grundlage trifft, zur Rechenschaft ziehen.

Der **vierte Schritt** betrifft die **Auswahl und Anwendung der zusätzlichen Maßnahmen**, die erforderlich sind, um ein Schutzniveau für die übermittelten Daten zu erzielen, das der Sache nach dem unionsrechtlichen Standard gleichwertig ist. Dieser Schritt ist allerdings nur erforderlich, wenn die Beurteilung ergibt, dass die Rechtsvorschriften und/oder Praktiken im Drittland die Effektivität der vom Datenexporteur gewählten Übermittlungsinstrumente in Artikel 46 DSGVO im Kontext der von ihm durchgeführten oder beabsichtigten Übermittlung beeinträchtigen. Diese Empfehlungen enthalten (im Anhang 2) eine nicht erschöpfende Liste von Beispielen für zusätzliche Maßnahmen und

die Voraussetzungen für deren Effektivität. Ähnlich wie im Fall der geeigneten Garantien, die in den Übermittlungsinstrumenten nach Artikel 46 enthalten sind, kann es auch bei den zusätzlichen Maßnahmen so sein, dass sie in einigen Ländern effektiv sind, in anderen jedoch nicht. Der Datenexporteur ist dafür verantwortlich, ihre Effektivität im Kontext der betreffenden Übermittlung und im Lichte der Rechtsvorschriften und Praktiken im Drittland und des ausgewählten Übermittlungsinstruments zu beurteilen, wobei er für die von ihm auf dieser Grundlage getroffene Entscheidung rechenschaftspflichtig ist. Unter Umständen ist es auch erforderlich, mehrere zusätzliche Maßnahmen zu kombinieren. Es kann vorkommen, dass der Datenexporteur letztendlich feststellt, dass es keinerlei zusätzliche Maßnahme gibt, die für die vorgesehene Übermittlung ein der Sache nach gleichwertiges Schutzniveau gewährleisten kann. In Fällen, in denen es keine geeignete zusätzliche Maßnahme gibt, muss der Datenexporteur die Übermittlung vermeiden, sie aussetzen oder beenden, um eine Beeinträchtigung des Schutzniveaus für die personenbezogenen Daten zu verhindern. Auch die Bewertung der zusätzlichen Maßnahmen ist mit der gebotenen Gründlichkeit durchzuführen und zu dokumentieren.

Der **fünfte Schritt** ist die **Einleitung aller förmlichen Verfahrensschritte**, die ggf. für die zusätzliche Maßnahme erforderlich sind, je nachdem, welches der in Artikel 46 DSGVO genannten Übermittlungsinstrumente der Datenexporteur auswählt. Einige dieser Verfahrensschritte sind in diesen Empfehlungen angegeben. Für einige dieser Verfahrensschritte kann es erforderlich sein, dass der Datenexporteur mit seiner zuständigen Aufsichtsbehörde Rücksprache nimmt.

Der **sechste und letzte Schritt** besteht darin, dass der Datenexporteur die Beurteilung des Schutzniveaus in den Drittländern, in die er die personenbezogenen Daten übermittelt, in geeigneten Abständen überprüfen und **neu bewerten** sowie laufend daraufhin überwachen muss, ob es Entwicklungen gibt, die das Schutzniveau beeinträchtigen könnten. Der Grundsatz der Rechenschaftspflicht erfordert ständige Wachsamkeit hinsichtlich des Schutzniveaus für die personenbezogenen Daten.

Die Aufsichtsbehörden werden die ihnen übertragene Aufgabe, die Anwendung der DSGVO zu überwachen und die DSGVO durchzusetzen, weiter wahrnehmen. Die Aufsichtsbehörden werden die Maßnahmen, die die Datenexporteure ergreifen, um für die von ihnen übermittelten Daten ein der Sache nach gleichwertiges Schutzniveau zu gewährleisten, genau prüfen. Der Gerichtshof erinnert daran, dass die Aufsichtsbehörden Datenübermittlungen aussetzen oder verbieten, wenn eine Untersuchung oder Beschwerde ergibt, dass die Gewährleistung eines der Sache nach gleichwertiges Schutzniveau nicht möglich ist.

Die Datenschutzbehörden werden weiterhin Leitlinien für Datenexporteure erarbeiten und ihre Maßnahmen im EDSA koordinieren, um eine einheitliche Anwendung des Datenschutzrechts der Union zu gewährleisten.

INHALTSVERZEICHNIS

Der Europäische Datenschutzausschuss –

gestützt auf Artikel 70 Absatz 1 Buchstabe e der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (im Folgenden: DSGVO),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum (EWR), insbesondere auf Anhang XI und das Protokoll 37, in der durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018 geänderten Fassung[1],

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung –

in Erwägung nachstehender Gründe:

(1) Der Gerichtshof der Europäischen Union (Gerichtshof) kommt in seinem Urteil vom 16. Juli 2020 in der Rechtssache *Data Protection Commissioner gegen Facebook Ireland Ltd, Maximillian Schrems*, C-311/18 zu dem Ergebnis, dass Artikel 46 Absatz 1 und Artikel 46 Absatz 2 Buchstabe c der DSGVO dahin auszulegen sind, dass die nach diesen Vorschriften erforderlichen geeigneten Garantien, durchsetzbaren Rechte und wirksamen Rechtsbehelfe gewährleisten müssen, dass die Rechte der Personen, deren personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt werden, ein Schutzniveau genießen, das dem in der Europäischen Union durch diese Verordnung im Licht der Charta der Grundrechte der Europäischen Union garantierten Niveau der Sache nach gleichwertig ist.[2]

(2) Wie der Gerichtshof hervorgehoben hat, ist für natürliche Personen ein Schutzniveau zu gewährleisten, das der Sache nach demjenigen entspricht, das in der Europäischen Union durch die im Lichte der Charta ausgelegte DSGVO gewährleistet wird, unabhängig davon, aufgrund welcher Bestimmung des Kapitels V die jeweilige Übermittlung personenbezogener Daten in ein Drittland erfolgt. Die Bestimmungen in Kapitel V sollen nämlich den Fortbestand des hohen Schutzniveaus bei der Übermittlung personenbezogener Daten in ein Drittland gewährleisten.[3]

(3) Nach Erwägungsgrund 108 und Artikel 46 Absatz 1 DSGVO gilt für den Fall, dass kein unionsrechtlicher Angemessenheitsbeschluss vorliegt, dass der Verantwortliche oder der Auftragsverarbeiter als Ausgleich für die in einem Drittland bestehende Datenschutzlücke geeignete Garantien für den Schutz der betroffenen Person vorsehen muss. Der Verantwortliche oder Auftragsverarbeiter kann geeignete Garantien geben, ohne dass er dazu einer besonderen aufsichtsbehördlichen Genehmigung bedarf, indem er von einem der in Artikel 46 Absatz 2 DSGVO

[1] Soweit hierin auf „Mitgliedstaaten“ Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten“ zu verstehen.
[2] Urteil des EuGH vom 16. Juli 2020, Data Protection Commissioner gegen Facebook Ireland Ltd, Maximillian Schrems, (C-311/18, ECLI:EU:C:2020:559) (im Folgenden: C-311/18 (Schrems II)), Tenor, Nr. 2.
[3] C-311/18 (Schrems II), Rn. 92 und 93.

aufgeführten Übermittlungsinstrumente Gebrauch macht, z. B. indem er Standarddatenschutzklauseln verwendet.

(4) Der Gerichtshof hat klargestellt, dass die von der Kommission erlassenen Standarddatenschutzklauseln nur darauf abzielen, den in der Europäischen Union ansässigen Verantwortlichen bzw. Auftragsverarbeitern vertragliche Garantien zu bieten, die in allen Drittländern einheitlich gelten. Wegen ihres Vertragscharakters können Standarddatenschutzklauseln drittstaatliche Behörden, die ja nicht Vertragspartei sind, nicht binden. Es kann sich daher als notwendig erweisen, die Garantien in den Standarddatenschutzklauseln um zusätzliche Maßnahmen zu ergänzen, um in einem bestimmten Drittland das durch das Unionsrecht verbürgte Schutzniveau sicherzustellen. Der Gerichtshof verweist auf Erwägungsgrund 109 der DSGVO, der diese Möglichkeit erwähnt und Verantwortliche und Auftragsverarbeiter ermutigt, davon Gebrauch zu machen.[4]

(5) Der Gerichtshof hat ausgeführt, dass es vor allem dem Datenexporteur obliegt, in jedem Einzelfall – falls angemessen, in Zusammenarbeit mit dem Datenimporteuer – zu prüfen, ob das Recht des Bestimmungsdrittlands nach Maßgabe des Unionsrechts einen der Sache nach gleichwertigen Schutz der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleistet, und, soweit erforderlich, über die durch diese Klauseln gebotenen Garantien hinaus zusätzliche Maßnahmen zu ergreifen.[5]

(6) Kann der in der Europäischen Union ansässige Verantwortliche bzw. Auftragsverarbeiter keine hinreichenden zusätzlichen Maßnahmen ergreifen, um einen der Sache nach gleichwertigen Schutz zu gewährleisten, ist er – bzw. in zweiter Linie die zuständige Aufsichtsbehörde – verpflichtet, die Übermittlung personenbezogener Daten in das betreffende Drittland auszusetzen oder zu beenden.[6]

(7) Weder in der DSGVO noch im Urteil des Gerichtshofs sind die „zusätzlichen Garantien", „zusätzlichen Maßnahmen" oder „ergänzenden Maßnahmen" definiert, die die Verantwortlichen und Auftragsverarbeiter über die in den Übermittlungsinstrumenten in Artikel 46 Absatz 2 DSGVO enthaltenen Garantien hinaus geben bzw. ergreifen können, um in einem bestimmten Drittland das durch das Unionsrecht verbürgte Schutzniveau sicherzustellen.

(8) Der EDSA hat beschlossen, diese Frage von sich aus zu untersuchen und den als Datenexporteure handelnden Verantwortlichen und Auftragsverarbeitern Empfehlungen zu dem Verfahren zu geben, nach dem sie zusätzliche Maßnahmen auswählen und anwenden können. Diese Empfehlungen sollen den Datenexporteuren eine Methode an die Hand geben, nach der sie feststellen können, ob – und ggf. welche – ergänzenden Maßnahmen sie für ihre Datenübermittlungen benötigen. Die Verantwortung dafür, dass für die übermittelten Daten im Drittland ein Schutzniveau gewährleistet ist, das dem Schutzniveau im EWR der Sache nach vergleichbar ist, liegt in erster Linie bei den Datenexporteuren. Mit diesen Empfehlungen möchte der EDSA im Rahmen der ihm übertragenen Aufgabe eine einheitliche Anwendung der DSGVO und der Entscheidung des Gerichtshofs sicherstellen[7] –

HAT FOLGENDE EMPFEHLUNGEN ANGENOMMEN:

---

[4] C-311/18 (Schrems II), Rn. 132 und 133.
[5] C-311/18 (Schrems II), Rn. 134.
[6] C-311/18 (Schrems II), Rn. 135.
[7] Artikel 70 Absatz 1 Buchstabe e DSGVO.

1 RECHENSCHAFTSPFLICHT IM BEREICH DER DATENÜBERMITTLUNG

1. Im Primärrecht der Union ist das Recht auf Datenschutz als Grundrecht geschützt.[8] Das Recht auf Datenschutz genießt daher ein hohes Maß an Schutz und jede Einschränkung muss gesetzlich vorgesehen sein und den Wesensgehalt des Rechts achten; sie muss verhältnismäßig und erforderlich sein und den von der Union anerkannten, dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.[9] Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden.[10]

2. Wenn Daten in Drittländer außerhalb des EWR übermittelt werden, müssen sie auch dort ein der Sache nach gleichwertiges Schutzniveau genießen, damit gewährleistet ist, dass das durch die DSGVO verbürgte Schutzniveau nicht untergraben wird.

3. Das Recht auf Datenschutz erfordert aktives Handeln. Eine passive Einhaltung – dass Datenexporteure und Datenimporteure (ob Verantwortliche und/oder Auftragsverarbeiter) das Recht einfach nur anerkennen oder jedenfalls nicht dagegen verstoßen – genügt nicht.[11] Die Verantwortlichen und Auftragsverarbeiter müssen aktiv und kontinuierlich dafür sorgen, dass das Recht auf Datenschutz stets eingehalten ist, indem sie rechtliche, technische und organisatorische Maßnahmen ergreifen, die die Wirksamkeit des Rechts gewährleisten. Die Verantwortlichen und Auftragsverarbeiter müssen diese Maßnahmen auch den betroffenen Personen und den Datenschutzaufsichtsbehörden gegenüber nachweisen können. Dies ist der sogenannte Grundsatz der Rechenschaftspflicht.[12]

4. Der Grundsatz der Rechenschaftspflicht, der zur Sicherstellung der wirksamen Anwendung des durch die DSGVO verbürgten Schutzniveaus erforderlich ist, gilt auch für Datenübermittlungen in Drittländer[13], da diese als solche eine Form der Datenverarbeitung darstellen[14]. Wie der Gerichtshof in seinem Urteil hervorgehoben hat, ist ein Schutzniveau zu gewährleisten, das im Wesentlichen dem in der Europäischen Union durch die im Lichte der Charta ausgelegte DSGVO gewährleisteten entspricht, unabhängig davon, aufgrund welcher Bestimmung des Kapitels VI die Übermittlung personenbezogener Daten ins Drittland erfolgt.[15]

5. In seinem Schrems II-Urteil hat der Gerichtshof betont, dass die Datenexporteure und Datenimporteure dafür verantwortlich sind, sicherzustellen, dass die personenbezogenen Daten aktuell und künftig das nach dem Datenschutzrecht der Union verbürgte Schutzniveau genießen,

---

[8] Artikel 8 Absatz 1 der Charta der Grundrechte und Artikel 16 Absatz 1 AEUV, Erwägungsgrund 1 und Artikel 1 Absatz 2 DSGVO.
[9] Artikel 52 Absatz 1 der Charta der Grundrechte.
[10] Erwägungsgrund 4 der DSGVO und Urteil des Gerichtshofs vom 24.9.2019, Google (Räumliche Reichweite der Auslistung) (C-507/17, ECLI:EU:C:2019:772, Rn. 60).
[11] Schlussanträge der Generalanwältin Eleanor Sharpston vom 17. Juni 2010 in der Rechtssache Volker und Markus Schecke und Eifert (C-92/09 und C-93/09, ECLI:EU:C:2010:353, Nr. 71).
[12] Artikel 5 Absatz 2 und Artikel 28 Absatz 3 Buchstabe h DSGVO.
[13] Artikel 44 und Erwägungsgrund 101 DSGVO wie auch Artikel 47 Absatz 2 Buchstabe d DSGVO.
[14] Urteil des EuGH vom 6. Oktober 2015, *Maximillian Schrems gegen Data Protection Commissioner*, (C-362/14, EU:C:2015:650 (im Folgenden: Schrems I), Rn. 45).
[15] C-311/18 (Schrems II), Rn. 92 und 93.

und dass die Datenexporteure die Übermittlung aussetzen und/oder vom Vertrag zurücktreten müssen, wenn dem Datenimporteur die Einhaltung der in den einschlägigen Vertrag zwischen dem Datenexporteur und dem Datenimporteur aufgenommenen Standarddatenschutzklauseln nicht oder nicht mehr möglich ist.[16] Der als Datenexporteur handelnde Verantwortliche oder Auftragsverarbeiter muss sicherstellen, dass die Datenimporteure hinsichtlich ihrer Erfüllung dieser Verantwortlichkeiten mit ihm zusammenarbeiten, um ihn z. B. über die Entwicklungen auf dem Laufenden zu halten, die das Schutzniveau betreffen, das für die personenbezogenen Daten im Land des Importeurs gilt, wenn diese dort befinden.[17] Diese Verantwortlichkeiten ergeben sich aus der Anwendung des in der DSGVO niedergelegten Grundsatzes der Rechenschaftspflicht auf Datenübermittlungen.[18]

2 FAHRPLAN: DIE ANWENDUNG DES GRUNDSATZES DER RECHENSCHAFTSPFLICHT AUF DATENÜBERMITTLUNGEN IN DER PRAXIS

6. Es folgt ein Fahrplan, der angibt, wie der Datenexporteur vorgehen muss, um festzustellen, ob er zur rechtmäßigen Übermittlung in ein Land außerhalb des EWR zusätzliche Maßnahmen ergreifen muss. Dieses Dokument richtet sich an den als Datenexporteur handelnden Verantwortlichen oder Auftragsverarbeiter,[19] der personenbezogene Daten im Sinne der DSGVO verarbeitet – dies betrifft die Verarbeitung durch private Stellen wie auch durch staatliche Stellen im Zuge der Datenübermittlung an private Stellen.[20] Was Übermittlungen personenbezogener Daten zwischen staatlichen Stellen angeht, wird auf die spezifischen Ausführungen in den Leitlinien 2/2020 zu Artikel 46 Absatz 2 Buchstabe a und Artikel 46 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] verwiesen.[21]

7. Diese Bewertung wie auch die zusätzlichen Maßnahmen, die vom Datenexporteur ausgewählt und angewendet werden, sind ordnungsgemäß zu dokumentieren; die Dokumentation ist der zuständigen Aufsichtsbehörde auf Verlangen vorzulegen.[22]

---

[16] C-311/18 (Schrems II), Rn. 134, 135, 139, 140, 141 und 142.
[17] C-311/18 (Schrems II), Rn. 134.
[18] Artikel 5 Absatz 2 und Artikel 28 Absatz 3 Buchstabe h DSGVO.
[19] Daher gelten Sie beispielsweise nicht als Datenexporteur, wenn Sie eine betroffene Person sind, die Ihre personenbezogenen Daten über einen Online-Fragebogen an einen in einem Drittland niedergelassenen Verantwortlichen weitergibt.
[20] Vgl. EDSA, Leitlinien 3/2018 zum räumlichen Anwendungsbereich der DSGVO (Artikel 3) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_de
[21] EDSA, Leitlinien 2/2020 zu Artikel 46 Absatz 2 Buchstabe a und Artikel 46 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; vgl. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_de
[22] Artikel 5 Absatz 2 DSGVO und Artikel 24 Absatz 1 DSGVO.

2.1 Schritt 1: Die Datenübermittlungen kennen

8. Möchte ein Datenexporteur festzustellen, was er tun muss, um künftig die Übermittlung personenbezogener Daten fortzusetzen oder neu zu beginnen,[23] muss er im ersten Schritt sicherstellen, dass er volle Kenntnis von allen seinen Übermittlungen hat („Know your Transfers"). Die Aufzeichnung und Erfassung sämtlicher Übermittlungen kann recht kompliziert sein, wenn es sich um eine Organisation handelt, die regelmäßig eine Vielzahl verschiedener Übermittlungen in Drittländer vornimmt und dafür mehrere Auftragsverarbeiter und Unterauftragsverarbeiter einsetzt. Alle diese Übermittlungen zu kennen ist aber der wesentliche erste Schritt zur Erfüllung der sich aus dem Grundsatz der Rechenschaftspflicht ergebenden Obliegenheiten.

9. Um sich volle Kenntnis der eigenen Übermittlungen zu verschaffen, kann man auf das Verzeichnis von Verarbeitungstätigkeiten zurückgreifen, dass man als Verantwortlicher oder Auftragsverarbeiter gemäß Artikel 30 DSGVO zu führen verpflichtet ist.[24] Es kann auch hilfreich sein, auf die Mitteilungen zurückzugreifen, mit denen der Datenexporteur seine Pflichten aus Artikel 13 Absatz 1 Buchstabe f und Artikel 14 Absatz 1 Buchstabe f erfüllt und betroffene Personen über die Übermittlung ihrer personenbezogenen Daten in Drittländer unterrichtet hat.[25]

10. Bei der Erfassung der Übermittlungen ist darauf zu achten, dass auch die Weiterübermittlung erfasst wird, wenn beispielsweise die für den Datenexporteur tätigen Auftragsverarbeiter außerhalb des EWR die personenbezogenen Daten, die sie vom Datenexporteur empfangen haben, an einen Unterauftragsverarbeiter in einem anderen Drittland oder im selben Drittland übermitteln.[26]

---

[23] Dabei ist zu beachten, dass auch der Fernzugriff, den eine Stelle in einem Drittland auf im EWR befindliche Daten hat, eine Übermittlung darstellt.

[24] Vgl. Artikel 30 DSGVO, insbesondere Absatz 1 Buchstabe e und Absatz 2 Buchstabe c. Das vom Datenexporteur geführte Verzeichnis von Verarbeitungstätigkeiten sollte auch eine Beschreibung der Verarbeitungstätigkeiten enthalten (einschließlich unter anderem der Kategorien betroffener Person, der Kategorien personenbezogener Daten und der Verarbeitungszwecke sowie spezifischen Angaben zu den Datenübermittlungen). Es gibt einige Verantwortliche und Auftragsverarbeiter, für die die Pflicht, ein Verzeichnis von Verarbeitungstätigkeiten zu führen, nicht gilt (Artikel 30 Absatz 5 DSGVO). Hinsichtlich dieser Ausnahme vgl. Artikel-29-Datenschutzgruppe, Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30.5 GDPR [Positionspapier zu den Ausnahmen von der Verpflichtung, ein Verzeichnis von Verarbeitungstätigkeiten im Sinne von Artikel 30 Absatz 5 DSGVO zu führen] (vom EDSA gebilligt am 25. Mai 2018).

