Stellungnahme 15/2026 zu den Europrivacy-Zertifizierungskriterien im Hinblick auf ihre Genehmigung durch den Ausschuss als Europäisches Datenschutzsiegel zur Verwendung als Übermittlungsgrundlage gemäß den Artikeln 42 und 46 DSGVO

Angenommen am 15 April 2026

Inhaltsverzeichnis

Der Europäische Datenschutzausschuss –

gestützt auf Artikel 63, Artikel 64 Absatz 2, Artikel 42 und Artikel 46 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (im Folgenden „DSGVO"),

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

gestützt auf die Artikel 10 und 22 seiner Geschäftsordnung,

1 Die Mitgliedstaaten, die Aufsichtsbehörden, der Europäische Datenschutzausschuss (im Folgenden „EDSA" oder „Ausschuss") und die Europäische Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzrechtlichen Zertifizierungsverfahren (im Folgenden „Zertifizierungsverfahren") und von Datenschutzsiegeln und -prüfzeichen, die dazu dienen nachzuweisen, dass die DSGVO bei Verarbeitungsvorgängen von Verantwortlichen und Auftragsverarbeitern eingehalten wird, wobei den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen Rechnung zu tragen ist[2]. Darüber hinaus kann die Einführung von Zertifizierungsverfahren die Transparenz erhöhen und den betroffenen Personen einen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen[3].

2 Zusätzlich zur Einhaltung durch die unter die DSGVO fallenden Verantwortlichen oder Auftragsverarbeiter können auch datenschutzspezifische Zertifizierungsverfahren, Siegel oder Prüfzeichen, die gemäß Artikel 42 Absatz 5 DSGVO genehmigt worden sind, eingesetzt werden, um nachzuweisen, dass die Verantwortlichen oder Auftragsverarbeiter, die gemäß Artikel 3 nicht unter die DSGVO fallen, im Rahmen der Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen (im Folgenden „Datenimporteure") nach Maßgabe von Artikel 46 Absatz 2 Buchstabe f DSGVO geeignete Garantien bieten[4].

3 Die als Übermittlungsgrundlage verwendete Zertifizierung ist ein neuer Übermittlungsmechanismus, der mit Artikel 46 DSGVO eingeführt wurde, um sicherzustellen, dass, falls kein Beschluss gemäß Artikel 45 Absatz 3 DSGVO vorliegt, ein Verantwortlicher oder ein Auftragsverarbeiter, der der DSGVO unterliegt (im Folgenden „EWR-Datenexporteur") personenbezogene Daten in ein Drittland oder an eine internationale Organisation nur übermitteln darf, wenn er geeignete Garantien bietet und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Insbesondere können diese geeigneten Garantien gemäß Artikel 46 Absatz 2 Buchstabe f DSGVO im Wege eines genehmigten Zertifizierungsverfahrens nach Artikel 42 DSGVO geboten werden, wenn dieses Verfahren mit rechtsverbindlichen und durchsetzbaren Verpflichtungen der Datenimporteure hinsichtlich der Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, einhergeht. Die Zertifizierungskriterien sind integraler Bestandteil jedes Zertifizierungsverfahrens. Folglich wird in der DSGVO die Genehmigung der Kriterien für ein nationales Zertifizierungsverfahren durch die zuständige Aufsichtsbehörde (Artikel 42 Absatz 5 und Artikel 43 Absatz 2

[1] Soweit in dieser Stellungnahme auf „Mitgliedstaaten" Bezug genommen wird, ist dies als Bezugnahme auf „EWR-Mitgliedstaaten" zu verstehen.
[2] Artikel 42 Absatz 1 DSGVO.
[3] Erwägungsgrund 100 DSGVO.
[4] Siehe Artikel 42 Absatz 2 DSGVO.

Buchstabe b DSGVO) oder im Falle eines europäischen Datenschutzsiegels durch den EDSA (Artikel 42 Absatz 5 und Artikel 70 Absatz 1 Buchstabe o DSGVO) erteilt.

4 Beabsichtigt eine Aufsichtsbehörde, dem EDSA die Genehmigung eines europäischen Datenschutzsiegels gemäß Artikel 42 Absatz 5 DSGVO vorzuschlagen, so sollte die Aufsichtsbehörde die Absicht des Programmeigners darlegen, das Zertifizierungsverfahren in allen Mitgliedstaaten anzubieten. In diesem Fall besteht die Hauptaufgabe des EDSA darin, die einheitliche Anwendung der DSGVO durch das Kohärenzverfahren gemäß den Artikeln 63, 64 und 65 DSGVO sicherzustellen. In diesem Rahmen werden die Zertifizierungskriterien gemäß Artikel 64 Absatz 2 DSGVO durch den EDSA genehmigt.

5 Ein gemäß Artikel 42 Absatz 5 DSGVO genehmigtes europäisches Datenschutzsiegel, das als Nachweis dienen soll, dass die Datenimporteure geeignete Garantien zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen bieten, dient als Grundlage, mit dem Datenübermittlungen aus allen EWR-Mitgliedstaaten an Drittländer oder internationale Organisationen abgedeckt werden[5].

6 Die Prüfung eines Zertifizierungsverfahrens, das als Übermittlungsgrundlage genutzt werden soll, erfolgt auf der Grundlage der Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679 (im Folgenden „Leitlinien“) und ihres Addendums Leitlinien für die Bewertung von Zertifizierungskriterien (im Folgenden „Addendum“) sowie der Leitlinien 7/2022 über die Zertifizierung als Instrument für Übermittlungen (im Folgenden „Leitlinien über die Zertifizierung als Instrument für Übermittlungen“).

