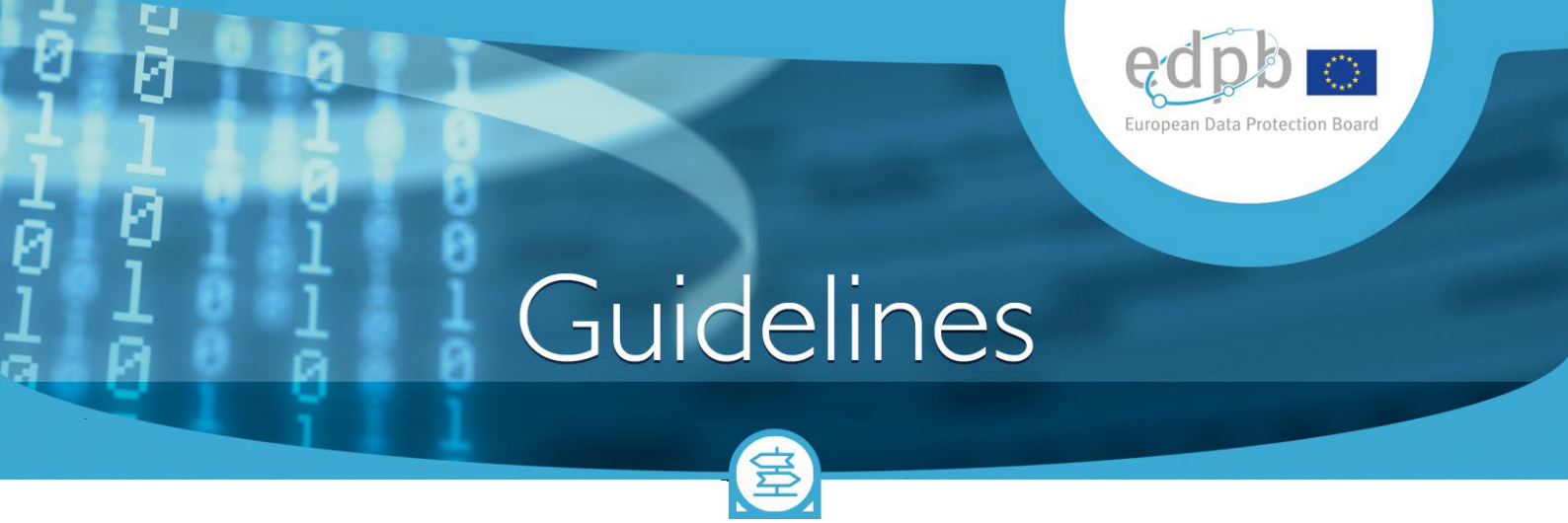


Leitlinien 7/2022 über die Zertifizierung als Instrument für Übermittlungen

Version 2.0

Angenommen am 14. Februar 2023

[Nicholas Vollmer:

Gemäß Artikel 46 (2f) kann ein Unternehmen im Drittland sich zertifizieren lassen und somit einen angemessenen Datenschutz nachweisen.

Auf der vorletzten Seite wird erwähnt, dass vielleicht die Rechtsvorschriften und Gepflogenheiten des Drittlandes auch eine Rolle spielen könnten. Im Juli 2022 kann man wohl sagen: Jegliche Zertifizierung für US-Unternehmen ist sinnlos, weil die US-Sicherheitsdienste nach Ansicht des EuGH zu weitgehende Zugriffsrechte haben.]

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

VERSIONSÜBERBLICK

Version 1.0	14. Juni 2022	Annahme der Leitlinien für die öffentliche Konsultation
Version 2.0	14. Februar 2023	Annahme der Leitlinien nach öffentlicher Konsultation

ZUSAMMENFASSUNG

In Artikel 46 der Datenschutz-Grundverordnung (im Folgenden „DSGVO“) heißt es, dass Datenexporteure geeignete Garantien für die Übermittlung von personenbezogenen Daten an ein Drittland oder eine internationale Organisation vorsehen müssen. In diesem Sinne werden mit der DSGVO die geeigneten Garantien, die von Datenexporteuren gemäß Artikel 46 für die Übermittlung von Daten an ein Drittland vorgesehen sind, erweitert, indem unter anderem die Zertifizierung als neues Verfahren für die Übermittlung eingeführt wird (Artikel 42 Absatz 2 und Artikel 46 Absatz 2 Buchstabe f DSGVO).

Diese Leitlinien dienen als Orientierungshilfe für die Anwendung von Artikel 46 Absatz 2 Buchstabe f DSGVO in Bezug auf Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen auf der Grundlage einer Zertifizierung. Das Dokument ist in vier Kapitel sowie einen Anhang aufgeteilt.

Im ersten Teil dieses Dokuments („ALLGEMEINES“) wird klargestellt, dass die Leitlinien die bereits bestehenden allgemeinen Leitlinien 1/2018 für die Zertifizierung ergänzen. Ferner wird auf spezifische Anforderungen des Kapitels V DSGVO im Zusammenhang mit der Verwendung der Zertifizierung als Übermittlungsinstrument eingegangen. Gemäß Artikel 44 DSGVO müssen bei jedweder Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation neben der Einhaltung des Kapitels V DSGVO die Bedingungen der sonstigen Bestimmungen der DSGVO eingehalten werden. Daher muss im ersten Schritt die Einhaltung der allgemeinen Vorschriften der DSGVO sichergestellt werden, woraufhin im zweiten Schritt die Bestimmungen des Kapitels V DSGVO eingehalten werden müssen. Es werden die beteiligten Akteure und ihre wesentlichen Rollen in diesem Kontext beschrieben, insbesondere die des Datenimporteurs, dem eine Zertifizierung erteilt wird, und des Datenexporteurs, der die Zertifizierung als Instrument für seine Übermittlungen verwendet (wobei er weiterhin verantwortlich für die rechtmäßige Datenverarbeitung ist). In diesem Zusammenhang kann die Zertifizierung auch Maßnahmen beinhalten, die Übermittlungsinstrumente zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten ergänzen. Der erste Teil der Leitlinien enthält außerdem Informationen über das Verfahren zum Erhalt einer Zertifizierung, die als Instrument für Übermittlungen verwendet werden kann.

Im zweiten Teil dieser Leitlinien („HINWEISE ZUR UMSETZUNG DER AKKREDITIERUNGSANFORDERUNGEN“) wird daran erinnert, dass die Anforderungen an die Akkreditierung einer Zertifizierungsstelle in der ISO 17065 enthalten sind und sich aus der Auslegung der Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 der Datenschutz-Grundverordnung und ihres Anhangs vor dem Hintergrund von Kapitel V DSGVO ergeben. In den vorliegenden Leitlinien werden jedoch einige Akkreditierungsanforderungen für Zertifizierungsstellen im Zusammenhang mit Übermittlungen näher erläutert.

Der dritte Teil dieser Leitlinien („SPEZIFISCHE ZERTIFIZIERUNGSKRITERIEN“) bietet Orientierung zu den Zertifizierungskriterien, die bereits in den Leitlinien 1/2018 aufgeführt sind. Zudem werden zusätzliche spezifische Kriterien festgelegt, die in ein Zertifizierungsverfahren, das als Instrument für Übermittlungen an ein Drittland vorgesehen ist, einbezogen werden sollten. Diese Kriterien umfassen die Bewertung der Rechtsvorschriften des Drittlands, die allgemeinen Pflichten von Exporteuren und Importeuren, Vorschriften zu Weiterübermittlungen, Rechtsschutz und Durchsetzung, das Verfahren und Vorgehen, wenn nationale Rechtsvorschriften und Gepflogenheiten die Einhaltung der im Rahmen der Zertifizierung eingegangenen Verpflichtungen verhindern, sowie den Umgang mit Anträgen von Drittstaatsbehörden auf Datenzugriff.