[25] Gemäß den Transparenzregeln der DSGVO muss der Datenexporteur die betroffenen Personen über die Übermittlung ihrer Daten in Drittländer unterrichten (Artikel 13 Absatz 1 Buchstabe f und Artikel 14 Absatz 1 Buchstabe f DSGVO). Insbesondere muss er mitteilen, ob es einen Angemessenheitsbeschluss der Europäischen Kommission gibt oder nicht; im Falle von Übermittlungen gemäß Artikel 46, Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 DSGVO sind die geeigneten oder angemessenen Garantien anzugeben, wobei auch mitzuteilen ist, wo die betreffenden Dokumente angefordert oder eingesehen werden können. Die der betroffenen Person mitgeteilten Angaben müssen zutreffend und aktuell sein und insbesondere den sich aus der Rechtsprechung des Gerichtshofs ergebenden Anforderungen an Übermittlungen genügen.

[26] Dies bedarf gemäß Artikel 28 Absatz 2 DSGVO stets der vorherigen gesonderten oder allgemeinen schriftlichen Genehmigung des Verantwortlichen.

11. Gemäß dem DSGVO-Grundsatz der „Datenminimierung“[27] muss der Datenexporteur auch überprüfen, dass die von ihm übermittelten Daten angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sind.

12. All dies muss geschehen sein, bevor die Übermittlung erstmals erfolgt bzw., falls die Datenübermittlung ausgesetzt worden ist, bevor die Datenübermittlung wieder aufgenommen wird. Der Datenexporteur muss wissen, wo sich die von ihm exportierten Daten befinden bzw. wo sie von den Datenimporteuren verarbeitet werden (Karte der Bestimmungsdrittländer).

13. Dabei ist zu beachten, dass auch der Fernzugriff aus einem Drittland (z. B. im Support-Fall) und/oder zur Speicherung in einer Cloud außerhalb des EWR durch einen Diensteanbieter als Übermittlung anzusehen ist.[28] Insbesondere wenn der Datenexporteur eine internationale Cloud-Infrastruktur benutzt, muss er feststellen, ob seine Daten in Drittländer übermittelt werden, und ggf. in welche Länder, es sei denn, der Cloud-Provider ist im EWR niedergelassen und hat im Vertrag ausdrücklich angegeben, dass keinerlei Verarbeitung der Daten in Drittländern stattfindet.

2.2 Schritt 2: Auswahl der eingesetzten Übermittlungsinstrumente

14. Im zweiten Schritt ist zu ermitteln, welche der in Kapitel V DSGVO aufgeführten und vorgesehenen Übermittlungsinstrumente der Datenexporteur verwendet.

Angemessenheitsbeschlüsse

15. Die Europäische Kommission kann mit ihren **Angemessenheitsbeschlüssen** für einige oder sämtliche der Drittländer, in die Datenexporteure personenbezogene Daten übermitteln, anerkennen, dass dort ein angemessenes Schutzniveau für personenbezogene Daten besteht.[29]

16. Ein solcher Angemessenheitsbeschluss hat die Wirkung, dass personenbezogene Daten aus dem EWR an dieses Drittland fließen können, ohne dass es nötig ist, von einem der in Artikel 46 DSGVO aufgeführten Übermittlungsinstrumente Gebrauch zu machen.

17. Angemessenheitsbeschlüsse können für ein gesamtes Land gelten oder auf einen Teil beschränkt sein. Angemessenheitsbeschlüsse können für alle Datenübermittlungen in ein Land gelten oder auf bestimmte Arten von Übermittlungen beschränkt sein (z. B. Übermittlungen in einen bestimmten Sektor).[30]

---

[27] Artikel 5 Absatz 1 Buchstabe c DSGVO.
[28] Siehe Frage Nr. 11: „…dabei ist jedoch zu beachten, dass auch die Gewährung des Zugangs zu Daten aus einem Drittland, beispielsweise zu Verwaltungszwecken, einer Übermittlung gleichkommt“; 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, 23.7.2020.
[29] Gemäß Artikel 45 DSGVO kann die Europäische Kommission ggf. für ein Land außerhalb der EU durch Beschluss feststellen, dass es ein angemessenes Datenschutzniveau bietet. In gleicher Weise kann die Europäische Kommission auch für eine internationale Organisation durch Beschluss feststellen, dass diese ein angemessenes Schutzniveau bietet.
[30] Artikel 45 Absatz 1 DSGVO.

18. Die Europäische Kommission veröffentlicht eine Liste ihrer Angemessenheitsbeschlüsse auf ihrer Website.[31]

19. Ein Datenexporteur, der personenbezogene Daten in ein Drittland, ein Gebiet oder einen oder mehrere spezifische Sektoren in diesem Drittland übermittelt, für welche(s) die Kommission einen einschlägigen Angemessenheitsbeschluss erlassen hat, **muss keine der weiteren in diesen Empfehlungen beschriebenen Schritte befolgen**.[32] Allerdings muss er fortlaufend überwachen, ob die für seine Übermittlungen relevanten Angemessenheitsbeschlüsse möglicherweise widerrufen oder für ungültig erklärt worden sind.[33]

20. Allerdings hindert ein Angemessenheitsbeschluss betroffene Personen nicht daran, Beschwerde einzulegen. Auch die Aufsichtsbehörden sind, wenn sie Zweifel an der Gültigkeit des Angemessenheitsbeschlusses haben, nicht gehindert, Klage vor den nationalen Gerichten zu erheben, damit diese um eine Vorabentscheidung des Gerichtshofs über die Gültigkeit des Angemessenheitsbeschlusses ersuchen können.[34]

Beispiel:

Herr Schrems, ein Unionsbürger, legte im Juni 2013 beim irischen Data Protection Commissioner (DPC) eine Beschwerde ein, mit der er diesen im Wesentlichen aufforderte, die Untersagung oder Aussetzung der Übermittlung seiner personenbezogenen Daten durch Facebook Ireland in die Vereinigten Staaten anzuordnen; dazu machte Herr Schrems geltend, dass nach dem Recht und der Praxis der Vereinigten Staaten kein ausreichender Schutz der dort gespeicherten personenbezogenen Daten vor den Überwachungstätigkeiten der dortigen Behörden gewährleistet sei. Die Beschwerde wurde vom DPC als unbegründet zurückgewiesen, der sich insbesondere auf die Entscheidung 2000/520 (die Safe-Harbor-Entscheidung) der Kommission stützte, in der den Vereinigten Staaten im Rahmen der Safe-Harbour-Regelung ein angemessenes Schutzniveau für die übermittelten personenbezogenen Daten attestiert worden war. Herr Schrems erhob gegen die Entscheidung des DPC Klage beim irischen High Court, der seinerseits den Gerichtshof der Europäischen Union (EuGH) um eine Vorabentscheidung zur

[31] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[32] Dies gilt, sofern Datenexporteur und Datenimporteur Maßnahmen ergriffen haben, die zur Erfüllung der übrigen nach der DSGVO bestehenden Verpflichtungen erforderlich sind; ist dies nicht der Fall, sind derartige Maßnahmen zu ergreifen.

[33] Die Europäische Kommission muss alle Angemessenheitsbeschlüsse regelmäßig überprüfen und überwachen, ob die Drittländer, für die Angemessenheitsbeschlüsse erlassen wurden, nach wie vor ein angemessenes Schutzniveau gewährleisten (vgl. Artikel 45 Absätze 3 und 4 DSGVO). Angemessenheitsbeschlüsse können auch vom Gerichtshof für ungültig erklärt werden (vgl. die Urteile in den Rechtssachen C-362/14 (Schrems I) und C-311/18 (Schrems II)).

[34] C-311/18 (Schrems II), Rn. 118 bis 120. Das Fehlen eines angemessenen Schutzniveaus ist, für sich genommen, kein Grund, der die Aufsichtsbehörden berechtigen würde, einen Angemessenheitsbeschluss unangewendet zu lassen oder die Übermittlung personenbezogener Daten in die betreffenden Länder auszusetzen oder zu untersagen. Die aufsichtsbehördliche Aussetzung oder Untersagung der Übermittlung personenbezogener Daten in das betreffende Drittland muss vielmehr auf andere Gründe gestützt sein (z. B. Verstoß gegen Artikel 32 DSGVO wegen unzureichender Sicherheitsvorkehrungen; Verstoß gegen Artikel 6 DSGVO mangels gültiger Rechtsgrundlage für die Verarbeitung). Die nationalen Aufsichtsbehörden können in völliger Unabhängigkeit prüfen, ob bei der Datenübermittlung die in der DSGVO festgelegten Anforderungen gewahrt werden, und gegebenenfalls Klage vor den nationalen Gerichten erheben, damit diese, falls sie Zweifel an der Gültigkeit des Angemessenheitsbeschlusses der Kommission haben, den Gerichtshof der Europäischen Union um eine Vorabentscheidung über die Gültigkeit des Angemessenheitsbeschlusses ersuchen.

Frage der Gültigkeit der Entscheidung 2000/520 ersuchte. Die Entscheidung der Kommission 2000/520 über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ gewährleisteten Schutzes wurde vom EuGH für ungültig befunden.[35]

In Artikel 46 DSGVO vorgesehene Übermittlungsinstrumente

21. In Artikel 46 DSGVO sind eine Reihe von Übermittlungsinstrumenten aufgeführt, die „*geeignete Garantien*“ enthalten und von Datenexporteuren verwendet werden können, um personenbezogene Daten in Drittländer, für die es keine Angemessenheitsbeschlüsse gibt, zu übermitteln. Bei den in Artikel 46 DSGVO genannten Arten von Übermittlungsinstrumenten handelt es sich im Wesentlichen um:

- Standarddatenschutzklauseln (auch als Standardvertragsklauseln (SVK) bezeichnet);
- verbindliche interne Datenschutzvorschriften (BCR);
- Verhaltensregeln;
- Zertifizierungsmechanismen (auch als Zertifizierungsverfahren bezeichnet);
- ad hoc vereinbarte Vertragsklauseln.

22. Ganz gleich, für welches in Artikel 46 DSGVO vorgesehene Übermittlungsinstrument man sich entscheidet, ist stets sicherzustellen, dass die übermittelten personenbezogenen Daten insgesamt ein der Sache nach gleichwertiges Schutzniveau genießen.

23. Die in Artikel 46 DSGVO vorgesehenen Übermittlungsinstrumente enthalten vor allem geeignete vertragliche Garantien, die für alle Drittländer einheitlich angewendet werden können. Wegen der besonderen Gegebenheiten in dem Drittland, in das die Daten übermittelt werden, kann es allerdings erforderlich sein, dass der Datenexporteur diese Übermittlungsinstrumente um zusätzliche Maßnahmen (zuweilen auch als „ergänzende Maßnahmen“ bezeichnet) ergänzt, um ein der Sache nach gleichwertiges Schutzniveau zu gewährleisten.[36]

Ausnahmen

24. Neben Angemessenheitsbeschlüssen und Übermittlungsinstrumenten gemäß Artikel 46 DSGVO sieht die DSGVO noch einen dritten Weg vor, auf dem die Übermittlung personenbezogener Daten unter bestimmten Umständen zulässig sein kann. Sofern bestimmte Voraussetzungen erfüllt sind, kann der Datenexporteur die personenbezogenen Daten auch aufgrund eines der in Artikel 49 DSGVO vorgesehenen Ausnahmetatbestände übermitteln.

25. Artikel 49 DSGVO ist eine Ausnahmeregelung. Die darin enthaltenen Ausnahmen müssen so ausgelegt werden, dass sie nicht im Widerspruch zur Natur der Ausnahmeregelungen stehen, da sie Ausnahmen von der Regel darstellen, dass personenbezogene Daten nur dann in ein Drittland übermittelt werden dürfen, wenn das Land ein angemessenes Datenschutzniveau oder alternativ geeignete Garantien vorsieht. Ausnahmen dürfen jedoch in der Praxis nicht zur „Regel“ werden,

[35] Rechtssache C-362/14 (Schrems I).
[36] C-311/18 (Schrems II), Rn. 130 und 133. Siehe auch nachstehend Abschnitt 2.3.

sondern müssen auf bestimmte Situationen beschränkt werden. Der EDSA hat dazu seine Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679 erlassen. [37]

26. Wer sich auf einen Ausnahmetatbestand in Artikel 49 DSGVO stützen will, muss sehr genau prüfen, ob die beabsichtigte Übermittlung tatsächlich die sehr strengen Tatbestandsvoraussetzungen erfüllt, die für die einzelnen Ausnahmen gelten.

***

27. Ein Datenexporteur, für dessen Übermittlung weder ein Angemessenheitsbeschluss noch ein Ausnahmetatbestand nach Artikel 49 als Rechtsgrundlage in Betracht kommt, muss Schritt 3 befolgen.

2.3 Schritt 3: Beurteilung der Wirksamkeit des ausgewählten Übermittlungsinstruments gemäß Artikel 46 DSGVO im Hinblick auf die Gesamtumstände der Übermittlung

28. Das gewählte Übermittlungsinstrument nach Artikel 46 DSGVO muss wirksam sicherstellen, dass das durch die DSGVO garantierte Schutzniveau durch die Übermittlung in der Praxis nicht untergraben wird. [38]

29. Insbesondere muss der Schutz der übermittelten personenbezogenen Daten im Drittland der Sache nach dem Schutz gleichwertig sein, der im EWR durch die DSGVO im Licht der Charta der Grundrechte der Europäischen Union garantiert wird. [39] Dies ist nicht der Fall, wenn der Datenimporteur wegen der Rechtsvorschriften und Praktiken, die im Drittland für die Übermittlung einschließlich des Transits der Daten vom Datenexporteur in das Land des Datenimporteurs gelten, daran gehindert ist, seine Verpflichtungen, die sich aus dem aus Artikel 46 DSGVO ausgewählten Übermittlungsinstruments ergeben, einzuhalten. [40]

30. Der Datenexporteur muss also – gegebenenfalls in Zusammenarbeit mit dem Datenimporteur – prüfen, ob die Wirksamkeit der geeigneten Garantien, die das vom Datenexporteur aus Artikel 46 DSGVO ausgewählte Übermittlungsinstrument bietet, im Kontext der vorgesehenen Übermittlung möglicherweise durch das geltende Recht und/oder die geltenden Praktiken [41] des Drittlands beeinträchtigt wird. Dies setzt voraus, dass der Datenexporteur festgestellt, ob seine Übermittlung in den Anwendungsbereich von Rechtsvorschriften und/oder Praktiken fällt, die die Wirksamkeit seines Übermittlungsinstruments nach Artikel 46 DSGVO beeinträchtigen könnten. Die Beurteilung muss zunächst und vornehmlich auf die öffentlich zugänglichen Rechtsvorschriften gestützt sein.

---

[37] Weitere Informationen hierzu finden Sie unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_de.

[38] Artikel 44 DSGVO und C-311/18 (Schrems II), Rn. 126, 137 und 148.

[39] C-311/18 (Schrems II), Rn. 105 und Tenor, Nr. 2.

[40] Vgl. C-311/18 (Schrems II), Rn. 183 in Verbindung mit Rn. 184.

[41] Siehe Rn. 126 des Urteils in der Rechtssache C-311/18 (Schrems II), in der der Gerichtshof ausdrücklich auf die „Rechtslage und die Praxis im betreffenden Drittland" verweist und fordert, „(...) in der Praxis den effektiven Schutz der in das betreffende Drittland übermittelten personenbezogene Daten zu gewährleisten." (Hervorhebung hinzugefügt), und Rn. 158.

31. Diese Beurteilung muss Angaben enthalten, die den Zugriff der Behörden des Drittlands des Datenimporteurs auf Daten betreffen, wie z. B.:

    - Angaben dazu, ob Behörden des Drittlands des Importeurs unter Berücksichtigung der Rechtsvorschriften, der Praxis und der gemeldeten Präzedenzfälle mit oder ohne Wissen des Datenimporteurs um Zugriff auf die Daten ersuchen können;
    - Angaben dazu, ob Behörden des Drittlands des Datenimporteurs 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.

Ermittlung von Rechtsvorschriften und Praktiken, die unter Berücksichtigung aller Umstände der Übermittlung relevant sind

32. Dazu ist es erforderlich, sich die Umstände jeder der vorgesehenen Übermittlungen genau anzusehen und die Rechtsvorschriften und/oder Praktiken zu ermitteln, die in dem Land, in das Daten übermittelt (oder weiterübermittelt) werden, für die betreffende Übermittlungen gelten. Der Umfang der Prüfung durch den Datenexporteur beschränkt sich somit auf die Rechtsvorschriften und Praktiken, die für den Schutz der von ihm übermittelten spezifischen Daten relevant sind, im Gegensatz zu den allgemeinen und umfassenden Prüfungen der Angemessenheit, die die Europäische Kommission gemäß Artikel 45 DSGVO durchführt.

33. Die einschlägigen Rechtsvorschriften und/oder Praktiken werden von den besonderen Umständen der Übermittlung abhängen, insbesondere von:

    - den Zwecken, zu denen die Daten übermittelt und verarbeitet werden (z. B. Marketing, Personalwesen, Speicherung, IT-Support, klinische Prüfungen);
    - der Art der an der Verarbeitung beteiligten Stellen (staatlich/privat; Verantwortliche/Auftragsverarbeiter);
    - dem Sektor, in dem die Übermittlung stattfindet (z. B. AdTech, Telekommunikation, Finanzsektor usw.);
    - den Kategorien der übermittelten personenbezogenen Daten (so gelten z. B. für personenbezogene Daten, die Kinder betreffen, im Drittland möglicherweise besondere Rechtsvorschriften);[42]
    - davon, ob die Daten im Drittland gespeichert werden oder ob nur ein Fernzugriff auf in der EU / im EWR gespeicherte Daten erfolgt;

[42]Die Übermittlung personenbezogener Daten ist ein Verarbeitungsvorgang (Artikel 4 Absatz 2 DSGVO). Wenn der Datenexporteur sensible Daten übermitteln möchte, die unter die Artikel 9 und 10 DSGVO fallen, darf er eine Übermittlung nur dann vornehmen, wenn sie unter eine der Ausnahmen und Bedingungen gemäß den Artikeln 9 und 10 DSGVO und dem Recht der EU-Mitgliedstaaten fällt. Gemäß Artikel 32 DSGVO muss der Datenexporteur auch mit dem Datenimporteur, der als Verantwortlicher oder Auftragsverarbeiter fungiert, geeignete technische und organisatorische Maßnahmen ergreifen, um ein Schutzniveau zu gewährleisten, das den Risiken für die Rechte und Freiheiten der betroffenen Personen, die durch eine potenzielle Verletzung der übermittelten Daten entstehen, angemessen ist (Artikel 4 Absatz 12 DSGVO). Die Kategorien der übermittelten Daten und ihre Sensibilität werden für die Bewertung des Risikos und der Angemessenheit der Maßnahmen von Bedeutung sein.

- vom Format der zu übermittelnden Daten (z. B. Klartext / pseudonymisiert oder verschlüsselt[43]);
- davon, ob die Daten möglicherweise der Weiterübermittlung aus dem ersten Drittland in ein weiteres Drittland unterliegen.[44]

34. Die vom Datenexporteur vorzunehmende Beurteilung sollte alle an der Übermittlung beteiligten Akteure (z. B. Verantwortliche, Auftragsverarbeiter und Unterauftragsverarbeiter, die die Daten im Drittland verarbeiten) berücksichtigen. Je mehr Verantwortliche, Auftragsverarbeiter oder Datenimporteure beteiligt sind, desto komplexer ist die vorzunehmende Beurteilung. Bei der Beurteilung werden auch etwaige geplante Weiterübermittlungen zu bedenken sein.

35. Dabei sind alle Rechtsvorschriften, die relevant sein könnten, besonders genau zu prüfen, insbesondere solche, in denen die Voraussetzungen für die Offenlegung personenbezogener Daten gegenüber staatlichen Stellen oder die Gewährung des Zugriffs staatlicher Stellen (z. B. für Zwecke der Strafverfolgung, für Aufsichtszwecke oder Zwecke der nationalen Sicherheit) auf personenbezogene Daten geregelt sind. Wenn diese Voraussetzungen oder Befugnisse die Grundrechte betroffener Personen unter Wahrung ihres Wesensgehalts einschränken und in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahmen sind, um wichtige Ziele zu wahren, die auch im Unionsrecht oder in den Rechtsvorschriften der EU-Mitgliedstaaten anerkannt sind[45], dürfen sie sich nicht auf die Verpflichtungen auswirken, die in dem vom Datenexporteur aus Artikel 46 DSGVO ausgewählten Übermittlungsinstrument enthalten sind.

36. Der Datenexporteur muss einschlägige Vorschriften und Praktiken allgemeiner Art prüfen, soweit sie sich auf die wirksame Anwendung der Garantien in den Übermittlungsinstrumenten nach Artikel 46 DSGVO auswirken.

37. Für die vorzunehmende Beurteilung können auch andere Elemente der Rechtsordnung des Drittlands, z. B. die in Artikel 45 Absatz 2 DSGVO aufgeführten Elemente, von Belang sein. So kann z. B. für die Beurteilung der Wirksamkeit der den betroffenen Personen zur Verfügung stehenden (gerichtlichen) Rechtsbehelfe gegen den rechtswidrigen Zugriff staatlicher Stellen auf personenbezogene Daten der Stand der Rechtsstaatlichkeit im betreffenden Drittland relevant sein. Das Vorhandensein eines umfassenden Datenschutzrechts oder einer unabhängigen Datenschutzbehörde wie auch die Einhaltung internationaler Übereinkommen über Datenschutzgarantien können Faktoren sein, die die Verhältnismäßigkeit staatlicher Eingriffe gewährleisten.

---

[43] In einigen Ländern ist der Import verschlüsselter Daten nicht gestattet.
[44] Dies bedarf gemäß Artikel 28 Absatz 2 DSGVO stets der vorherigen gesonderten oder allgemeinen schriftlichen Genehmigung des Verantwortliche.
[45] Vgl. Artikel 47 und 52 der Charta der Grundrechte der Europäischen Union, Artikel 23 Absatz 1 DSGVO sowie EDSA, Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, 10. November 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_de.