7 Der EDSA erkannt an, dass jedes Zertifizierungsverfahren einzeln zu behandeln ist und die Bewertung anderer Zertifizierungsverfahren unberührt lässt.

8 Als Übermittlungsgrundlage verwendete Zertifizierungsverfahren sollten es Datenimporteuren ermöglichen, das Vorhandensein geeigneter Garantien nachzuweisen, um sicherzustellen, dass das durch die DSGVO gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird, wenn übermittelte personenbezogene Daten außerhalb des EWR verarbeitet werden [6] . Daher sollten die Kriterien den in der DSGVO festgelegten Anforderungen und Grundsätzen in Bezug auf den Schutz personenbezogener Daten angemessen Rechnung tragen, um sicherzustellen, dass der durch die DSGVO gewährte Schutz bei der Übermittlung personenbezogener Daten erhalten bleibt[7].

9 Gleichzeitig sollte der Programmeigner sicherstellen, dass das Zertifizierungsverfahren an allen aufgenommenen oder herangezogenen ISO-Normen und der Zertifizierungspraxis orientiert ist und mit ihnen im Einklang steht.

10 Folglich sollten Zertifizierungen Datenimporteuren einen Mehrwert bieten, indem sie zur Umsetzung standardisierter und spezifizierter organisatorischer und technischer Maßnahmen beitragen, mit denen nachgewiesen wird, dass bei der Verarbeitung personenbezogener Daten, die von EWR-Datenexporteuren übermittelt werden, geeignete Garantien bestehen. In diesem Zusammenhang weist der EDSA darauf hin, dass der Gegenstand der Zertifizierung – der mit dem Zertifizierungsgegenstand (ToE) im Rahmen der Zertifizierung übereinstimmt –

[5] EDSA-Leitlinien 7/2022 über die Zertifizierung als Instrument für Übermittlungen, Version 2.0, angenommen am 14. Februar 2023, Rn. 30.
[6] Artikel 44 DSGVO.
[7] Siehe Mitteilung der Kommission an das Europäische Parlament und den Rat „Austausch und Schutz personenbezogener Daten in einer globalisierten Welt“ (COM(2017) 7 final), S. 4.

generell in der Verarbeitung der an den Datenimporteur im Drittland übermittelten Daten und dem Transit, wenn dieser unter der Kontrolle dieses Importeurs liegt, bestehen sollte[8].

11 Zertifizierungen bieten auch dem Datenexporteur einen Mehrwert, wenn er sich dafür entscheidet, die von einem Datenimporteur erlangte Zertifizierung als Übermittlungsgrundlage gemäß Artikel 46 Absatz 2 Buchstabe f DSGVO zu nutzen und um die Erfüllung von Pflichten, z. B. gemäß Artikel 24 Absatz 3 oder Artikel 28 Absatz 5 DSGVO, nachzuweisen[9].

12 In diesem Zusammenhang weist der EDSA darauf hin, dass der Datenexporteur, der eine Zertifizierung als geeignete Garantie gemäß Artikel 46 Absatz 2 Buchstabe f DSGVO verwenden möchte, verpflichtet ist, 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 Datenübermittlung in den Geltungsbereich der Zertifizierung fällt sowie, ob Weiterübermittlungen vorgesehen sind und eine angemessene Dokumentation zu ihnen vorgelegt wird[10].

13 Zusätzlich muss der Datenexporteur 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 anderen Verantwortlichen in einem Datenaustauschvertrag mit dem Datenimporteur darauf hinweisen, dass die Zertifizierung als Übermittlungsgrundlage verwendet wird[11]. Er muss auch die in Artikel 13 Absatz 1 Buchstabe f DSGVO vorgesehenen spezifischen Pflichten erfüllen, insbesondere die Unterrichtung der betroffenen Person über die verwendeten geeigneten Garantien, d. h. im Falle einer Zertifizierung nach Artikel 46 Absatz 2 Buchstabe f DSGVO das Zertifikat, das der Datenimporteur nach einem spezifischen Zertifizierungsverfahren erhalten hat, und die Möglichkeit, wie eine Kopie des Zertifikats und die in den Zertifizierungskriterien enthaltenen Garantien zu erhalten ist, oder wo sie verfügbar sind.

14 Der EDSA begrüßt die Bemühungen der Programmeigner , Zertifizierungsmechanismen auszuarbeiten, die als praktikable und potenziell kosteneffiziente Instrumente mehr DSGVO-Konformität gewährleisten und durch mehr Transparenz das Recht der betroffenen Personen auf Schutz ihrer Privatsphäre und Datenschutz zu stärken.

15 Der EDSA weist darauf hin, dass Zertifizierungen freiwillige Instrumente der Rechenschaftspflicht sind und dass die Einhaltung eines Zertifizierungsverfahrens die Aufsichtsbehörden nicht daran hindert, ihre Aufgaben und Befugnisse gemäß der DSGVO und den einschlägigen nationalen Rechtsvorschriften wahrzunehmen. Dies gilt im Zusammenhang mit Zertifizierungen, die als Übermittlungsgrundlage verwendet werden, insbesondere hinsichtlich der bestehenden Pflichten der Datenimporteure gegenüber den Datenexporteuren auf der Grundlage rechtsverbindlicher und durchsetzbarer Verpflichtungen, die im Zertifizierungsverfahren vorgesehenen geeigneten Garantien anzuwenden, auch im Hinblick auf die Rechte der betroffenen Personen.

