

Leitlinien 07/2022 zur Zertifizierung als Instrument für Datentransfers

**Version 1.0**

**Angenommen am 14. Juni 2022**

Versionsgeschichte

|  |  |  |
| --- | --- | --- |
| Version 1.0 | 14. Juni 2022 | Verabschiedung der Leitlinien für die öffentliche Konsultation |

# KURZFASSUNG

Die Datenschutz-Grundverordnung schreibt in Artikel 46 vor, dass Datenexporteure geeignete Garantien für die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen vorsehen müssen. Zu diesem Zweck diversiert die DSGVO die angemessenen Garantien, die von Datenexporteuren gemäß Artikel 46 für Rahmenübermittlungen in Drittländer verwendet werden können, indem sie unter anderem die Zertifizierung als neuen Übermittlungsmechanismus einführt (Artikel 42 Absatz 2 und 46 Absatz 2 Buchstabe f DSGVO).

Diese Leitlinien enthalten Hinweise zur Anwendung von Artikel 46 Absatz 2 Buchstabe f der Datenschutz-Grundverordnung auf die Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen auf der Grundlage von Zertifizierungen. Das Dokument ist in vier Abschnitte und einen Anhang gegliedert.

Im ersten Teil dieses Dokuments ("ALLGEMEINES") wird klargestellt, dass die Leitlinien die bereits bestehenden allgemeinen Leitlinien 1/2018 zur Zertifizierung ergänzen und spezifische Anforderungen aus Kapitel V der DSGVO behandeln, wenn die Zertifizierung als Übermittlungsinstrument verwendet wird. Gemäß Artikel 44 der Datenschutz-Grundverordnung muss jede Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen zusätzlich zur Einhaltung von Kapitel V der Datenschutz-Grundverordnung die Bedingungen der anderen Bestimmungen der Datenschutz-Grundverordnung erfüllen. Daher muss in einem ersten Schritt die Einhaltung der allgemeinen Bestimmungen der Datenschutz-Grundverordnung und in einem zweiten Schritt die Einhaltung der Bestimmungen von Kapitel V der Datenschutz-Grundverordnung gewährleistet werden. Die beteiligten Akteure und ihre Hauptaufgaben in diesem Zusammenhang werden beschrieben, wobei der Schwerpunkt auf der Rolle des Datenimporteurs liegt, dem eine Zertifizierung erteilt wird, sowie auf der Rolle des Datenexporteurs, der sie als Instrument zur Gestaltung seiner Übermittlungen nutzt (unter Berücksichtigung der Tatsache, dass die Verantwortung für die Einhaltung der Datenverarbeitung beim Datenexporteur verbleibt). In diesem Zusammenhang kann die Zertifizierung auch zusätzliche Maßnahmen enthalten, die die Übermittlungsinstrumente ergänzen, um die Einhaltung des EU-Schutzniveaus für personenbezogene Daten zu gewährleisten. Teil eins der Leitlinien enthält auch Informationen über das Verfahren zur Erlangung einer Zertifizierung, die als Instrument für Übermittlungen verwendet werden kann.

Der zweite Teil dieser Leitlinien ("IMPLEMENTING GUIDANCE ON THE ACCREDITATION REQUIRE- MENTS") erinnert daran, dass die Anforderungen für die Akkreditierung einer Zertifizierungsstelle in der ISO 17065 zu finden sind, und interpretiert die Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 der DSGVO und deren Anhang vor dem Hintergrund von Kapitel V. Im Zusammenhang mit einer Übertragung werden in diesen Leitlinien jedoch einige der für die Zertifizierungsstelle geltenden Akkreditierungsanforderungen näher erläutert.

Der dritte Teil dieser Leitlinien ("BESONDERE ZERTIFIZIERUNGSKRITERIEN") enthält Leitlinien zu den bereits in den Leitlinien 1/2018 aufgeführten Zertifizierungskriterien und legt zusätzliche spezifische Kriterien fest, die in einem Zertifizierungsmechanismus enthalten sein sollten, der als Instrument für Übermittlungen in Drittländer verwendet werden soll. Diese Kriterien betreffen die Bewertung der Rechtsvorschriften des Drittlandes, die allgemeinen Verpflichtungen von Exporteuren und Importeuren, Regeln für Weiterübermittlungen, Rechtsbehelfe und Durchsetzung, Verfahren und Maßnahmen für Situationen, in denen nationale Rechtsvorschriften und Praktiken die Einhaltung der im Rahmen der Zertifizierung eingegangenen Verpflichtungen verhindern, sowie Anträge auf Datenzugriff durch Drittlandsbehörden.

Teil vier dieser Leitlinien ("Verbindliche und durchsetzbare Verpflichtungen") enthält Elemente, die in den verbindlichen und durchsetzbaren Verpflichtungen behandelt werden sollten, die für die Verarbeitung Verantwortliche oder Auftragsverarbeiter, die nicht der Datenschutz-Grundverordnung unterliegen, eingehen sollten, um angemessene Garantien für in Drittländer übermittelte Daten zu bieten. Diese Verpflichtungen, die in verschiedenen Instrumenten, einschließlich Verträgen, festgelegt werden können, müssen insbesondere eine Garantie enthalten, dass der Importeur keinen Grund zu der Annahme hat, dass die für die betreffende Verarbeitung geltenden Gesetze und Praktiken in dem Drittland, einschließlich etwaiger Anforderungen an die Offenlegung personenbezogener Daten oder Maßnahmen, die den Zugang öffentlicher Stellen ermöglichen, ihn daran hindern, seinen Verpflichtungen im Rahmen der Zertifizierung nachzukommen.

Der ANHANG dieser Leitlinien enthält einige Beispiele für ergänzende Maßnahmen, die mit den in Anhang II der Empfehlungen 01/2020 (Empfehlungen 01/2020 zu Maßnahmen, die die Übermittlungsinstrumente ergänzen, um die Einhaltung des EU-Schutzniveaus für personenbezogene Daten zu gewährleisten) aufgeführten Maßnahmen im Zusammenhang mit der Verwendung einer Zertifizierung als Übermittlungsinstrument übereinstimmen.

Inhaltsübersicht

[KURZFASSUNG3](#_bookmark0)

1. [ALLGEMEIN6](#_bookmark1)
   1. [Zweck und Anwendungsbereich6](#_bookmark2)
   2. [Allgemeine Regeln für internationale Überweisungen6](#_bookmark3)
   3. [Wer sind die beteiligten Akteure und welche Rolle spielen sie bei der Zertifizierung als Instrument für den Transfer? 8](#_bookmark4)
   4. [Welchen Umfang und Zweck hat die Zertifizierung als Instrument für den Transfer? 9](#_bookmark6)
   5. [Welche Rolle sollte der Exporteur bei der Nutzung der Zertifizierung als Instrument für Transfers spielen? 10](#_bookmark7)
   6. [Wie sieht das Verfahren für die Zertifizierung als Instrument für den Transfer aus? 10](#_bookmark8)
2. [LEITLINIEN FÜR DIE UMSETZUNG DER AKKREDITIERUNGSANFORDERUNGEN11](#_bookmark9)
3. [SPEZIFISCHE ZERTIFIZIERUNGSKRITERIEN12](#_bookmark10)
   1. [DURCHFÜHRUNGSHINWEISE ZU DEN ZERTIFIZIERUNGSKRITERIEN 13](#_bookmark11)
   2. [ZUSÄTZLICHE SPEZIFISCHE ZERTIFIZIERUNGSKRITERIEN 14](#_bookmark12)
4. [Bewertung der Rechtsvorschriften des Drittlandes 14](#_bookmark13)
5. [Allgemeine Verpflichtungen der Ausführer und Einführer 14](#_bookmark14)
6. [Regeln für die Weiterübermittlung 14](#_bookmark15)
7. [Rechtsbehelf und Vollstreckung 15](#_bookmark16)
8. [Verfahren und Maßnahmen für Situationen, in denen die nationalen Rechtsvorschriften die Einhaltung der im Rahmen der Zertifizierung eingegangenen Verpflichtungen verhindern 15](#_bookmark17)
9. [Umgang mit Anträgen auf Datenzugang durch Drittlandsbehörden 15](#_bookmark18)
10. [Zusätzliche Schutzmaßnahmen für den Exporteur 15](#_bookmark19)
11. [VERBINDLICHE UND DURCHSETZBARE VERPFLICHTUNGEN, DIE UMGESETZT WERDEN MÜSSEN16](#_bookmark20)