38. Man kann davon ausgehen, dass sich die aus solchen Rechtsvorschriften und Praktiken ergebenden Verpflichtungen oder Befugnisse nachteilig auf die Verpflichtungen aus dem Übertragungsinstrument nach Artikel 46 DSGVO auswirken oder damit unvereinbar sind, wenn sie[46]

    - 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, wie die in Artikel 23 Absatz 1 DSGVO aufgeführten Ziele.

39. Der Datenexporteur sollte überprüfen, dass die Verpflichtungen des Datenimporteurs, die es den betroffenen Personen ermöglichen, ihre Rechte gemäß Artikel 46 DSGVO auszuüben (z. B. ihr Recht auf Auskunft, auf Berichtigung und auf Löschung der übermittelten Daten), in der Praxis tatsächlich wirksam ausgeübt werden können und nicht durch die Rechtsvorschriften und/oder Praktiken im Bestimmungsdrittland vereitelt werden.

40. Für die Beurteilung, ob ein solcher Zugriff staatlicher Stellen auf das beschränkt ist, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, und ob den betroffenen Personen ein wirksamer Rechtsbehelf zur Verfügung steht, ist auf unionsrechtliche Standards wie Artikel 47 und 52 der Charta der Grundrechte der Europäischen Union abzustellen.

41. Die Empfehlungen, die der EDSA in den „Wesentlichen europäischen Garantien“[47] ausspricht, enthalten Klarstellungen zu den Elementen, anhand derer sich beurteilen lässt, ob der rechtliche Rahmen, der in einem Drittland für den Zugriff staatlicher Stellen (etwa für die nationale Sicherheit oder Strafverfolgung zuständiger Behörden) auf personenbezogene Daten gilt, als gerechtfertigter Eingriff[48] angesehen werden kann oder nicht. Diese Elemente sind insbesondere dann sehr genau zu berücksichtigen, wenn die Rechtsvorschriften, die den Datenzugriff staatlicher Stellen regeln, unklar oder nicht allgemein zugänglich sind. Die erste Anforderung der „Wesentlichen europäischen Garantien“ besteht darin, dass es für einen solchen Zugriff einen Rechtsrahmen geben sollte, der öffentlich zugänglich und hinreichend klar ist

42. Bei der Anwendung auf Datenübermittlungen, die auf Übermittlungsinstrumente in Artikel 46 gestützt sind, können die in den „Wesentlichen europäischen Garantien“ des EDSA gegebenen Empfehlungen dem Datenexporteur und dem Datenimporteur Orientierung bieten für die Beurteilung der Frage, 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 DSGVO oder seinen Verpflichtungen im Rahmen des Übertragungsinstruments nachzukommen. Das Fehlen eines des Sache nach gleichwertigen

---

[46] Siehe Artikel 47 und 52 der Charta der Grundrechte der Europäischen Union, Artikel 23 Absatz 1 DSGVO, C-311/18 (Schrems II), Rn. 174 und 187, und die Empfehlungen 02/2020 des EDSA zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, 10. November 2020.

[47] Empfehlungen 02/2020 des EDSA zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, 10. November 2020.

[48] Und daher nicht als in die Verpflichtungen eingreifend, die im Rahmen des Übertragungsinstruments nach Artikel 46 DSGVO eingegangen wurden.

Schutzniveaus ist insbesondere dann offenkundig, wenn die Rechtsvorschriften und/oder die Praktiken in dem Drittland, in das die Übermittlung erfolgt, nicht den in den „Wesentlichen europäischen Garantien“ niedergelegten Anforderungen genügen. Der EDSA bekräftigt, dass die wesentlichen europäischen Garantien ein Maßstab für die Bewertung von Grundrechtseingriffen sind, die im Rahmen internationaler Datenübermittlung in Verbindung mit Überwachungsmaßnahmen eines Drittlands erfolgen. Diese Standards ergeben sich aus dem Unionsrecht und der für die Mitgliedstaaten verbindlichen Rechtsprechung des EuGH und des EGMR.

43. Die Beurteilung muss zunächst und vornehmlich auf die öffentlich zugänglichen Rechtsvorschriften gestützt sein. Die Prüfung der Praktiken der Behörden des Drittlandes wird es dem Datenexporteur ermöglichen, zu überprüfen, ob die im Instrument für die Übermittlung von Daten nach Artikel 46 DSGVO vorgesehenen Garantien ein ausreichendes Mittel darstellen können, um in der Praxis den wirksamen Schutz der übermittelten personenbezogenen Daten zu gewährleisten.[49] Die Prüfung der in dem Drittland geltenden Praktiken ist für die Beurteilung durch den Datenexporteur in den nachstehend beschriebenen Situationen von besonderer Bedeutung.

43.1 **Die einschlägigen Rechtsvorschriften in dem Drittland mögen formell den EU-Standards in Bezug auf Grundrechte und Grundfreiheiten sowie die Notwendigkeit und Verhältnismäßigkeit von Beschränkungen entsprechen.** Die Praktiken der Behörden dieses Landes (z. B. beim Zugriff auf personenbezogene Daten, die sich im Besitz des Privatsektors befinden, oder bei der Durchsetzung von Rechtsvorschriften als Aufsichts- oder Justizbehörden) können jedoch ein eindeutiger Hinweis darauf sein, dass sie die Rechtsvorschriften, die grundsätzlich für ihre Tätigkeiten gelten, in der Regel nicht anwenden/sie nicht einhalten. In diesem Fall muss der Datenexporteur diese Praktiken bei seiner Beurteilung berücksichtigen und in Erwägung ziehen, dass das Instrument nach Artikel 46 DSGVO nicht in der Lage sein wird, für sich genommen (d. h. ohne zusätzliche Maßnahmen) ein der Sache nach gleichwertiges Schutzniveau zu gewährleisten. In einem solchen Fall muss er angemessene ergänzende Maßnahmen ergreifen, wenn er die Übermittlung fortsetzen möchten.

43.2 **Es fehlt möglicherweise in dem Drittland an einschlägigen Rechtsvorschriften (z. B. über den Zugriff auf personenbezogene Daten, die sich im Besitz des Privatsektors befinden).** In diesem Fall kann der Datenexporteur aus dem Fehlen einschlägiger Rechtsvorschriften nicht automatisch ableiten, dass sein Übermittlungsinstrument nach Artikel 46 DSGVO wirksam angewandt werden kann. Er muss prüfen, ob es Hinweise auf in dem Land geltende Praktiken gibt, die mit dem EU-Recht und den Verpflichtungen gemäß dem Übermittlungsinstrument nach Artikel 46 DSGVO unvereinbar sind. Im Falle unvereinbarer Praktiken wird das Übermittlungsinstrument nach Artikel 46 DSGVO nicht in der Lage sein, für sich genommen (d. h. ohne angemessene ergänzende Maßnahmen) ein der Sache nach gleichwertiges Schutzniveau zu gewährleisten. In einem solchen Fall muss er angemessene ergänzende Maßnahmen ergreifen, wenn er die Übermittlung fortsetzen möchten.

[49] C-311/18 (Schrems II), Rn. 126.

43.3 **Die Beurteilung kann ergeben, dass einschlägige Rechtsvorschriften in dem Land möglicherweise problematisch sind[50] und dass die übermittelten Daten und/oder der betreffende Datenimporteur unter diese problematischen Rechtsvorschriften fallen/fällt oder fallen könnte(n).[51]**

Angesichts der Unsicherheiten in Bezug auf die mögliche Anwendung problematischer Rechtsvorschriften auf seine Übermittlung kann der Datenexporteur beschließen,

- die Übermittlung aussetzen;
- zusätzliche Maßnahmen[52] zu ergreifen, um das Risiko zu vermeiden, dass Rechtsvorschriften und/oder Praktiken des Drittlands des Datenimporteurs auf seinen Datenimporteur und/oder auf seine übermittelten Daten angewandt werden, die die vertraglichen Garantien des Übertragungsinstruments eines Schutzniveaus, das dem im EWR garantierten Schutzniveau der Sache nach gleichwertig ist, beeinträchtigen können, oder
- Alternativ kann der Datenexporteur beschließen, die Übermittlung vorzunehmen, ohne zusätzliche Maßnahmen ergreifen zu müssen, wenn er seiner Auffassung nach keinen Grund zu der Annahme hat, dass in der Praxis einschlägige und problematische Rechtsvorschriften auf seine übermittelten Daten und/oder seinen Datenimporteur angewandt werden. Er muss durch seine Beurteilung – gegebenenfalls in Zusammenarbeit mit dem Datenimporteur – nachweisen und dokumentieren, dass die Rechtsvorschriften in der Praxis nicht so ausgelegt und/oder angewandt werden, dass sie seine übermittelten Daten und seinen Datenimporteur abdecken, wobei auch die Erfahrungen anderer Akteure, die in demselben Sektor tätig sind und/oder mit ähnlichen übermittelten personenbezogenen Daten zu tun haben, sowie die nachstehend beschriebenen weiteren Informationsquellen zu berücksichtigen sind.[53]

  Daher muss er anhand eines ausführlichen Berichts[54] nachweisen und dokumentieren , dass in der Praxis problematische Rechtsvorschriften nicht auf seine übermittelten Daten

---

[50] „Problematische Rechtsvorschriften“ sind Rechtsvorschriften, die 1) dem Empfänger personenbezogener Daten aus der Europäischen Union Verpflichtungen auferlegen und/oder die übermittelten Daten in einer Weise beeinflussen, die die vertragliche Garantie eines der Sache nach gleichwertigen Schutzniveaus durch die Übermittlungsinstrumente beeinträchtigen kann, und 2) den Wesensgehalt der in der Charta der Grundrechte der Europäischen Union anerkannten Grundrechte und Grundfreiheiten 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 Recht der Union oder der EU-Mitgliedstaaten anerkannt sind, wie die in Artikel 23 Absatz 1 DSGVO aufgeführten.

[51] Es kann unklar sein, ob der Datenimporteur und/oder die übermittelten Daten unter allgemeine Begriffe fallen, die häufig in den Rechtsvorschriften über die nationale Sicherheit zur Beschränkung ihres Anwendungsbereichs verwendet werden, wie z. B. „Anbieter elektronischer Kommunikationsdienste“ und „Erkenntnisse ausländischer Nachrichtendienste“.

[52] Siehe Erwägungsgrund 109 DSGVO und C-311/18 (Schrems II), Rn. 132.

[53] Vgl. die Ziffern 45 bis 47.

[54] Die von ihm zu erstellenden Berichte müssen umfassende Informationen über die rechtliche Würdigung der Rechtsvorschriften und Praktiken sowie über ihre Anwendung auf die konkreten Übermittlungen, das interne Verfahren zur Erstellung der Beurteilung (einschließlich Angaben zu den an der Beurteilungen beteiligten

und/oder seinen Datenimporteur angewandt werden, und dass sie folglich den Datenimporteur nicht daran hindern, seinen Verpflichtungen aus dem Übermittlungsinstrument nach Artikel 46 DSGVO nachzukommen.[55]

Mögliche Informationsquellen

44. Der Datenimporteur sollte dem Datenexporteur die einschlägigen Fundstellen und Informationen für das Drittland, in dem er seinen Sitz hat und dessen Recht die Übermittlung unterliegt, mitteilen.

45. Der Datenexporteur und sein Datenimporteur können Ihre Beurteilung durch Informationen ergänzen, die aus Quellen wie z. B. den in Anhang 3 als Beispiele aufgeführten Quellen stammen.

46. Zusätzlich zu dem für die Übermittlung geltenden Rechtsrahmen des Drittlands sollten Quellen und Informationen relevant, objektiv, zuverlässig, überprüfbar und öffentlich verfügbar oder anderweitig zugänglich sein, damit festgestellt werden kann, ob das vom Datenexporteur gewählte Übermittlungsinstrument nach Artikel 46 wirksam angewandt werden kann[56], und er muss prüfen und dokumentieren, dass dem so ist.

Relevant: Die Informationen müssen für die konkrete Übermittlung und/oder den entsprechenden Datenimporteur und deren Übereinstimmung mit den Anforderungen des EU-Rechts und des Übermittlungsinstruments nach Artikel 46 DSGVO relevant und dürfen nicht zu allgemein oder abstrakt sein.

Objektive Informationen: Darunter versteht man Informationen, die durch empirische Daten gestützt werden, die auf Erkenntnissen aus der Vergangenheit und nicht auf Annahmen über potenzielle Ereignisse und Risiken beruhen.

Zuverlässig: Datenexporteur und -importeur müssen die Zuverlässigkeit der Informationsquelle und der Informationen selbst objektiv beurteilen und jeder für sich bewerten.

Überprüfbar: Informationen und Schlussfolgerungen sollten im Rahmen einer Gesamtbeurteilung nachprüfbar oder mit anderen Arten von Informationen oder Quellen abgleichbar sein, damit die zuständige Aufsichts- oder Justizbehörde bei Bedarf die Objektivität und Zuverlässigkeit dieser Informationen überprüfen kann.

Akteure, z. B. Anwaltskanzleien, Berater oder interne Dienststellen) und die Daten der Kontrollen enthalten. Die Berichte sollten vom gesetzlichen Vertreter des Datenexporteurs gebilligt werden.

[55]Der Nachweis, dass problematische Rechtsvorschriften in der Praxis nicht auf seine übermittelten Daten und den Datenimporteur angewandt werden, und auch die Berücksichtigung von Erfahrungen anderer Akteure, die in demselben Sektor tätig sind und/oder mit ähnlichen übermittelten personenbezogenen Daten zu tun haben, entbindet den Datenexporteur nicht von der Verpflichtung, zusätzliche Maßnahmen zum Schutz personenbezogener Daten während der Übermittlung und Verarbeitung im Bestimmungsdrittland vorzusehen (z. B. End-to-End-Verschlüsselung von Daten – siehe Beispiele für zusätzliche technische Maßnahmen in Anhang 2), wenn seine Analyse der geltenden Rechtsvorschriften des Bestimmungsdrittlands darauf hindeutet, dass auch ohne das Eingreifen des Datenimporteurs zum Zeitpunkt der Übermittlung Zugriff auf Daten gewährt werden kann. Möglicherweise hat er solche Maßnahmen bereits für den Datenimporteur vorgesehen, wenn dieser als Verantwortlicher oder Auftragsverarbeiter im Sinne von Artikel 32 DSGVO fungiert.

[56]Anhang 3 enthält eine nicht erschöpfende Liste der Informationsquellen, die Datenexporteur und -importeur heranziehen können.

Öffentlich verfügbare oder anderweitig zugängliche Informationen: Diese Informationen sollten vorzugsweise öffentlich oder zumindest zugänglich sein, um die Überprüfung der oben genannten Kriterien zu erleichtern und ihre mögliche Weitergabe an Aufsichtsbehörden, Justizbehörden und letztlich betroffene Personen sicherzustellen.

47. Der Datenexporteur kann auch dokumentierte praktische Erfahrungen des Datenimporteurs mit einschlägigen früheren Fällen von Ersuchen von Behörden in dem Drittland auf Zugriff berücksichtigen. Er kann die Erfahrungen des Datenimporteurs nur dann als zusätzliche Informationsquelle nutzen, wenn der Rechtsrahmen des Drittlands es dem Datenimporteur nicht verbietet, Informationen über Offenlegungsersuchen von Behörden oder über das Ausbleiben solcher Ersuchen zur Verfügung zu stellen (und er sollte eine solche Bewertung auch dokumentieren). Es sei jedoch darauf hingewiesen, dass das Ausbleiben früherer Ersuchen an den Datenimporteur für sich genommen niemals als entscheidender Faktor für die Wirksamkeit des Übermittlungsinstruments nach Artikel 46 DSGVO angesehen werden kann, der es ermöglicht, die Übermittlung ohne zusätzliche Maßnahmen vorzunehmen. Der Datenexporteur kann diese Informationen zusammen mit anderen Informationen aus anderen Quellen im Rahmen seiner Gesamtbeurteilung der Rechtsvorschriften und Praktiken des Drittlands in Bezug auf seine Übermittlung berücksichtigen. Die einschlägige und dokumentierte Erfahrung des Datenimporteurs sollte durch relevante, objektive, zuverlässige, überprüfbare und öffentlich verfügbare oder anderweitig zugängliche Informationen über die praktische Anwendung der einschlägigen Rechtsvorschriften (z. B. das Vorliegen oder Ausbleiben von Ersuchen auf Zugriff bei anderen Akteuren, die in demselben Sektor tätig sind und/oder mit ähnlichen übermittelten personenbezogenen Daten zu tun haben[57], und/oder die Anwendung der Rechtsvorschriften in der Praxis, wie Rechtsprechung und Berichte unabhängiger Aufsichtsstellen) untermauert und nicht widerlegt werden.

Ergebnisse der Beurteilung durch den Datenexporteur

48. Der Datenexporteur sollte diese Gesamtbeurteilung der für seine Übermittlung geltenden Rechtsvorschriften und Praktiken des Drittlands seines Datenimporteurs mit der gebotenen Sorgfalt durchführen und sorgfältig dokumentieren. Seine zuständigen Aufsichts- und/oder Justizbehörden können dies verlangen und ihn für jede auf dieser Grundlage getroffenen Entscheidung zur Rechenschaft ziehen.[58]

49. Die vom Datenexporteur vorgenommene Beurteilung kann ergeben, dass das von ihm aus Artikel 46 DSGVO ausgewählte Übermittlungsinstrument

    - entweder wirksam gewährleistet, dass die übermittelten personenbezogenen Daten in dem Drittland ein Schutzniveau genießen, das dem im EWR garantierten Niveau der Sache nach gleichwertig ist. Nach den Rechtsvorschriften und Praktiken des Drittlands, die auf die Übermittlung Anwendung finden, ist es dem Datenimporteur möglich, seine sich aus dem ausgewählten Übermittlungsinstrument ergebenden Verpflichtungen zu erfüllen. Dieses

[57]Die Erfahrung könnte auch von anderen dem Datenexporteur unmittelbar aufgrund früherer Übermittlungen derselben Art, wie er sie durchgeführt hat, bekannten Stellen stammen, oder aus der einschlägigen Rechtsprechung, Berichten von NRO usw. (siehe Anhang 3).
[58] Artikel 5 Absatz 2 DSGVO.

Ergebnis ist in geeigneten Abständen oder bei Bekanntwerden erheblicher Änderungen zu überprüfen (siehe Schritt 6);

- oder keine wirksame Gewährleistung eines der Sache nach gleichwertigen Schutzniveaus bietet. Der Datenimporteur kann seinen Verpflichtungen nicht nachkommen, da die für die Datenübermittlung geltenden Rechtsvorschriften und/oder Praktiken des Drittlands nicht den EU-Standards im Bereich der Grundrechte und -freiheiten und der Notwendigkeit und Verhältnismäßigkeit von Beschränkungen entsprechen, um legitime Ziele von öffentlichem Interesse zu wahren. Der Gerichtshof hat hervorgehoben, dass, falls die in Artikel 46 DSGVO vorgesehenen Übermittlungsinstrumente nicht ausreichen, der Datenexporteur dafür verantwortlich ist, entweder wirksame zusätzliche Maßnahmen vorzusehen oder von der Übermittlung der personenbezogenen Daten abzusehen.[59]

Beispiel:

Hintergrund:
So hat der Gerichtshof z. B. entschieden, dass Abschnitt 702 des US-amerikanischen FISA nicht den im Unionsrecht nach dem Grundsatz der Verhältnismäßigkeit bestehenden Mindestanforderungen genügt, so dass nicht angenommen werden kann, dass die Vorschrift auf das zwingend erforderliche Maß beschränkt ist. Dies bedeutet, dass die auf Abschnitt 702 FISA gestützten Überwachungsprogramme den nach Unionsrecht erforderlichen Garantien nicht der Sache nach gleichwertig sind.

Beurteilung:
Wenn der Datenexporteur aufgrund seiner Beurteilung der einschlägigen US-Rechtsvorschriften zu der Auffassung gelangt, dass seine Übermittlung in den Anwendungsbereich von Abschnitt 702 FISA fallen könnte, er sich jedoch nicht sicher ist, ob sie tatsächlich in den Anwendungsbereich des Gesetzes fällt, kann er entweder entscheiden,

1. die Übermittlung zu beenden;
2. geeignete ergänzende Maßnahmen zu ergreifen, die einen wirksamen Schutz der übermittelten Daten gewährleisten, der dem im EWR garantierten Schutzniveau der Sache nach gleichwertig ist, oder
3. weitere objektive, zuverlässige, relevante, überprüfbare und vorzugsweise öffentlich verfügbare Informationen (einschließlich der ihm von seinem Datenimporteur zur Verfügung gestellten Informationen) zu prüfen, um den Anwendungsbereich von Abschnitt 702 FISA in der Praxis auf seine Übermittlung zu klären. Diese Informationen sollten Antworten auf einige relevante Fragen geben, wie z. B. die folgenden:

- Geht aus öffentlich verfügbaren Informationen hervor, dass es ein gesetzliches Verbot gibt, über ein bestimmtes Ersuchen um Zugriff auf erhaltene Daten zu informieren, und dass es weitreichende Beschränkungen für die Bereitstellung allgemeiner Informationen über eingegangene bzw. ausgebliebene Ersuchen um Zugriff auf Daten gibt?

- Hat sein Datenimporteur bestätigt, dass er in der Vergangenheit von US-Behörden Ersuchen auf Zugriff auf Daten erhalten hat? Oder hat sein Datenimporteur bestätigt, dass er in der Vergangenheit

[59]EuGH, C-311/18 (Schrems II), Rn. 134 und 135.

keine Ersuchen von US-Behörden auf Zugriff auf Daten erhalten hat und dass es ihm nicht untersagt ist, Informationen über solche Ersuchen oder deren Ausbleiben zur Verfügung zu stellen?

