Stellungnahme 7/2024 zum Beschlussentwurf der deutschen Aufsichtsbehörde Nordrhein-Westfalen über die Zertifizierungskriterien von European Cloud Service Data Protection (Auditor)

Annahme: 17. April 2024

Inhaltsverzeichnis

Der Europäische Datenschutzausschuss —

gestützt auf Artikel 63, Artikel 64 Absatz 1 Buchstabe c und Artikel 42 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, geändert durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018[1],

gestützt auf Artikel 64 Absatz 1 Buchstabe c DSGVO und die Artikel 10 und 22 seiner Geschäftsordnung.

in Erwägung nachstehender Gründe:

(1) Die Mitgliedstaaten, die Aufsichtsbehörden, der Europäische Datenschutzausschuss (im Folgenden „EDSA“) und die Europäische Kommission fördern insbesondere auf Unionsebene die Einrichtung von Datenschutzzertifizierungsverfahren (im Folgenden „Zertifizierungsverfahren“) und von Datenschutzsiegeln und -prüfzeichen, um die Einhaltung der DSGVO bei Verarbeitungsvorgängen durch Verantwortliche und Auftragsverarbeiter nachzuweisen, wobei den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen Rechnung zu tragen ist.[2] Darüber hinaus kann die Einführung von Zertifizierungen die Transparenz erhöhen und es den betroffenen Personen ermöglichen, das Datenschutzniveau einschlägiger Produkte und Dienstleistungen zu bewerten.[3]

(2) Die Zertifizierungskriterien sind ein fester Bestandteil eines jeden Zertifizierungsverfahrens. Folglich wird in der DSGVO die Genehmigung nationaler Zertifizierungskriterien für ein Zertifizierungsverfahren durch die zuständige Aufsichtsbehörde (Artikel 42 Absatz 5 und Artikel 43 Absatz 2 Buchstabe b DSGVO) oder im Falle eines Europäischen Datenschutzsiegels durch den EDSA (Artikel 42 Absatz 5 und Artikel 70 Absatz 1 Buchstabe o DSGVO) verpflichtend festgelegt.

(3) Beabsichtigt eine Aufsichtsbehörde, eine Zertifizierung gemäß Artikel 42 Absatz 5 DSGVO zu genehmigen, besteht die Hauptaufgabe des EDSA darin, die einheitliche Anwendung der DSGVO durch das in den Artikeln 63, 64 und 65 DSGVO genannte Kohärenzverfahren sicherzustellen. In diesem Rahmen ist der EDSA gemäß Artikel 64 Absatz 1 Buchstabe c DSGVO verpflichtet, eine Stellungnahme zum Entwurf eines Beschlusses der Aufsichtsbehörde zur Genehmigung der Zertifizierungskriterien abzugeben.

(4) Mit dieser Stellungnahme soll die einheitliche Anwendung der DSGVO sichergestellt werden, auch durch die Aufsichtsbehörden, Verantwortlichen und Auftragsverarbeiter im Lichte der Kernelemente, die Zertifizierungsverfahren enthalten müssen. Die Bewertung des EDSA

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

erfolgt insbesondere 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 mit „Leitlinien zur Bewertung der Zertifizierungskriterien“ (im Folgenden „Addendum“), für die die Frist für die öffentliche Konsultation am 26. Mai 2021 endete.

(5) Dementsprechend erkennt der EDSA an, dass jedes Zertifizierungsverfahren individuell zu behandeln ist und die Bewertung anderer Zertifizierungsverfahren unberührt lässt.

(6) Zertifizierungsverfahren sollten es den Verantwortlichen und Auftragsverarbeitern ermöglichen, die Einhaltung der DSGVO nachzuweisen; daher sollten die Zertifizierungskriterien den in der DSGVO festgelegten Anforderungen und Grundsätze in Bezug auf den Schutz personenbezogener Daten angemessen Rechnung tragen und zu ihrer einheitlichen Anwendung beitragen.

(7) Gleichzeitig sollten die Zertifizierungskriterien andere Normen wie ISO-Normen und Zertifizierungsverfahren berücksichtigen und gegebenenfalls mit ihnen interoperabel sein.

(8) In diesem Zusammenhang sollten Zertifizierungen einen Mehrwert für eine Organisation schaffen, indem sie zur Umsetzung standardisierter und spezifischer organisatorischer und technischer Maßnahmen beitragen, die die Einhaltung der Verarbeitungsvorgänge unter Berücksichtigung sektorspezifischer Anforderungen nachweislich erleichtern und verbessern.

(9) Der EDSA begrüßt die Bemühungen der Systeminhaber, Zertifizierungsverfahren auszuarbeiten, die praktische und potenziell kosteneffiziente Instrumente sind, um eine größere Kohärenz mit der DSGVO zu gewährleisten und das Recht der betroffenen Personen auf Privatsphäre und Datenschutz durch mehr Transparenz zu fördern.

(10) Der EDSA weist darauf hin, dass Zertifizierungen Instrumente der freiwilligen Rechenschaftspflicht sind und dass die Einhaltung eines Zertifizierungsverfahrens weder die Verantwortung der Verantwortlichen oder Auftragsverarbeiter für die Einhaltung der DSGVO einschränkt noch die Aufsichtsbehörden daran hindert, ihre Aufgaben und Befugnisse gemäß der DSGVO und den einschlägigen nationalen Rechtsvorschriften wahrzunehmen.