[ANHANG18](#_bookmark21)

1. [BEISPIELE FÜR ZUSÄTZLICHE MASSNAHMEN, DIE DER EINFÜHRER DURCHFÜHREN MUSS, WENN DIE DURCHFUHR IN DEN GELTUNGSBEREICH DER ZERTIFIZIERUNG FÄLLT 18](#_bookmark22)
2. [BEISPIELE FÜR ZUSÄTZLICHE MASSNAHMEN FÜR DEN FALL, DASS DIE DURCHFUHR NICHT DURCH DIE BESCHEINIGUNG ABGEDECKT IST UND DER EXPORTEUR SIE SICHERSTELLEN MUSS 19](#_bookmark23)

### 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 EWR-Abkommen, insbesondere auf Anhang XI und Protokoll 37, geändert durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 20181 ,

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung,

### HAT DIE FOLGENDEN LEITLINIEN ANGENOMMEN

# ALLGEMEINES

## Zweck und Anwendungsbereich

1. Dieses Dokument soll eine Orientierungshilfe für die Anwendung von Artikel 46 Absatz 2 Buchstabe f der Datenschutz-Grundverordnung auf die Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen auf der Grundlage einer Zertifizierung bieten. Der EDPB hat bereits allgemeine Leitlinien für die Zertifizierung2 und die Akkreditierung3 im Rahmen der Datenschutz-Grundverordnung veröffentlicht. Diese neuen Leitlinien spiegeln daher nur die spezifischen Aspekte der Zertifizierung als Instrument für Übermittlungen wider. Sie präzisieren die Anwendung von Artikel 46 Absatz 2 Buchstabe f und Artikel 42 Absatz 2 der Datenschutz-Grundverordnung, indem sie diesbezüglich praktische Hinweise geben und neue Elemente in die bereits veröffentlichten Leitlinien aufnehmen.
2. Der EDPB wird die Funktionsweise dieser Leitlinien im Lichte der Erfahrungen mit ihrer Anwendung in der Praxis bewerten und weitere Leitlinien zur Klärung der Anwendung der oben aufgeführten Elemente bereitstellen.

## Allgemeine Regeln für internationale Überweisungen

1. Gemäß Artikel 44 der Datenschutz-Grundverordnung muss jede Übermittlung personenbezogener Daten an Drittländer4 oder internationale Organisationen die Bedingungen der anderen Bestimmungen der Datenschutz-Grundverordnung zusätzlich zur Einhaltung von Kapitel V der Datenschutz-Grundverordnung erfüllen. Daher muss jede Übermittlung unter anderem den Datenschutzgrundsätzen in Artikel 5 DSGVO entsprechen, gemäß Artikel 6 DSGVO rechtmäßig sein und im Falle besonderer Datenkategorien mit Artikel 9 DSGVO übereinstimmen. Daher muss ein zweistufiger Test durchgeführt werden. In einem ersten Schritt muss die Einhaltung der allgemeinen Bestimmungen der Datenschutz-Grundverordnung gewährleistet werden, und in einem zweiten Schritt müssen die Bestimmungen von Kapitel V der Datenschutz-Grundverordnung eingehalten werden.

Artikel 44 GDPR (Allgemeiner Grundsatz für Übermittlungen)

Zertifizierung als Instrument für die Übertragung (geeignete Schutzmaßnahmen).

Verbindliche und durchsetzbare Verpflichtungen des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters im Drittland zur Anwendung geeigneter Garantien, auch in Bezug auf die Rechte der betroffenen Personen.

Zweistufiges Modell.

Einhaltung der allgemeinen Bestimmungen der Datenschutz-Grundverordnung (insbesondere Kapitel II)

Einhaltung der Grundsätze in Artikel 5 DSGVO und, falls von einem für die Verarbeitung Verantwortlichen zu überprüfen, insbesondere die Rechtmäßigkeit gemäß Artikel 6 DSGVO und die Einhaltung von Artikel 9 DSGVO (im Falle besonderer Datenkategorien).

GDPR-Übertragungs-Toolbox (Kapitel V)

1. In Artikel 46 der DSGVO heißt es: "*Liegt keine Entscheidung nach Artikel 45 Absatz 3 vor, darf ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten nur dann in ein Drittland oder an eine internationale Organisation übermitteln, wenn der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und unter der Voraussetzung, dass durchsetzbare Rechte der betroffenen Person und wirksame Rechtsbehelfe für die betroffenen Personen zur Verfügung stehen*". Gemäß Artikel 46 Absatz 2 Buchstabe f der Datenschutz-Grundverordnung können solche angemessenen Garantien durch einen zugelassenen Zertifizierungsmechanismus in Verbindung mit verbindlichen und durchsetzbaren Verpflichtungen des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der angemessenen Garantien, auch in Bezug auf die Rechte der betroffenen Personen, vorgesehen werden.
2. Infolgedessen könnte der Datenexporteur beschließen, sich auf die von einem Datenimporteur erhaltene Zertifizierung zu stützen, um die Einhaltung seiner Verpflichtungen z. B. gemäß Artikel 24 Absatz 3 oder Artikel 28 Absatz 5 DSGVO nachzuweisen, wenn er ein für die Verarbeitung Verantwortlicher in einer Übermittlungsverarbeitung ist. Der Datenimporteur könnte beschließen, eine Zertifizierung zu beantragen, um nachzuweisen, dass das durch die Datenschutz-Grundverordnung garantierte Schutzniveau für natürliche Personen nicht untergraben wird.
3. Sowohl der Datenexporteur als auch der Datenimporteur können je nach der Verarbeitung innerhalb von Kapitel V unterschiedliche Rollen (z. B. als für die Verarbeitung Verantwortlicher oder als Auftragsverarbeiter) wahrnehmen5 , was zu unterschiedlichen Verantwortlichkeiten führt:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Controller  (Datenexporteur) |  | Controller  (Datenexporteur) |  | Prozessor  (Datenexporteur) |  | Prozessor  (Datenexporteur) |
| Controller  (Datenimporteur) |  | Prozessor  (Datenimporteur) |  | Prozessor  (Datenimporteur) |  | Controller  (Datenimporteur) |

1. Abgesehen von der Zertifizierung oder anderen in den Artikeln 45 und 46 genannten Übermittlungsinstrumenten oder -mechanismen sieht Artikel 49 DSGVO vor, dass in einer begrenzten Anzahl spezifischer Situationen internationale Datenübermittlungen stattfinden können, wenn kein anderer Mechanismus in Kapitel V eingehalten wird6 . Wie in früheren Leitlinien des EDSB erläutert, sind die in Artikel 49 DSGVO vorgesehenen Ausnahmeregelungen jedoch restriktiv auszulegen und beziehen sich hauptsächlich auf gelegentliche und nicht wiederkehrende Verarbeitungen7 .