- Gibt es öffentlich verfügbare Informationen über die US-Rechtsprechung und Berichte von Aufsichtsbehörden, Organisationen der Zivilgesellschaft und wissenschaftlichen Einrichtungen[60], aus denen hervorgeht, dass Datenimporteure derselben Branche wie Ihr Datenimporteur in der Vergangenheit Ersuchen auf Zugriff zu Daten für ähnliche übertragene Daten erhalten haben?

Aufgrund der Antworten auf diese Fragen, die der Datenexporteur im Rahmen seiner Gesamtbeurteilung erhält, gelangt er zu dem Schluss, dass

- Abschnitt 702 FISA in der Praxis für seine konkrete Übermittlung gilt und daher die Wirksamkeit seines Übermittlungsinstruments nach Artikel 46 DSGVO beeinträchtigt. Wenn er die Übermittlung fortsetzen möchte, muss er daher – gegebenenfalls in Zusammenarbeit mit dem Datenimporteur – prüfen, ob er zusätzliche Maßnahmen ergreifen kann, die wirksam ein Schutzniveau für die übermittelten Daten gewährleisten, das dem im EWR garantierten Schutzniveau der Sache nach gleichwertig ist. Kann er keine wirksamen zusätzlichen Maßnahmen finden, darf er die personenbezogenen Daten nicht übermitteln.

Oder

- Abschnitt 702 FISA in der Praxis für seine konkrete Übermittlung nicht gilt und daher nicht die Wirksamkeit seines Übermittlungsinstruments nach Artikel 46 DSGVO beeinträchtigt. Er kann dann die Übermittlung ohne zusätzliche Maßnahmen vornehmen.

2.4 Schritt 4: Zusätzliche Maßnahmen ergreifen

50. Ergibt die vom Datenexporteur in Schritt 3 vorgenommene Beurteilung, dass das von ihm aus Artikel 46 DSGVO ausgewählte Übermittlungsinstrument nicht effektiv ist, ist – gegebenenfalls in Zusammenarbeit mit dem Datenimporteur – darüber nachzudenken, ob es zusätzliche Maßnahmen gibt, die, als Ergänzung zu den in den Übermittlungsinstrumenten enthaltenen Garantien im Drittland ein Schutzniveau gewährleisten könnten, das dem in der Union garantierten Schutzniveau der Sache nach gleichwertig ist.[61] „Zusätzliche Maßnahmen" sind *per definitionem* eine Ergänzung der Garantien, die bereits in dem in Artikel 46 DSGVO vorgesehenen Übermittlungsinstrument enthalten sind, sowie aller anderen anwendbaren Sicherheitsanforderungen (z. B. technischen Sicherheitsmaßnahmen), die in der DSGVO festgelegt sind.[62]

[60] z. B. Bestimmungen von Abschnitt 702 FISA; Verfahrensordnung des Foreign Intelligence Surveillance Court (FISC), freigegebene Stellungnahmen und Entscheidungen des FISC, Rechtsprechung von US-Gerichten; Berichte und Anhörungsprotokolle des Privacy and Civil Liberties Oversight Board (PCLOB); Berichte des Amts des Generalinspekteurs – US-Justizministerium; Berichte des NSA-Direktors des Amts für bürgerliche Freiheiten und Privatsphäre; Berichte des Wissenschaftlichen Dienstes des Kongresses; Berichte der American Civil Liberties Union Foundation (ACLU).

[61] C-311/18 (Schrems II), Rn. 96.

[62] Erwägungsgrund 109 der DSGVO und C-311/18 (Schrems II), Rn. 133.

51. Der Datenexporteur muss in jedem Einzelfall für die betreffenden Übermittlungen in ein bestimmtes Drittland, die auf eines der Übermittlungsinstrumente in Artikel 46 DSGVO gestützt sind, feststellen, welche zusätzlichen Maßnahmen in Betracht kommen, um effektiven Schutz zu bieten. Er muss die Beurteilung nicht jedes Mal wiederholen, wenn er eine bestimmte Art von Daten in ein und dasselbe Drittland übermitteln. Bei einigen der für die Übermittlung vorgesehenen Daten sind möglicherweise ergänzende Maßnahmen erforderlich, bei anderen Daten hingegen nicht (unter Berücksichtigung der formalen und/oder praktischen Anwendung des Drittstaatsrechts). Der Datenexporteur kann dabei auf die bereits in den vorhergehenden Schritten 1, 2 und 3 vorgenommenen Beurteilungen sowie deren Schlussfolgerungen zurückgreifen und anhand der dort getroffenen Feststellungen die potenzielle Effektivität der zusätzlichen Maßnahmen für die Gewährleistung des erforderlichen Schutzniveaus beurteilen.

52. Grundsätzlich können zusätzliche Maßnahmen vertraglicher, technischer oder organisatorischer Art sein. Indem man verschiedene Maßnahmen so kombiniert, dass sie einander unterstützen und aufeinander aufbauen, lässt sich das Schutzniveau möglicherweise verbessern und den unionsrechtlichen Standards annähern.

53. Vertragliche und organisatorische Maßnahmen allein werden den Zugriff von Behörden des Drittlands auf personenbezogene Daten auf der Grundlage problematischer Rechtsvorschriften und/oder Praktiken in der Regel nicht überwinden.[63] In der Tat wird es Situationen geben, insbesondere wenn der Zugriff zu Überwachungszwecken erfolgt, in denen es nur mit korrekt umgesetzten technischen Maßnahmen möglich ist, den Zugriff staatlicher Stellen im Drittland auf personenbezogene Daten zu verhindern oder ineffektiv zu machen.[64] In solchen Situationen können vertragliche oder organisatorische Maßnahmen die technischen Maßnahmen ergänzen und das Datenschutzniveau insgesamt stärken (z. B. durch die Einführung von Kontrollen und Ausschaltungsmechanismen für Versuche staatlicher Stellen, in nicht den unionsrechtlichen Standards genügender Weise auf Daten zuzugreifen.

54. Der Datenexporteur kann, soweit angemessen, in Zusammenarbeit mit dem Datenimporteur, anhand der folgenden (nicht erschöpfenden) Liste von Faktoren feststellen, welche zusätzlichen Maßnahmen am wirksamsten wären, um die übermittelten Daten vor Ersuchen von Behörden um Zugriff auf der Grundlage problematischer, in der Praxis angewandter Rechtsvorschriften zu schützen:

---

[63] „Problematische Rechtsvorschriften“ sind Rechtsvorschriften, die 1) dem Empfänger personenbezogener Daten aus der Europäischen Union Verpflichtungen auferlegen und/oder die übermittelten Daten in einer Weise beeinflussen, die die vertragliche Garantie eines der Sache nach gleichwertigen Schutzniveaus durch die Übermittlungsinstrumente beeinträchtigen kann, und 2) den Wesensgehalt der in der Charta der Grundrechte der Europäischen Union anerkannten Grundrechte und Grundfreiheiten 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 Recht der Union oder der EU-Mitgliedstaaten anerkannt sind, wie die in Artikel 23 Absatz 1 DSGVO aufgeführten.

[64] Wenn ein solcher Zugriff über das hinausgeht, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt; vgl. Artikel 47 und 52 der Charta der Grundrechte der Europäischen Union, Artikel 23 Absatz 1 DSGVO sowie die vom EDSA erlassenen Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, 10. November 2020 https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

- Format der zu übermittelnden Daten (z. B. im Klartext/pseudonymisiert oder verschlüsselt);
- Art der Daten (z. B. wird im EWR für Kategorien von Daten, die unter die Artikel 9 und 10 DSGVO fallen, ein höheres Schutzniveau gewährt);[65]
- Dauer und Komplexität der Datenverarbeitung, Anzahl der an der Verarbeitung mitwirkenden Akteure und deren Verhältnis untereinander (ob z. B. an den Übermittlungen mehrere Verantwortliche oder aber sowohl Verantwortliche als auch Auftragsverarbeiter mitwirken, die die Daten vom Datenexporteur zum Datenimporteur übermitteln, wobei auf die für diese geltenden Bestimmungen nach dem Recht des Bestimmungsdrittlands abzustellen ist;[66]
- Technik oder Parameter der praktischen Anwendung des in Schritt 3 abgeschlossenen Drittstaatsrechts;
- Möglichkeit der Weiterübermittlung der Daten, sei es innerhalb desselben Drittlands oder sogar in ein anderes Drittland (z. B. unter Mitwirkung von Unterauftragsverarbeitern des Datenimporteurs[67]).

Beispiele für zusätzliche Maßnahmen

55. Einige Beispiele für technische, vertragliche und organisatorische Maßnahmen, die in Betracht gezogen werden könnten, soweit sie nicht bereits in dem verwendeten Übermittlungsinstrument nach Artikel 46 DSGVO enthalten sind, sind in den nicht erschöpfenden Listen in Anhang 2 zu finden.

***

56. Wenn der Datenexporteur effektive zusätzliche Maßnahmen vorgesehen hat, die in Verbindung mit dem von ihm aus Artikel 46 DSGVO ausgewählten Übermittlungsinstrument ein Schutzniveau gewährleisten, das in der Kombination dem im EWR garantierten Schutzniveau der Sache nach gleichwertig ist, kann er mit den Übermittlungen beginnen.

57. Gelingt es dem Datenexporteur nicht, effektive zusätzliche Maßnahmen zu finden oder zu implementieren, die gewährleisten, dass die übermittelten personenbezogenen Daten ein der Sache nach gleichwertiges Schutzniveau genießen[68], darf der Datenexporteur nicht damit beginnen, personenbezogene Daten auf Grundlage des von ihm aus Artikel 46 DSGVO ausgewählten Übermittlungsinstruments in das Drittland zu übermitteln. Sollte er bereits mit der

[65] Siehe Fußnote 42.

[66] Den Verantwortlichen und den Auftragsverarbeitern werden durch die DSGVO jeweils besondere Verpflichtungen zugewiesen. Übermittlungen können von einem Verantwortlichen zum anderen, zwischen gemeinsam Verantwortlichen, vom Verantwortlichen an den Auftragsverarbeiter sowie, sofern der Verantwortliche dies genehmigt hat, vom Auftragsverarbeiter an den Verantwortlichen oder von einem Auftragsverarbeiter an einen anderen Auftragsverarbeiter erfolgen.

[67] Siehe Fußnote 26.

[68] Wenn ein solcher Zugriff über das hinausgeht, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt; vgl. Artikel 47 und 52 der Charta der Grundrechte der Europäischen Union, Artikel 23 Absatz 1 DSGVO sowie die vom EDSA erlassenen Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, 10. November 2020 https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_de.

Übermittlung begonnen haben, ist er gehalten, die Übermittlung personenbezogener Daten auszusetzen oder zu beenden.[69] Je nach den Garantien, die in dem vom Datenexporteur aus Artikel 46 DSGVO ausgewählten Übermittlungsinstrument enthalten sind, muss der Datenimporteur die Daten, die der Datenexporteur bereits in das Drittland übermittelt hat wie auch die Kopien der Daten, an den Datenexporteur zurückschicken oder vollständig vernichten.[70]

Beispiel:

Nach dem Recht des Drittlands sind die vom Datenexporteur ausgewählten zusätzlichen Maßnahmen verboten (z. B. weil Verschlüsselung verboten ist) oder aus anderen Gründen nicht effektiv. Der Datenexporteur darf nicht mit der Übermittlung personenbezogener Daten in das Land beginnen; falls die Übermittlung in das Land bereits erfolgt, ist sie einzustellen.

58. Die zuständigen Aufsichtsbehörden sind befugt, andere Abhilfemaßnahmen anzuordnen (z. B. Geldbußen), falls die Übermittlung begonnen oder fortgesetzt wird, obwohl der Datenexporteur keinen Nachweis dafür erbringen kann, dass das Schutzniveau im Drittland der Sache nach gleichwertig ist.

2.5 Schritt 5: Verfahrensschritte nach Ermittlung effektiver zusätzlicher Maßnahmen

59. Welche weiteren Verfahrensschritte erforderlich sind, nachdem der Datenexporteur effektive zusätzliche Maßnahmen festgestellt hat, hängt davon ab, welches der in Artikel 46 DSGVO vorgesehenen Übermittlungsinstrumente er verwendet oder zu verwenden beabsichtigt.

2.5.1 Standarddatenschutzklauseln („SCC“) (Artikel 46 Absatz 2 Buchstaben c und d DSGVO)

60. Hat der Datenexporteur die Absicht, zusätzliche Maßnahmen zu verwenden, die die Standarddatenschutzklauseln ergänzen, bedarf er für die Aufnahme von Klauseln oder zusätzlichen Garantien solcher Art keiner Genehmigung der zuständigen Aufsichtsbehörde, sofern die betreffenden zusätzlichen Maßnahmen weder unmittelbar noch mittelbar mit den Standarddatenschutzklauseln in Konflikt stehen und sofern sie hinreichende Gewähr dafür bieten, dass das durch die DSGVO verbürgte Schutzniveau nicht beeinträchtigt wird.[71] Datenexporteur

[69] C-311/18 (Schrems II), Rn. 135.

[70] Vgl. z. B. Klausel 12 im Anhang zum SCC-Beschluss 87/2010; vgl. die (optionale) zusätzliche Beendigungsklausel in Anhang B SCC-Entscheidung 2004/915/EG.

[71] Erwägungsgrund 109 der DSGVO lautet: „Die dem Verantwortlichen oder dem Auftragsverarbeiter offenstehende Möglichkeit, auf die von der Kommission oder einer Aufsichtsbehörde festgelegten Standard-Datenschutzklauseln zurückzugreifen, sollte den Verantwortlichen oder den Auftragsverarbeiter weder daran hindern, die Standard-Datenschutzklauseln auch in umfangreicheren Verträgen, wie zum Beispiel Verträgen zwischen dem Auftragsverarbeiter und einem anderen Auftragsverarbeiter, zu verwenden, noch ihn daran hindern, ihnen weitere Klauseln oder zusätzliche Garantien hinzuzufügen, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den von der Kommission oder einer Aufsichtsbehörde erlassenen Standard-Datenschutzklauseln stehen oder die Grundrechte und Grundfreiheiten der betroffenen Personen beschneiden.“ Ähnliche Bestimmungen gibt es in den von der Europäischen Kommission aufgrund der Richtlinie 95/45/EG angenommenen Standard-Datenschutzklauseln.

und Datenimporteur müssen sicherstellen, dass die zusätzlichen Klauseln nicht auf eine Weise ausgelegt werden können, die die in den Standarddatenschutzklauseln niedergelegten Rechte und Verpflichtungen einschränkt oder das Datenschutzniveau in sonstiger Weise reduziert. Dies muss der Datenexporteur – nach dem Grundsatz der Rechenschaftspflicht und wegen seiner Verpflichtung zur Gewährleistung eines ausreichenden Datenschutzniveaus – nachweisen können. Die zuständige Aufsichtsbehörde ist befugt, die ergänzenden Klauseln erforderlichenfalls zu prüfen (z. B. im Falle einer Beschwerde oder im Zuge von sich aus durchgeführter Untersuchungen).

61. Wenn der Datenexporteur beabsichtigt, die eigentlichen Standard-Datenschutzklauseln zu ändern, oder wenn die hinzugefügten ergänzenden Maßnahmen mit den Standardvertragsklauseln unmittelbar oder mittelbar in Konflikt stehen, kann nicht mehr angenommen werden, dass sich der Datenexporteur auf die Standardvertragsklauseln stützt[72]; der Datenexporteur muss dann gemäß Artikel 46 Absatz 3 Buchstabe a DSGVO die Genehmigung der zuständigen Aufsichtsbehörde einholen.

2.5.2 Verbindliche interne Datenschutzvorschriften (BCR) (Artikel 46 Absatz 2 Buchstabe b DSGVO)

62. Die Erwägungen im Schrems II-Urteil treffen auch auf andere in Artikel 46 Absatz 2 DSGVO vorgesehene Übermittlungsinstrumente zu, da alle diese Instrumente im Grunde vertraglicher Art sind, so dass die Behörden des Drittstaats durch die im Übermittlungsinstrument vorgesehenen Garantien und Verpflichtungen, die von den Vertragsparteien untereinander vereinbart werden, nicht gebunden werden.[73]

63. Das Schrems II-Urteil ist für die Übermittlung personenbezogener Daten auf Grundlage verbindlicher interner Datenschutzvorschriften relevant, weil drittstaatliche Rechtsvorschriften den durch solche Instrumente gewährten Schutz beeinträchtigen können.

64. Alle Verpflichtungen, die aufgenommen werden müssen, werden in den aktualisierten WP256/257-Referenzen[74] genannt, an die alle Gruppen, die sich auf BCR als Übertragungsinstrumente stützen, ihre bestehenden und künftigen BCR anpassen müssen.

---

[72] Vgl. entsprechend EDSA, Stellungnahme 17/2020 zu dem von der slowenischen Aufsichtsbehörde vorgelegten Entwurf für Standardvertragsklauseln (Artikel 28 Absatz 8 DSGVO) zu bereits festgelegten Standardvertragsklauseln nach Artikel 28 („Darüber hinaus erinnert der Ausschuss daran, dass die Möglichkeit, die von einer Aufsichtsbehörde festgelegten Standardvertragsklauseln zu verwenden, die Parteien nicht daran hindert, andere Klauseln oder zusätzliche Schutzmaßnahmen hinzuzufügen, vorausgesetzt diese stehen nicht direkt oder indirekt im Widerspruch zu den festgelegten Standardvertragsklauseln und beeinträchtigen nicht die Grundrechte oder Freiheiten der betroffenen Personen. Werden die Standard-Datenschutzklauseln geändert, wird allerdings nicht mehr vermutet, dass die Parteien festgelegte Standardvertragsklauseln umgesetzt haben"), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_de.pdf.

[73] EuGH, C-311/18 (Schrems II), Rn. 132.

[74] Artikel-29-Datenschutzgruppe, Arbeitsdokument mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher interner Datenschutzvorschriften (BCR), zuletzt überarbeitet und angenommen am 6. Februar 2018, WP 256 rev.01; Artikel-29-Datenschutzgruppe, Arbeitsdokument mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher interner Datenschutzvorschriften (BCR) für Auftragsverarbeiter, zuletzt überarbeitet und angenommen am 6. Februar 2018, WP 257 rev.01.

65. Der Gerichtshof hat darauf hingewiesen, dass es in der Verantwortung des Datenexporteurs und des Datenimporteurs liegt, zu beurteilen, ob das vom Unionsrecht geforderte Schutzniveau in dem betreffenden Drittland eingehalten wird, um dann auf dieser Grundlage festzustellen, ob die Garantien, die in Standardvertragsklauseln oder verbindlichen internen Datenschutzvorschriften (BCR) vorgesehen sind, auch in der Praxis eingehalten werden können. Sollte dies nicht der Fall sein, muss der der Datenexporteur prüfen, ob er zusätzliche Maßnahmen ergreifen kann, um ein der Sache nach gleichwertiges Schutzniveau wie im EWR zu gewährleisten; um jede Beeinträchtigung der Effektivität der zusätzlichen Maßnahmen zu verhindern, muss der Datenexporteur auch überprüfen, dass die zusätzlichen Maßnahmen weder durch das Recht noch durch die Praxis im Drittland beeinträchtigt werden.

2.5.3 Individualvereinbarungen über Vertragsklauseln (Artikel 46 Absatz 3 Buchstabe a DSGVO)

66. Die Erwägungen im Schrems II-Urteil treffen auch auf andere in Artikel 46 Absatz 2 DSGVO vorgesehene Übermittlungsinstrumente zu, da alle diese Instrumente im Grunde vertraglicher Art sind, so dass die darin vorgesehenen Garantien und Verpflichtungen, die von den Vertragsparteien vereinbart werden, drittstaatliche Behörden nicht binden können.[75] Das Schrems II-Urteil ist für die Übermittlung personenbezogener Daten auf Grundlage individuell vereinbarter Vertragsklauseln relevant, weil drittstaatliche Rechtsvorschriften den durch solche Instrumente gewährten Schutz beeinträchtigen können.

2.6 Schritt 6: Neubewertung in angemessenen Abständen

67. Der Datenexporteur muss die Lage in dem Drittland, in das er personenbezogene Daten übermittelt hat, fortlaufend – soweit angemessen in Zusammenarbeit mit dem Datenimporteur – auf Entwicklungen hin überwachen, die für seine ursprüngliche Beurteilung des Schutzniveaus und die von ihm getroffenen Entscheidungen bezüglich seiner Übermittlungen relevant sein könnten. Die Rechenschaftspflicht ist eine dauerhaft bestehende Verpflichtung (Artikel 5 Absatz 2 DSGVO).

68. Der Datenexporteur muss ausreichende Vorkehrungen treffen, die sicherstellen, dass Übermittlungen umgehend ausgesetzt oder beendet werden:

- wenn der Datenimporteur die Verpflichtungen, die er mit dem Übermittlungsinstrument gemäß Artikel 46 DSGVO eingegangen ist, verletzt hat oder ihm deren Erfüllung unmöglich ist; oder
- wenn die zusätzlichen Maßnahmen in dem betreffenden Drittland nicht mehr wirksam sind.

3 ERGEBNIS

69. In der DSGVO sind die Regeln niedergelegt, die für die Verarbeitung personenbezogener Daten im EWR gelten und somit den freien Verkehr personenbezogener Daten innerhalb des EWR ermöglichen. In Kapitel V der DSGVO, das Übermittlungen personenbezogener Daten in Drittländer regelt, werden hohe Anforderungen gestellt: Die Übermittlung darf das durch die

[75] EuGH, C-311/18 (Schrems II), Rn. 132.