[8] Siehe EDSA-Leitlinien 7/2022 über die Zertifizierung als Instrument für Übermittlungen, Version 2.0, angenommen am 14. Februar 2023, Rn. 16.
[9] Leitlinien 7/2022 über die Zertifizierung als Instrument für Übermittlungen, Rn. 5.
[10] Leitlinien 7/2022 über die Zertifizierung als Instrument für Übermittlungen, Rn. 20.
[11] Ebd.

16 Mit dieser Stellungnahme soll die einheitliche Anwendung der DSGVO sichergestellt werden, auch durch die Aufsichtsbehörden, Verantwortlichen und Auftragsverarbeiter im Hinblick auf die Kernelemente, die im Rahmen von Zertifizierungsverfahren festgelegt werden müssen. In dieser Stellungnahme sollen insbesondere die Zertifizierungskriterien bewertet werden, die von Datenimporteuren als Übermittlungsgrundlage verwendet werden. Daher befasst sich der EDSA darin mit Fragen wie dem Anwendungsbereich, der Anwendbarkeit und der Relevanz der Kriterien im Falle von Übermittlungen aus allen EWR-Mitgliedstaaten und/oder von Datenexporteuren im Anwendungsbereich der DSGVO.

17 Gegenstand der Stellungnahme des EDSA sind ausschließlich die Zertifizierungskriterien. Der EDSA benötigt möglicherweise hochwertige Informationen über die Evaluierungsmethoden, um die Überprüfbarkeit der Kriterien im Rahmen seiner Stellungnahme dazu eingehend bewerten zu können. Dies umfasst jedoch keinerlei Genehmigung solcher Evaluierungsmethoden.

18 Die Stellungnahme des EDSA wird gemäß Artikel 64 Absatz 2 DSGVO in Verbindung mit Artikel 10 Absatz 2 der Geschäftsordnung des EDSA binnen acht Wochen ab dem ersten Arbeitstag nach dem Beschluss des Vorsitzenden und der zuständigen Aufsichtsbehörde über die Vollständigkeit des Dossiers angenommen. Diese Frist kann unter Berücksichtigung der Komplexität der Angelegenheit auf Beschluss des Vorsitzes um weitere sechs Wochen verlängert werden. Gelangt der EDSA in seiner Stellungnahme zu dem Schluss, dass die in Rede stehenden Kriterien nicht genehmigt werden können, kann die Aufsichtsbehörde die Kriterien erneut zur Genehmigung vorlegen, sobald die in der ursprünglichen Stellungnahme des EDSA geäußerten Bedenken ausgeräumt sind —

Hat folgende Stellungnahme angenommen:

1 Zusammenfassung des Sachverhalts

19 Im Einklang mit Artikel 42 Absatz 2 und Artikel 46 Absatz 2 Buchstabe f DSGVO, den Leitlinien 1/2018 sowie den Leitlinien 7/2022 über die Zertifizierung als Instrument für Übermittlungen hat das European Centre for Certification and Privacy (im Folgenden „Programmeigner “) die Europrivacy-Version 82 (im Folgenden „Zertifizierungskriterien“) ausgearbeitet.

20 Der EDSA weist darauf hin, dass er die Europrivacy-Zertifizierungskriterien (Version 60) bereits am 10. Oktober 2022 durch die Veröffentlichung der Stellungnahme 28/2022 des EDSA als europäisches Datenschutzsiegel gemäß Artikel 42 Absatz 5 DSGVO, mit dem die Einhaltung der DSGVO gemäß Artikel 42 Absatz 1 DSGVO nachgewiesen werden kann, genehmigt hatte. Ein solches System stellte keine für Datenübermittlungen vorgesehene Zertifizierung nach Artikel 46 Absatz 2 Buchstabe f DSGVO dar.

21 Am 29. Januar 2026 übermittelte die Aufsichtsbehörde Luxemburgs dem EDSA eine aktualisierte Version der bereits genehmigten Zertifizierungskriterien des europäischen Datenschutzsiegels Europrivacy mit einem erweiterten Anwendungsbereich insbesondere hinsichtlich Antragstellern, die unter Artikel 3 Absatz 2 DSGVO fallen, sowie weiteren Änderungen in Bezug auf die Kernkriterien der Zertifizierung (Version 82). Der EDSA hat die Stellungnahme 14/2026 zu dieser aktualisierten Fassung (Version 82) der Europrivacy-Zertifizierungskriterien, die als Nachweis für die Einhaltung der DSGVO gemäß Artikel 42 Absatz 5 dienen sollen, angenommen.

22 Am selben Tag legte die Aufsichtsbehörde Luxemburgs dem EDSA auch eine Reihe zusätzlicher Zertifizierungskriterien (im Folgenden „Erweiterung des Europrivacy-

Zertifizierungssystems zur Zertifizierung von Datenimporteuren gemäß Artikel 46“), die als Instrument für Übermittlungen gemäß Artikel 46 Absatz 2 Buchstabe f DSGVO dienen sollen, zur Genehmigung gemäß Artikel 64 Absatz 2 DSGVO vor.

23 Der Beschluss über die Vollständigkeit dieses Dossiers erging am 31. März 2026.

2 Bewertung

24 Der EDSA führte seine Bewertung der Zertifizierungskriterien, die Datenimporteuren als Instrument für Übermittlungen dienen sollen, zu deren Genehmigung gemäß Artikel 42 Absatz 5 in Verbindung mit Artikel 46 Absatz 2 Buchstabe f DSGVO im Einklang mit der in Anhang 2 der Leitlinien 1/2018 (im Folgenden „Anhang“), dem Addendum zu diesen Leitlinien sowie den Leitlinien über die Zertifizierung als Übermittlungsgrundlage vorgesehenen Struktur durch[12].