## Wer sind die beteiligten Akteure und welche Rolle spielen sie bei der Zertifizierung als Instrument für den Transfer?

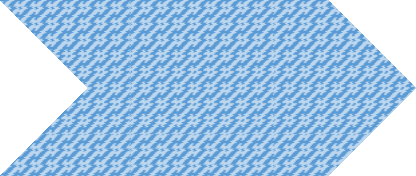
1. Der **Europäische Datenschutzausschuss (EDPB)** ist befugt, EWR-weite Zertifizierungskriterien (Europäisches Datenschutzsiegel) zu genehmigen und Stellungnahmen zu Entscheidungsentwürfen der Aufsichtsbehörden über Zertifizierungskriterien und Akkreditierungsanforderungen an die Zertifizierungsstellen abzugeben.
2. Die **Aufsichtsbehörden** genehmigen die Zertifizierungskriterien, wenn es sich bei dem Zertifizierungsmechanismus nicht um ein Europäisches Datenschutzsiegel handelt8 . Sie können auch die Zertifizierungsstelle akkreditieren, die Zertifizierungskriterien entwerfen und die Zertifizierung ausstellen, wenn dies im nationalen Recht des jeweiligen Mitgliedstaats vorgesehen ist9 .
3. Die **nationale Akkreditierungsstelle** kann Drittzertifizierungsstellen unter Verwendung der ISO 17065 und der zusätzlichen Akkreditierungsanforderungen der Aufsichtsbehörden akkreditieren, die die Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 der Datenschutz-Grundverordnung und deren Anhang vor dem Hintergrund von Kapitel V auslegen sollten.
4. Der **Eigentümer des Systems** ist eine identifizierbare Organisation, die die Zertifizierungskriterien und die Anforderungen, anhand derer die Konformität zu bewerten ist, festgelegt hat. Die Organisation, die die Bewertungen durchführt, könnte dieselbe Organisation sein, die das Programm entwickelt hat und dessen Eigentümerin ist, aber es könnte auch Vereinbarungen geben, bei denen eine Organisation Eigentümerin des Programms ist und eine andere (oder mehrere andere) die Bewertungen als Zertifizierungsstelle durchführt.
5. Je nach nationalem Recht können die **Zertifizierungsstellen**, die wie oben beschrieben akkreditiert sind, alternativ zu den SAs die Zertifizierungen ausstellen10 . Sie können Zertifizierungskriterien und/oder detaillierte Bewertungsmethoden für die Kriterien, d. h. das vollständige Zertifizierungsprogramm, entwickeln. Sie muss ihren Sitz im EWR haben, um z. B. die wirksame Ausübung der in Artikel 58 Absatz 2 Buchstabe f DSGVO verankerten Korrekturbefugnisse zu ermöglichen. Die Zertifizierungsstelle kann jedoch Tätigkeiten an lokale Experten oder Einrichtungen außerhalb des EWR untervergeben, die in ihrem Namen Audittätigkeiten durchführen11 . Allerdings darf eine Zertifizierungsstelle die Entscheidung über die Erteilung oder Nicht-Erteilung einer Zertifizierung nicht an Unterauftragnehmer vergeben.
6. Der **Datenimporteur** ist die Stelle (für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter) in einem Drittland, die Daten von einem Datenexporteur erhält.
7. Der **Datenexporteur** ist die Stelle (für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter), die Daten aus dem EWR an einen Datenimporteur übermittelt. Der Datenexporteur muss die Einhaltung von Kapitel V sicherstellen.

## Welchen Umfang und Zweck hat die Zertifizierung als Instrument für den Transfer?

1. Ein Zertifizierungsverfahren als Übermittlungsinstrument gemäß Artikel 42 Absatz 2 muss darauf abzielen, angemessene Garantien für die Verarbeitung personenbezogener Daten im Sinne von Artikel 46 Absatz 2 Buchstabe f zu gewährleisten. Mit der Zertifizierung ist nachzuweisen, dass die für die Verarbeitung Verantwortlichen oder die Auftragsverarbeiter außerhalb des EWR oder eine internationale Organisation, die Daten von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern aus dem EWR erhält, angemessene Garantien bieten, um den spezifischen Risiken der Übermittlung personenbezogener Daten zu begegnen.
2. Im Allgemeinen stellt der Vorgang der Übermittlung personenbezogener Daten aus einem Mitgliedstaat in ein Drittland an sich eine Verarbeitung personenbezogener Daten im Sinne von Artikel 4 Absatz 2 der Datenschutz-Grundverordnung dar, die in einem Mitgliedstaat durchgeführt wird12 . In einigen Fällen, die von der Art der Übermittlung durch den Importeur abhängen, könnte jedoch die Durchfuhr in den Anwendungsbereich der Zertifizierung als Instrument für die Übermittlung einbezogen werden. Folglich sollte der Gegenstand der Zertifizierung - der mit dem Ziel der Bewertung (Target of Evaluation, ToE) bei der Zertifizierung13 übereinstimmt - im Allgemeinen die Verarbeitung der aus dem EWR erhaltenen Daten durch den Datenimporteur in dem Drittland und alle Vorgänge unter der Kontrolle des Importeurs sein.

.g. Seekabel)

Die grundsätzliche Zertifizierung nach Art. 42 DSGVO und als Ausnahme nach Kapitel V



Verarbeitung im 3. Land

Zertifizierung nach Kapitel V GDPR

1. Der Gegenstand der Zertifizierung kann ein einzelner Verarbeitungsvorgang oder eine Reihe von Vorgängen sein. Diese können Governance-Prozesse im Sinne von organisatorischen Maßnahmen, also als integrale Bestandteile eines Verarbeitungsprozesses, umfassen14 .
2. Die antragstellende Stelle wäre also der Datenimporteur im Drittland in Bezug auf den Gegenstand der Zertifizierung.