DSGVO gewährleistete Schutzniveau für natürliche Personen nicht untergraben (Artikel 44 DSGVO). Das Schrems II-Urteil des Gerichtshofs (C-311/18) betont die Notwendigkeit, den Fortbestand des in der DSGVO verbürgten Schutzniveaus bei der Übermittlung personenbezogener Daten in ein Drittland zu gewährleisten.[76]

70. Die allererste Voraussetzung für die Gewährleistung eines der Sache nach gleichwertigen Schutzniveaus ist, dass der Datenexporteur seine Übermittlungen genau kennt. Der Datenexporteur muss auch überprüfen, ob die von ihm übermittelten Daten angemessen und relevant sind und auf das für die Zwecke, für die sie verarbeitet werden, erforderliche Maß beschränkt sind.

71. Der Datenexporteur muss entscheiden, welches der Übermittlungsinstrumente er für seine Übermittlung verwendet. Handelt es sich dabei nicht um einen Angemessenheitsbeschluss, muss er im Einzelfall, bezogen auf seine jeweilige Übermittlung, prüfen, ob das Recht oder die Praxis im Bestimmungsdrittland möglicherweise die Wirksamkeit der Garantien, die in den Artikel 46 DSGVO genannten Übermittlungsinstrumenten enthalten sind, beeinträchtigt. Wenn das aus Artikel 46 DSGVO ausgewählte Übermittlungsinstrument allein nicht ausreicht, für die vom Datenexporteur übermittelten personenbezogenen Daten ein der Sache nach gleichwertiges Schutzniveau zu erzielen, kann die Schutzlücke durch zusätzliche Maßnahmen geschlossen werden.

72. Gelingt es dem Datenexporteur nicht, effektive zusätzliche Maßnahmen zu finden oder zu implementieren, die gewährleisten, dass die übermittelten personenbezogenen Daten ein der Sache nach gleichwertiges Schutzniveau genießen, darf er nicht mit der Übermittlung personenbezogener Daten auf Grundlage des von ihm ausgewählten Übermittlungsinstruments in das Drittland beginnen. Sollte er bereits mit der Übermittlung begonnen haben, ist er gehalten, die Übermittlung personenbezogener Daten sofort auszusetzen oder zu beenden.

73. Die zuständige Aufsichtsbehörde ist befugt, die Übermittlung personenbezogener Daten in das Drittland auszusetzen oder zu beenden, falls der nach Unionsrecht (insbesondere nach Artikel 45 und 46 DSGVO und der Charta der Grundrechte) erforderliche Schutz der übermittelten Daten nicht gewährleistet ist.

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

(Andrea Jelinek)

[76] C-311/18 (Schrems II), Rn. 93.

ANHANG 1 BEGRIFFSBESTIMMUNGEN

- „Drittland“ bezeichnet ein Land, das nicht Mitgliedstaat des EWR ist.
- „EWR“ bezeichnet den Europäischen Wirtschaftsraum, welcher die Mitgliedstaaten der Europäischen Union sowie Island, Norwegen und Liechtenstein umfasst. Die DSGVO gilt gemäß dem Abkommen über den Europäischen Wirtschaftsraum, insbesondere Anhang XI und das Protokoll 37, auch für den EWR.
- „DSGVO“ bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).
- „Charta“ bezeichnet die Charta der Grundrechte der Europäischen Union, ABl. C 326 vom 26.10.2012, S. 391-407.
- „EuGH“ oder „Gerichtshof“ bezeichnet den Gerichtshof der Europäischen Union. Er ist das Rechtsprechungsorgan der Europäischen Union und wacht im Zusammenwirken mit den Gerichten der Mitgliedstaaten über die einheitliche Anwendung und Auslegung des Unionsrechts.
- „Datenexporteur“ bezeichnet den Verantwortlichen oder Auftragsverarbeiter im EWR, der personenbezogene Daten an einen Verantwortlichen oder Auftragsverarbeiter in einem Drittland übermittelt.
- „Datenimporteur“ bezeichnet den Verantwortlichen oder Auftragsverarbeiter in einem Drittland, der aus dem EWR übermittelte personenbezogene Daten empfängt oder dem Zugriff darauf gewährt wird.
- „Übermittlungsinstrument in Artikel 46 DSGVO“ bezieht sich auf eine der in Artikel 46 DSGVO aufgeführten Möglichkeiten, wie der Datenexporteur bei Übermittlungen personenbezogener Daten in Drittländer die erforderlichen geeigneten Garantien geben kann, falls es für das Drittland keinen Angemessenheitsbeschluss gemäß Artikel 45 Absatz 3 DSGVO gibt. Die Übermittlungsinstrumente in Artikel 46 DSGVO, von denen Verantwortliche und Auftragsverarbeiter Gebrauch machen können, sind in den Absätzen 2 und 3 dieses Artikels aufgeführt.
- „SVK“ bezeichnet von der Europäischen Kommission erlassene Standarddatenschutzklauseln (auch „Standardvertragsklauseln“ genannt), die für die Übermittlung personenbezogener Daten zwischen Verantwortlichen bzw. Auftragsverarbeitern im EWR und Verantwortlichen oder Auftragsverarbeitern außerhalb des EWR verwendet werden können. Die von der Europäischen Kommission angenommenen Standardvertragsklauseln sind ein Übermittlungsinstrument im Sinne der DSGVO, vgl. Artikel 46 Absatz 2 Buchstabe c und Absatz 5 DSGVO.

ANHANG 2: BEISPIELE FÜR ZUSÄTZLICHE MASSNAHMEN

74. Im Folgenden sind Beispiele für zusätzliche Maßnahmen aufgeführt, die der Datenexporteur in Betracht ziehen kann, wenn er zu Schritt 4 „Zusätzliche Maßnahmen ergreifen“ gelangt ist. Dies ist keine erschöpfende Liste. Der Datenexporteur kann weitere ergänzende Maßnahmen prüfen. Künftige technologische, rechtliche oder organisatorische Entwicklungen können zur Entstehung neuer ergänzender Maßnahmen führen, die der Datenexporteur in Erwägung ziehen muss. Nur weil man eine oder mehrere dieser Maßnahmen ausgewählt und angewendet hat, bedeutet das noch nicht unbedingt, dass systematisch sichergestellt ist, dass die vorgesehene Übermittlung den unionsrechtlichen Anforderungen (Gewährleistung eines der Sache nach gleichwertigen Schutzniveaus) genügt. Bei der Auswahl ist darauf zu achten, dass die zusätzlichen Maßnahmen den erforderlichen Schutz der vorgesehenen Übermittlungen effektiv gewährleisten.

75. Eine zusätzliche Maßnahme ist nur dann als effektiv im Sinne des „Schrems II“-Urteils des Gerichtshofs anzusehen, sofern und soweit sie – für sich genommen oder in Verbindung mit anderen – genau die Rechtsschutzlücken schließt, die der Datenexporteur bei seiner Prüfung der für seine Übermittlung geltenden Rechtsvorschriften und Praktiken im Drittland festgestellt hat. Sollte es dem Datenexporteur letztendlich nicht möglich sein, ein der Sache nach gleichwertiges Schutzniveau zu erzielen, darf er die personenbezogenen Daten nicht übermitteln.

76. Als Verantwortlicher oder Auftragsverarbeiter ist der Datenexporteur unter Umständen ohnehin gehalten, einige der in diesem Anhang beschriebenen Maßnahmen zu ergreifen, um die Anforderungen der DSGVO zu erfüllen. Dies bedeutet, dass für im EWR verarbeitete personenbezogene Daten, die an einen Datenimporteur, für den ein Angemessenheitsbeschluss gilt, oder an andere Drittländer übermittelt werden, möglicherweise ähnliche Maßnahmen getroffen werden müssen.[77]

2.1 Technische Maßnahmen

77. In diesem Abschnitt werden einige Beispiele für technische Maßnahmen beschrieben, wobei es sich jedoch nicht um eine erschöpfende Darstellung handelt. Diese technischen Maßnahmen können die Garantien, die die Übermittlungsinstrumente in Artikel 46 DSGVO bieten, ergänzen, um sicherzustellen, dass der unionsrechtlich erforderliche Schutz auch bei der Übermittlung personenbezogener Daten in ein Drittland gewährleistet ist. Diese Maßnahmen sind insbesondere dann erforderlich, wenn das Recht des betreffenden Drittlands dem Datenimporteur Verpflichtungen auferlegt, die den genannten Garantien der Übermittlungsinstrumente in Artikel 46 DSGVO zuwiderlaufen und daher geeignet sind, die vertragliche Garantie eines der Sache nach gleichwertigen Schutzniveaus, was den behördlichen Datenzugriff im Drittland angeht, zu untergraben.[78]

78. Zur weiteren Klarstellung werden in diesem Abschnitt zunächst einige Beispiele für Szenarien beschrieben, bei denen einige technische Maßnahmen potenziell wirksam sein könnten, um ein der Sache nach gleichwertiges Schutzniveau zu gewährleisten. Anschließend werden einige

[77] Artikel 5 Absatz 2 DSGVO, Artikel 32 DSGVO.
[78] C-311/18 (Schrems II), Rn. 135.

Szenarien geschildert, in denen keine technischen Maßnahmen zur Gewährleistung dieses Schutzniveaus gefunden werden konnten.

Beispiele für Szenarien, für die sich *wirksame* Maßnahmen finden ließen

79. Die nachstehenden Maßnahmen sollen sicherstellen, dass der Zugriff durch Behörden in Drittländern auf die übermittelten Daten die Effektivität der in Artikel 46 DSGVO aufgeführten geeigneten Garantien nicht untergräbt. Diese Maßnahmen wären notwendig, um ein Schutzniveau zu gewährleisten, das dem im EWR garantierten Schutzniveau der Sache nach gleichwertig ist, selbst wenn der behördliche Zugriff mit dem Recht im Land des Datenimporteurs in Einklang steht, wenn dieser Zugriff in der Praxis über das hinausgeht, was in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist.[79] Diese Maßnahmen zielen darauf ab, potenziell rechtsverletzende Zugriffe auszuschließen, indem sie die Behörden daran hindern, betroffene Personen zu identifizieren, Informationen über sie zu erschließen, sie in anderen Kontexten zu ermitteln oder die übermittelten Daten mit anderen Datensätzen im Behördenbesitz zu verknüpfen, die unter anderem Daten über Online-Kennungen der Geräte, Anwendungen, Tools und Protokolle enthalten, die die betroffenen Personen in anderen Zusammenhängen benutzt haben.

80. Behörden in Drittländern können auf verschiedene Weise versuchen, auf übermittelte Daten zuzugreifen:

    a) während der Übermittlung, indem die Behörden auf die Kommunikationsleitungen zugreifen, die für die Übermittlung der Daten ins Empfängerland verwendet werden. Dieser Zugriff kann passiv erfolgen, z. B, indem die Kommunikationsinhalte, möglicherweise nachdem eine Auswahl getroffen wurde, einfach kopiert werden. Es kann sich aber auch um einen aktiven Zugriff handeln, indem sich die Behörden aktiv in den Kommunikationsprozess einschalten und den Inhalt nicht nur lesen, sondern ihn auch manipulieren oder zum Teil unterdrücken;

    b) während sich die Daten im Besitz des vorgesehenen Datenempfängers befinden, indem die Behörden entweder auf die Verarbeitungseinrichtungen selbst zugreifen oder aber den Datenempfänger dazu anhalten, die Daten zu finden und die Daten, die für die Behörden interessant sind, zu extrahieren und herauszugeben.

81. In diesem Abschnitt werden Szenarien betrachtet, in denen die angewendeten Maßnahmen in beiden Fällen effektiv sind. Je nach den konkreten Umständen der Übermittlung sind verschiedene zusätzliche Maßnahmen möglich; wenn nach dem Recht des Empfängerlands nur eine einzige Zugriffsmöglichkeit vorgesehen ist, kann auch schon eine einzige zusätzliche Maßnahme genügen. Der Datenexporteur muss deshalb, mit Unterstützung des Datenimporteurs, sehr genau prüfen, welchen Verpflichtungen der Datenimporteur unterliegt.

Ein Beispiel: Für Datenimporteure in den USA, die 50 USC § 1881a (FISA 702) unterliegen, gilt hinsichtlich der importierten Daten, die sich in ihrem Besitz oder Gewahrsam oder unter ihrer Kontrolle befinden, eine direkte Verpflichtung, den Zugriff darauf zu gewähren oder diese herauszugeben. Diese

[79] Siehe Artikel 47 und 52 der Charta der Grundrechte der Europäischen Union, Artikel 23 Absatz 1 DSGVO, und die Empfehlungen 02/2020 des EDSA zu den grundlegenden europäischen Garantien für Überwachungsmaßnahmen, 10. November 2020.

Verpflichtung kann sich auch auf die kryptografischen Schlüssel erstrecken, ohne die die Daten nicht lesbar sind.

82. In den Szenarien werden spezifische Umstände und Maßnahmen beschrieben, die als Beispiel dienen sollen. Weicht ein Szenario auch nur geringfügig von dem hier geschilderten ab, kann das Ergebnis anders ausfallen. Die Szenarien beziehen sich auf Situationen, in denen der Schluss gezogen wurde, dass in erster Linie zusätzliche Maßnahmen erforderlich sind, d. h. in denen in der Praxis problematische Rechtsvorschriften des Drittstaats auf die betreffende Übermittlung angewandt werden.

83. Unabhängig von dem Schutz, den die für den Datenimporteur geltenden Rechtsvorschriften bieten, kann es sein, dass Verantwortliche nur einige oder aber sämtliche der hier beschriebenen Maßnahmen ergreifen müssen, weil diese unter den konkreten Umständen der Übermittlung zur Einhaltung der Artikel 25 und 32 DSGVO erforderlich sind. Mit anderen Worten: Datenexporteure sind unter Umständen selbst dann gehalten, die hier beschriebenen Maßnahmen zu ergreifen, wenn für ihren Datenimporteur ein Angemessenheitsbeschluss gilt; dies ist nicht anders als bei der Verarbeitung von Daten innerhalb des EWR, wo ebenfalls eine solche Verpflichtung zur Anwendung zusätzlicher Maßnahmen bestehen kann.

Anwendungsfall 1: Datenspeicherung zu Backup- und anderen Zwecken, die nicht den Zugang zu unverschlüsselten Daten erfordern

84. Ein Datenexporteur nutzt einen Hosting-Anbieter in einem Drittland zur Speicherung personenbezogener Daten, z. B. für Backup-Zwecke.

Wenn

1. die personenbezogenen Daten vor der Übermittlung unter Verwendung einer starken Verschlüsselung verarbeitet werden und die Identität des Datenimporteurs überprüft wird,
2. der Verschlüsselungsalgorithmus und seine Parametrisierung (z. B. ggf. Schlüssellänge, Betriebsmodus) dem Stand der Technik entsprechen und – unter Berücksichtigung der zur Verfügung stehenden Ressourcen und technischen Möglichkeiten (z. B. Rechenleistung für Brute-Force-Angriffe) – Robustheit gegen die von den Behörden im Empfängerland durchgeführte Kryptoanalyse bieten;[80]
3. die Verschlüsselungsstärke die Schlüssellänge den spezifischen Zeitraum berücksichtigt, für den die Vertraulichkeit der verschlüsselten personenbezogenen Daten sicherzustellen ist;[81]

[80]Für die Bewertung der Stärke von Verschlüsselungsalgorithmen, ihrer Konformität mit dem Stand der Technik und ihrer Robustheit gegen Kryptoanalyse im Zeitverlauf können sich Datenexporteure auf technische Leitlinien stützen, die von den für Cybersicherheit zuständigen Behörden der EU und ihrer Mitgliedstaaten veröffentlicht wurden. Siehe z. B. den ENISA-Bericht „Was ist der ‚Stand der Technik' im Bereich der IT-Sicherheit?", 2019, https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security; Hinweise des Bundesamtes für Informationssicherheit in seinen Technischen Leitlinien der Reihe TR-02102 und „Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 – Projekt 645421, D5.4, ECRYPT-CSA, 02/2018" unter https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.

[81]Die Schutzkapazität kryptografischer Algorithmen sinkt im Laufe der Zeit aufgrund der Entdeckung neuer kryptoanalytischer Techniken, des Aufkommens neuer Rechenparadigmen wie Quanteninformatik und der

4. der Verschlüsselungsalgorithmus korrekt und durch ordnungsgemäß gewartete Software ohne bekannte Schwachstellen implementiert ist, deren Konformität mit der Spezifikation des ausgewählten Algorithmus z. B. durch Zertifizierung bestätigt wurde;
5. die Schlüssel zuverlässig verwaltet werden (erzeugt, angewandt, gespeichert, gegebenenfalls mit der Identität eines vorgesehenen Empfängers verknüpft und widerrufen) [82], und
6. die Kontrolle über die Schlüssel allein beim Datenexporteur oder bei einer anderen vom Datenexporteur mit dieser Aufgabe betrauten Stelle im EWR oder einer Rechtsordnung liegt, die ein Schutzniveau bietet, das dem im EWR garantierten Schutzniveau der Sache nach gleichwertig ist;

stellt die vorgenommene Verschlüsselung nach Ansicht des EDSA eine effektive zusätzliche Maßnahme dar.

Anwendungsfall 2: Übermittlung pseudonymisierter Daten

85. Ein Datenexporteur pseudonymisiert die von ihm gehaltenen Daten, bevor er sie zur Analyse ins Drittland übermittelt, z. B. zu Forschungszwecken.

Wenn

1. der Datenexporteur die personenbezogenen Daten in solcher Weise übermittelt, dass die personenbezogenen Daten weder einer spezifischen betroffenen Person zugeordnet noch dazu verwendet werden können, die betroffene Person in einer größeren Gruppe zu identifizieren;[83]
2. die zusätzlichen Informationen allein vom Datenexporteur und separat gehalten werden, und zwar in einem Mitgliedstaat oder in einem Drittland, bei einer vom Datenexporteur mit dieser Aufgabe betrauten Stelle im EWR oder einer Rechtsordnung, die ein Schutzniveau bietet, das dem im EWR garantierten Schutzniveau der Sache nach gleichwertig ist;

---

allgemeinen Steigerung der verfügbaren Rechenleistung, es sei denn, die angewandten Algorithmen haben sich als theoretisch sicher erwiesen. Dies gilt insbesondere für öffentliche Schlüsselalgorithmen, die zum Zeitpunkt der Abfassung gemeinhin verwendet werden. Folglich muss der Datenexporteur davon ausgehen, dass sich Behörden unter den unter Nummer 80 beschriebenen Umständen verpflichten können, auf verschlüsselte Daten zuzugreifen und diese zu speichern, bis ihre Ressourcen für eine Entschlüsselung ausreichen. Die ergänzende Maßnahme kann nur dann als wirksam angesehen werden, wenn eine solche Entschlüsselung und anschließende Weiterverarbeitung zu diesem Zeitpunkt keine Verletzung der Rechte betroffener Personen mehr darstellen würde, z. B., weil die Daten nicht mehr zur direkten oder indirekten Identifizierung dieser Personen verwendet werden können.

[82] NIST-Sonderveröffentlichung 800-57, Empfehlung für Schlüsselmanagement https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

[83] Gemäß Artikel 4 Absatz 5 DSGVO bezeichnet: „‚Pseudonymisierung' die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne die Hinzuziehung zusätzlicher Informationen nicht mehr einer bestimmten betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen getrennt aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer bestimmten oder identifizierbaren natürlichen Person zugeordnet werden;" zusätzliche Daten können aus Tabellen bestehen, in denen die Pseudonyme mit den Identifizierungsattributen verknüpft werden, die sie ersetzen, kryptografischen Schlüsseln oder anderen Parametern für die Umwandlung von Attributen oder anderen Daten, die die Zuordnung der pseudonymisierten Daten zu identifizierten oder identifizierbaren natürlichen Personen ermöglichen.

3. die Offenlegung oder die unerlaubte Verwendung der zusätzlichen Informationen durch geeignete technische und organisatorische Garantien verhindert wird und sichergestellt ist, dass die Kontrolle über den Algorithmus oder den Datenspeicher, der die Re-Identifizierung anhand der zusätzlichen Informationen ermöglicht, allein beim Datenexporteur liegt, und
4. der Verantwortliche durch gründliche Analyse der betreffenden Daten, unter Berücksichtigung sämtlicher Informationen, von denen zu erwarten ist, dass sie den Behörden im Empfängerland zur Verfügung stehen und von ihnen genutzt werden, festgestellt hat, dass die pseudonymisierten personenbezogenen Daten keiner identifizierten oder identifizierbaren natürlichen Person zugeordnet werden können, selbst wenn sie mit derartigen Informationen abgeglichen werden sollten,

stellt die vorgenommene Pseudonymisierung nach Ansicht des EDSA eine effektive zusätzliche Maßnahme dar.

86. Es ist zu beachten, dass es häufig anhand von für die körperliche, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität spezifischen Faktoren, dem Standort oder der Interaktion einer natürlichen Person mit Online-Diensten zu bestimmten Zeitpunkten[84] möglich sein dürfte, die betreffende Person zu identifizieren, selbst wenn deren Name, Anschrift oder andere klare Identifikationsmerkmale nicht mitgeteilt werden.

87. Dies gilt insbesondere, wenn die Daten die Nutzung von Informationsdiensten betreffen (Zugriffszeitpunkt, Reihenfolge der aufgerufenen Seiten, Merkmale des verwendeten Geräts usw.). Es kann durchaus sein, dass derartige Dienste, wie auch der Importeur personenbezogener Daten, verpflichtet sind, den Behörden in ihrem Land Zugriff zu gewähren; die Behörden werden dann wahrscheinlich Daten darüber besitzen, wie die Zielperson(en) die betreffenden Informationsdienste nutzen.