Im vierten Teil dieser Leitlinien („UMZUSETZENDE VERBINDLICHE UND DURCHSETZBARE VERPFLICHTUNGEN“) werden Elemente genannt, die im Rahmen der verbindlichen und durchsetzbaren Verpflichtungen geregelt werden sollten, die nicht unter die DSGVO fallende Verantwortliche oder Auftragsverarbeiter eingehen müssen, um geeignete Garantien für die Datenübermittlung an Drittländer vorzusehen. Diese Verpflichtungen, die in unterschiedlichen Instrumenten, darunter Verträgen, festgelegt sein können, umfassen insbesondere eine Zusicherung, dass der Importeur keinen Grund zu der Annahme hat, dass die für die betreffende Verarbeitung geltenden Rechtsvorschriften und Gepflogenheiten im Drittland, einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten, den Importeur an der Erfüllung seiner Pflichten gemäß dieser Zertifizierung hindern.

Der ANHANG dieser Leitlinien enthält einige Beispiele für zusätzliche Maßnahmen im Zusammenhang mit der Verwendung einer Zertifizierung als Instrument für Übermittlungen, die im Einklang mit den Maßnahmen stehen, die in Anhang 2 der Empfehlungen 01/2020 (Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten) aufgeführt sind. Die Beispiele sind derart gestaltet, dass sie auf kritische Situationen aufmerksam machen.

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 (Datenschutz-Grundverordnung, im Folgenden „DSGVO"),

gestützt auf das EWR-Abkommen, 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 —

HAT FOLGENDE LEITLINIEN ANGENOMMEN:

1 ALLGEMEINES

1.1 Zweck und Umfang

1. Dieses Dokument soll eine Orientierungshilfe für die Anwendung von Artikel 46 Absatz 2 Buchstabe f DSGVO in Bezug auf Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen auf der Grundlage einer Zertifizierung bieten. Der EDSA hat bereits allgemeine Leitlinien zur Zertifizierung[2] und zur Akkreditierung[3] im Rahmen der DSGVO veröffentlicht. In diesen neuen Leitlinien werden daher nur die spezifischen Aspekte in Bezug auf die Zertifizierung als Instrument für Übermittlungen berücksichtigt. Es wird näher ausgeführt, wie Artikel 46 Absatz 2 Buchstabe f und Artikel 42 Absatz 2 DSGVO anzuwenden sind, indem praktische Anleitungen diesbezüglich gegeben und neue Elemente mit Blick auf die bereits veröffentlichten Leitlinien eingeführt werden.

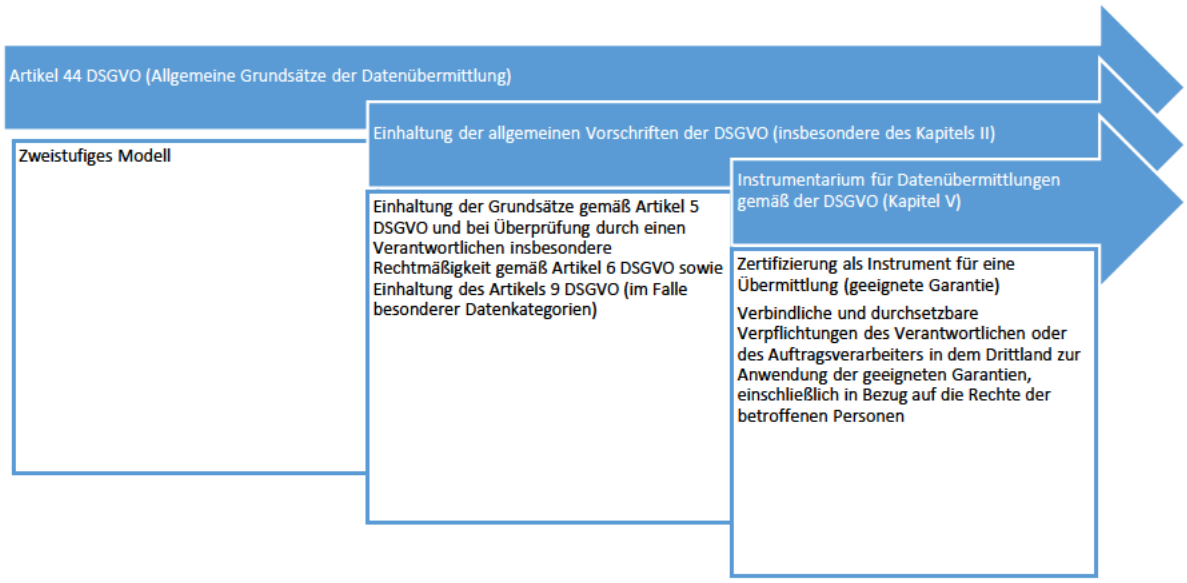
2. Der EDSA wird die Funktionsweise der vorliegenden Leitlinien vor dem Hintergrund der Erfahrungen mit ihrer Anwendung in der Praxis bewerten und weitere Leitlinien zur Klärung der Anwendung der unten dargelegten Elemente bereitstellen, einschließlich der Rolle einer Zertifizierungsvereinbarung in Bezug auf die verbindlichen und durchsetzbaren Verpflichtungen gemäß Artikel 46 Absatz 2 Buchstabe f DSGVO.

1.2 Allgemeine Vorschriften für internationale Datenübermittlungen

3. Gemäß Artikel 44 DSGVO müssen bei jedweder Übermittlung personenbezogener Daten an ein Drittland[4] oder eine internationale Organisation neben der Einhaltung des Kapitels V DSGVO die Bedingungen der sonstigen Bestimmungen der DSGVO eingehalten werden. Daher muss jede Übermittlung u. a. mit den Datenschutzgrundsätzen in Artikel 5 DSGVO in Übereinstimmung stehen, im Einklang mit Artikel 6 DSGVO rechtmäßig sein und im Falle besonderer Datenkategorien Artikel 9 DSGVO entsprechen. Folglich ist eine zweistufige Prüfung durchzuführen. Im ersten Schritt muss die Einhaltung der

[1] Soweit in diesem Dokument auf „Mitgliedstaaten" Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten" zu verstehen.
[2] Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679.
[3] Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 der Datenschutz-Grundverordnung (2016/679).
[4] Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, S. 4.

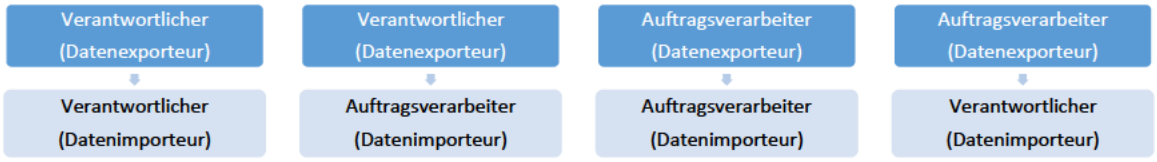
allgemeinen Vorschriften der DSGVO sichergestellt werden, woraufhin im zweiten Schritt die Bestimmungen des Kapitels V DSGVO eingehalten werden müssen.



4. In Artikel 46 der DSGVO heißt es: „Falls kein Beschluss nach Artikel 45 Absatz 3 vorliegt, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen." Gemäß Artikel 46 Absatz 2 Buchstabe f DSGVO können solche geeigneten Garantien in einem genehmigten Zertifizierungsverfahren zusammen mit verbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, bestehen.

5. Daher kann der Datenexporteur beschließen, sich auf die Zertifizierung eines Datenimporteurs zu stützen, um die Erfüllung seiner Pflichten nachzuweisen, beispielsweise gemäß Artikel 24 Absatz 3 oder Artikel 28 Absatz 5 DSGVO. Der Datenimporteur kann beschließen, eine Zertifizierung zu beantragen, um das Vorliegen geeigneter Garantien nachzuweisen.

6. Sowohl der Datenexporteur als auch der Datenimporteur können je nach Verarbeitung gemäß Kapitel V unterschiedliche Rollen einnehmen (beispielsweise als Verantwortlicher oder Auftragsverarbeiter)[5], die unterschiedliche Verantwortlichkeiten mit sich bringen:



[5] Siehe unten: HINWEISE ZUR UMSETZUNG DER ZERTIFIZIERUNGSKRITERIEN.