## Welche Rolle sollte der Exporteur bei der Nutzung der Zertifizierung als Instrument für Transfers spielen?

1. Die Übermittlungsverarbeitung durch den Datenexporteur als solche fällt im Allgemeinen direkt unter die DSGVO. Das bedeutet, dass der Exporteur seinen Verpflichtungen aus der DSGVO nachkommen und insbesondere sicherstellen muss, dass die Daten auf sichere Weise gemäß Artikel 32 übermittelt werden und mit geeigneten Garantien gemäß Kapitel V versehen sind, um zu gewährleisten, dass das durch diese Verordnung garantierte Schutzniveau für natürliche Personen nicht untergraben wird (Artikel 44 DSGVO). Dies kann natürlich gemäß Artikel 42 Absatz 1 bescheinigt werden.
2. Darüber hinaus ist der Datenexporteur, der eine Zertifizierung als geeignete Schutzmaßnahme gemäß Artikel 46 Absatz 2 Buchstabe f verwenden will, insbesondere verpflichtet zu überprüfen, ob die Zertifizierung, auf die er sich stützen will, angesichts der Merkmale der beabsichtigten Verarbeitung wirksam ist. Zu diesem Zweck muss der Datenexporteur prüfen, ob die Zertifizierung gültig und nicht abgelaufen ist, ob sie sich auf die vorgesehene Übermittlung bezieht und ob die Durchfuhr personenbezogener Daten in den Geltungsbereich der Zertifizierung fällt, sowie ob Weiterübermittlungen betroffen sind und eine angemessene Dokumentation darüber vorliegt. Darüber hinaus muss der Exporteur prüfen, ob es einen Vertrag oder ein anderes rechtsverbindliches Instrument zwischen dem zertifizierten Datenimporteur und der Zertifizierungsstelle gibt, d. h. die "Zertifizierungsvereinbarung". Die Zertifizierungsvereinbarung ist der Vertrag, auf den in Punkt 4.1.2 der ISO 17065 und in den zusätzlichen Anforderungen der Leitlinien 4/2018 Bezug genommen wird und in dem sich der Datenimporteur verpflichtet, die Zertifizierungskriterien auf die ToE (d. h. alle im Rahmen der Zertifizierung übermittelten personenbezogenen Daten) anzuwenden, auch in Bezug auf die Kriterien im Zusammenhang mit den Rechten der betroffenen EWR-Bürger, deren Daten übermittelt werden sollen. Darüber hinaus sollte der Datenexporteur im Datenverarbeitungsvertrag gemäß Artikel 28 DSGVO bei Übermittlungen von für die Verarbeitung Verantwortlichen an Auftragsverarbeiter oder in einem Vertrag über die gemeinsame Nutzung von Daten zusammen mit verbindlichen und durchsetzbaren Verpflichtungen mit dem Datenimporteur bei Übermittlungen von für die Verarbeitung Verantwortlichen an für die Verarbeitung Verantwortliche auf die Verwendung der Zertifizierung als Instrument für die Übermittlung verweisen.
3. Da der Exporteur für die Anwendung aller Bestimmungen des Kapitels V verantwortlich ist, muss er - je nach seiner konkreten Rolle als für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter - auch beurteilen, ob die Zertifizierung, auf die er sich stützen will, im Lichte der im Drittland geltenden Rechtsvorschriften und Praktiken wirksam ist. Die dokumentierte Bewertung der Rechtsvorschriften und Gepflogenheiten des Drittlandes durch den Datenimporteur (siehe nachstehend Abschnitt 1.6) kann im Rahmen dieser Bewertung im Namen des Exporteurs als Nachweis für die Einhaltung der Vorschriften herangezogen werden.
4. Hat die Prüfung des Importeurs ergeben, dass er und/oder der Datenexporteur möglicherweise zusätzliche Maßnahmen ergreifen müssen, die in der Zertifizierung vorgesehen sind, um ein im Wesentlichen gleichwertiges Schutzniveau wie im EWR zu gewährleisten, muss der Datenexporteur die vom Datenimporteur, der über eine Zertifizierung verfügt, ergriffenen zusätzlichen Maßnahmen überprüfen und prüfen, ob er in der Lage ist, die vom Datenimporteur geforderten technischen und (gegebenenfalls) zusätzlichen Maßnahmen zu erfüllen.
5. Werden diese Bedingungen nicht erfüllt, muss der Datenexporteur vom Importeur verlangen, dass er angepasste zusätzliche Maßnahmen ergreift oder diese selbst festlegt.

## Wie sieht das Verfahren für die Zertifizierung als Instrument für den Transfer aus?

1. Das Zertifizierungsverfahren muss freiwillig und über einen transparenten Prozess verfügbar sein. Die Datenschutz-Grundverordnung setzt großes Vertrauen in private Zertifizierungsverfahren als "regulierte Selbstregulierung". Dementsprechend müssen diese Mechanismen sicherstellen, dass die Zertifikate die in Artikel 46 DSGVO definierten Anforderungen an angemessene Garantien erfüllen.
2. Daher basiert die Zertifizierung auf der Bewertung von Zertifizierungskriterien nach einer verbindlichen Audit-Methodik. Diese Kriterien werden von den nationalen Aufsichtsbehörden oder im Falle der Anwendung des in Artikel 42 Absatz 5 DSGVO beschriebenen Kohärenzverfahrens vom Europäischen Datenschutzbeauftragten genehmigt. Die Kriterien für die Zertifizierung umfassen Anforderungen für eine Bewertung des einschlägigen Rechtsrahmens des Drittlandes, um den spezifischen Risiken der Übermittlung personenbezogener Daten in das betreffende Drittland und der vom Datenimporteur durchgeführten Weiterverarbeitung zu begegnen.
3. Während des Zertifizierungsprozesses wird der Evaluierungsgegenstand anhand der Zertifizierungskriterien von einer Zertifizierungsstelle überprüft, die von der nationalen Akkreditierungsstelle oder von der zuständigen SA15 akkreditiert ist.
4. Gemäß Artikel 43 Absatz 1 DSGVO stellen Zertifizierungsstellen, die über ein angemessenes Maß an Fachwissen in Bezug auf den Datenschutz verfügen, nach Unterrichtung der Aufsichtsbehörde, damit diese erforderlichenfalls ihre Befugnisse gemäß Artikel 58 Absatz 2 Buchstabe h) DSGVO ausüben kann, Zertifizierungen aus und erneuern diese.
5. Gemäß Artikel 43 (5) der Datenschutz-Grundverordnung müssen die Zertifizierungsstellen den zuständigen Aufsichtsbehörden die Gründe für die Erteilung oder den Entzug der beantragten Zertifizierung mitteilen. Dies bedeutet nicht, dass die Zertifizierungsstelle die Genehmigung der ORKB benötigt, um die Zertifizierung auszustellen. Die Zertifizierungsstelle wird die Einhaltung der Zertifizierungskriterien durch ihre Kunden überwachen.
6. Die Aufsichtsbehörde ist befugt, eine Zertifizierung zu widerrufen oder anzuordnen, dass eine gemäß Artikel 42 und 43 DSGVO ausgestellte Zertifizierung widerrufen wird, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung auszustellen, wenn die Anforderungen für die Zertifizierung nicht mehr erfüllt sind. Ein Europäisches Datenschutzsiegel für internationale Datenübermittlungen kann als Instrument dienen, um Übermittlungen in Drittländer zusammen mit verbindlichen und durchsetzbaren Verpflichtungen abzudecken16 .
7. Allerdings können auch Zertifizierungen, die nach nationalen, in den EWR-Staaten genehmigten Zertifizierungssystemen ausgestellt wurden, als Instrument für die Verbringung verwendet werden. Als solche sind sie nur für Verbringungen in Drittländer durch Exporteure in dem EWR-Mitgliedstaat gültig, in dem das Zertifizierungssystem genehmigt wurde, da es keine gegenseitige Anerkennung von Zertifizierungen aus verschiedenen EWR-Staaten gibt. Es steht den zuständigen Behörden in verschiedenen EWR-Staaten jedoch frei, dasselbe Zertifizierungssystem für Verbringungen zu genehmigen.