88. Im Hinblick darauf, dass einige Informationsdienste ohnehin ihrer Art wegen in öffentlicher Weise genutzt werden bzw. dass Stellen, die über erhebliche Ressourcen verfügen, sich diese Informationsdienste zunutze machen können, werden die Verantwortlichen besonders sorgfältig prüfen müssen, ob die Behörden in ihrem Land wahrscheinlich Daten darüber besitzen, wie ihre Zielpersonen Informationsdienste nutzen.

89. Wenn im Zuge der Pseudonymisierung die in den personenbezogenen Daten enthaltenen Attribute mithilfe eines kryptografischen Algorithmus umgewandelt werden, gelten die Leitlinien in den Fußnoten 80 und 81. Künftig wird empfohlen, auf die ausschließliche Nutzung der Verschlüsselung zu verzichten und Transformationen auf der Grundlage von Tabellen-Look-up-Mechanismen anzuwenden.

[84] Artikel 4 Absatz 1 DSGVO: „‚personenbezogene Daten' [bezeichnet] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann".

Anwendungsfall 3: Verschlüsselung von Daten zum Schutz vor dem Zugriff durch Behörden des Drittlands des Datenimporteurs, wenn sich die Daten im Transit zwischen Datenexporteur und Datenimporteur befinden

90. Ein Datenexporteur möchte Daten an einen Bestimmungsort übermitteln, an dem die Rechtsvorschriften und/oder Praktiken Behörden den Zugriff auf Daten während des Transits zwischen dem Land des Exporteurs und dem Bestimmungsland gestatten.

Wenn

1. der Datenexporteur personenbezogene Daten an einen Datenimporteur in einem Land übermittelt, in dem die Rechtsvorschriften und/oder Praktiken es den Behörden gestatten, auf Daten zuzugreifen, während sie über das Internet in dieses Drittland ohne die wesentlichen europäischen Garantien für diesen Zugriff transportiert werden, und eine Transportverschlüsselung verwendet wird, für die sichergestellt ist, dass die verwendeten Verschlüsselungsprotokolle dem neuesten Stand der Technik entsprechen und einen wirksamen Schutz gegen aktive und passive Angriffe mit den den Behörden dieses Drittlands bekanntermaßen zur Verfügung stehenden Ressourcen bieten,
2. die an der Kommunikationen Beteiligten sich auf eine vertrauenswürdige Zertifizierungsstelle oder Infrastruktur für öffentliche Schlüssel einigen,
3. spezifische Schutzmaßnahmen und modernste Maßnahmen gegen aktive und passive Angriffe auf die Sende- und Empfangssysteme, die Transportverschlüsselung bieten, eingesetzt werden, einschließlich Tests auf Software-Schwachstellen und mögliche Hintertüren;
4. personenbezogene Daten auch in der Anwendungsschicht mit dem Stand der Technik entsprechenden Verschlüsselungsmethoden End-to-End-verschlüsselt werden, falls die Erfahrung gezeigt hat, dass die Transportverschlüsselung allein wegen Schwachstellen der verwendeten Infrastruktur oder Software keine geeignete Sicherheit bieten dürfte,
5. der Verschlüsselungsalgorithmus und seine Parametrisierung (z. B. ggf. Schlüssellänge, Betriebsmodus) dem Stand der Technik entsprechen und – unter Berücksichtigung der zur Verfügung stehenden Ressourcen und technischen Möglichkeiten (z. B. Rechenleistung für Brute-Force-Angriffe) – der von den Behörden im Transitland durchgeführten Kryptoanalyse widerstehen; (siehe weiter oben Fußnote 80),[85]
6. die Verschlüsselungsstärke den spezifischen Zeitraum berücksichtigt, für den die Vertraulichkeit der verschlüsselten personenbezogenen Daten sicherzustellen ist;
7. der Verschlüsselungsalgorithmus korrekt und durch ordnungsgemäß gewartete Software ohne bekannte Schwachstellen implementiert ist, deren Konformität mit der Spezifikation des ausgewählten Algorithmus z. B. durch Zertifizierung bestätigt wurde;
8. die Schlüssel zuverlässig verwaltet (erzeugt, angewandt, gespeichert, falls relevant, mit der Identität des vorgesehenen Empfängers verknüpft sowie widerrufen) werden und zwar vom Datenexporteur oder von einer Stelle, der der Datenexporteur vertraut und die in einem Land ansässig ist, das ein der Sache nach gleichwertiges Schutzniveau bietet,

stellt die Transportverschlüsselung, erforderlichenfalls in Kombination mit End-to-End-Verschlüsselung, nach Ansicht des EDSA eine effektive zusätzliche Maßnahme dar.

[85] Siehe Fußnote 80 für einige Verweise auf technische Leitlinien, die von den für die Cybersicherheit zuständigen Behörden der EU und der Mitgliedstaaten veröffentlicht wurden.

Anwendungsfall 4: Geschützter Empfänger

91. Ein Datenexporteur übermittelt personenbezogene Daten an einen Datenimporteur in einem Drittland, der nach dem Recht des betreffenden Landes besonderen Schutz genießt; dies geschieht z. B. zu dem Zweck der gemeinsamen ärztlichen Behandlung eines Patienten oder der gemeinsamen Erbringung von Rechtsdienstleistungen für einen Mandanten.

Wenn

1. ein ansässiger Datenimporteur nach dem Recht des Drittlands im Hinblick auf Daten, die er für einen bestimmten Zweck hält, von Zugriffen, die rechtsverletzend sein könnten, ausgenommen ist (z. B. wegen einer für den Datenimporteur geltenden beruflichen Schweigepflicht),
2. diese Ausnahme für sämtliche im Besitz des Datenimporteurs befindlichen Informationen gilt, die dazu verwendet werden könnten, den Schutz geheimer Informationen zu umgehen (kryptografische Schlüssel, Passwörter, sonstige Anmeldedaten usw.),
3. der Datenimporteur weder Dienstleistungen eines Auftragsverarbeiters in Anspruch nimmt, die den Behörden den Zugriff auf die Daten ermöglichen könnten, solange sich diese beim Auftragsverarbeiter befinden, noch die Daten an eine andere Stelle weiterleitet, ohne dass dies auf Grundlage von in Artikel 46 DSGVO vorgesehenen Übermittlungsinstrumente geschieht,
4. die personenbezogenen Daten vor der Übermittlung verschlüsselt werden, und zwar mit einer Methode, die dem Stand der Technik entspricht und die für den gesamten Zeitraum, für den die Daten zu schützen sind, garantiert, dass ohne Kenntnis des Entschlüsselungsschlüssels (End-to-End-Verschlüsselung) keine Entschlüsselung möglich ist,
5. der Entschlüsselungsschlüssel sich im alleinigen Gewahrsam des geschützten Datenimporteurs und gegebenenfalls des Exporteurs selbst oder einer anderen vom Datenexporteur mit dieser Aufgabe betrauten Stelle im EWR oder in einer Rechtsordnung, die ein Schutzniveau bietet, das dem im EWR garantierten Schutzniveau der Sache nach gleichwertig ist, befindet und durch technische und organisatorische Maßnahmen, die dem Stand der Technik entsprechen, angemessen dagegen geschützt ist, unbefugt benutzt oder offengelegt zu werden, und
6. der Datenexporteur sich zuverlässig davon überzeugt hat, dass der Verschlüsselungsschlüssel, den er zu benutzen beabsichtigt, zu dem vom Empfänger gehaltenen Entschlüsselungsschlüssel passt,

stellt die vorgenommene Transportverschlüsselung nach Ansicht des EDSA eine effektive zusätzliche Maßnahme dar.

Anwendungsfall 5: Aufgeteilte Verarbeitung oder Verarbeitung durch mehrere Beteiligte (Multi-party Processing)

92. Der Datenexporteur möchte eine gemeinsame Verarbeitung personenbezogener Daten durch mindestens zwei unabhängige Auftragsverarbeiter, die in verschiedenen Ländern ansässig sind, ohne diesen den Dateninhalt offenzulegen. Vor der Übermittlung werden die Daten so aufgeteilt, dass die Daten, die jeder einzelne Auftragsverarbeiter hat, nicht ausreichen, die personenbezogenen Daten ganz oder zum Teil zu rekonstruieren. Der Datenexporteur erhält von jedem der Auftragsverarbeiter dessen Verarbeitungsergebnis und fügt deren Ergebnisse zum Endergebnis zusammen, bei dem es sich um personenbezogene oder aggregierte Daten handeln kann.

Wenn

1. ein Datenexporteur personenbezogene Daten so aufteilt, dass sie in mindestens zwei Datenstücke aufgeteilt sind, wobei die einzelnen Datenstücke ohne Verwendung zusätzlicher Informationen nicht mehr interpretiert oder einer bestimmten betroffenen Person zugeordnet werden können;
2. jedes der Datenstücke an einen gesonderten Auftragsverarbeiter, der in einem anderen Land ansässig ist, übermittelt wird;
3. die Auftragsverarbeiter die Möglichkeit haben, die Daten gemeinsam, z. B. unter Verwendung von Secure Multi-Party Computation, zu verarbeiten, wobei keinem von ihnen Informationen bekannt werden, die sie nicht bereits vor der Verarbeitung besaßen;
4. der für die gemeinsame Verarbeitung verwendete Algorithmus Sicherheit gegen aktive Angreifer bietet;
5. der Verantwortliche durch gründliche Analyse der betreffenden Daten, unter Berücksichtigung sämtlicher Informationen, die den Behörden in den Empfängerländern zur Verfügung stehen mögen, festgestellt hat, dass die von ihm übermittelten Datenstücke keiner identifizierten oder identifizierbaren natürlichen Person zugeordnet werden können, selbst wenn sie mit derartigen Informationen abgeglichen werden sollten;
6. es keine Anzeichen für eine Zusammenarbeit der Behörden in den Ländern, in denen die einzelnen Auftragsverarbeiter ansässig sind, gibt, die es diesen ermöglichen würde, sich den Zugang zu sämtlichen Datensätzen der von den Auftragsverarbeitern gehaltenen personenbezogenen Daten zu verschaffen, so dass sie den Inhalt der personenbezogenen Daten entschlüsseln und nutzen könnten, um sie in einer Weise zu nutzen, bei der der Wesensgehalt der Grundrechte und Grundfreiheiten der betroffenen Personen nicht geachtet wäre. Auch die Behörden der einzelnen Länder dürften nicht ermächtigt sein, auf personenbezogene Daten zuzugreifen, die von den Auftragsverarbeitern in den verschiedenen betroffenen Ländern gehalten werden;

stellt die aufgeteilte Verarbeitung nach Ansicht des EDSA eine effektive zusätzliche Maßnahme dar.

Beispiele für Szenarien, für die sich *keine wirksamen* Maßnahmen finden ließen

93. Die nachstehend beschriebenen Maßnahmen böten in bestimmten Situationen keine wirksame Gewährleistung eines der Sache nach gleichwertigen Schutzniveaus für die in das Drittland übermittelten Daten. Sie kämen daher nicht als zusätzliche Maßnahmen in Betracht.

Anwendungsfall 6: Übermittlung an Cloud-Service-Anbieter oder andere Verarbeiter, die Zugang zu unverschlüsselten Daten benötigen

94. Ein Datenexporteur übermittelt personenbezogene Daten, entweder elektronisch oder durch Bereitstellung an einen Cloud-Service-Anbieter oder einen anderen Auftragsverarbeiter, um personenbezogene Daten gemäß seinen Weisungen in einem Drittland verarbeiten zu lassen (z. B. für die Bereitstellung technischer Unterstützung oder jede Art der Cloud-Verarbeitung), und diese Daten sind nicht - oder können nicht -, wie in Anwendungsfall 2 beschrieben, pseudonymisiert (werden) oder, wie in Anwendungsfall 1 beschrieben, verschlüsselt (werden), da für die Verarbeitung ein Zugriff auf unverschlüsselte Daten erforderlich ist.

Wenn

1. ein Verantwortlicher personenbezogene Daten an einen Cloud-Service-Anbieter oder sonstigen Auftragsverarbeiter übermittelt;
2. der Cloud-Service-Anbieter oder sonstige Auftragsverarbeiter Zugang zu den unverschlüsselten Daten benötigt, um die ihm übertragene Aufgabe auszuführen, und
3. die den Behörden des Empfängerlands eingeräumte Befugnis, auf die in Rede stehenden übermittelten Daten zuzugreifen, über das hinausgeht, was in einer demokratischen Gesellschaft, in der in der Praxis problematische Rechtsvorschriften des Drittstaats auf die betreffenden Übermittlungen anwendbar sind, erforderlich und verhältnismäßig ist (siehe Schritt 3).[86]

ist für den EDSA nach dem heutigen Stand der Technik keine wirksame technische Maßnahme vorstellbar, die im Falle eines solchen Zugriffs die Verletzung der Grundrechte der betroffenen Person verhindern könnte. Der EDSA schließt nicht aus, dass durch künftige technische Entwicklungen Maßnahmen möglich werden könnten, die die beabsichtigten Geschäftszwecke erfüllen, ohne dass ein Zugriff auf die unverschlüsselten Daten benötigt würde.

95. In den vorgenannten Szenarien, in denen der Auftragsverarbeiter für seine Dienstleistung unverschlüsselte personenbezogene Daten benötigt, stellen Transportverschlüsselung und Data-at-Rest-Verschlüsselung – selbst in der Kombination – keine zusätzliche Maßnahme dar, die ein der Sache nach gleichwertiges Schutzniveau gewährleistet, wenn der Datenimporteur im Besitz der kryptografischen Schlüssel ist.

Anwendungsfall 7: Übermittlung personenbezogener Daten zu geschäftlichen Zwecken, auch im Wege des Fernzugriffs

96. Ein Datenexporteur übermittelt personenbezogene Daten – in ein Drittland zur Verwendung für gemeinsame Geschäftszwecke – durch elektronische Übermittlung oder durch Bereitstellung für den Fernzugriff durch den Datenimporteur, und diese Daten sind nicht – oder können nicht –, wie in Anwendungsfall 2 beschrieben, pseudonymisiert (werden) oder, wie in Anwendungsfall 1 beschrieben, verschlüsselt (werden), da für die Verarbeitung ein Zugriff auf unverschlüsselte Daten erforderlich ist. Eine typische Konstellation wäre etwa, dass ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter personenbezogene Daten an einen in einem Drittland ansässigen Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, übermittelt. Der Datenimporteur kann die Daten, die er empfängt, z. B. dazu nutzen, Personaldienstleistungen für den Datenexporteur zu erbringen, für die er dessen Personaldaten braucht, oder dazu, mit Kunden des Datenexporteurs, die in der Europäischen Union wohnen, per Telefon oder E-Mail zu kommunizieren.

Wenn

1. ein Datenexporteur personenbezogene Daten an einen Datenimporteur in einem Drittland übermittelt, indem er die Daten in einem Informationssystem so zur Verfügung stellt, dass der

[86]Siehe Artikel 47 und 52 der Charta der Grundrechte der Europäischen Union, Artikel 23 Absatz 1 DSGVO, und die Empfehlungen 02/2020 des EDSA zu den grundlegenden europäischen Garantien für Überwachungsmaßnahmen, 10. November 2020.

Datenimporteur direkt auf Daten zugreifen kann, die er selbst ausgewählt hat, oder indem er ihm diese direkt, sei es einzeln oder in großen Mengen, über einen Kommunikationsdienst übermittelt,

2. der Datenimporteur[87] die unverschlüsselten Daten in dem Drittland (auch für seine eigenen Zwecke, wenn der Datenimporteur auch Verantwortlicher ist) verarbeitet,
3. die den Behörden des Empfängerlandes eingeräumte Befugnis, auf die übermittelten Daten zuzugreifen, über das hinausgeht, was in einer demokratischen Gesellschaft, in der in der Praxis problematische Rechtsvorschriften des Drittstaats für die betreffenden Übermittlungen gelten, erforderlich und verhältnismäßig ist (siehe Schritt 3),

ist für den EDSA keine effektive technische Maßnahme vorstellbar, die im Falle eines solchen Zugangs die Verletzung der Grundrechte der betroffenen Person verhindern könnte.

97. In den vorgenannten Szenarien, in denen der Auftragsverarbeiter für seine Dienstleistung unverschlüsselte personenbezogene Daten benötigt, stellen Transportverschlüsselung und Data-at-Rest-Verschlüsselung – selbst in der Kombination – keine zusätzliche Maßnahme dar, die ein im Wesentlichen gleichwertiges Schutzniveau gewährleistet, wenn der Datenimporteur im Besitz der kryptografischen Schlüssel ist.

[87] „Datenimporteur“ bezeichnet den Verantwortlichen oder Auftragsverarbeiter in einem Drittland, der aus dem EWR übermittelte personenbezogene Daten empfängt oder dem Zugriff darauf gewährt wird.

2.2 Zusätzliche vertragliche Maßnahmen

98. Bei diesen Maßnahmen handelt es sich im Allgemeinen um einseitige, zweiseitige oder mehrseitige[88] vertragliche Verpflichtungen.[89] Wird eines der Übermittlungsinstrumente in Artikel 46 DSGVO verwendet, enthält es zumeist bereits eine Reihe (vorwiegend vertraglicher) Verpflichtungen des Datenexporteurs und des Datenimporteurs, die als Garantien für die personenbezogenen Daten gedacht sind.[90]

99. In manchen Fällen können derartige Maßnahmen die Garantien, die das Übermittlungsinstrument und die einschlägigen Rechtsvorschriften im Drittland bieten, ergänzen und verstärken, soweit die Garantien, unter Berücksichtigung sämtlicher Umstände der Übermittlung, nicht alle Voraussetzungen erfüllen, die erforderlich sind, um ein Schutzniveau zu gewährleisten, das dem im EWR gewährten der Sache nach gleichwertig ist. Da die vertraglichen Maßnahmen ihrer Art nach die Behörden des Drittlands im Allgemeinen nicht binden können, wenn diese nicht selbst Vertragspartei sind,[91] müssen sie möglicherweise häufig mit anderen technischen und organisatorischen Maßnahmen kombiniert werden, um das erforderliche Datenschutzniveau zu gewährleisten. Nur weil man eine oder mehrere dieser Maßnahmen ausgewählt und angewendet hat, bedeutet das noch nicht unbedingt, dass systematisch sichergestellt ist, dass die vorgesehene Übermittlung den unionsrechtlichen Anforderungen (Gewährleistung eines der Sache nach gleichwertigen Schutzniveaus) genügt.

100. Je nachdem, welche vertraglichen Maßnahmen bereits im verwendeten Übermittlungsinstrument in Artikel 46 DSGVO enthalten sind, können zusätzliche vertragliche Maßnahmen auch dazu eingesetzt werden, den im EWR ansässigen Datenexporteuren zu helfen, über die neuen Entwicklungen auf dem Laufenden zu bleiben, die den Schutz der in Drittländer übermittelten Daten beeinträchtigen könnten.

101. Wie erwähnt, können vertraglichen Maßnahmen die Anwendung von im Drittland geltenden Rechtsvorschriften, die nicht den in den „Wesentlichen europäischen Garantien" aufgestellten Anforderungen des EDSA genügen, nicht verhindern; dies ist z. B. der Fall, wenn Datenimporteure aufgrund solcher Rechtsvorschriften auf behördliche Anordnung hin zur Offenlegung von Daten verpflichtet sind.[92]

102. Nachstehend sind einige Beispiele für in Betracht kommende vertragliche Maßnahmen aufgeführt und ihrer Art nach klassifiziert:

---

[88] Z. B. in verbindlichen internen Datenschutzvorschriften (BCR), die auf jeden Fall einige der nachstehend aufgeführten Maßnahmen vorsehen sollten.

[89] Sie sind zivilrechtlicher Art und nicht als dem Völkerrecht unterliegende internationale Vereinbarungen anzusehen. Sie können folglich, wie der Gerichtshof im Schrems II-Urteil hervorgehoben hat, die Behörden des Drittlands nicht binden, da die Behörden nicht Partei der mit Privatpersonen im Drittland geschlossenen Verträge sind (vgl. Urteil in der Rechtssache C-311/18 (Schrems II), Rn. 125).

[90] Siehe Urteil in der Rechtssache C-311/18 (Schrems II), Rn. 137, wo der Gerichtshof folglich anerkannt hat, dass die SVK „wirksame Mechanismen [enthalten], die in der Praxis gewährleisten können, dass das vom Unionsrecht verlangte Schutzniveau eingehalten wird und dass auf solche Klauseln gestützte Übermittlungen personenbezogener Daten ausgesetzt oder verboten werden, wenn gegen diese Klauseln verstoßen wird oder ihre Einhaltung unmöglich ist"; vgl. ferner Rn. 148.

[91] C-311/18 (Schrems II), Rn. 125.

[92] EuGH, Urteil in der Rechtssache C-311/18 (Schrems II), Rn. 132.

Vertragliche Verpflichtung zur Verwendung spezifischer technischer Maßnahmen

103. Je nach den jeweiligen Umständen der Übermittlungen (einschließlich der praktischen Anwendung der Rechtsvorschriften des Drittlands) kann es sein, dass im Vertrag vorgesehen sein muss, dass die Übermittlungen nur stattfinden können, wenn bestimmte technische Maßnahmen implementiert worden sind (vgl. dazu die obigen Erläuterungen zu technischen Maßnahmen).

104. Wirksamkeitsvoraussetzungen:

- Diese Klausel könnte in den Fällen effektiv sein, in denen der Datenexporteur erkannt hat, dass technische Maßnahmen erforderlich sind. Sie müsste dann rechtsverbindlich vereinbart werden, damit sichergestellt ist, dass sich der Datenimporteur erforderlichenfalls dazu verpflichtet hat, die notwendigen technischen Maßnahmen zu ergreifen.