7. Abgesehen von der Verwendung einer Zertifizierung oder der sonstigen Übermittlungsinstrumente bzw. -verfahren gemäß den Artikeln 45 und 46 heißt es in Artikel 49 DSGVO, dass internationale Datenübermittlungen in einer begrenzten Zahl von bestimmten Fällen stattfinden können, wenn kein anderes in Kapitel V vorgesehenes Verfahren befolgt wird.[6] Wie in früheren Leitlinien des EDSA erläutert, sind die in Artikel 49 DSGVO vorgesehenen Ausnahmen jedoch restriktiv auszulegen und beziehen sich hauptsächlich auf Verarbeitungstätigkeiten, die gelegentlich und nicht wiederholt erfolgen.[7]

1.3 Welche Akteure sind beteiligt und welche Rolle spielen sie mit Blick auf die Zertifizierung als Instrument für Übermittlungen?

8. Der **Europäische Datenschutzausschuss (EDSA)** ist befugt, EWR-weite Zertifizierungskriterien zu genehmigen (Europäisches Datenschutzsiegel) und Stellungnahmen zu den Beschlussentwürfen der Aufsichtsbehörden über Zertifizierungskriterien und Akkreditierungsanforderungen der Zertifizierungsstellen abzugeben, um für Kohärenz zu sorgen. Er ist ferner dafür zuständig, alle Zertifizierungsverfahren und Datenschutzsiegel und -prüfzeichen in ein Register aufzunehmen und sie zu veröffentlichen.[8]

9. Die **Aufsichtsbehörden** genehmigen Zertifizierungskriterien, wenn es sich beim Zertifizierungsverfahren nicht um ein Europäisches Datenschutzsiegel handelt.[9] Sie können zudem Zertifizierungsstellen akkreditieren, Zertifizierungskriterien gestalten und Zertifizierungen erteilen, wenn dies in den nationalen Rechtsvorschriften ihres Mitgliedstaats festgelegt ist.[10]

10. Die **nationale Akkreditierungsstelle** kann Drittzertifizierungsstellen akkreditieren, indem sie die ISO 17065 und die zusätzlichen Akkreditierungsanforderungen der Aufsichtsbehörde anwendet, die mit Kapitel 2 dieser Leitlinien im Einklang stehen sollten. In einigen Mitgliedstaaten kann die Akkreditierung sowohl durch die zuständige Aufsichtsbehörde als auch durch eine nationale Akkreditierungsstelle oder durch beide erfolgen.

11. Der **Eigentümer des Zertifizierungsprogramms** ist eine Organisation, die Zertifizierungskriterien und methodische Anforderungen festgelegt hat, anhand derer die Konformität bewertet werden soll. Die Organisation, die die Bewertungen durchführt, kann dieselbe Organisation sein, die der Entwickler und Eigentümer des Zertifizierungsprogramms ist. Es kann jedoch auch der Fall sein, dass eine Organisation der Eigentümer des Zertifizierungsprogramms ist und eine oder mehrere andere die Bewertungen als Zertifizierungsstellen durchführen.

12. Je nach nationalem Recht kann alternativ statt der Aufsichtsbehörde eine wie zuvor beschrieben akkreditierte **Zertifizierungsstelle** Zertifizierungen erteilen.[11] Sie kann Zertifizierungskriterien gestalten und somit Eigentümer des Zertifizierungsprogramms sein (siehe Rn. 11). Sie muss eine Niederlassung im EWR haben, damit insbesondere die in Artikel 58 Absatz 2 Buchstabe f DSGVO verankerten Abhilfebefugnisse wirksam ausgeübt werden können. Die Zertifizierungsstelle kann jedoch Unteraufträge an lokale Sachverständige oder Niederlassungen außerhalb des EWR vergeben, die in ihrem Auftrag

---

[6] Weitere Informationen zu Artikel 49 und dessen Zusammenspiel mit Artikel 46 im Allgemeinen sind in den Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung (EU) 2016/679 enthalten.
[7] Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, S. 4 f.
[8] Artikel 42 Absatz 8 DSGVO.
[9] Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679, Unterkapitel 2.2.
[10] Artikel 42 Absatz 5 und Artikel 43 Absatz 1 DSGVO.
[11] Artikel 42 Absatz 5 DSGVO.

Prüfungstätigkeiten durchführen.[12] Allerdings ist es der Zertifizierungsstelle nicht erlaubt, die Entscheidung über die Gewährung oder Nichtgewährung einer Zertifizierung als Unterauftrag zu vergeben.

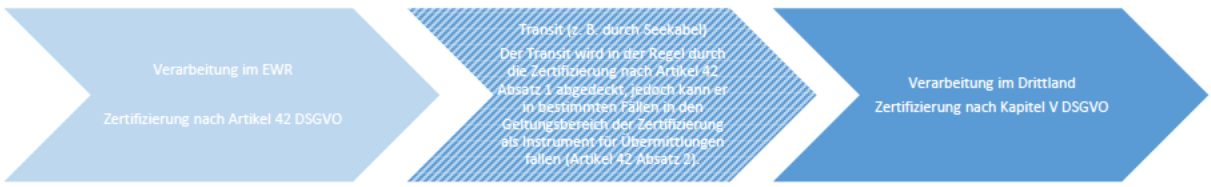
13. Der **Datenimporteur** ist die Stelle (Verantwortlicher oder Auftragsverarbeiter) im Drittland, die Daten von einem Datenexporteur erhält.

14. Der **Datenexporteur** ist die Stelle (Verantwortlicher oder Auftragsverarbeiter), die Daten aus dem EWR an einen Datenimporteur übermittelt. Der Datenexporteur muss die Einhaltung des Kapitels V sicherstellen.

1.4 Welchen Anwendungsbereich und Gegenstand hat eine Zertifizierung als Instrument für Übermittlungen?

15. Ein Zertifizierungsverfahren als Übermittlungsinstrument gemäß Artikel 42 Absatz 2 muss darauf abzielen, geeignete Garantien für die Verarbeitung personenbezogener Daten nach Maßgabe von Artikel 46 Absatz 2 Buchstabe f sicherzustellen. Mit der Zertifizierung wird nachgewiesen, dass Verantwortliche oder Auftragsverarbeiter, die außerhalb des EWR ansässig sind oder eine internationale Organisation darstellen und Daten von Verantwortlichen oder Auftragsverarbeitern im EWR erhalten, geeignete Garantien vorsehen, um den spezifischen Risiken im Zusammenhang mit der Übermittlung personenbezogener Daten zu begegnen.

16. Im Allgemeinen stellt die Übermittlung personenbezogener Daten aus einem Mitgliedstaat an ein Drittland als solche eine Verarbeitung personenbezogener Daten im Sinne von Artikel 4 Nummer 2 DSGVO dar, die im Hoheitsgebiet eines Mitgliedstaats vorgenommen wird[13] und daher nach Artikel 42 Absatz 1 DSGVO zertifizierbar ist. In einigen Fällen kann es je nach Kontext jedoch so sein, dass der Transit in den Geltungsbereich der Zertifizierung als Instrument für Übermittlungen fällt. Folglich sollte der Gegenstand der Zertifizierung – der mit dem Evaluierungsgegenstand (EVG) im Rahmen der Zertifizierung übereinstimmt[14] – generell in der Verarbeitung der Daten, die der Datenimporteur im Drittland aus dem EWR erhält, und dem Transit bestehen, wenn dieser unter der Kontrolle des Importeurs liegt.



17. Gegenstand einer Zertifizierung können einzelne Verarbeitungsvorgänge oder Vorgangsreihen sein. Diese können Steuerungsprozesse im Sinne von organisatorischen Maßnahmen beinhalten, die dementsprechend fester Bestandteil eines Verarbeitungsvorgangs sind.[15]

---

[12] Die Zertifizierungsstellen müssen ihre lokalen Sachverständigen im Einklang mit der ISO 17065 und den zusätzlichen von der Aufsichtsbehörde festgelegten Anforderungen an die Akkreditierung bewerten (Artikel 43 Absatz 1 Buchstabe b DSGVO).

[13] Urteil des Gerichtshofs (Große Kammer) vom 16. Juli 2020, Data Protection Commissioner/Facebook Ireland Ltd und Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559, Rn. 83.

[14] Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679, S. 19.

[15] Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679, S. 18 (z. B. Mechanismen zur Bearbeitung etwaiger Beschwerden).

18. Die beantragende Stelle wäre daher der Datenimporteur im Drittland in Bezug auf den Gegenstand der Zertifizierung.

1.5 Worin sollte die Rolle des Exporteurs bei der Verwendung einer Zertifizierung als Instrument für Übermittlungen bestehen?