# DURCHFÜHRUNGSHINWEISE ZU AKKREDITIERUNGSANFORDERUNGEN

1. Die Anforderungen an die Akkreditierung einer Zertifizierungsstelle im Hinblick auf Zertifizierungen als Instrument für Übermittlungen sind in der ISO 17065 und durch Auslegung der Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 der DSGVO und ihres Anhangs vor dem Hintergrund von Kapitel V zu finden.
2. Nach Ansicht des EDPB decken die zusätzlichen Akkreditierungsanforderungen, die auf der Grundlage der Leitlinien 4/2018 und der ISO 17065 erstellt und gemäß Artikel 64 Absatz 1 Buchstabe c DSGVO angenommen wurden, bereits die spezifischen Anforderungen ab, die für die Akkreditierung einer Zertifizierungsstelle in Bezug auf Zertifizierungen als Instrument für Transfers erforderlich sind. Sie möchte jedoch darauf hinweisen, dass einige Anforderungen, wenn es um ein Übertragungsszenario geht, in Form von Erläuterungen und Auslegungen präzisiert werden müssen.
3. Im Hinblick auf die Ressourcenanforderungen (siehe Anforderung 6 der Leitlinien 4/2018 - Anhang 1) muss die Zertifizierungsstelle sicherstellen, dass sie über die erforderlichen Ressourcen verfügt, um überprüfen zu können, ob der Importeur, wie in den Zertifizierungskriterien gefordert, die erforderliche Bewertung der Rechtslage und der Praktiken des/der Drittlandes/Drittländer, in dem/denen er sich befindet, ordnungsgemäß und korrekt durchgeführt hat17 . Dies umfasst die Verarbeitungstätigkeiten, die als Teil der ToE im Hinblick auf die angemessenen Garantien aus Artikel 46 DSGVO zu zertifizieren sind, einschließlich der vom Importeur ermittelten und umgesetzten zusätzlichen Maßnahmen, sofern erforderlich. Dazu gehören z. B. auch umfassende Kenntnisse der einschlägigen lokalen Gesetze und Praktiken sowie angemessene Sprachkenntnisse in Bezug auf das Drittland/die Drittländer.
4. In Bezug auf die Prozessanforderungen (siehe Anforderung 7 der Leitlinien 4/2018, Anhang 1) muss die Zertifizierungsstelle sicherstellen, dass der Zertifizierungsprozess in Bezug auf die Verarbeitung, die in dem/den Drittland/Drittländern stattfindet, durchgeführt wird, und die Bewertung sollte auch die praktische Umsetzung der bestehenden Gesetze und Strategien in dem/den Drittland/Drittländern mit möglichen Audits vor Ort umfassen.
5. Im Hinblick auf die Anforderungen in Bezug auf Änderungen, die sich auf die Zertifizierung auswirken (siehe Anforderung 7.10 der Leitlinien 4/2018, Anhang 1), muss die Zertifizierungsstelle Änderungen in der Gesetzgebung und/oder Rechtsprechung von Drittländern überwachen, die sich auf die in den Anwendungsbereich der ToE fallende Verarbeitung auswirken können.

# SPEZIFISCHE ZERTIFIZIERUNGSKRITERIEN

1. Im Rahmen der Betrachtung der spezifischen Zertifizierungskriterien stützt sich dieser Leitfaden auf den Leitfaden 1/2018 zur Zertifizierung und Identifizierung von Zertifizierungskriterien gemäß Artikel 42 und 43 der Verordnung (Version 3.0), den entsprechenden Anhang 2 zur Überprüfung und Bewertung von Zertifizierungskriterien gemäß Artikel 42 (5) und den Leitfaden zur Bewertung von Zertifizierungskriterien Addendum.
2. Nach Ansicht des EDPB decken die auf der Grundlage des Leitfadens 1/2018, Anhang 2, und des Leitfadens zur Bewertung von Zertifizierungskriterien - Addendum - ausgearbeiteten Zertifizierungskriterien bereits den Großteil der Zertifizierungskriterien ab, die bei der Ausarbeitung eines Zertifizierungsprogramms, das als Instrument für Transfers verwendet werden soll, berücksichtigt werden müssen. Es könnte jedoch erforderlich sein, einige dieser bestehenden Kriterien weiter zu spezifizieren, um sie auf ein spezifisches Transferszenario zuzuschneiden (siehe Abschnitt 3.1). Darüber hinaus könnte es erforderlich sein, zusätzliche Kriterien für die Anwendung angemessener Garantien, auch im Hinblick auf die Rechte der betroffenen Personen, zu formulieren (siehe Absatz 3.2).

## LEITLINIEN FÜR DIE ANWENDUNG DER ZERTIFIZIERUNGSKRITERIEN

1. Der Anwendungsbereich des Zertifizierungsverfahrens und der Evaluierungsgegenstand (siehe Anhang 2, Abschnitt 2.a) sollten klar beschrieben werden, auch im Hinblick auf die Übermittlung personenbezogener Daten in ein Drittland, oder ob auch deren Durchfuhr erfasst werden soll.
2. Im Hinblick auf den Anwendungsbereich des Zertifizierungsverfahrens und den Evaluationsgegenstand (siehe Anhang 2, Abschnitt 2.b) sollte konkret beschrieben werden, für welche Art von Stelle (z. B. für den für die Verarbeitung Verantwortlichen und/oder den Auftragsverarbeiter) das Zertifizierungsverfahren anwendbar ist.
3. Im Hinblick auf den Geltungsbereich des Zertifizierungsmechanismus und den Evaluationsgegenstand (siehe Anhang 2, Abschnitt 2.f) sollten die Kriterien ausreichend beschreiben, wie der Evaluationsgegenstand konkret definiert werden sollte, um Missverständnisse zu vermeiden. Dies sollte mindestens Folgendes beinhalten:
   1. den/die Verarbeitungsvorgang(e), auch für den Fall, dass eine Weiterübermittlung vorgesehen ist
   2. der Zweck
   3. die Art der Einrichtung (z. B. für die Verarbeitung Verantwortlicher und/oder Auftragsverarbeiter)
   4. die Art der übermittelten Daten, wobei zu berücksichtigen ist, ob es sich um besondere Kategorien personenbezogener Daten im Sinne von Artikel 9 DSGVO handelt
   5. die Kategorien der betroffenen Personen
   6. die Länder, in denen die Datenverarbeitung stattfindet
4. Im Hinblick auf die Transparenz und die Rechte der betroffenen Personen (siehe Anhang 2, Abschnitt 8) sollten die Zertifizierungskriterien:
   1. Informationen über die Verarbeitungstätigkeiten, auch über die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation und über die Verwendung der Zertifizierung als Instrument für die Übermittlung (siehe Artikel 12, 13 und 14 DSGVO), vorschreiben
   2. verlangen, dass den betroffenen Personen das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung, Benachrichtigung über die Berichtigung oder Löschung oder Einschränkung, Widerspruch gegen die Verarbeitung und das Recht, keinen Entscheidungen unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruhen, einschließlich Profiling, wie in den Artikeln 15 bis 19, 21 und 22 DSGVO vorgesehen, garantiert wird
   3. ein geeignetes Verfahren zur Bearbeitung von Beschwerden vorzusehen, das der zertifizierte Datenimporteur einrichten muss, um die wirksame Umsetzung der Rechte der betroffenen Personen zu gewährleisten
   4. angemessen darauf eingehen, ob und inwieweit diese Rechte für die betroffenen Personen in dem betreffenden Drittland durchsetzbar sind oder ob gegebenenfalls geeignete Maßnahmen zu ihrer Durchsetzung ergriffen werden müssen.
5. In Bezug auf die technischen und organisatorischen Maßnahmen zur Gewährleistung des Schutzes (Anhang 2, Abschnitt 10.q) sollten die Zertifizierungskriterien vorsehen, dass der Importeur den Exporteur und, wenn der Importeur als für die Verarbeitung Verantwortlicher handelt, die zuständige Aufsichtsbehörde über Datenschutzverletzungen informiert und diese den betroffenen Personen mitteilt, wenn die Verletzung wahrscheinlich ein hohes Risiko für ihre Rechte und Freiheiten zur Folge hat.