25 Der Ausschuss betont, dass das derzeitige System im Einklang mit den in Artikel 42 Absatz 2 und Artikel 46 Absatz 2 Buchstabe f DSGVO festgelegten Bedingungen zur Verwendung als Übermittlungsgrundlage vorgesehen ist und dass die im Rahmen dieses Systems erteilten Zertifizierungen daher von Datenexporteuren im Sinne von Kapitel V DSGVO (d. h. von Verantwortlichen oder Auftragsverarbeitern, die für die betreffende Verarbeitung unter die DSGVO fallen[13]) genutzt werden könnten, um personenbezogene Daten an zertifizierte Datenimporteure, die gemäß Artikel 3 nicht unter die DSGVO fallen, zu übermitteln[14]. Dies bedeutet, dass personenbezogene Daten nur dann an den Datenimporteur in dem Drittland übermittelt werden können, wenn dieser zertifiziert wurde und gegenüber dem EWR-Datenexporteur rechtsverbindliche und durchsetzbare Verpflichtungen unterzeichnet hat, bei der Verarbeitung der im Rahmen des ToE übermittelten personenbezogenen Daten die in den Zertifizierungskriterien vorgesehenen geeigneten Garantien anzuwenden, einschließlich in Bezug auf die Rechte der betroffenen Personen.

26 Im Zusammenhang mit dieser Stellungnahme und zur Genehmigung der als Übermittlungsinstrument vorgesehenen Europrivacy-Zertifizierungskriterien hat der EDSA Folgendes bewertet: Anwendung und Zertifizierungsgegenstand – Vorabprüfungen und Kontrollen für Datenimporteure (ADI); die Europrivacy-DSGVO-Kernkriterien für Datenimporteure (GI); die Überprüfungen und Kontrollen der technischen und organisatorischen Maßnahmen (T).

27 In Bezug auf das Zertifizierungsverfahren betont der EDSA, dass die Besonderheiten der als Übermittlungsgrundlage verwendeten Zertifizierung große Transparenz erfordern, und begrüßt die diesbezüglichen Klarstellungen im Europrivacy-Zertifizierungssystem, wonach Übermittlungen nicht beginnen können, bevor die Zertifizierung erteilt wurde. Der EDSA erkennt die hierzu im Europrivacy-Zertifizierungssystem enthaltenen Festlegungen an. Demnach kann vor der Übermittlung personenbezogener Daten „die Bewertung mit nicht der DSGVO unterliegenden personenbezogenen Daten oder mit nicht-personenbezogenen Daten durchgeführt werden, wobei erforderlichenfalls simulierte Daten für die Bewertung bestimmter Kriterien verwendet werden können“, und nachdem die Datenübermittlung

[12] Siehe insbesondere: Abschnitte 3 und 4 der Leitlinien 07/2022.
[13] Siehe Leitlinien 5/2021 über das Zusammenspiel zwischen der Anwendung des Artikels 3 und der Bestimmungen über internationale Übermittlungen nach Kapitel V DSGVO, Version 2.0, angenommen am 14. Februar 2023, Rn. 9.
[14] Artikel 42 Absatz 2 DSGVO.

begonnen hat, „muss der Prüfer diese Kriterien bei dem folgenden Überwachungsaudit erneut bewerten“[15].

28 Der EDSA weist darauf hin, dass bei der Akkreditierung von Zertifizierungsstellen im Hinblick auf eine als Übermittlungsgrundlage dienende Zertifizierung möglicherweise einige Anpassungen im Einklang mit den Leitlinien über die Zertifizierung als Instrument für Übermittlungen vorzunehmen sind[16]. In der vorliegenden Stellungnahme wird diese Frage jedoch nicht behandelt, da sie nicht in die Zuständigkeit des EDSA fällt.

29 Der EDSA weist ferner darauf hin, dass die Zertifizierungskriterien im Einklang mit Artikel 42 Absatz 8 DSGVO und im Falle einer als Übermittlungsgrundlage verwendeten Zertifizierung insbesondere im Einklang mit Artikel 13 Absatz 1 Buchstabe f DSGVO den betroffenen Personen, deren personenbezogene Daten auf der Grundlage der dem Datenimporteur erteilten Zertifizierung übermittelt werden, zur Verfügung gestellt werden müssen.

30 Der Ausschuss stellt fest, dass nach den Begriffsbestimmungen des Systems mit dem Ausdruck „zuständige Datenschutzbehörden“ im gesamten System auf Datenschutzbehörden im EWR Bezug genommen wird[17].

31 Ebenso stellt der Ausschuss fest, dass im Europrivacy-System mit den Ausdrücken „anwendbares Recht“ und „Recht von Drittländern“ auf das Recht Bezug genommen wird, das auf den Antragsteller und/oder auf die im Zertifizierungsgegenstand verarbeiteten personenbezogenen Daten anwendbar ist. Dies gilt, soweit dieses Recht keine Beschränkungen der Datenschutzrechte auferlegt, die über das in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maß hinausgehen, um eines der in Artikel 23 Absatz 1 DSGVO aufgeführten Ziele sicherzustellen, in einem angemessenen Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen vorsieht.