19. Die Übermittlung durch den Datenexporteur als solche fällt generell unmittelbar unter die DSGVO. Das bedeutet, dass der Exporteur seine Pflichten gemäß der DSGVO erfüllen und insbesondere dafür Sorge tragen muss, dass die Daten gemäß Artikel 32 und Kapitel V sicher übermittelt werden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird (Artikel 44 DSGVO).[16] Dies kann selbstverständlich gemäß Artikel 42 Absatz 1 zertifiziert werden.

20. Darüber hinaus ist der Datenexporteur, der eine Zertifizierung als geeignete Garantie gemäß Artikel 46 Absatz 2 Buchstabe f DSGVO verwenden will, insbesondere verpflichtet, zu überprüfen, ob die Zertifizierung, auf die er sich stützen will, in Anbetracht der Eigenschaften der vorgesehenen Verarbeitung wirksam ist. Zu diesem Zweck muss der Datenexporteur prüfen, ob die erteilte Zertifizierung gültig und nicht abgelaufen ist, ob sie die spezifische durchzuführende Übermittlung abdeckt und ob der Transit personenbezogener Daten in den Geltungsbereich der Zertifizierung fällt sowie ob Weiterübermittlungen vorgesehen sind und eine angemessene Dokumentation zu ihnen vorgelegt wird. Zusätzlich muss der Exporteur kontrollieren, ob die Zertifizierungsstelle, die die Zertifizierung erteilt hat, von einer nationalen Akkreditierungsstelle oder einer zuständigen Aufsichtsbehörde akkreditiert wurde. Des Weiteren sollte der Datenexporteur im Falle von Übermittlungen von einem Verantwortlichen an einen Auftragsverarbeiter im Datenverarbeitungsvertrag gemäß Artikel 28 DSGVO oder im Falle von Übermittlungen von einem Verantwortlichen an einen Verantwortlichen in einem Datenaustauschvertrag mit dem Datenimporteur darauf hinweisen, dass er die Zertifizierung als Instrument für Übermittlungen verwendet.

21. Da der Exporteur dafür verantwortlich ist, dass sämtliche Bestimmungen in Kapitel V angewandt werden, muss er auch prüfen, ob die Zertifizierung, auf die er sich als Instrument für Übermittlungen stützen will, in Anbetracht der geltenden Rechtsvorschriften und Gepflogenheiten im Drittland, die für die betreffende Übermittlung von Bedeutung sind, wirksam ist. Für die Zwecke dieser Prüfung und als wichtiger Gesichtspunkt, um nachzuweisen, dass er seiner Verantwortung nachkommt, kann sich der Datenexporteur auf die von der Zertifizierungsstelle vorgenommene Überprüfung der vom Importeur dokumentierten Bewertung der Rechtsvorschriften und Gepflogenheiten im Drittland stützen.

22. Sollte die Bewertung des Importeurs gezeigt haben, dass dieser und/oder der Datenexporteur möglicherweise für im Rahmen der Zertifizierung vorgesehene zusätzliche Maßnahmen sorgen müssen, um ein der Sache nach gleichwertiges Schutzniveau wie im EWR sicherzustellen, muss der Datenexporteur

[16] Diesbezüglich ist darauf hinzuweisen, dass Artikel 44 DSGVO eindeutig vorsieht, dass eine Übermittlung nicht nur von einem Verantwortlichen, sondern auch von einem Auftragsverarbeiter durchgeführt werden kann. Daher gibt es Übermittlungssituationen, in denen ein Auftragsverarbeiter auf Weisung seines Verantwortlichen Daten an einen anderen Auftragsverarbeiter oder sogar an einen Verantwortlichen in einem Drittland sendet (Artikel 28 Absatz 3 Buchstabe a DSGVO). In diesen Fällen fungiert der Auftragsverarbeiter im Auftrag des Verantwortlichen als Datenexporteur und muss nach Maßgabe der Weisungen des Verantwortlichen sicherstellen, dass die Bestimmungen des Kapitels V bei der betreffenden Übermittlung eingehalten werden, darunter auch, dass ein geeignetes Übermittlungsinstrument verwendet wird. Da es sich bei der Datenübermittlung um eine im Auftrag des Verantwortlichen vorgenommene Verarbeitungstätigkeit handelt, trägt dieser ebenfalls eine Verantwortung und kann gemäß Kapitel V haftbar sein. Ferner muss er sicherstellen, dass der Auftragsverarbeiter hinreichend Garantien nach Artikel 28 bietet.

die zusätzlichen Maßnahmen des zertifizierten Datenimporteurs überprüfen und für sich selbst prüfen, ob er die vom Datenimporteur geforderten technischen und ggf. zusätzlichen Maßnahmen bieten kann.

23. Wenn die Vorgaben nicht erfüllt werden, muss der Datenexporteur vom Importeur eine Anpassung der zusätzlichen Maßnahmen verlangen oder diese angepassten Maßnahmen selbst festlegen.

1.6 Wie sieht das Verfahren für die Zertifizierung als Instrument für Übermittlungen aus?

24. Eine Zertifizierung ist freiwillig, muss im Falle einer Beantragung jedoch in einem transparenten Verfahren auf der Grundlage zwingender Vorschriften gewährt werden. Die DSGVO setzt großes Vertrauen in private Zertifizierungsverfahren als „regulierte Selbstregulierung". Entsprechend müssen diese Verfahren sicherstellen, dass die Zertifizierungen den inhaltlichen Anforderungen an geeignete Garantien gemäß Artikel 46 DSGVO genügen.

25. Die Zertifizierung muss deshalb auf der Bewertung von Zertifizierungskriterien entsprechend einer verbindlichen Prüfmethodik beruhen. Diese Kriterien werden, wie in Artikel 42 Absatz 5 DSGVO beschrieben, von den nationalen Aufsichtsbehörden oder vom EDSA genehmigt. Die Kriterien für die Zertifizierung umfassen Anforderungen in Bezug auf eine Bewertung der vom Datenimporteur vorgenommenen Verarbeitung, einschließlich Weiterübermittlungen, und des einschlägigen Rechtsrahmens des Drittlands, um zu vermeiden, dass die Vorschriften und Gepflogenheiten des Drittlands den Importeur daran hindern, seine Pflichten im Rahmen der Zertifizierung zu erfüllen.

26. Während des Zertifizierungsverfahrens wird der Evaluierungsgegenstand anhand von Zertifizierungskriterien von einer Zertifizierungsstelle überprüft, die durch die nationale Akkreditierungsstelle oder die zuständige Aufsichtsbehörde akkreditiert wurde[17].

27. Gemäß Artikel 43 Absatz 1 DSGVO erteilen oder verlängern Zertifizierungsstellen, die über das geeignete Fachwissen hinsichtlich des Datenschutzes verfügen, nach Unterrichtung der Aufsichtsbehörde – damit diese erforderlichenfalls von ihren Befugnissen gemäß Artikel 58 Absatz 2 Buchstabe h DSGVO Gebrauch machen kann – die Zertifizierung.

28. Nach Artikel 43 Absatz 5 DSGVO teilen die Zertifizierungsstellen den zuständigen Aufsichtsbehörden die Gründe für die Erteilung oder den Widerruf der beantragten Zertifizierung mit. Dies bedeutet nicht, dass die Zertifizierungsstelle für die Erteilung der Zertifizierung die Genehmigung der Aufsichtsbehörde benötigt. Die Zertifizierungsstelle überwacht die Einhaltung der Zertifizierungskriterien durch die betreffenden Stellen.

29. Die Aufsichtsbehörde verfügt über Abhilfebefugnisse, die es ihr gestatten, eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, eine gemäß den Artikel 42 und 43 DSGVO erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht mehr erfüllt werden.

[17] Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 der Datenschutz-Grundverordnung (2016/679), S. 9 f.