Transparenzanforderungen:

105. Der Datenexporteur könnte dem Vertrag Anhänge mit vom Datenimporteur vor Vertragsabschluss nach besten Kräften beigebrachten Informationen über den behördlichen (auch nachrichtendienstlichen) Datenzugriff im Bestimmungsland hinzufügen, vorausgesetzt die Rechtsvorschriften stehen mit den „Wesentlichen europäischen Garantien“ des EDSA in Einklang. Dies könnte dem Datenexporteur helfen, seine Beurteilung des Schutzniveaus im Drittland zu dokumentieren, wozu er verpflichtet ist. Es könnte auch unterstreichen, dass der Datenimporteur verpflichtet ist, den Datenexporteur bei seiner Beurteilung zu unterstützen und seiner Verantwortung nachzukommen, indem er ihm objektive, zuverlässige, relevante, überprüfbare und öffentlich verfügbare oder anderweitig zugängliche Informationen zur Verfügung stellt.

106. Der Datenimporteur könnte z. B. verpflichtet werden:

(1) die einschlägigen Gesetze und Verordnungen des Bestimmungslands aufzuführen, denen der Datenimporteur oder seine (Unter-)Auftragsverarbeiter sowie die übermittelten Daten unterliegen und die den Behörden den Zugriff auf die übermittelten personenbezogenen Daten insbesondere zu nachrichtendienstlichen, Strafverfolgungs-, Verwaltungs- und Aufsichtszwecken gestatten würden;

(2) falls es keine Rechtsvorschriften gibt, die den behördlichen Datenzugriff regeln, Informationen und Statistiken zu liefern, die auf der Erfahrung des Datenimporteurs oder auf Berichten aus verschiedenen Quellen (z. B. Partner, allgemein zugängliche Quellen, Gerichtsentscheidungen und aufsichtsbehördliche Entscheidungen im betreffenden Land) über den behördlichen Zugriff auf personenbezogene Daten der Art beruhen, um die es bei der betreffenden Datenübermittlung geht (d. h. in dem spezifischen regulatorischen Bereich; für Unternehmen von der Art des Datenimporteurs, usw.);

(3) anzugeben, welche Maßnahmen (ggf.) ergriffen werden, um den Zugriff auf die übermittelten Daten zu verhindern;

(4) hinreichend detaillierte Angaben über alle behördlichen Ersuchen um Zugriff auf personenbezogene Daten zu machen, die der Datenimporteur in einem bestimmten Zeitraum

erhalten hat[93], insbesondere in den oben unter (1) genannten Bereichen; mit Angaben zu den ihm zugegangenen Ersuchen, den angeforderten Daten, der ersuchenden Behörde und der Rechtsgrundlage für die Offenlegung sowie dazu, in welchem Umfang der Datenimporteur dem Ersuchen nachgekommen ist;[94]

(5) anzugeben, ob und inwieweit es dem Datenimporteur rechtlich untersagt ist, die oben unter (1) bis (5) aufgeführten Angaben zu machen.

107. Diese Informationen könnten mit einem klar gegliederten Fragebogen erfasst werden, der vom Datenimporteur auszufüllen und zu unterzeichnen wäre, wobei der Datenimporteur darüber hinaus vertraglich zu verpflichten wäre, Veränderungen bezüglich dieser Angaben binnen einer bestimmten Frist mitzuteilen, so wie es z. B. in Due-Diligence-Verfahren üblich ist.

108. Wirksamkeitsvoraussetzungen:

- Der Datenimporteur muss dem Datenexporteur diese Informationen, um deren Beschaffung er sich nach besten Kräften bemühen muss, nach seinem besten Wissen mitteilen können.
- Diese dem Datenimporteur auferlegte Verpflichtung soll sicherstellen, dass sich der Datenexporteur der mit der Übermittlung der Daten in ein Drittland verbundenen Risiken bewusst wird und bewusst bleibt. Sie versetzt den Datenexporteur in die Lage, vom Vertragsabschluss abzusehen oder, falls sich die Informationen nach Vertragsabschluss ändern, seine Verpflichtung zur Aussetzung der Übermittlung und/oder zum Rücktritt vom Vertrag zu erfüllen, falls die Rechtslage im Drittland, die im verwendeten Übermittlungsinstrument in Artikel 46 DSGVO enthaltenen Garantien oder jegliche zusätzlichen Garantien, die vereinbart worden sein mögen, nicht mehr ein dem Schutzniveau im EWR der Sache nach gleichwertiges Schutzniveau sicherzustellen vermögen. Diese Verpflichtung kann jedoch weder eine Offenlegung personenbezogener Daten durch den Datenimporteur rechtfertigen, noch Grund zu der Erwartung geben, dass es keine weiteren Offenlegungsersuchen mehr geben wird.

***

109. Der Datenexporteur könnte auch Klauseln hinzufügen, in denen der Datenimporteur bestätigt, (1) dass er nicht absichtlich Hintertüren (back doors) oder Ähnliches programmiert hat, was dazu genutzt werden könnte, auf das System und/oder die personenbezogenen Daten zuzugreifen; (2) dass er nicht absichtlich seine Geschäftsprozesse so eingerichtet oder geändert hat, dass der Zugriff auf personenbezogene Daten oder Systeme möglich ist; und (3) dass der Datenimporteur aufgrund nationalen Rechts bzw. der Regierungspolitik weder verpflichtet ist, Hintertüren (back doors) zu schaffen oder aufrechtzuerhalten, noch verpflichtet ist, personenbezogene Daten oder Systeme zugänglich zu machen oder den Verschlüsselungsschlüssels besitzen oder herausgeben zu müssen.*[95]*

---

[93] Die Länge des Zeitraums sollte von den Gefahren für die Rechte und Freiheiten der betroffenen Personen, deren Daten übermittelt werden, abhängen – z. B. das letzte Jahr vor dem Abschluss des Datenexportvertrags mit dem Datenexporteur.

[94] Die Erfüllung dieser Pflicht allein bietet noch keinen angemessenen Schutz. Jede tatsächlich erfolgte unangemessene Offenlegung bedeutet jedoch, dass zusätzliche Maßnahmen notwendig sind.

[95] Diese Klausel ist wichtig, um ein angemessenes Schutzniveau für die übermittelten personenbezogenen Daten zu garantieren, und sollte deshalb in der Regel erforderlich sein.

110. Wirksamkeitsvoraussetzungen:

- Wenn Datenimporteure aufgrund der Rechtsvorschriften oder der Regierungspolitik daran gehindert sind, diese Informationen mitzuteilen, könnte diese Klausel unwirksam sein. Der Datenimporteur wird dann den Vertrag nicht abschließen können oder er wird dem Datenexporteur mitteilen müssen, dass er nicht weiter in der Lage ist, seine vertraglichen Verpflichtungen zu erfüllen.
- Der Vertrag muss für den Fall, dass der Datenimporteur nicht angibt, dass es Hintertüren (back doors) oder ähnliche Programmteile oder manipulierte Geschäftsprozesse oder Verpflichtungen zu deren Implementierung gibt, oder dass er den Datenexporteur nicht umgehend verständigt, sobald ihm bekannt wird, dass solche vorhanden sind, Vertragsstrafen und/oder für den Datenexporteur die Möglichkeit vorsehen, den Vertrag kurzfristig zu kündigen.
- In Fällen, in denen der Datenimporteur personenbezogene Daten offengelegt hat, die unter Verstoß gegen die Verpflichtungen im Rahmen des gewählten Übermittlungsinstruments übermittelt wurden, kann der Vertrag auch eine Entschädigung des Datenimporteurs an eine betroffene Person für erlittenen materiellen und immateriellen Schaden umfassen.

***

111. Der Datenexporteur könnte seine Befugnis, die Datenverarbeitungseinrichtungen des Datenimporteurs vor Ort und/oder aus der Ferne Prüfungen[96] oder Inspektionen zu unterziehen, verstärken, um zu überprüfen, ob Daten Behörden gegenüber offengelegt wurden und, falls ja, zu welchen Bedingungen (der Zugang darf nicht über das hinausgehen, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt); dabei kommen z. B. kurze Ankündigungsfristen und Mechanismen in Betracht, die ein schnelles Handeln der Prüfgremien gewährleisten und die Entscheidungskompetenz des Datenimporteurs bei der Auswahl der Prüfgremien stärken.

112. Wirksamkeitsvoraussetzungen:

- Volle Wirksamkeit setzt voraus, dass der Prüfungsumfang die rechtlichen und technischen Aspekte aller von den Auftragsverarbeitern und Unterauftragsverarbeitern des Datenimporteurs durchgeführten Verarbeitungen der in das Drittland übermittelten personenbezogenen Daten umfasst.
- Zugriffsprotokolle und andere ähnliche Pfade sollten manipulationssicher sein (z. B. sollten sie unter Verwendung modernster Verschlüsselungstechniken wie Hashing unverändlich gemacht und auch dem Datenexporteur in regelmäßigen Abständen systematisch übermittelt werden), damit die Prüfer Nachweise für eine Offenlegung finden können. Zugriffsprotokolle und ähnliche Prüfpfade sollten zwischen Zugriffen im Rahmen des gewöhnlichen Geschäftsbetriebs und Zugriffen, die auf Anordnung der Datenoffenlegung oder entsprechende Ersuchen hin erfolgen, unterscheiden.

[96] Vgl. z. B. Klausel 5 Buchstabe f der SVK zwischen Verantwortlichen und Auftragsverarbeitern (Beschluss der Kommission 2010/87/EU). Die Prüfungen könnten auch in Verhaltensregeln oder durch Zertifizierung vorgesehen werden.

***

113. Auch wenn die erste Beurteilung von Recht und Praxis im Drittland des Datenimporteurs ergibt, dass dieses für die vom Datenexporteur übermittelten Daten ein Schutzniveau bietet, dass dem in der EU der Sache nach gleichwertig ist, könnte der Datenexporteur dennoch dem Datenimporteur weitere Verpflichtungen auferlegen, etwa, dass dieser den Datenexporteur umgehend benachrichtigen muss, wenn er seine vertraglichen Verpflichtungen – und damit das erforderliche „der Sache nach gleichwertige Schutzniveau" – nicht mehr einhalten kann.[97]

114. Grund dafür, dass Verpflichtungen nicht mehr eingehalten werden können, können Änderungen der Rechtsvorschriften oder Praxis im Drittland sein.[98] Die Klauseln könnten spezifische und strikt einzuhaltende Fristen und Verfahren für die umgehende Aussetzung der Datenübermittlung und/oder den Rücktritt vom Vertrag sowie für die Rückgabe oder Löschung der empfangenen Daten durch den Datenimporteur vorsehen. Wenn der Datenexporteur den Überblick über die ergangenen Offenlegungsersuchen, deren Gegenstand und die Effektivität der dagegen getroffenen Maßnahmen behält, dürfte er genügend Informationen haben, um seine Pflicht zur Aussetzung oder Einstellung der Übermittlung und/oder zum Rücktritt vom Vertrag erfüllen zu können.

115. Wirksamkeitsvoraussetzungen:

- Die Benachrichtigung muss erfolgten, bevor der Zugriff auf die Daten gewährt wird. Andernfalls könnten die Rechte der natürlichen Person zu dem Zeitpunkt, zu dem der Datenexporteur die Benachrichtigung erhält, bereits verletzt worden sein (wenn nämlich das Ersuchen auf Rechtsvorschriften des Drittlands beruht, die Eingriffe gestatten, die über die nach Unionsrecht zulässigen Eingriffe hinausgehen). Die Benachrichtigung könnte aber immer noch dazu dienen, künftige Verletzungen zu verhindern und dem Datenexporteur die Einhaltung seiner Pflicht zur Aussetzung der Übermittlung der personenbezogenen Daten in das Drittland und/oder zum Rücktritt vom Vertrag zu ermöglichen.
- Der Datenimporteur muss alle rechtlichen und politischen Entwicklungen überwachen, die dazu führen könnten, dass er seine Verpflichtungen nicht mehr erfüllen kann; und er muss den Datenexporteur unverzüglich über alle derartigen Änderungen und Entwicklungen unterrichten (falls möglich noch vor deren Inkrafttreten), damit der Datenexporteur die Möglichkeit hat, die Daten vom Datenimporteur zurückzuerlangen.
- Die Klauseln sollten für den Fall, dass eine bestimmte, zwischen Datenexporteur und Datenimporteur vereinbarte Schwelle[99] erreicht wird, ein schnelles Verfahren vorsehen, durch das der Datenexporteur dem Datenimporteur gestattet, die Daten umgehend zu sichern oder an den Datenexporteur zurückzugeben oder, falls dies nicht möglich ist, die Daten zu

---

[97] Klausel 5 Buchstaben a und d Ziffer i des SVK-Beschlusses 2010/87/EU.

[98] Vgl. C-311/18 (Schrems II), Rn. 139, wo es heißt: „Im Übrigen ist der Empfänger der Übermittlung personenbezogener Daten zwar nach Klausel 5 Buchst. d Ziff. i berechtigt, den in der Union ansässigen Verantwortlichen nicht über rechtlich bindende Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten zu informieren, falls ihm diese Information rechtlich untersagt ist, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen. Allerdings ist er auch in diesem Fall gemäß Klausel 5 Buchst. a verpflichtet, den Verantwortlichen davon in Kenntnis zu setzen, dass er die Standarddatenschutzklauseln nicht einhalten kann."

[99] Dieser Schwellenwert sollte sicherstellen, dass betroffenen Personen weiterhin ein Schutzniveau gewährt wird, das dem im EWR garantierten Schutzniveau gleichwertig ist.

löschen oder sicher zu verschlüsseln, ohne notwendigerweise Weisungen des Datenexporteurs abwarten zu müssen. Der Datenimporteur sollte dieses Verfahren gleich zu Beginn der Datenübermittlung implementieren und es regelmäßig testen, um sicherzustellen, dass es kurzfristig angewendet werden kann.

- In weiteren Klauseln könnte dem Datenexporteur die Befugnis eingeräumt werden, die Einhaltung dieser Verpflichtungen durch den Datenimporteur durch Prüfungen, Inspektionen und andere Überprüfungsmaßnahmen zu überwachen und mit dem Datenimporteur drohenden Vertragsstrafen durchzusetzen bzw. die Übermittlung auszusetzen und/oder fristlos vom Vertrag zurückzutreten.

***

116. Soweit dies nach dem nationalen Recht des Drittlands gestattet ist, könnte der Vertrag die Transparenzpflichten des Datenimporteurs verstärken, indem diesem auferlegt wird, regelmäßig (z. B. mindestens alle 24 Stunden) „Warrant Canary"-Erklärungen abzugeben. Diese Erklärungen sind kryptografisch signierte Mitteilungen, mit denen der Datenexporteur informiert wird, dass dem Datenimporteur bis zu einem bestimmten Zeitpunkt (Datum und Uhrzeit) kein Ersuchen um Offenlegung personenbezogener Daten o. Ä. zugegangen ist. Wenn eine solche Erklärung dann ausbleibt, ist das für den Datenexporteur ein Hinweis darauf, dass dem Datenimporteur ein solches Ersuchen zugegangen sein könnte.

117. Wirksamkeitsvoraussetzungen:

- Nach den Vorschriften im Drittland muss es dem Datenimporteur gestattet sein, dem Datenexporteur eine solche Benachrichtigung in passiver Form zukommen zu lassen.
- Der Datenexporteur muss den Eingang der „Warrant-Canary"-Erklärungen automatisch überwachen.
- Der Datenimporteur muss sicherstellen, dass sein privater Schlüssel zum Signieren der „Warrant-Canary"-Erklärung sicher ist und dass er nicht nach den Vorschriften im Drittland gezwungen werden kann, falsche „Warrant-Canary"-Erklärungen abzugeben. Es könnte deshalb nützlich sein, wenn mehrere Signaturen verschiedener Personen erforderlich wären und/oder wenn die „Warrant-Canary"-Erklärung von einer Person außerhalb des gerichtlichen Zuständigkeitsbereichs des Drittlands abgegeben würde.

Verpflichtungen zum Ergreifen bestimmter Maßnahmen

118. Der Datenimporteur könnte sich verpflichten, die Rechtmäßigkeit jeglicher Anordnungen der Datenoffenlegung nach dem Recht des Bestimmungslands zu prüfen, insbesondere im Hinblick darauf, ob die Behörde befugt ist, um Offenlegung zu ersuchen, sowie gegen die Anordnung vorzugehen, falls er zu dem Schluss gelangt, dass es nach dem Recht des Bestimmungslands guten Grund dafür gibt, sich zur Wehr zu setzen. Wenn der Datenimporteur gegen eine Anordnung vorgeht, sollte er einstweiligen Rechtsschutz beantragen, damit die Anordnung erst vollzogen werden kann, wenn das Gericht abschließend über die Sache entschieden hat. Der Datenimporteur könnte sich verpflichten, die personenbezogenen Daten nicht offenzulegen, solange er nicht nach den einschlägigen Verfahrensregeln dazu verpflichtet ist. Außerdem könnte sich der Datenimporteur für den Fall, dass er einer Anordnung Folge leisten muss, verpflichten,

nur die Mindestmenge an Informationen mitzuteilen, die – bei angemessener Auslegung der Anordnung – genügt.

119. Wirksamkeitsvoraussetzungen:

- Die Rechtsordnung des Drittlands muss wirksamen Rechtsschutz bieten, der ein Vorgehen gegen Anordnungen der Datenoffenlegung ermöglicht.
- Der zusätzliche Schutz, den diese Klausel bietet, wird sich stets in Grenzen halten, da eine Anordnung der Datenoffenlegung nach der Rechtsordnung des Drittlands durchaus rechtmäßig sein könnte; es kann aber sein, dass die betreffende Rechtsordnung den unionsrechtlichen Standards nicht genügt. Diese vertragliche Maßnahme kann deshalb allenfalls andere zusätzliche Maßnahmen ergänzen.
- Die gegen Anordnungen gegebenen Rechtsbehelfe müssen nach dem Recht des Drittlands aufschiebende Wirkung (Suspensiveffekt) haben. Andernfalls wäre es den Behörden immer noch möglich, auf die Daten natürlicher Personen zuzugreifen, und alle späteren Rechtsbehelfe der betroffenen Personen hätten nur begrenzte Wirkung, da diese nur Schadensersatz für die negativen Folgen der Datenoffenlegung fordern könnten.
- Der Datenimporteur muss die Maßnahmen, die er nach besten Kräften zur Erfüllung dieser Verpflichtung ergriffen hat, dokumentieren und dem Datenexporteur nachweisen können.

***

120. In der vorstehend beschriebenen Situation könnte sich der Datenimporteur dazu verpflichten, der Behörde, die das Ersuchen stellt, mitzuteilen, dass dieses nicht mit den im Übermittlungsinstrument in Artikel 46 DSGVO[100] enthaltenen Garantien vereinbar ist, so dass sich für den Datenimporteur eine Pflichtenkollision ergibt. Der Datenimporteur müsste dann, soweit dies nach der Rechtsordnung im Drittland möglich ist, gleichzeitig und baldmöglichst den Datenexporteur und/oder die zuständige Aufsichtsbehörde im EWR benachrichtigen.

121. Wirksamkeitsvoraussetzungen:

- Eine solche Unterrichtung über den unionsrechtlich gewährten Schutz und die Pflichtenkollision sollte nach der Rechtsordnung des Drittlands rechtliche Wirkung haben, z. B. indem sie zur Überprüfung der Zugriffsanordnung oder des Zugriffsersuchens durch ein Gericht oder eine Behörde führt, eine gerichtliche Anordnung erforderlich macht und/oder die einstweilige Aussetzung der Anordnung bewirkt, damit die Daten zusätzlichen Schutz genießen.
- Die Rechtsordnung des Landes darf den Datenimporteur nicht daran hindern, den Datenexporteur oder zumindest die zuständige Aufsichtsbehörde im EWR über die Zugriffsanordnung oder das Ersuchen zu unterrichten.

---

[100] So ist z. B. in den SVK vorgesehen, dass die Datenverarbeitung (einschließlich der Datenübermittlung) gemäß dem „*anwendbare[n] Datenschutzrecht*“ durchgeführt wurde und auch weiterhin so durchgeführt wird. Das anwendbare Datenschutzrecht ist definiert als „*die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre im Hinblick auf die Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, für den für die Verarbeitung Verantwortlichen gelten*“. Der EuGH hat bestätigt, dass die Bestimmungen der DSGVO – im Licht der EU-Grundrechtecharta betrachtet – zu diesen Vorschriften gehören, vgl. EuGH C-311/18 (Schrems II), Rn. 138.

- Der Datenimporteur muss die Maßnahmen, die er nach besten Kräften zur Erfüllung dieser Verpflichtung ergriffen hat, dokumentieren und dem Datenexporteur nachweisen können.

Befugnis der betroffenen Personen zur Ausübung ihrer Rechte

122. Der Vertrag könnte vorsehen, dass der Zugriff auf personenbezogene Daten, die im gewöhnlichen Geschäftsgang (einschließlich in Support-Fällen) unverschlüsselt übermittelt werden, nur mit ausdrücklicher oder impliziter Zustimmung des Datenexporteurs und/oder der betroffenen Person zu einem bestimmten Datenzugriff gestattet ist.