## ZUSÄTZLICHE SPEZIFISCHE ZERTIFIZIERUNGSKRITERIEN

1. In Anbetracht der Garantien, die für andere Übermittlungsinstrumente gemäß Artikel 46 der Datenschutz-Grundverordnung festgelegt wurden (z. B. verbindliche unternehmensinterne Vorschriften oder Verhaltenskodizes), und zur Gewährleistung eines einheitlichen Schutzniveaus sowie unter Berücksichtigung des Schrems-II-Urteils des EuGH ist der EDSB der Ansicht, dass der Zertifizierungsmechanismus, der als Instrument für Übermittlungen in Drittländer verwendet werden soll, auch die unten aufgeführten Kriterien umfassen sollte.

## Bewertung der Rechtsvorschriften des Drittlandes

1. Erfordern die Kriterien, dass der Importeur die Rechtslage und die Praktiken des Drittlandes, in dem er tätig ist, im Hinblick auf die angemessenen Garantien aus Artikel 46 DSGVO bewertet hat, wobei zu berücksichtigen ist, dass auch zu prüfen ist, ob die geltenden Rechtsvorschriften und Praktiken des Drittlandes das Ziel der Zertifizierung beeinträchtigen könnten?
2. Verpflichten die Kriterien den Importeur, die Bewertung der Rechtslage und der Praktiken des Drittlandes, in dem er tätig ist, zu dokumentieren und die Dokumentation der Zertifizierungsstelle und den zuständigen Datenschutzbehörden auf Anfrage zur Verfügung zu stellen?
3. Erfordern die Kriterien, dass der Importeur die organisatorischen und technischen Maßnahmen ermittelt und umgesetzt hat, um die angemessenen Garantien gemäß Artikel 46 DSGVO unter Berücksichtigung der "Empfehlungen 01/2020 zu Maßnahmen, die Übermittlungsinstrumente ergänzen, um die Einhaltung des EU-Schutzniveaus für personenbezogene Daten zu gewährleisten", falls die Durchfuhr in den Geltungsbereich der Zertifizierung als Instrument für Übermittlungen einbezogen ist?
4. Erfordern die Kriterien, dass der Importeur die organisatorischen und technischen Maßnahmen ergriffen hat, um die angemessenen Garantien gemäß Artikel 46 DSGVO unter Berücksichtigung der "Empfehlungen 01/2020 zu Maßnahmen, die Übermittlungsinstrumente ergänzen, um die Einhaltung des EU-Schutzniveaus für personenbezogene Daten zu gewährleisten", falls die Durchfuhr nicht in den Geltungsbereich der Zertifizierung als Instrument für Übermittlungen fällt?
5. Müssen die Kriterien vorsehen, dass der Importeur die organisatorischen und technischen Maßnahmen dokumentiert, die wirksam umgesetzt wurden, um die angemessenen Garantien gemäß Artikel 46 DSGVO zu bieten, und die Dokumentation der Zertifizierungsstelle und den zuständigen Datenschutzbehörden auf Anfrage zur Verfügung stellt?
6. Erfordern die Kriterien eine Verpflichtung gegenüber der Zertifizierungsstelle und dem Exporteur, dass der Importeur keinen Grund zu der Annahme hat, dass die für ihn geltenden Rechtsvorschriften und Praktiken ihn an der Erfüllung seiner Verpflichtungen im Rahmen der Zertifizierung hindern könnten?

## Allgemeine Verpflichtungen der Exporteure und Importeure

1. Müssen die Kriterien in vertraglichen Vereinbarungen (z. B. in einem bestehenden Dienstleistungsvertrag) zwischen Exporteuren und Importeuren festgelegt werden, in denen die spezifische Übermittlung beschrieben wird, für die die Zertifizierung gilt, und in denen den betroffenen Personen die Rechte von Drittbegünstigten zuerkannt werden?
2. Sofern diese Vereinbarungen oder Instrumente ein Zertifizierungskriterium darstellen und eine Vorlage zur Verfügung gestellt wird, verlangen die Kriterien, dass sie auch Gegenstand der Bewertung sind?

## Regeln für die Weiterübermittlung

a) Erfordern die Kriterien, dass die für die bescheinigte Übermittlung geltenden Garantien auch für die Weiterübermittlung gemäß Kapitel V der Datenschutz-Grundverordnung gelten, um sicherzustellen, dass das im EWR gewährleistete Schutzniveau im Falle der Weiterübermittlung nicht untergraben wird, und

Sehen die Kriterien vor, dass der Zertifizierungsstelle und den zuständigen Datenschutzbehörden auf Anfrage geeignete Unterlagen zur Verfügung gestellt werden?

## Rechtsbehelf und Vollstreckung

1. Sehen die Kriterien vor, dass betroffene Personen ihre Rechte als Drittbegünstigte gegenüber dem Datenimporteur vor den zuständigen Gerichten des EWR im Einklang mit Artikel 79 DSGVO oder bei einer internationalen Organisation geltend machen können, einschließlich des Ersatzes des Schadens, den die betroffene Person erlitten hat, wenn der Importeur das einschlägige Zertifizierungssystem nicht einhält?
2. Ermöglichen es die Kriterien, angemessen zu beurteilen, ob ein Importeur im EWR für den Schaden haftet, den die betroffene Person im Falle der Nichteinhaltung des einschlägigen Zertifizierungssystems erlitten hat?
3. Sehen die Kriterien vor, dass die betroffenen Personen gemäß Artikel 77 DSGVO eine Beschwerde bei der zuständigen Aufsichtsbehörde im EWR einreichen können?
4. Sehen die Kriterien vor, dass der Importeur mit der für den/die Datenexporteur(e) zuständigen Aufsichtsbehörde im EWR zusammenarbeitet und sich bereit erklärt, von ihr (ihnen) geprüft und kontrolliert zu werden**,** ihre Ratschläge zu berücksichtigen und sich an ihre Entscheidungen zu halten?