30. Ein Europäisches Datenschutzsiegel für internationale Datenübermittlungen kann zusammen mit verbindlichen und durchsetzbaren Verpflichtungen als Instrument für Übermittlungen an Drittländer dienen.[18]

31. Dennoch können Zertifizierungen, die als Instrument für Übermittlungen verwendbar sind, auch gemäß genehmigten nationalen Zertifizierungsprogrammen in den EWR-Staaten erteilt werden. Solche Zertifizierungen gelten nur für Übermittlungen an Drittländer durch Exporteure im EWR-Mitgliedstaat, in dem das Zertifizierungsprogramm genehmigt wurde, da die Zertifizierungen der verschiedenen EWR-Staaten nicht gegenseitig anerkannt werden. Den Aufsichtsbehörden in den einzelnen EWR-Staaten steht es jedoch frei, dasselbe Zertifizierungsverfahren für Übermittlungen zu genehmigen.[19]

2 HINWEISE ZUR UMSETZUNG DER AKKREDITIERUNGSANFORDERUNGEN

32. Die Anforderungen an die Akkreditierung einer Zertifizierungsstelle in Bezug auf Zertifizierungen als Instrument für Übermittlungen ergeben sich aus der ISO 17065 und der Auslegung der Leitlinien 4/201820 vor dem Hintergrund von Kapitel V, wie nachfolgend erläutert.

33. Nach Ansicht des EDSA 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 erlassen werden, bereits die erforderlichen spezifischen Anforderungen an die Akkreditierung einer Zertifizierungsstelle in Bezug auf Zertifizierungen als Instrument für Übermittlungen ab. In einem Übermittlungsszenario ist es jedoch erforderlich, einige Anforderungen im Hinblick auf Erläuterungen und die Auslegung zu verfeinern.

34. Was die Anforderungen an Ressourcen (siehe Anforderung 6 der Leitlinien 4/2018 – Anhang 1) anbelangt, stellt die Zertifizierungsstelle sicher, dass sie über die notwendigen Ressourcen verfügt, um überprüfen zu können, dass der Importeur, wie es nach den Zertifizierungskriterien geboten ist, die erforderliche Bewertung der Rechtslage und Gepflogenheiten der Drittländer, in denen er ansässig oder tätig ist, ordnungsgemäß und richtig vorgenommen hat.[21] Diese Bewertung sollte in Bezug auf die Verarbeitungstätigkeiten durchgeführt werden, die im Hinblick auf die geeigneten Garantien nach Artikel 46 DSGVO als Teil des EVG zertifiziert werden sollen, und umfasst gegebenenfalls die vom Importeur festgelegten und umgesetzten zusätzlichen Maßnahmen. Hierbei spielen auch beispielsweise ein

---

[18] Siehe Artikel 42 Absatz 5 DSGVO und Rn. 35 der Leitlinien 1/2018 des EDSA für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679.

[19] Wenn eine Aufsichtsbehörde im Rahmen einer nationalen Initiative bestimmte Zertifizierungskriterien annimmt und andere Länder anschließend unter

Berücksichtigung der Programmkriterien und geltenden spezifischen nationalen Vorschriften dieselben

Zertifizierungskriterien annehmen wollen, können sie dies tun, ohne dass eine Stellungnahme des EDSA nach Artikel 64 DSGVO abgegeben werden muss, und sich gemäß Artikel 64 Absatz 3 DSGVO auf die Stellungnahme stützen, die der ersten Aufsichtsbehörde vorgelegt wurde. Siehe diesbezüglich „Guidance – Addendum (Annex to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation)“, Rn. 66.

20 Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 der Datenschutz-Grundverordnung (2016/679), einschließlich ihres Anhangs.

[21] Siehe Rn. 12.

umfangreiches Wissen über die einschlägigen lokalen Rechtsvorschriften und Gepflogenheiten sowie angemessene Sprachkenntnisse im Zusammenhang mit dem Drittland/den Drittländern eine Rolle.

35. Was die Anforderungen an Prozesse (siehe Anforderung 7 der Leitlinien 4/2018 – Anhang 1) betrifft, stellt die Zertifizierungsstelle sicher, dass das Zertifizierungsverfahren durch mögliche Prüfungen vor Ort ergänzt werden kann, dass es in Bezug auf die spätere Verarbeitung in dem Drittland/den Drittländern durchgeführt wird und dass die Bewertung auch die praktische Umsetzung der bestehenden Rechtsvorschriften und politischen Maßnahmen in dem Drittland/den Drittländern abdeckt.

36. Im Zusammenhang mit den Anforderungen in Bezug auf Änderungen, die sich auf die Zertifizierung auswirken (siehe Anforderung 7.10 der Leitlinien 4/2018 – Anhang 1), überwacht die Zertifizierungsstelle Änderungen der Rechtsvorschriften und/oder der Rechtsprechung in den Drittländern, die sich möglicherweise auf die in den Bereich des EVG fallende Verarbeitung auswirken.

3 SPEZIFISCHE ZERTIFIZIERUNGSKRITERIEN

37. Hinsichtlich der Betrachtung der spezifischen Zertifizierungskriterien beruhen diese Leitlinien auf den Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679 (Version 3.0), dem entsprechenden Anhang 2 über die Überprüfung und Bewertung von Zertifizierungskriterien nach Artikel 42 Absatz 5 und dem Addendum zum Leitfaden zur Bewertung von Zertifizierungskriterien.

38. Nach Ansicht des EDSA decken die Zertifizierungskriterien, die auf der Grundlage des Anhangs 2 der Leitlinien 1/2018 und des Addendums zum Leitfaden zur Bewertung von Zertifizierungskriterien erstellt werden, bereits den Großteil der Zertifizierungskriterien ab, die bei der Ausarbeitung eines Zertifizierungsprogramms zur Verwendung als Instrument für Übermittlungen berücksichtigt werden müssen. Es könnte jedoch erforderlich sein, einige dieser bestehenden Kriterien zu präzisieren, um sie mit Blick auf ein bestimmtes Übermittlungsszenario anzupassen (siehe Unterkapitel 3.1). Darüber hinaus könnte es erforderlich sein, zusätzliche Kriterien für die Zwecke der Anwendung geeigneter Garantien festzulegen, einschließlich in Bezug auf die Rechte der betroffenen Personen (siehe Unterkapitel 3.2).

3.1 HINWEISE ZUR UMSETZUNG DER ZERTIFIZIERUNGSKRITERIEN

39. Der Anwendungsbereich des Zertifizierungsverfahrens und der Evaluierungsgegenstand (EVG) sollten in den entsprechenden Unterlagen eindeutig beschrieben werden (siehe Anhang 2 Kapitel 2 Buchstabe a), einschließlich in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder die Frage, ob auch der Transit der Daten in den Anwendungsbereich fällt.

40. In den einschlägigen Unterlagen zum Anwendungsbereich des Zertifizierungsverfahrens und EVG sollte konkret beschrieben werden, für welche Art von Stelle (z. B. Verantwortlicher und/oder Auftragsverarbeiter) das Zertifizierungsverfahren gilt (siehe Anhang 2 Kapitel 2 Buchstabe b).

41. Die Zertifizierungskriterien sollten es erforderlich machen, dass der EVG konkret definiert wird (siehe Anhang 2 Kapitel 2 Buchstabe f), um Missverständnisse zu vermeiden. Dies sollte zumindest Folgendes umfassen:

42. die Verarbeitungsvorgänge, auch für den Fall, dass Weiterübermittlungen vorgesehen sind,

    a) den Zweck,

    b) die Art der Stelle (z. B. Verantwortlicher und/oder Auftragsverarbeiter),

c) die Art der übermittelten Daten, wobei berücksichtigt wird, ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 DSGVO betroffen sind,

d) die Kategorien betroffener Personen,

e) die Länder, in denen die Datenverarbeitung stattfindet.