123. Wirksamkeitsvoraussetzungen:

- Diese Klausel könnte in Situationen greifen, in denen Datenimporteure von Behörden zur freiwilligen Zusammenarbeit aufgefordert werden – wenn es sich also nicht um einen behördlichen Zugriff handelt, der ohne Wissen des Datenimporteurs oder gegen dessen Willen erfolgt.
- Zuweilen mag es der betroffenen Person nicht möglich sein, sich gegen den Zugriff zur Wehr zu setzen oder eine Zustimmung zu erteilen, die allen unionsrechtlichen Anforderungen genügt (also eine freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung darstellt) (etwa im Fall von Arbeitnehmern).[101]
- Nationale Rechtsvorschriften oder Grundsätze, die dem Datenimporteur die Offenlegung der Zugriffsanordnung untersagen, können dazu führen, dass diese Klausel wirkungslos ist, wenn sie nicht um technische Methoden ergänzt wird, die zur Datenentschlüsselung der Mitwirkung des Datenexporteurs oder der betroffenen Person bedürfen. Solche technischen Maßnahmen zur Zugriffsbeschränkung können insbesondere dann in Betracht kommen, wenn der Zugriff nur für konkrete Support- oder Serviceleistungen gewährt wird, die Daten selbst aber im EWR gespeichert sind.

***

124. Der Vertrag könnte den Datenimporteur und/oder Datenexporteur verpflichten, die betroffene Person unverzüglich über im Drittland ergangene behördliche Ersuchen oder Anordnungen oder aber darüber, dass der Datenimporteur seine vertraglichen Verpflichtungen nicht einhalten kann, zu unterrichten, damit die betroffene Person Informationen einholen und einen wirksamen Rechtsbehelf einlegen kann (indem sie z. B. bei der zuständigen Aufsichtsbehörde Beschwerde einlegt oder beim zuständigen Gericht Klage erhebt und ihr Rechtsschutzinteresse bei den Gerichten im Drittland geltend macht), einschließlich einer Entschädigung durch den Datenimporteur für jeden materiellen und immateriellen Schaden, der ihr durch die Offenlegung ihrer personenbezogenen Daten, die im Rahmen des gewählten Übermittlungsinstruments unter Verstoß gegen die darin enthaltenen Verpflichtungen übermittelt wurden, entstanden ist.

125. Wirksamkeitsvoraussetzungen:

- Die Benachrichtigung könnte die betroffene Person warnen, dass ihre Daten im Drittland möglicherweise behördlichen Zugriffen ausgesetzt sind. Die betroffene Person könnte

[101] Artikel 4 Absatz 11 DSGVO.

zusätzliche Informationen beim Datenexporteur anfordern und bei ihrer zuständigen Aufsichtsbehörde Beschwerde einlegen. Diese Klausel könnte auch einigen der Schwierigkeiten entgegenwirken und sie ausgleichen, die eine natürliche Person vor den Gerichten im Drittland beim Nachweis ihres Rechtsschutzinteresses (Klagebefugnis) bezüglich des behördlichen Zugriffs auf ihre Daten haben kann.

- Es kann sein, dass es nationale Rechtsvorschriften und Grundsätze gibt, die der Unterrichtung der betroffenen Person entgegenstehen. Datenexporteur und Datenimporteur könnten sich dennoch verpflichten, die betroffene Person zu unterrichten, sobald die Beschränkungen zur Datenoffenlegung aufgehoben sind, sowie sich nach besten Kräften zu bemühen, einen Verzicht auf das Offenlegungsverbot zu erwirken. Zumindest sollte der Datenexporteur oder die zuständige Aufsichtsbehörde die betroffene Person darüber unterrichten können, dass die Übermittlung ihrer personenbezogenen Daten ausgesetzt oder beendet wurde, weil der Datenimporteur seine vertraglichen Verpflichtungen wegen eines Zugriffsersuchens nicht mehr einhalten konnte.

***

126. Der Vertrag könnte den Datenexporteur und Datenimporteur verpflichten, der betroffenen Person zu helfen, ihre Rechte im Drittland auszuüben, etwa durch individuell vereinbarte Rechtsschutzmechanismen und Rechtsberatung.

127. Wirksamkeitsvoraussetzungen:

- Einige nationale Vorschriften erlauben es dem Datenimporteur möglicherweise nicht, betroffenen Personen diese Art der Unterstützung direkt zu gewähren, obwohl sie es dem Datenimporteur gestatten, diese Unterstützung für die betroffenen Personen zu beschaffen.
- Es kann sein, dass es nationale Rechtsvorschriften und Grundsätze gibt, die die Wirksamkeit der individuell vereinbarten Rechtsschutzmechanismen untergraben.
- Rechtsberatung für die betroffene Person könnte nützlich sein, insbesondere wenn man bedenkt, wie kompliziert und kostspielig es für die betroffene Person sein kann, die Rechtsordnung des Drittlands zu verstehen und im Ausland den Rechtsweg zu beschreiten, möglicherweise auch noch in einer fremden Sprache. Der zusätzliche Schutz, den diese Klausel bietet, wird sich jedoch immer in Grenzen halten, da es mit Hilfe und Rechtsberatung für betroffene Personen allein nicht getan ist, wenn die Rechtsordnung des Drittlands kein Schutzniveau bietet, das dem im EWR gewährleisteten Schutzniveau der Sache nach gleichwertig ist. Diese vertragliche Maßnahme kann deshalb allenfalls andere zusätzliche Maßnahmen ergänzen.
- Diese zusätzliche Maßnahme wäre nur effektiv, wenn das Recht des Drittlands Rechtsschutz vor seinen nationalen Gerichten vorsähe oder wenn es einen individuell vereinbarten Rechtsschutzmechanismus, einschließlich gegen Überwachungsmaßnahmen, gäbe.

2.3 Organisatorische Maßnahmen

128. Bei den zusätzlichen organisatorischen Maßnahmen kann es sich um interne Strategien, Organisationsmethoden und Standards handeln, die die Verantwortlichen und Auftragsverarbeiter bei sich selbst anwenden und den Datenimporteuren in Drittländern auferlegen könnten. Diese können zu einem im gesamten Verarbeitungszyklus einheitlichen Schutz personenbezogener Daten beitragen. Organisatorische Maßnahmen können auch dazu beitragen, dass sich die Datenexporteure der Risiken bezüglich des Datenzugriffs in Drittländern und entsprechender Zugriffsversuche besser bewusst sind und besser darauf reagieren können. Nur weil man eine oder mehrere dieser Maßnahmen ausgewählt und angewendet hat, bedeutet das noch nicht unbedingt, dass systematisch sichergestellt ist, dass die vorgesehene Übermittlung den unionsrechtlichen Anforderungen (Gewährleistung eines der Sache nach gleichwertigen Schutzniveaus) genügt. Je nach den besonderen Umständen der Übermittlung und der durchgeführten Beurteilung der Rechtslage im Drittland sind organisatorische Maßnahmen zur Ergänzung der vertraglichen und/oder technischen Maßnahmen erforderlich, um sicherzustellen, dass der Schutz der personenbezogenen Daten dem im EWR gewährleisteten Schutzniveau der Sache nach gleichwertig ist.

129. Welche Maßnahmen die geeignetsten sind, ist jeweils im Einzelfall zu beurteilen, wobei zu beachten ist, dass die Verantwortlichen und Auftragsverarbeiter dem Grundsatz der Rechenschaftspflicht genügen müssen. Nachstehend hat der EDSA einige Beispiele für organisatorische Maßnahmen aufgeführt, die Datenexporteure ergreifen können; dies ist jedoch keine erschöpfende Liste und auch andere Maßnahmen können durchaus geeignet sein.

Interne Grundsätze für den Regelungsrahmen für Übermittlungen (insbesondere innerhalb von Unternehmensgruppen)

130. Aufstellung angemessener interner Grundsätze mit klarer Zuweisung der Verantwortlichkeiten für Datenübermittlungen, Berichtswege und Standardarbeitsanweisungen für den Fall formeller oder informeller behördlicher Ersuchen um Datenzugriff. Insbesondere wenn es sich um Übermittlungen innerhalb von Unternehmensgruppen handelt, können diese Grundsätze unter anderem vorsehen, dass ein eigenes Team aus Experten für IT, Datenschutz und Datenschutzrecht benannt wird, das für Ersuchen zuständig ist, die sich auf aus dem EWR übermittelte personenbezogene Daten beziehen. Ferner könnten sie sich befassen mit der Benachrichtigung der Rechtsabteilung und der Unternehmensleitung sowie des Datenexporteurs über Ersuchen, mit dem Vorgehen gegen unverhältnismäßige oder rechtswidrige Ersuchen sowie der transparenten Unterrichtung betroffener Personen.

131. Für die Mitarbeiter, die behördliche Ersuchen um Zugriff auf personenbezogene Daten bearbeiten, sind spezifische Schulungsprogramme auszuarbeiten, die regelmäßig zu aktualisieren sind, um neuen Entwicklungen in der Gesetzgebung und Rechtsprechung im Drittland wie auch im EWR Rechnung zu tragen. Die Schulungsprogramme sollten die unionsrechtlichen Anforderungen an den behördlichen Zugriff auf personenbezogene Daten umfassen, insbesondere die Anforderungen, die sich aus Artikel 52 Absatz 1 der Charta der Grundrechte ergeben. Das Personal ist für die Problematik zu sensibilisieren, insbesondere anhand praktischer Beispiele für behördliche Ersuchen um Datenzugriff und die Anwendung des sich aus Artikel 52 Absatz 1 der Charta der Grundrechte ergebenden Standards auf die Beispielsfälle. Derartige Schulungen könnten auch die besondere Situation des Datenimporteurs berücksichtigen, z. B. die

Rechtsvorschriften und Verordnungen im Drittland, denen der Datenimporteur unterliegt; die Schulungen sollten, wenn möglich, in Zusammenarbeit mit dem Datenexporteur ausgearbeitet werden.

132. Wirksamkeitsvoraussetzungen:

- Diese Grundsätze können nur für die Fälle vorgesehen werden, in denen das Ersuchen der Behörden im Drittland mit dem Unionsrecht vereinbar ist.[102] Ist das Ersuchen nicht damit vereinbar, würden diese Grundsätze nicht genügen, ein gleichwertiges Schutzniveau für die personenbezogenen Daten zu gewährleisten; die Übermittlungen wären dann, wie oben erläutert, einzustellen oder es müssten geeignete zusätzliche Maßnahmen ergriffen werden, um den Zugriff zu verhindern.

Maßnahmen in Bezug auf Transparenz und Rechenschaftspflicht

133. Dokumentierung und Aufzeichnung der von Behörden gestellten Zugriffsersuchen und deren Beantwortung, einschließlich der rechtlichen Begründung und Angaben zu den beteiligten Stellen (z. B. ob Benachrichtigung des Datenexporteurs erfolgt ist, dessen Erwiderung, die von dem für derartige Ersuchen zuständigen Team vorgenommene Beurteilung usw.). Diese Aufzeichnungen sind dem Datenexporteur zur Verfügung zu stellen, der sie wiederum auf Verlangen den betroffenen Personen zur Verfügung stellt.

134. Wirksamkeitsvoraussetzungen:

- Es kann sein, dass es wegen der nationalen Rechtsvorschriften im Drittland nicht möglich ist, Ersuchen oder wesentliche Informationen darüber offenzulegen; in einem solche Fall wäre diese Verfahrensweise wirkungslos. Der Datenimporteur sollte dem Datenexporteur ggf. mitteilen, dass er die Dokumente und Aufzeichnungen nicht liefern kann, so dass der Datenexporteur die Möglichkeit hat, die Übermittlungen auszusetzen, falls dieses Unvermögen des Datenimporteurs das Schutzniveau beeinträchtigt.

***

135. Regelmäßige Veröffentlichung von Transparenzberichten oder Zusammenfassungen bezüglich der von staatlichen Stellen gestellten Ersuchen um Datenzugriff und deren Beantwortung, soweit die Veröffentlichung nach dem im Land geltenden Recht gestattet ist.

136. Wirksamkeitsvoraussetzungen:

- Die mitgeteilten Informationen sollten so relevant, klar und detailliert wie möglich sein. Es kann sein, dass die nationalen Rechtsvorschriften des Drittlands der Offenlegung detaillierter Informationen entgegenstehen. Gegebenenfalls sollte der Datenimporteur sich nach besten Kräften bemühen, statistische Angaben oder aggregierte Informationen vergleichbarer Art zu liefern.

[102] Vgl. Rechtssachen C-362/14 (Schrems I), Rn. 94; C-311/18 (Schrems II), Rn. 168, 174, 175 und 176.

Organisationsmethoden und Maßnahmen zur Datenminimierung

137. Bereits nach dem Grundsatz der Rechenschaftspflicht bestehende organisatorische Anforderungen, etwa strikter und granularer Datenzugriff sowie Geheimhaltungsgrundsätze und bewährte Verfahren, die auf einem strikt einzuhaltenden „Need-to-know"-Grundsatz beruhen, mit Überwachung durch regelmäßige Überprüfungen und Durchsetzung durch Disziplinarmaßnahmen – all diese Maßnahmen können auch im Zusammenhang mit Datenübermittlungen nützlich sein. Diesbezüglich ist auch die Datenminimierung in Betracht zu ziehen, um möglichst wenig personenbezogene Daten der Gefahr unbefugter Zugriffe auszusetzen. In einigen Fällen ist die Übermittlung bestimmter Daten u. U. nicht unbedingt erforderlich (z. B. im Falle des Fernzugriffs auf EWR-Daten, etwa in Support-Fällen, wenn anstatt des vollen Zugriffs nur eingeschränkter Zugriff gewährt wird oder wenn eine Dienstleistung lediglich die Übermittlung eines Teils der Daten, nicht der gesamten Datenbank, erfordert).

138. Wirksamkeitsvoraussetzungen:

- Es sollten regelmäßige Überprüfungen und strenge Disziplinarmaßnahmen vorgesehen sein, um die Einhaltung der Maßnahmen zur Datenminimierung auch im Zusammenhang mit Datenübermittlungen zu überwachen und durchzusetzen.
- Der Datenexporteur sollte die in seinem Besitz befindlichen personenbezogenen Daten vor der Übermittlung daraufhin untersuchen, welche Datenbestände für die Zwecke der Übermittlung nicht erforderlich sind und deshalb nicht an den Datenimporteur weitergegeben werden.
- Die Maßnahmen zur Datenminimierung sollten mit technischen Maßnahmen verbunden werden, um sicherzustellen, dass die Daten keinem unbefugten Zugriff unterliegen. So kann z. B. durch „Secure Multiparty Computation"-Mechanismen und die Verteilung verschlüsselter Datenmengen auf verschiedene vertrauenswürdige Stellen schon durch die Technikgestaltung verhindert werden, dass ein Zugriff von nur einer Seite zur Offenlegung identifizierbarer Daten führen würde.

***

139. Entwicklung bewährter Verfahren für die angemessene und rechtzeitige Einbeziehung sowohl (ggf.) des Datenschutzbeauftragten, dem Zugang zu den Informationen zu gewähren ist, als auch der Rechtsabteilung und Innenrevision in allen Angelegenheiten, die internationale Übermittlungen personenbezogener Daten betreffen.

140. Wirksamkeitsvoraussetzungen:

- Der Datenschutzbeauftragte (falls vorhanden) sowie die Rechtsabteilung und die Innenrevision, denen alle für die Übermittlung relevanten Informationen mitzuteilen sind, sind zur Notwendigkeit der Übermittlung und etwaiger zusätzlicher Garantien zu konsultieren.
- Zu den relevanten Informationen zählen z. B. die Beurteilung der Notwendigkeit der Übermittlung der spezifischen personenbezogenen Daten, ein Überblick über die einschlägigen Gesetze im Drittland sowie die Garantien, zu deren Implementierung sich der Datenimporteur verpflichtet hat.

Annahme von Normen und bewährten Verfahren

141. Aufstellung strikter Grundsätze in Bezug auf Datensicherheit und Datenschutz, auf Grundlage unionsrechtlicher Zertifizierung oder Verhaltensregeln oder internationaler Normen (z. B. ISO-Normen) und bewährter Verfahren (z. B. ENISA), unter gebotener Beachtung des Stands der Technik, abgestimmt auf das Risiko der verarbeiteten Datenkategorien.

Sonstiges

142. Annahme und regelmäßige Überprüfung interner Grundsätze zur Beurteilung der Eignung der implementierten ergänzenden Maßnahmen sowie erforderlichenfalls Identifizierung und Implementierung zusätzlicher oder alternativer Lösungen, um sicherzustellen, dass für die übermittelten personenbezogenen Daten ein dem im EWR gewährten Schutzniveau der Sache nach vergleichbares Schutzniveau eingehalten wird.

***

143. Verpflichtungen des Datenimporteurs, von jeder Weiterübermittlung der personenbezogenen Daten, sei es innerhalb desselben Landes oder in andere Drittländer, abzusehen oder laufende Übermittlungen auszusetzen, wenn im Drittland kein dem im EWR gewährten Schutzniveau der Sache nach gleichwertiges Schutzniveau eingehalten werden kann.[103]

[103] C-311/18 (Schrems II), Rn. 135 und 137.

ANHANG 3: IN BETRACHT KOMMENDE INFORMATIONSQUELLEN ZUR BEURTEILUNG DES DRITTLANDS

144. Der Datenimporteur sollte in der Lage sein, dem Datenexporteur erforderlichenfalls die einschlägigen Fundstellen und Informationen für das Drittland, in dem er seinen Sitz hat und dessen Recht die Übermittlung unterliegt, mitzuteilen, darunter auch die Rechtsvorschriften und Praktiken, die auf den Datenimporteur und die übermittelten Daten Anwendung finden. Datenexporteur und Datenimporteur können sich auf mehrere Informationsquellen stützen, wie z. B. die nachstehend nicht erschöpfend aufgeführten Informationsquellen, die in der Reihenfolge ihrer Präferenz dargestellt werden:

- Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) und des Europäischen Gerichtshofs für Menschenrechte (EGMR)[104], vgl. dazu die Empfehlungen in den „Wesentlichen europäischen Garantien“;[105]
- Angemessenheitsbeschlüsse für das Bestimmungsland, falls die Übermittlung auf eine andere Rechtsgrundlage gestützt ist;[106]
- Entschließungen und Berichte zwischenstaatlicher Organisationen, z. B. des Europarats[107], anderer regionaler Organisationen[108] und der UN-Organisationen (z. B. UN-Menschenrechtsrat[109], UN-Menschenrechtskommission[110]);
- Berichte und Analysen von zuständigen Regulierungsnetzen wie der Global Privacy Assembly (GPA);[111]
- Nationale Rechtsprechung oder Entscheidungen unabhängiger Justiz- oder Verwaltungsbehörden mit Zuständigkeit für den Schutz der Privatsphäre und den Datenschutz in Drittländern;
- Berichte von unabhängigen Kontrollorganen oder parlamentarischen Gremien;
- Berichte auf der Grundlage praktischer Erfahrungen mit früheren behördlichen Ersuchen um Offenlegung oder dem Nichtvorliegen solcher Ersuchen von Einrichtungen, die in derselben Branche wie der Datenimporteur tätig sind;

---

[104] Vgl. das Factsheet des EMRG zu seiner Rechtsprechung zum Thema Massenüberwachung: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

[105] Empfehlungen 02/2020 des EDSA zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, 10. November 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_de

[106] C-311/18 (Schrems II), Rn. 141; vgl. Angemessenheitsbeschlüsse in https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[107] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[108] Vgl. z. B. die Länderberichte der Interamerikanischen Menschenrechtskommission (IAMRK), https://www.oas.org/en/iachr/reports/country.asp.

[109] Siehe https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx

[110] Siehe: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5

[111] Siehe z. B. https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf

- „Warrant Canaries“ anderer Stellen, die Daten im selben Bereich wie der Datenimporteur verarbeiten;
- Berichte, die von Handelskammern, Industrie-, Berufs- und Handelsverbänden, staatlichen diplomatischen Stellen, Handels- und Investitionsagenturen des Datenexporteurs oder anderer Drittländer erstellt oder in Auftrag gegeben wurden, die in das Drittland ausführen, in das die Übermittlung erfolgt;
- Berichte akademischer Institutionen und zivilgesellschaftlicher Organisationen (z. B. Nichtregierungsorganisationen).
- Berichte privater Anbieter von Unternehmensinformationen über Finanz-, Regulierungs- und Reputationsrisiken für Unternehmen;
- Eigene „Warrant Canaries“ des Datenimporteurs;[112]
- Transparenzberichte, sofern darin ausdrücklich erwähnt wird, dass keine Zugriffsersuchen eingegangen sind. Transparenzberichte, die zu diesem Punkt einfach schweigen, würden nicht als ausreichende Nachweise gelten, da diese Berichte in den meisten Fällen auf von Strafverfolgungsbehörden eingegangene Zugriffsersuchen abheben und nur Zahlen zu diesem Aspekt enthalten, während sie zu den eingegangenen Ersuchen um Zugriff aus Gründen der nationalen Sicherheit nicht Stellung nehmen. Dies bedeutet nicht, dass keine Zugriffsersuchen eingegangen sind, sondern vielmehr, dass diese Informationen nicht weitergegeben werden können;[113]
- Interne Erklärungen oder Aufzeichnungen des Datenimporteurs, aus denen ausdrücklich hervorgeht, dass über einen ausreichend langen Zeitraum keine Zugriffsersuchen eingegangen sind; die Präferenz liegt hier bei Erklärungen oder Aufzeichnungen, die die Haftung des Datenimporteurs begründen und/oder von internen Positionen mit einer gewissen Autonomie wie internen Prüfern, DSB usw. stammen.[114]

[112] Siehe die Bedingungen für die Berücksichtigung der dokumentierten praktischen Erfahrungen des Datenimporteurs mit einschlägigen früheren Fällen von behördlichen Zugriffsersuchen in dem Drittland unter Nummer 47.
[113] *Ebenda.*
[114] *Ebenda.*