## Verfahren und Maßnahmen für Situationen, in denen die nationalen Rechtsvorschriften die Einhaltung der im Rahmen der Zertifizierung eingegangenen Verpflichtungen verhindern

1. Sehen die Kriterien eine Verpflichtung vor, dass der Datenimporteur in einem Drittland oder eine internationale Organisation, wenn er Grund zu der Annahme hat, dass Änderungen der für ihn geltenden Rechtsvorschriften und Praktiken ihn daran hindern könnten, seinen Verpflichtungen im Rahmen der Zertifizierung nachzukommen, dies der Zertifizierungsstelle und dem Datenexporteur unverzüglich mitteilt, damit dieser beurteilen kann, ob er die Übermittlungen unverzüglich einstellen muss?
2. Erfordern die Kriterien eine Beschreibung der Schritte, die zu unternehmen sind (einschließlich der Benachrichtigung des Ausführers im EWR und der Ergreifung geeigneter zusätzlicher Maßnahmen), wenn der für die Verarbeitung Verantwortliche/Verarbeiter in einem Drittland Kenntnis von Rechtsvorschriften eines Drittlandes erhält, die die Einhaltung der Verpflichtungen im Rahmen der Zertifizierung verhindern, sowie der Maßnahmen, die im Falle von Auskunftsersuchen von Drittlandsbehörden zu ergreifen sind (einschließlich der Verpflichtung, die Rechtmäßigkeit des Ersuchens zu überprüfen und die weitergegebenen Informationen auf ein Minimum zu beschränken)?

## Bearbeitung von Anträgen auf Datenzugang durch Drittlandsbehörden

1. Sehen die Kriterien vor, dass der Datenimporteur den Datenexporteur im Falle von Auskunftsersuchen von Drittlandsbehörden unverzüglich informiert?
2. Erfordern die Kriterien, dass massive und wahllose Übermittlungen aufgrund von Auskunftsersuchen von Drittlandsbehörden nicht stattfinden sollten?

## Zusätzliche Schutzmaßnahmen für den Exporteur

1. Erfordern die Kriterien, dass der Datenimporteur, soweit vorgesehen, sicherstellt, dass den von ihm ermittelten zusätzlichen Maßnahmen entsprechende zusätzliche Maßnahmen auf Seiten des Datenexporteurs unter Berücksichtigung der EDPB-Empfehlungen 01/2020 und der Anwendungsfälle gegenüberstehen, um erforderlichenfalls eine voll wirksame Umsetzung der zusätzlichen Maßnahmen des Importeurs auch durch diesbezügliche verbindliche Anforderungen an den Datenexporteur sicherzustellen?

# VERBINDLICHE UND DURCHSETZBARE VERPFLICHTUNGEN, DIE UMGESETZT WERDEN MÜSSEN

1. Artikel 42 Absatz 2 der Datenschutz-Grundverordnung schreibt vor, dass für die Verarbeitung Verantwortliche und Auftragsverarbeiter, die nicht der Datenschutz-Grundverordnung unterliegen und sich einem Zertifizierungsmechanismus für Übermittlungen anschließen, durch vertragliche oder andere rechtsverbindliche Instrumente verbindliche und durchsetzbare Verpflichtungen eingehen, um die im Zertifizierungsmechanismus vorgesehenen angemessenen Garantien auch im Hinblick auf die Rechte der betroffenen Personen anzuwenden.
2. Wie in der Datenschutz-Grundverordnung festgelegt, können solche Verpflichtungen durch einen Vertrag eingegangen werden, was die einfachste Lösung zu sein scheint. Es könnten auch andere Instrumente verwendet werden, sofern die für die Verarbeitung Verantwortlichen/Verarbeiter, die sich dem Zertifizierungsverfahren anschließen, in der Lage sind, den verbindlichen und durchsetzbaren Charakter dieser anderen Mittel nachzuweisen.
3. In jedem Fall muss das Instrument im Einklang mit dem EU-Recht verbindlich und durchsetzbar sein und sollte auch für die betroffenen Personen als Drittbegünstigte verbindlich und durchsetzbar sein.
4. So könnte beispielsweise ein Vertrag zwischen dem für die Verarbeitung Verantwortlichen/Verarbeiter im Drittland (d. h. dem Datenimporteur) und der Stelle, die ihm Daten aus dem EWR übermittelt (d. h. dem Datenexporteur), unterzeichnet werden. In der Praxis könnten die Parteien einen bestehenden Vertrag verwenden (z. B. einen Dienstleistungsvertrag zwischen dem Exporteur und dem Datenimporteur, den Vertrag über die Datenverarbeitung gemäß Artikel 28 DSGVO zwischen für die Verarbeitung Verantwortlichen und Auftragsverarbeitern oder eine Vereinbarung über die gemeinsame Nutzung von Daten zwischen verschiedenen für die Verarbeitung Verantwortlichen), in den die verbindlichen und durchsetzbaren Verpflichtungen aufgenommen werden könnten. Diese Verpflichtungen sollten klar von allen anderen Klauseln unterschieden werden. Eine weitere Option könnte darin bestehen, sich auf einen separaten Vertrag zu stützen, indem beispielsweise dem für Übermittlungen vorgesehenen Zertifizierungsmechanismus ein Mustervertrag hinzugefügt wird, der dann von den für die Verarbeitung Verantwortlichen/Verarbeitern im Drittland und allen Exporteuren unterzeichnet werden müsste.
5. Es sollte die Möglichkeit bestehen, je nach Situation die am besten geeignete Option zu wählen.
6. Wenn das Zertifizierungsverfahren für Übertragungen und Weiterübertragungen eines Auftragsverarbeiters an Unterauftragsverarbeiter verwendet werden soll, sollte in der zwischen dem Auftragsverarbeiter und seinem für die Verarbeitung Verantwortlichen unterzeichneten Auftragsverarbeitervereinbarung ebenfalls auf das Zertifizierungsverfahren und das Instrument, das verbindliche und durchsetzbare Verpflichtungen vorsieht, Bezug genommen werden.

Controller oder Prozessor

die dem GDPR unterliegen (Datenexporteur)

TRANSFER

Controller oder Prozessor

die nicht der DSGVO unterliegen und über eine Zertifizierung für die Übermittlung von Daten verfügen (Datenimporteur)

Vertrag mit verbindlicher und

einklagbare Verpflichtungen

1. Im Allgemeinen muss in dem Vertrag oder einem anderen Instrument festgelegt werden, dass der für die Verarbeitung Verantwortliche/Verarbeiter, der über eine Zertifizierung verfügt und als Importeur handelt, sich verpflichtet, bei der Verarbeitung der aus dem EWR erhaltenen einschlägigen Daten die in der für die Übermittlung bestimmten Zertifizierung festgelegten Vorschriften einzuhalten, und dass er keinen Grund zu der Annahme hat, dass die für die betreffende Verarbeitung geltenden Rechtsvorschriften und Praktiken in dem Drittland, einschließlich etwaiger Vorschriften über die Offenlegung personenbezogener Daten oder Maßnahmen zur Genehmigung des Zugangs von Behörden, ihn daran hindern, seinen Verpflichtungen im Rahmen der Zertifizierung nachzukommen, und dass er den Exporteur über einschlägige Änderungen der Rechtsvorschriften oder Praktiken unterrichten wird.
2. Der Vertrag oder ein anderes Instrument muss auch Mechanismen vorsehen, die es ermöglichen, diese Verpflichtungen im Falle von Verstößen gegen die Vorschriften der Zertifizierung durch den für die Verarbeitung Verantwortlichen/Verarbeiter, der als Importeur handelt, durchzusetzen, insbesondere im Hinblick auf die Rechte der betroffenen Personen, deren Daten im Rahmen der Zertifizierung übermittelt werden.
3. Insbesondere sollte der Vertrag oder ein anderes Instrument Folgendes regeln:

* Das Recht der betroffenen Personen, deren Daten im Rahmen der Zertifizierung übermittelt werden, als Drittbegünstigte die Verpflichtungen durchzusetzen, die der zertifizierte Datenimporteur im Rahmen der Zertifizierung eingegangen ist.
* Die Frage der Haftung bei Verstößen gegen die Zertifizierungsvorschriften durch einen Datenimporteur mit einer Zertifizierung außerhalb des EWR. Betroffene Personen haben die Möglichkeit, im Falle eines Verstoßes gegen die Zertifizierungsvorschriften durch einen Datenimporteur mit einer Zertifizierung außerhalb des EWR unter Berufung auf ihr Recht als Drittbegünstigter eine Klage, auch auf Schadenersatz, gegen diese Stelle bei einem EWR-SA und einem EWR-Gericht des gewöhnlichen Aufenthalts der betroffenen Person einzureichen. Der Exporteur, der im Besitz einer Zertifizierung ist, muss die Entscheidung der betroffenen Person, dies zu tun, akzeptieren. Die betroffenen Personen haben auch die Möglichkeit, alle Ansprüche, die sich aus der Einhaltung der Zertifizierung durch den Importeur ergeben, gegen den Datenexporteur vor der internationalen Kontrollinstanz oder dem Gericht des Sitzes des Datenexporteurs oder des gewöhnlichen Aufenthalts der betroffenen Person geltend zu machen. Diese Haftung sollte unbeschadet der im Rahmen der Zertifizierung mit der Zertifizierungsstelle umzusetzenden Mechanismen gelten, die auch gegen die zertifizierten für die Verarbeitung Verantwortlichen/Verarbeiter in Übereinstimmung mit der Zertifizierung vorgehen kann, indem sie Abhilfemaßnahmen auferlegt. Der Datenimporteur und der Datenexporteur sollten auch akzeptieren, dass die betroffene Person unter den in Artikel 80 Absatz 1 der Datenschutz-Grundverordnung genannten Bedingungen durch eine gemeinnützige Einrichtung, Organisation oder Vereinigung vertreten werden kann.
* Das Recht des Exporteurs, als zertifizierter Datenimporteur die Bestimmungen der Zertifizierung als Drittbegünstigter gegenüber dem Datenimporteur durchzusetzen.
* Die Verpflichtung des Datenimporteurs, der über eine Zertifizierung verfügt, den Exporteur und die Aufsichtsbehörde des Datenexporteurs über alle Maßnahmen zu informieren, die von der Zertifizierungsstelle als Reaktion auf einen festgestellten Verstoß gegen die Zertifizierung durch denselben Datenimporteur ergriffen wurden.

# ANHANG

## BEISPIELE FÜR ZUSÄTZLICHE MASSNAHMEN, DIE DER IMPORTEUR DURCHFÜHREN MUSS, WENN DIE DURCHFUHR IN DEN GELTUNGSBEREICH DER ZERTIFIZIERUNG FÄLLT

Anwendungsfall 1: Datenspeicherung für Sicherungszwecke und andere Zwecke, die keinen Zugriff auf unverschlüsselte Daten erfordern

Es müssen Kriterien in Bezug auf die Verschlüsselungsstandards und die Sicherheit des Entschlüsselungsschlüssels, insbesondere Kriterien in Bezug auf die Rechtslage im Drittland, festgelegt werden. Wenn der Importeur gezwungen werden kann, Entschlüsselungscodes weiterzugeben, kann die zusätzliche Maßnahme nicht als wirksam angesehen werden18 .

Anwendungsfall 2: Übermittlung von pseudonymisierten Daten

Im Falle von pseudonymisierten Daten sind insbesondere Kriterien für die Sicherheit der zusätzlichen Informationen festzulegen, die erforderlich sind, um die übermittelten Daten einer bestimmten oder bestimmbaren Person zuordnen zu können:

* Kriterien bezüglich der Rechtslage im Drittland. Wenn der Importeur gezwungen werden kann, auf zusätzliche Daten zuzugreifen oder diese zu verwenden, um die Daten einer bestimmten oder bestimmbaren Person zuzuordnen, kann die Maßnahme nicht als wirksam angesehen werden19 .
* Kriterien für die Definition zusätzlicher Informationen, die Drittlandsbehörden zur Verfügung stehen und ausreichen könnten, um die Daten einer bestimmten oder bestimmbaren Person zuzuordnen.

Anwendungsfall 3: Verschlüsselung von Daten, um sie vor dem Zugriff der Behörden des Drittlandes des Importeurs zu schützen, wenn sie zwischen dem Exporteur und seinem Importeur übermittelt werden

Im Falle von verschlüsselten Daten sind alle Kriterien für die Sicherheit der Durchfuhr zu berücksichtigen. Wenn der Einführer gezwungen werden kann, kryptografische Schlüssel zur Entschlüsselung oder Authentifizierung weiterzugeben oder eine für die Durchfuhr verwendete Komponente so zu verändern, dass ihre Sicherheitseigenschaften untergraben werden, kann die zusätzliche Maßnahme nicht als wirksam angesehen werden20 .

Anwendungsfall 4: Geschützter Empfänger

Bei geschützten Empfängern müssen Kriterien für die Grenzen des Privilegs festgelegt werden. Die Datenverarbeitung muss sich innerhalb der Grenzen des gesetzlichen Privilegs bewegen. Dies gilt auch für die Verarbeitung durch (Unter-)Verarbeiter und Weiterübermittlungen, deren Empfänger ebenfalls privilegiert sein müssen21 .

## BEISPIELE FÜR ZUSÄTZLICHE MASSNAHMEN FÜR DEN FALL, DASS DIE DURCHFUHR NICHT DURCH DIE BESCHEINIGUNG ABGEDECKT IST UND DER EXPORTEUR DIESE SICHERSTELLEN MUSS

Anwendungsfall 2: Übermittlung von pseudonymisierten Daten

Es sind Kriterien für die den Drittlandsbehörden vorliegenden zusätzlichen Informationen anzugeben, die ausreichen könnten, um die Daten einer bestimmten oder bestimmbaren Person zuzuordnen.

Anwendungsfall 3: Verschlüsselung von Daten, um sie vor dem Zugriff der Behörden des Drittlandes des Importeurs zu schützen, wenn sie zwischen dem Exporteur und seinem Importeur übermittelt werden

Es sind Kriterien für die Vertrauenswürdigkeit der verwendeten Zertifizierungsstelle oder Infrastruktur für öffentliche Schlüssel, die Sicherheit der für die Authentifizierung oder Entschlüsselung verwendeten kryptografischen Schlüssel und die Zuverlässigkeit der Schlüsselverwaltung sowie die Verwendung ordnungsgemäß gewarteter Software ohne bekannte Schwachstellen anzugeben.

Wenn der Einführer gezwungen werden kann, kryptografische Schlüssel zur Entschlüsselung oder Authentifizierung offenzulegen oder eine für die Durchfuhr verwendete Komponente zu verändern, um ihre Sicherheitseigenschaften zu untergraben, kann die Maßnahme nicht als wirksam angesehen werden22 .

Anwendungsfall 4: Geschützter Empfänger

Bei geschützten Empfängern müssen Kriterien für die Grenzen des Privilegs festgelegt werden. Die Datenverarbeitung muss sich innerhalb der Grenzen des gesetzlichen Privilegs bewegen. Dies gilt auch für die Verarbeitung durch (Unter-)Verarbeiter und Weiterübermittlungen, deren Empfänger ebenfalls privilegiert sein müssen23 .