43. In Bezug auf Transparenz und die Rechte der betroffenen Person (siehe Anhang 2 Kapitel 8) sollten die Zertifizierungskriterien vorsehen, dass

a) den betroffenen Personen Informationen zu den Verarbeitungstätigkeiten übermittelt werden, gegebenenfalls einschließlich in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation (siehe die Artikel 12, 13 und 14 DSGVO),

b) die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung, Mitteilung im Zusammenhang mit der Berichtigung, Löschung oder Einschränkung, Widerspruch gegen die Verarbeitung sowie ihr Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung, einschließlich Profiling, beruhenden Entscheidung unterworfen zu werden, gewährleistet werden und den in den Artikeln 15 bis 19, 21 und 22 DSGVO vorgesehenen Rechten im Wesentlichen gleichwertig sind,

c) der Datenimporteur, der eine Zertifizierung besitzt, ein geeignetes Verfahren zur Bearbeitung etwaiger Beschwerden einrichtet, um die wirksame Umsetzung der Rechte betroffener Personen sicherzustellen,

d) geprüft wird, ob und in welchem Maße diese Rechte für die betroffenen Personen im entsprechenden Drittland durchsetzbar sind und welche zusätzlichen geeigneten Maßnahmen zur Durchsetzung möglicherweise ergriffen werden müssen, wobei beispielsweise vom Importeur verlangt werden kann, dass er sich in Verfahren, die darauf abzielen, die Einhaltung dieser Rechte sicherzustellen, der Zuständigkeit der für den/die Exporteur(e) zuständigen Aufsichtsbehörde unterwirft und mit dieser kooperiert und insbesondere zustimmt, auf Anfragen zu antworten, sich Prüfungen zu unterziehen und die Maßnahmen der genannten Aufsichtsbehörde einzuhalten, einschließlich Korrektur- und Entschädigungsmaßnahmen.

44. Was technische und organisatorische Schutzvorkehrungen anbelangt, sollten die Zertifizierungskriterien vorschreiben (siehe Anhang 2 Kapitel 10 Buchstabe q), dass der Importeur den Exporteur und – falls der Importeur als Verantwortlicher handelt – die für den/die Datenexporteur(e) zuständige Aufsichtsbehörde im EWR über eine Verletzung des Datenschutzes unterrichtet und die betroffene Person im Einklang mit den Anforderungen des Artikels 34 DSGVO von der Verletzung benachrichtigt, wenn diese voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der Person zur Folge hat.

3.2 ZUSÄTZLICHE SPEZIFISCHE ZERTIFIZIERUNGSKRITERIEN

45. Der EDSA ist der Ansicht, dass Zertifizierungsverfahren, die als Instrument für Übermittlungen an Drittländer dienen, in Anbetracht der festgelegten Garantien für andere Übermittlungsinstrumente nach Artikel 46 DSGVO (etwa verbindliche interne Datenschutzvorschriften oder Verhaltensregeln), zur Sicherstellung eines einheitlichen Schutzniveaus und unter Berücksichtigung des Schrems-II-Urteils des EuGH auch die nachfolgend aufgeführten Kriterien umfassen sollten:

1. Bewertung der Rechtsvorschriften des Drittlands

a) Schreiben die Kriterien vor, dass der Importeur die Vorschriften und Gepflogenheiten des Drittlands, in dem er tätig ist, bewertet und prüft, ob sie ihn daran hindern, seine Verpflichtungen im Rahmen der Zertifizierung zu erfüllen?

b) Sehen die Kriterien vor, dass der Importeur die Bewertung der Vorschriften und Gepflogenheiten des Drittlands, in dem er tätig ist, dokumentiert und die Unterlagen bereithält, damit sie der Zertifizierungsstelle und auf Verlangen der für den Datenexporteur zuständigen Aufsichtsbehörde im EWR und dem Datenexporteur zur Verfügung stehen?

c) Machen es die Kriterien erforderlich, dass der Importeur unter Berücksichtigung der „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten“ die notwendigen organisatorischen und technischen Maßnahmen festlegt und umsetzt, um die geeigneten Garantien nach Artikel 46 DSGVO zu bieten?

d) Sehen die Kriterien vor, dass der Importeur die organisatorischen und technischen Maßnahmen dokumentiert, die er tatsächlich umsetzt, um die geeigneten Garantien nach Artikel 46 DSGVO zu bieten, und die Unterlagen bereithält, damit sie der Zertifizierungsstelle und auf Verlangen den zuständigen Datenschutzbehörden und dem Datenexporteur zur Verfügung stehen?

e) Machen es die Kriterien erforderlich, dass der Importeur unter Berücksichtigung der „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten“ die organisatorischen und technischen Maßnahmen festlegt und umsetzt, um die Sicherheit der übermittelten personenbezogenen Daten sicherzustellen, wenn der Transit in den Geltungsbereich der Zertifizierung als Instrument für Übermittlungen fällt?

f) Verlangen die Kriterien eine Zusicherung für die Zertifizierungsstelle und den Exporteur, dass der Importeur keinen Grund zu der Annahme hat, dass die für ihn geltenden Rechtsvorschriften und Gepflogenheiten ihn möglicherweise daran hindern, seine Pflichten im Rahmen der Zertifizierung zu erfüllen?

2. Allgemeine Pflichten von Exporteuren und Importeuren

a) Ist es den Kriterien zufolge erforderlich, in einer vertraglichen Vereinbarung (z. B. in einem bestehenden Dienstleistungsvertrag) zwischen einem Exporteur und einem Importeur die spezifische Übermittlung, für die die Zertifizierung gilt, zu beschreiben und die Rechte der betroffenen Personen als Drittbegünstigte anzuerkennen?

b) Müssen diese vertraglichen Vereinbarungen oder Instrumente, sofern die Kriterien bestimmte Inhalte für sie vorsehen und eine Vorlage bereitgestellt wird, den Kriterien zufolge auch Gegenstand einer Evaluierung sein?

3. Vorschriften zu Weiterübermittlungen

a) Setzen die Kriterien voraus, dass Weiterübermittlungen bestimmten Garantien im Einklang mit den Anforderungen des Kapitels V DSGVO unterliegen, um sicherzustellen, dass das im EWR geltende Schutzniveau nicht untergraben wird, und sehen die Kriterien vor, dass entsprechende Unterlagen bereitgehalten werden, damit sie der Zertifizierungsstelle, der für den Datenexporteur zuständigen Aufsichtsbehörde im EWR und dem Datenexporteur auf Verlangen zur Verfügung stehen?

4. Rechtsschutz und Durchsetzung

a) Sehen die Kriterien vor, dass eine betroffene Person ihre Rechte als Drittbegünstigte gegenüber dem Datenimporteur, einschließlich einer internationalen Organisation, vor einem Gericht des EWR an ihrem gewöhnlichen Aufenthaltsort durchsetzen kann, auch im Zusammenhang mit Schadenersatz für die betroffene Person aufgrund einer Nichteinhaltung des betreffenden Zertifizierungsprogramms durch den Importeur?
b) Ermöglichen die Kriterien es, angemessen zu beurteilen, ob ein Importeur aufgrund einer Nichteinhaltung des betreffenden Zertifizierungsprogramms im EWR für den Schaden haften muss, der der betroffenen Person entstanden ist?
c) Schreiben die Kriterien vor, dass die betroffene Person eine Beschwerde gegen den Importeur bei einer Aufsichtsbehörde im EWR einlegen kann, insbesondere bei einer Aufsichtsbehörde, die sich im EWR-Staat befindet, in dem die Person ihren gewöhnlichen Aufenthaltsort oder Arbeitsplatz hat, oder die für den/die Datenexporteur(e) zuständig ist?
d) Verlangen die Kriterien, dass der Importeur mit der für den/die Datenexporteur(e) zuständigen Aufsichtsbehörde im EWR kooperiert und zustimmt, von ihr überprüft und kontrolliert zu werden, ihre Ratschläge zu berücksichtigen und sich an ihre Entscheidungen zu halten?

5. Verfahren und Vorgehen, wenn nationale Rechtsvorschriften die Einhaltung der im Rahmen der Zertifizierung eingegangenen Verpflichtungen verhindern

a) Sehen die Kriterien vor, dass sich der Datenimporteur, der sich in einem Drittland befindet oder eine internationale Organisation ist, dazu verpflichtet, die Zertifizierungsstelle und den Datenexporteur unverzüglich zu unterrichten, wenn er Grund zu der Annahme hat, dass Änderungen der für ihn geltenden Rechtsvorschriften und Gepflogenheiten ihn möglicherweise daran hindern, seine Pflichten im Rahmen der Zertifizierung zu erfüllen, sodass der Datenexporteur entscheiden kann, ob er die Übermittlungen umgehend beendet?
b) Erfordern die Kriterien eine Beschreibung der zu unternehmenden Schritte (darunter die Benachrichtigung des Exporteurs im EWR und die Ergreifung geeigneter zusätzlicher Maßnahmen) für den Fall, dass der Datenimporteur Kenntnis von Rechtsvorschriften oder Gepflogenheiten eines Drittlands erhält, die eine Erfüllung der Pflichten im Rahmen der Zertifizierung verhindern, sowie eine Beschreibung der zu treffenden Maßnahmen im Falle von Informationsersuchen von Drittstaatsbehörden (darunter die verpflichtende Überprüfung und gegebenenfalls Anfechtung der Rechtmäßigkeit des Ersuchens sowie die verpflichtende Beschränkung der offengelegten Informationen auf ein Mindestmaß)?