2.1 Anwendungsbereich des Zertifizierungsverfahrens und Zertifizierungsgegenstand (ToE)

32 Die Erweiterung des Europrivacy-Zertifizierungssystems auf die Zertifizierung von Datenimporteuren gemäß Artikel 46 soll im Sinne von Artikel 42 Absatz 2 und Artikel 46 Absatz 2 Buchstabe f DSGVO von Datenimporteuren mit Sitz außerhalb des EWR, die gemäß Artikel 3 nicht unter die DSGVO fallen, verwendet werden, um nachzuweisen, dass sie im Rahmen der Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen geeignete Garantien bieten. Ihr Anwendungsbereich unterscheidet sich somit von dem der in Randnummer 3 genannten Europrivacy-Zertifizierung nach Artikel 42 Absatz 1 durch die Festlegung spezifischer Kriterien, die anzuwenden und einzuhalten sind, wenn eine

[15] Siehe Europrivacy™/® Certification Scheme Extension for Certifying Data Importers under Article 46 GDPR (Erweiterung des Europrivacy-Zertifizierungssystems auf die Zertifizierung von Datenimporteuren gemäß Artikel 46), EP-CS.1.DI, Abschnitt 6.1.
[16] Leitlinien 7/2022, Abschnitt 2.
[17] Siehe die in den Europrivacy-Kriterien vorgesehene Definition des Begriffs „Competent SA“: „*‚Competent Data Protection Authority‘ refers to data protection authorities in the EEA. Overall, it refers to the national data protection authorities that have competence to enforce compliance of the personal data processed by the Target of Evaluation. In the case of a GDPR certification delivered to a Data Importer under Article 46 GDPR, the competent Data Protection Authority is the one of the Data Exporter in the EEA, except for lodging a complaint where any authority in the EEA is competent*“ („Zuständige Datenschutzbehörde“ bezeichnet Datenschutzbehörden im EWR. Insgesamt bezieht sich der Begriff auf die nationalen Datenschutzbehörden, die für die Durchsetzung der Einhaltung der Vorschriften in Bezug auf die vom Zertifizierungsgegenstand verarbeiteten personenbezogenen Daten zuständig sind. Im Falle einer DSGVO-Zertifizierung, die einem Datenimporteur gemäß Artikel 46 DSGVO erteilt wird, ist die zuständige Datenschutzbehörde die des Datenexporteurs im EWR, außer im Fall einer Beschwerdeeinreichung, bei der jede Behörde im EWR zuständig ist“).

Europrivacy-Zertifizierung Antragstellern (Verantwortlichen oder Auftragsverarbeitern) erteilt wird, deren Sitz außerhalb des EWR liegt und die als Datenimporteure fungieren sollen.

33 Das Europrivacy-Zertifizierungssystem als Übermittlungsgrundlage ist ein System, das sowohl für einzelne Übermittlungen verwendbar sein soll als auch für eine Reihe von Übermittlungen, wenn letztere eng miteinander verbunden sind. Das Zertifizierungssystem enthält Zertifizierungskriterien für Verarbeitungsvorgänge personenbezogener Daten im Rahmen des Zertifizierungsgegenstands (ToE), die an den Datenimporteur übermittelt wurden und umfassen auch den Transit, wenn dieser unter der Kontrolle desselben Importeurs liegt[18].

34 Der EDSA nimmt zur Kenntnis, dass der Anwendungsbereich dieses Zertifizierungssystems nicht für gemeinsam Verantwortliche gilt und festgelegt ist, dass die Ausstellung der Zertifizierung von der Zertifizierungsstelle abzulehnen ist, wenn der ToE gemeinsame Verantwortlichkeit vorsieht[19].

2.2 Verarbeitungsvorgänge

35 Die Zertifizierungskriterien beziehen sich auf die maßgeblichen Komponenten der Verarbeitungsvorgänge für die im Rahmen des ToE übermittelten personenbezogenen Daten. Insbesondere sehen die Zertifizierungskriterien Garantien für die Verarbeitung besonderer Kategorien personenbezogener Daten vor (Abschnitt GI.2 betreffend die Verarbeitung besonderer Daten). In diesem Zusammenhang begrüßt der Ausschuss, dass die Zertifizierungskriterien (Kriterium GI.2.1.3 betreffend zusätzliche Garantien für die Verarbeitung besonderer Kategorien personenbezogener Daten) auch vorsehen, dass der Antragsteller zusätzliche Beschränkungen und Garantien bieten muss, die an die besondere Art der Daten und die damit verbundenen Risiken angepasst sind, wenn besondere Kategorien personenbezogener Daten von der Verarbeitung betroffen sind.

2.3 Grundsätze der Datenverarbeitung

36 In Abschnitt GI.1 der Zertifizierungskriterien werden die Datenschutzgrundsätze, wie sie auch in Artikel 5 DSGVO vorgesehen sind, angemessen behandelt, wodurch sichergestellt werden soll, dass die Datenverarbeitung im ToE rechtmäßig und verhältnismäßig ist.

37 Insbesondere werden im Rahmen des Zertifizierungskriteriums GI.1.1.2 der Grundsatz der Zweckbindung und die einschlägigen Pflichten des Antragstellers in Bezug auf die Einhaltung dieses Grundsatzes gebührend ausgeführt. Der EDSA stellt fest, dass übermittelte personenbezogene Daten nur für die Zwecke verarbeitet werden dürfen, für die sie übermittelt wurden. Im Zertifizierungskriterium GI.1.1.3 sind im Einklang mit den aktuellen von der Europäischen Kommission angenommenen Standardvertragsklauseln [20] die einzigen Ausnahmen festgelegt, unter denen Daten für andere Zwecke als diejenigen, für die sie ursprünglich erhoben wurden, weiterverarbeitet werden dürfen (d. h. vorherige informierte Einwilligung, rechtliche Verpflichtung, lebenswichtige Interessen der betroffenen Personen und Rechtsansprüche).