6. Umgang mit Anträgen von Drittstaatsbehörden auf Datenzugriff

a) Ist in den Kriterien vorgesehen, dass der Datenimporteur den Datenexporteur im Falle von Anträgen von Drittstaatsbehörden auf Datenzugriff unverzüglich unterrichtet und geeignete zusätzliche Maßnahmen ergreift?
b) Verbieten die Kriterien Übermittlungen infolge von unverhältnismäßigen Anträgen von Drittstaatsbehörden auf Datenzugriff, insbesondere von Anträgen, die massive und willkürliche Übermittlungen personenbezogener Daten verlangen?

7. Zusätzliche Garantien in Bezug auf den Exporteur

46. Schreiben die Kriterien vor, dass der Datenimporteur – wenn dies vorgesehen ist – unter Berücksichtigung der Empfehlungen 01/2020 des EDSA und der Anwendungsfälle sowie auch mittels verbindlicher Anforderungen in dieser Hinsicht für den Datenexporteur sicherstellt, dass den von ihm festgelegten zusätzlichen Maßnahmen entsprechende zusätzliche Maßnahmen seitens des Datenexporteurs gegenüberstehen, um für eine wirksame Umsetzung der zusätzlichen Maßnahmen des Importeurs zu sorgen?

4 UMZUSETZENDE VERBINDLICHE UND DURCHSETZBARE VERPFLICHTUNGEN

47. Nach Artikel 42 Absatz 2 DSGVO müssen Verantwortliche und Auftragsverarbeiter, die nicht unter die DSGVO fallen, aber ein für Übermittlungen vorgesehenes Zertifizierungsverfahren einhalten, zusätzlich mittels vertraglicher oder sonstiger rechtlich bindender Instrumente[22] verbindliche und durchsetzbare Verpflichtungen eingehen, die im Zertifizierungsverfahren vorgesehenen geeigneten Garantien anzuwenden, auch im Hinblick auf die Rechte der betroffenen Personen.

48. Wie in der DSGVO festgelegt, können solche Verpflichtungen durch einen Vertrag eingegangen werden, was wohl die einfachste Lösung darstellt. Es könnten auch andere Instrumente eingesetzt werden, unter der Voraussetzung, dass die Verantwortlichen/Auftragsverarbeiter, die das Zertifizierungsverfahren einhalten, den verbindlichen und durchsetzbaren Charakter dieser anderen Instrumente nachweisen können.

49. In jedem Fall muss der verbindliche und durchsetzbare Charakter nach dem EU-Recht sichergestellt sein, und die Verpflichtungen sollten auch für die betroffenen Personen als Drittbegünstigte verbindlich und durchsetzbar sein.

50. Eine einfache Möglichkeit wäre es, die verbindlichen und durchsetzbaren Verpflichtungen in den Vertrag zwischen dem Datenexporteur und dem Datenimporteur aufzunehmen. In der Praxis könnten die Parteien einen bestehenden Vertrag (z. B. eine Dienstleistungsvereinbarung zwischen dem Exporteur und dem Datenimporteur, den Datenverarbeitungsvertrag gemäß Artikel 28 DSGVO zwischen dem Verantwortlichen und dem Auftragsverarbeiter oder eine Datenaustauschvereinbarung zwischen verschiedenen Verantwortlichen) verwenden, in den die verbindlichen und durchsetzbaren Verpflichtungen aufgenommen werden. Diese Verpflichtungen sollten sich von anderen Klauseln eindeutig unterscheiden. Eine weitere Möglichkeit besteht darin, einen separaten Vertrag aufzusetzen, indem beispielsweise zu dem für Übermittlungen vorgesehenen Zertifizierungsverfahren ein Standardvertrag hinzugefügt wird, der dann von den Verantwortlichen/Auftragsverarbeitern im Drittland und allen Exporteuren unterzeichnet werden muss.

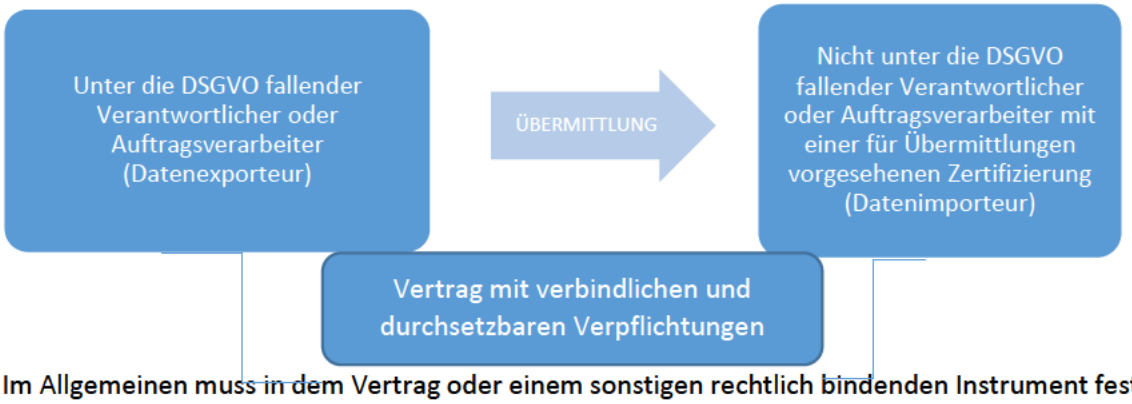
51. Es sollte die Möglichkeit bestehen, je nach Situation die am besten geeignete Option zu wählen.

52. Wird das Zertifizierungsverfahren für Übermittlungen und Weiterübermittlungen durch einen Auftragsverarbeiter an Unterauftragsverarbeiter verwendet, sollte auch in der zwischen dem Auftragsver-

[22] Dieses rechtlich bindende Instrument darf kein anderes Instrument gemäß Kapitel V sein (wie beispielsweise die Standardvertragsklauseln), da die in Artikel 46 Absatz 2 Buchstabe f genannten verbindlichen und durchsetzbaren Verpflichtungen so gestaltet werden müssen, dass sie sicherstellen, dass der Importeur die Zertifizierungskriterien einhält.

arbeiter und dem Verantwortlichen unterzeichneten Vereinbarung ein Verweis auf das Zertifizierungsverfahren und das Instrument, das die durchsetzbaren und verbindlichen Verpflichtungen vorsieht, enthalten sein.

Beispiel für verbindliche und durchsetzbare Verpflichtungen im Vertrag zwischen dem Datenexporteur und dem Datenimporteur:



53. Im Allgemeinen muss in dem Vertrag oder einem sonstigen rechtlich bindenden Instrument festgelegt sein, dass der Verantwortliche/Auftragsverarbeiter, der eine Zertifizierung besitzt und als Importeur fungiert, sich dazu verpflichtet, die in der Zertifizierung festgelegten Regeln für Übermittlungen bei der Verarbeitung der entsprechenden Daten aus dem EWR einzuhalten, und zusichert, dass er keinen Grund zu der Annahme hat, dass die für die betreffende Verarbeitung relevanten Rechtsvorschriften und Gepflogenheiten im Drittland, einschließlich etwaiger Vorschriften zur Offenlegung personenbezogener Daten oder Maßnahmen zur Genehmigung des Zugriffs für Behörden, ihn daran hindern, seine Verpflichtungen im Rahmen der Zertifizierung zu erfüllen, und dass er den Exporteur über etwaige wichtige Änderungen der Rechtsvorschriften oder Gepflogenheiten in dieser Hinsicht unterrichtet.