38 Der EDSA stellt ferner fest, dass der Antragsteller verpflichtet ist, eine schriftliche Bewertung vorzulegen, um sicherzustellen, dass die Rechtslage und -praxis in dem Drittland den

[18] Siehe Zertifizierungskriterien GI.11.1.5 und GI.11.1.6.
[19] Europrivacy™/® Certification Scheme Extension for Certifying Data Importers under Article 46 GDPR, EP-CS.1.DI, Abschnitt 3.2.2, wo auch klar festgelegt ist, dass die gemeinsame Verantwortlichkeit vom Anwendungsbereich des Systems für Antragsteller gemäß Artikel 46 ausgenommen ist.
[20] Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates.

Antragsteller nicht daran hindern, die Europrivacy-Kriterien einzuhalten, den Wesensgehalt der Grundrechte und Grundfreiheiten der betroffenen Personen wahren und nicht über das in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maß hinausgehen, um eines der in Artikel 23 Absatz 1 DSGVO aufgeführten Ziele sicherzustellen. Die zertifizierte Stelle muss die Bewertung überprüfen, wenn regulatorische oder organisatorische Änderungen die Einhaltung der Kriterien behindern oder den ToE oder die Rechte der betroffenen Personen beeinträchtigen könnten und die Zertifizierungsstelle unterrichtet werden sollte (Kriterium GI.1.1.1).

2.4 Allgemeine Pflichten von Verantwortlichen und Auftragsverarbeitern

39 Die Zertifizierungskriterien bilden die Pflichten des Verantwortlichen gemäß Artikel 24 DSGVO ab (Abschnitt GI.4) und umfassen die Anforderung, dass die vertraglichen Vereinbarungen zwischen Auftragsverarbeiter und Verantwortlichem gemäß Artikel 28 DSGVO (Abschnitt GI.5 der Zertifizierungskriterien betreffend Auftrags- und Unterauftragsverarbeiter) zu evaluieren sind. Dadurch soll sichergestellt werden, dass die an der Datenverarbeitung des ToE beteiligten Auftragsverarbeiter das gleiche Datenschutzniveau bieten, das in den Europrivacy-Kriterien vorgeschrieben ist. In diesem Zusammenhang begrüßt der EDSA, dass für Antragsteller, die als Verantwortliche oder Auftragsverarbeiter fungieren, andere Zertifizierungskriterien für die Beauftragung von Unterauftragsverarbeitern festgelegt sind, da mit dieser Unterscheidung die Trennung der Rollen und Zuständigkeiten zwischen den Akteuren in der Verarbeitungskette besser wiedergegeben wird (Abschnitt GI.5.1).

40 Nach den Zertifizierungskriterien müssen alle Antragsteller einen Datenschutzbeauftragten (DSB) benennen, auch diejenigen, die gemäß Artikel 37 DSGVO nicht dazu verpflichtet sind. Mit den Zertifizierungskriterien wird kontrolliert, ob der DSB dieselben Anforderungen erfüllt, die auch in den Artikeln 37 bis 39 DSGVO (Abschnitt GI.9 betreffend die Benennung des Datenschutzbeauftragten) vorgesehen sind. Dadurch soll sichergestellt werden, dass Rolle, Funktion und Qualifikation des Datenschutzbeauftragten, der die Konformität der Datenverarbeitung im ToE überwacht, den notwendigen Anforderungen entsprechen. In diesem Zusammenhang stellt der Ausschuss fest, dass die Benennung eines DSB für Verantwortliche und Auftragsverarbeiter nach der DSGVO keine zwingende Pflicht darstellt, sofern nicht die in Artikel 37 Absatz 1 DSGVO vorgesehenen Bedingungen vorliegen.

41 Die Zertifizierungskriterien sehen vor, dass der Inhalt der Verzeichnisse von Verarbeitungstätigkeiten im Einklang mit Artikel 30 DSGVO überprüft werden muss (Abschnitt GI.5.3 betreffend Aufzeichnungen über Verarbeitungstätigkeiten). In diesem Zusammenhang begrüßt der Ausschuss, dass in den Zertifizierungskriterien eindeutig vorgeschrieben ist, dass die Antragsteller mit den für die Exporteure zuständigen Datenschutzbehörden im EWR kooperieren und diesen auf Anfrage das Verzeichnis von Verarbeitungstätigkeiten zur Verfügung stellen müssen (Kriterium GI.5.3.5).

2.5 Rechte der betroffenen Personen

42 In den Zertifizierungskriterien werden die Rechte betroffener Personen im Einklang mit Kapitel III DSGVO behandelt und ist festgelegt, dass entsprechende Maßnahmen getroffen werden müssen, um sicherzustellen, dass die Verarbeitung im ToE die Rechte betroffener Personen wahrt und die wirksame Ausübung dieser Rechte ermöglicht. Abschnitt GI.3 der Zertifizierungskriterien betreffend transparente Informationen, Kommunikation und Modalitäten in Bezug auf die Ausübung der Rechte der betroffenen Person sieht neben anderen Garantien vor, dass betroffene Personen das Recht haben, über die

Datenverarbeitung selbst sowie darüber informiert zu werden, wie sie ihre Rechte ausüben können. Der EDSA begrüßt insbesondere die in den Zertifizierungskriterien vorgesehene Anforderung, dass der Antragsteller über Verfahren oder einen Mechanismus verfügen muss, auf deren Grundlage Anträge betroffener Personen bearbeitet werden und im Falle der Nichtbearbeitung von Anträgen betroffener Personen diese über die Gründe der Nichtbearbeitung und über das Recht auf Beschwerde bei einer EWR-Datenschutzbehörde und auf Einlegung eines gerichtlichen Rechtsbehelfs informiert werden.

2.6 Technische und organisatorische Maßnahmen und Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen

43 Die Zertifizierungskriterien sehen vor, dass technische und organisatorische Maßnahmen angewendet werden müssen, die im Einklang mit den Artikeln 25 und 32 DSGVO ein dem Risiko der Verarbeitung angemessenes Sicherheitsniveau bieten und Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ermöglichen (Abschnitt GI.6 der Zertifizierungskriterien betreffend Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sowie Sicherheit der Verarbeitung). Dadurch sollen für die im ToE verarbeiteten Daten die angemessene Sicherheit und der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sichergestellt werden. Darüber hinaus enthalten die Zertifizierungskriterien einen speziellen Abschnitt (Kriterium T für technische und organisatorische Maßnahmen, Überprüfungen und Kontrollen), in dem technische und organisatorische Maßnahmen ausführlich behandelt werden.

44 Durch die Zertifizierungskriterien wird die Anwendung von Maßnahmen vorgeschrieben, mit denen sichergestellt wird, dass die Pflichten zur Meldung von Verletzungen des Schutzes personenbezogener Daten im Einklang mit den Artikeln 33 und 34 DSGVO rechtzeitig und in dem dort vorgesehenen Umfang erfüllt werden (Abschnitt GI.7 betreffend die Behandlung von Verletzungen des Schutzes personenbezogener Daten).

45 In diesem Zusammenhang stellt der Ausschuss fest, dass die Zertifizierungskriterien eine ausführliche Liste (Kriterium GI.7.1.1 betreffend die Pflicht zur Dokumentation von Verletzungen des Schutzes personenbezogener Daten) der Informationen enthalten, die vom Antragsteller im Falle einer Verletzung des Schutzes personenbezogener Daten zu dokumentieren sind (z. B. die Kategorien der betroffenen oder möglicherweise betroffenen personenbezogenen Daten; die ungefähre Zahl der betroffenen oder möglicherweise betroffenen Personen; die Kategorien und die ungefähre Zahl der betroffenen oder möglicherweise betroffenen personenbezogenen Datensätze; die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten). Darüber hinaus begrüßt der EDSA, dass die Zertifizierungskriterien eindeutig vorsehen, dass der Antragsteller, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, über Vorschriften, ein Verfahren oder einen Mechanismus verfügen muss, um die für den/die Ausführer zuständige Datenschutzbehörde im EWR und die betroffenen Personen im Einklang mit den Anforderungen der Artikel 33 und 34 DSGVO zu informieren (Kriterium GI.7.1.2 betreffend die Pflicht des Verantwortlichen zur Meldung von Verletzungen des Schutzes personenbezogener Daten und zur Benachrichtigung über solche Verletzungen sowie Abschnitt GI.7.2 betreffend die Benachrichtigung der betroffenen Person über Verletzungen des Schutzes personenbezogener Daten).

46 Der EDSA begrüßt ferner die in den Zertifizierungskriterien vorgesehene Anforderung, im Einklang mit Artikel 35 DSGVO das Risiko für die Rechte und Freiheiten natürlicher Personen bei der Datenverarbeitung im Rahmen des ToE zu bewerten und dabei die für den/die Ausführer zuständige Datenschutzbehörde im EWR einzubeziehen (Abschnitt GI.8 betreffend die Pflicht zur Bewertung, ob eine Datenschutz-Folgenabschätzung erforderlich ist).

2.7 Kriterien für den Nachweis des Vorhandenseins geeigneter Garantien für die Übermittlung personenbezogener Daten

47 Die Zertifizierungskriterien sehen die Anforderung vor, dass alle Übermittlungen personenbezogener Daten in Drittländer und an internationale Organisationen, die am ToE beteiligt sind, ermittelt werden müssen und die Wahl der Grundlage zur Übermittlung im Sinne des Kapitel V DSGVO, die geeignete Garantien bieten, begründet werden muss (Abschnitt GI.10 betreffend die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen). Der EDSA nimmt zur Kenntnis, dass diese Zertifizierungskriterien im Falle einer Weiterübermittlung personenbezogener Daten im Zusammenhang mit dem ToE an dasselbe Drittland, in dem der Antragsteller ansässig ist, oder an ein anderes Drittland gelten sollen. Der Ausschuss begrüßt die in den Zertifizierungskriterien ausdrücklich festgelegte Anforderung, dass der Antragsteller eine klare Übersicht oder ein Verzeichnis zu allen personenbezogenen Datenströmen im Rahmen des ToE und allen ermittelten Übermittlungen in Drittländer und an internationale Organisationen führen und im Einklang mit den in Kapitel V DSGVO vorgesehenen Grundlagen eine geeignete Grundlage für die Übermittlung personenbezogener Daten anwenden muss, wobei die Pflicht zu beachten ist, das im EWR vorgesehene Schutzniveau für personenbezogene Daten nicht zu untergraben.

48 Der EDSA nimmt ferner zur Kenntnis, dass der Antragsteller laut den Zertifizierungskriterien eine Folgenabschätzung für die Übermittlung durchgeführt und erforderlichenfalls zusätzliche Maßnahmen ergriffen haben muss, um sicherzustellen, dass das Schutzniveau der übermittelten Daten nicht untergraben wird (Kriterium GI.10.1.5).