54. Der Vertrag oder ein anderes Instrument muss auch Mechanismen enthalten, die es ermöglichen, solche Verpflichtungen im Falle einer Nichteinhaltung der Regeln gemäß der Zertifizierung durch den als Importeur handelnden Verantwortlichen/Auftragsverarbeiter durchzusetzen, insbesondere im Hinblick auf die Rechte der betroffenen Personen, deren Daten im Rahmen der Zertifizierung übermittelt werden.

55. In dem Vertrag oder in einem anderen Instrument sollte insbesondere Folgendes thematisiert werden:

- das Bestehen eines Rechts für betroffene Personen, deren Daten im Rahmen der Zertifizierung übermittelt werden, die vom zertifizierten Datenimporteur im Rahmen der Zertifizierung eingegangenen Verpflichtungen als Drittbegünstigte durchzusetzen;

- die Frage der Haftung im Falle einer Nichteinhaltung der Regeln gemäß der Zertifizierung durch einen Datenimporteur mit Sitz außerhalb des EWR, der eine Zertifizierung besitzt; betroffene Personen haben im Falle einer Nichteinhaltung der Regeln gemäß der Zertifizierung durch einen Datenimporteur mit Sitz außerhalb des EWR, der eine Zertifizierung besitzt, die Möglichkeit, unter Berufung auf ihr Recht als Drittbegünstigte Ansprüche, auch auf Schadenersatz, gegen die betreffende Stelle bei einer Aufsichtsbehörde im EWR und einem Gericht des EWR am gewöhnlichen Aufenthaltsort der betroffenen Person geltend zu machen; der eine Zertifizierung besitzende Importeur akzeptiert die Entscheidung der betroffenen Person, so zu verfahren; die betroffenen Personen haben ferner in dem Fall, dass eine Nichteinhaltung durch den Importeur zur Haftung des Datenexporteurs führen könnte, die Möglichkeit, einen Anspruch gegen den Datenexporteur vor der Aufsichtsbehörde oder dem Gericht am Sitz des Datenexporteurs oder am

gewöhnlichen Aufenthaltsort der betroffenen Person geltend zu machen;23 der Datenimporteur und der Datenexporteur sollten auch akzeptieren, dass die betroffene Person unter den in Artikel 80 Absatz 1 DSGVO genannten Bedingungen durch eine Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht vertreten werden kann;

- das Bestehen eines Rechts für den Exporteur, die Regeln gemäß der Zertifizierung als Drittbegünstigter gegenüber dem Datenimporteur, der eine Zertifizierung besitzt, durchzusetzen;
- das Bestehen einer Verpflichtung des Datenimporteurs, der eine Zertifizierung besitzt, den Exporteur und die Aufsichtsbehörde des Datenexporteurs über jegliche Maßnahmen zu informieren, mit denen die Zertifizierungsstelle auf eine festgestellte Nichteinhaltung der Regeln der Zertifizierung durch den betreffenden Datenimporteur reagiert.

[23] Diese Haftung sollte unbeschadet der Verfahren gelten, die im Rahmen der Zertifizierung mit der Zertifizierungsstelle anzuwenden sind, die in Übereinstimmung mit der Zertifizierung auch Maßnahmen gegen die zertifizierten Verantwortlichen/Auftragsverarbeiter ergreifen und Abhilfemaßnahmen verhängen kann.

ANHANG

A. BEISPIELE FÜR VOM IMPORTEUR UMZUSETZENDE ZUSÄTZLICHE MAßNAHMEN, FALLS DER TRANSIT IN DEN ANWENDUNGSBEREICH DER ZERTIFIZIERUNG FÄLLT

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

Es müssen Kriterien in Bezug auf die Verschlüsselungsstandards und die Sicherheit des Entschlüsselungsschlüssels, insbesondere Kriterien bezüglich der Rechtslage im Drittland, festgelegt werden. Wenn der Importeur gezwungen werden kann, Entschlüsselungsschlüssel weiterzugeben, so kann die zusätzliche Maßnahme nicht als effektiv betrachtet werden.[24]

Anwendungsfall 2: Übermittlung pseudonymisierter Daten

Im Falle pseudonymisierter Daten werden Kriterien in Bezug auf die Sicherheit der zusätzlichen Informationen festgelegt, die notwendig sind, um die übermittelten Daten einer identifizierten oder identifizierbaren Person zuzuordnen. Insbesondere werden folgende Kriterien festgelegt:

– Kriterien bezüglich der Rechtslage im Drittland; wenn der Importeur gezwungen werden kann, auf zusätzliche Daten zuzugreifen oder diese zu verwenden, um die Daten einer identifizierten oder identifizierbaren Person zuzuordnen, so kann die Maßnahme nicht als effektiv betrachtet werden;[25]

– Kriterien in Bezug auf die Definition zusätzlicher Informationen, die Drittstaatsbehörden zur Verfügung stehen und ausreichen könnten, um die Daten einer identifizierten oder identifizierbaren Person zuzuordnen.

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

Im Falle verschlüsselter Daten müssen Kriterien für die Sicherheit des Transits einbezogen werden. Wenn der Importeur gezwungen werden kann, kryptografische Schlüssel für die Entschlüsselung oder Authentifizierung weiterzugeben oder eine für den Transit verwendete Komponente so zu verändern, dass ihre Sicherheitseigenschaften beeinträchtigt werden, so kann die zusätzliche Maßnahme nicht als effektiv betrachtet werden.[26]

Anwendungsfall 4: Geschützter Empfänger

Im Falle geschützter Empfänger müssen Kriterien für den Rahmen der Geheimhaltung bestimmt werden. Die Datenverarbeitung muss innerhalb des Rahmens der rechtlichen Geheimhaltung erfolgen.

---

[24] Anhang 2, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Version 2.0, Anwendungsfall 1: Datenspeicherung zu Backup- und anderen Zwecken, die nicht den Zugang zu unverschlüsselten Daten erfordern, Rn. 85. https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_de.pdf

[25] Siehe ebd., Rn. 86–89.

[26] Siehe ebd., Rn. 90.

Dies gilt auch für die Verarbeitung durch (Unter-)Auftragsverarbeiter und für Weiterübermittlungen, bei denen die Empfänger ebenfalls geschützt sein müssen.[27]

B. BEISPIELE FÜR VOM EXPORTEUR SICHERZUSTELLENDE ZUSÄTZLICHE MAßNAHMEN, FALLS DER TRANSIT NICHT VON DER ZERTIFIZIERUNG ABGEDECKT WIRD

Anwendungsfall 2: Übermittlung pseudonymisierter Daten

Es müssen Kriterien in Bezug auf die zusätzlichen Informationen geschaffen werden, die den Drittstaatsbehörden zur Verfügung stehen und ausreichen könnten, um die Daten einer identifizierten oder identifizierbaren Person zuzuordnen.

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

Notwendig sind Kriterien in Bezug auf die Vertrauenswürdigkeit der gewählten Zertifizierungsstelle oder Infrastruktur für öffentliche Schlüssel, die Sicherheit der für die Authentifizierung oder Entschlüsselung verwendeten kryptografischen Schlüssel, die Zuverlässigkeit des Schlüsselmanagements und die Verwendung ordnungsgemäß gewarteter Software ohne bekannte Schwachstellen.

Wenn der Importeur gezwungen werden kann, für die Entschlüsselung oder Authentifizierung geeignete kryptografische Schlüssel offenzulegen oder eine für den Transit verwendete Komponente zu verändern, um ihre Sicherheitseigenschaften zu beeinträchtigen, so kann die Maßnahme nicht als effektiv betrachtet werden.[28]

Anwendungsfall 4: Geschützter Empfänger

Im Falle geschützter Empfänger müssen Kriterien für den Rahmen der Geheimhaltung bestimmt werden. Die Datenverarbeitung muss innerhalb des Rahmens der rechtlichen Geheimhaltung erfolgen. Dies gilt auch für die Verarbeitung durch (Unter-)Auftragsverarbeiter und für Weiterübermittlungen, bei denen die Empfänger ebenfalls geschützt sein müssen.[29]

[27] Siehe ebd., Rn. 91.
[28] Siehe ebd., Rn. 90.
[29] Siehe ebd., Rn. 91.