3 Zusätzliche Kriterien für ein als Übermittlungsinstrument verwendetes europäisches Datenschutzsiegel

49 Gemäß den Leitlinien über die Zertifizierung als Instrument für Übermittlungen sollte das Zertifizierungssystem sicherstellen, dass der Datenimporteur „die Rechtslage und -praxis des Drittlands, in dem er tätig ist, bewertet und prüft, ob sie ihn daran hindern, seine Verpflichtungen im Rahmen der Zertifizierung zu erfüllen“. In diesem Zusammenhang stellt der Ausschuss fest, dass mit dem Kriterium ADI.2.1.5 Bedingungen festgelegt werden, die Antragsteller bei der Festlegung des ToE im Rahmen der Überprüfung ihres Antrags auf Zertifizierung erfüllen müssen. Insbesondere muss die Zertifizierungsstelle, bevor sie eine Zertifizierungsprüfung in Erwägung zieht, überprüfen, ob der Antragsteller nachweisen kann, dass die Rechtslage und -praxis des Drittlands die Erfüllung der Zertifizierungsanforderungen nicht behindern. Ist dies nicht der Fall, wird das Zertifizierungsverfahren bereits in der Antragsphase beendet.

50 Der Ausschuss stellt ferner fest, dass der Antragsteller nach dem Kriterium GI.11.1.3 die Rechtslage und -praxis des Drittlands analysieren und die potenziellen Auswirkungen auf die Rechte und Freiheiten der betroffenen Person, deren Daten möglicherweise importiert

werden, ermitteln sollte sowie über Vorschriften, Verfahren oder Strategien verfügen sollte, auf deren Grundlage er der Zertifizierungsstelle und den zuständigen Datenschutzbehörden auf Anfrage seine schriftliche Analyse der lokalen Rechtslage und -praxis zur Verfügung stellen kann.

51 Darüber hinaus sehen die Zertifizierungskriterien im Einklang mit den Leitlinien über die Zertifizierung als Instrument für Übermittlungen vor, dass der Antragsteller erforderlichenfalls zusätzliche Maßnahmen getroffen haben muss, um sicherzustellen, dass das Schutzniveau der übermittelten personenbezogenen Daten nicht untergraben wird, und dass, wenn dies nicht möglich ist, der Datenimporteur den Datenexporteur unterrichten muss und die Übermittlung personenbezogener Daten ausgesetzt oder eingestellt werden sollte (Kriterium GI.11.1.3).

52 Darüber hinaus stellt der Ausschuss fest, dass das Europrivacy-System im Einklang mit Artikel 42 Absatz 2 DSGVO vorsieht, dass vor jeder Übermittlung zwischen dem Datenimporteur und dem Datenexporteur ein Vertrag mit den einschlägigen rechtsverbindlichen und durchsetzbaren Verpflichtungen unterzeichnet werden sollte, und es ein Muster für einen solchen Vertrag enthält. In diesem Zusammenhang nimmt der EDSA zur Kenntnis, dass in den Zertifizierungskriterien im Einklang mit den Leitlinien über die Zertifizierung als Instrument für Übermittlungen die Inhalte der rechtsverbindlichen und durchsetzbaren Verpflichtungen, die der Antragsteller gegenüber jedem Exporteur im EWR eingehen sollte, ausführlich aufgelistet sind. Dazu gehören die Pflicht, das Recht der betroffenen Personen anzuerkennen, als Drittbegünstigte die Zertifizierungsvorschriften gegenüber dem zertifizierten Datenimporteur durchzusetzen, sowie die Pflicht, mit den für die Datenexporteure zuständigen Datenschutzbehörden im EWR zusammenzuarbeiten (u. a. indem ihren Prüfungen und Kontrollen zugestimmt wird, ihre Empfehlungen berücksichtigt und ihre Entscheidungen befolgt werden), sich an alle verbindlichen Entscheidungen zu halten, die von den zuständigen Behörden und Gerichten der EWR-Mitgliedstaaten im Zusammenhang mit der Zertifizierung erlassen werden, die erhaltenen Daten nur während der Gültigkeitsdauer des Zertifikats zu verarbeiten und bei Widerruf des Zertifikats die erhaltenen Daten zurückzugeben und/oder zu löschen. Die Zertifizierungskriterien sehen außerdem vor, dass der Antragsteller versichern sollte, keinen Grund zu der Annahme zu haben, dass die für die Verarbeitung im ToE geltende Rechtslage und -praxis in dem Drittland, einschließlich etwaiger Anforderungen an die Offenlegung personenbezogener Daten oder Maßnahmen zur Genehmigung des Zugangs durch Behörden, ihn daran hindern, seinen Verpflichtungen im Rahmen der Zertifizierung nachzukommen und den Datenexporteur über alle einschlägigen Änderungen der Rechtslage und -praxis in dieser Hinsicht zu unterrichten (Kriterium GI.11.1.1 betreffend rechtsverbindliche und durchsetzbare Verpflichtungen für Datenimporteure).

4 Schlussfolgerungen/Empfehlungen

53 Zusammenfassend ist der EDSA der Auffassung, dass die als Instrument für Übermittlungen vorgesehenen Europrivacy-Zertifizierungskriterien mit der DSGVO im Einklang stehen, und genehmigt sie gemäß der in Artikel 70 Absatz 1 Buchstabe o DSGVO festgelegten Aufgabe des Ausschusses, woraus eine gemeinsame Zertifizierung (europäisches Datenschutzsiegel) als Übermittlungsgrundlage resultiert.

54 Der EDSA betrachtet die Zertifizierungskriterien als integralen Bestandteil des Zertifizierungssystems und wird das Europrivacy-Zertifizierungssystem in das öffentliche Register der Zertifizierungsmechanismen und der Datenschutzsiegel und -prüfzeichen aufnehmen und die Kriterien gemäß Artikel 42 Absatz 8 DSGVO veröffentlichen.

5 Abschließende Bemerkungen

55 Diese Stellungnahme ist an die luxemburgische Aufsichtsbehörde gerichtet und wird gemäß Artikel 64 Absatz 5 Buchstabe b DSGVO veröffentlicht.

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

Anu Talus