(11) Gemäß Artikel 64 Absatz 1 Buchstabe c DSGVO in Verbindung mit Artikel 10 Absatz 2 der Satzung des EDSA hat die Annahme der Stellungnahme des EDSA binnen acht Wochen ab dem ersten Werktag, nachdem der Vorsitz und die zuständige Aufsichtsbehörde beschlossen haben, dass die Akte abgeschlossen ist, zu erfolgen. Diese Frist kann unter Berücksichtigung der Komplexität der Angelegenheit auf Beschluss des Vorsitzes um weitere sechs Wochen verlängert werden.

(12) Der Schwerpunkt der Stellungnahme des EDSA liegt auf den Zertifizierungskriterien. Für den Fall, dass der EDSA umfassende Informationen über die Bewertungsmethoden benötigt, um die Überprüfbarkeit des Entwurfs der Zertifizierungskriterien im Rahmen seines Gutachtens gründlich bewerten zu können, umfasst Letzteres keinerlei Genehmigungen solcher Bewertungsmethoden —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1 ZUSAMMENFASSUNG DES SACHVERHALTS

1. Gemäß Artikel 42 Absatz 5 DSGVO und den Leitlinien wurden die Prüfer-Zertifizierungskriterien (im Folgenden „Entwurf der Zertifizierungskriterien“ oder „Zertifizierungskriterien“) von EU Cloud Service Data Protection, einer juristischen Person in Deutschland, erarbeitet und der deutschen Aufsichtsbehörde Nordrhein-Westfalen vorgelegt.

2. Die deutsche Aufsichtsbehörde hat ihren Beschlussentwurf zur Genehmigung der Zertifizierungskriterien vorgelegt und den EDSA am 12. Februar 2024 um eine Stellungnahme gemäß Artikel 64 Absatz 1 Buchstabe c DSGVO ersucht. Der Beschluss über den Abschluss der Akte erging am 15. Februar 2024. Der Vorsitz beschloss, die Frist für die Annahme dieser Stellungnahme um weitere sechs Wochen, bis zum 16. Februar 2024 zu verlängern.

2 BEWERTUNG

3. Der Ausschuss hat seine Bewertung im Einklang mit der Struktur durchgeführt, die in Anhang 2 der Leitlinien (im Folgenden „Anhang“) und ihrem Addendum vorgesehen ist. Soweit diese Stellungnahme einen bestimmten Abschnitt des Entwurfs der Zertifizierungskriterien der deutschen Aufsichtsbehörde auslässt, sollte das so verstanden werden, dass der Ausschuss keine Anmerkungen hat und die deutsche Aufsichtsbehörde nicht auffordert, weitere Maßnahmen zu ergreifen.

4. Bei diesen Zertifizierungskriterien handelt es sich um nationale Kriterien gemäß Artikel 42 Absatz 5 DSGVO, die nicht dazu bestimmt sind, ein EU-Datenschutzsiegel zu sein.

5. Die vorliegende Zertifizierung ist keine Zertifizierung gemäß Artikel 46 Absatz 2 Buchstabe f DSGVO für die internationale Übermittlungen personenbezogener Daten und bietet daher keine geeigneten Garantien im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen gemäß den in Artikel 46 Absatz 2 Buchstabe f genannten Bedingungen. Die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf nur dann erfolgen, wenn die Bestimmungen in Kapitel V DSGVO eingehalten werden.

2.1 ALLGEMEINE BEMERKUNGEN

6. Der Ausschuss nimmt zur Kenntnis, dass die Zertifizierung zwar speziell auf die Datenverarbeitung von Cloud-Anbietern ausgerichtet ist, das Zertifizierungssystem jedoch allgemeine Kriterien für Auftragsverarbeiter festlegt und auch spezifische Leitlinien für die Tätigkeit von Cloud-Anbietern enthält.

7. Der Ausschuss stellt fest, dass die Zertifizierungskriterien drei Schutzkategorien definieren. Je nachdem, welche Schutzkategorie der Cloud-Anbieter während des Zertifizierungsantrags ausgewählt hat, sind die Kriterien für die Bewertung des Evaluierungsgegenstands unterschiedlich. Folglich bleibt der Cloud-Nutzer dafür verantwortlich, den geeigneten zertifizierten Cloud-Dienst auf der Grundlage seiner Schutzkategorie auszuwählen, um die „hinreichenden Garantien“ gemäß Artikel 28 DSGVO nachzuweisen.

8. Der Ausschuss möchte auf die Konsequenzen der folgenden Aussage in Bezug auf den Antragsteller als Verantwortlicher für die Datenverarbeitungsvorgänge und die Rechtsgrundlage für die Datenverarbeitung hinweisen, die in Kriterium 13 aufgeführt ist: *„Im Rahmen der Prüfer-Zertifizierung werden daher nur Datenverarbeitungsvorgänge betrachtet, die der Cloud-Anbieter durchführt, um den Cloud-Dienst gegenüber dem Cloud-Nutzer zu erbringen, um diesem die Nutzung zu ermöglichen und um den Dienst abzurechnen."* Der Ausschuss geht davon aus, dass der Cloud-Anbieter, wenn er Datenverarbeitungsvorgänge einführt, die für die Erfüllung des Vertrags mit dem Cloud-Nutzer bei der Erbringung seiner Dienstleistung nicht erforderlich sind, diese nicht in den Anwendungsbereich des Prüfer-Zertifizierungsverfahrens fallen.

9. Der Ausschuss stellt fest, dass in den Entwürfen der Zertifizierungskriterien Fachsprache verwendet wird, die der Terminologie der DSGVO oder anderen Konzepten und Definitionen entspricht. Generell empfiehlt der Ausschuss der deutschen Aufsichtsbehörde zu gewährleisten, dass die Begriffe der DSGVO, wenn sie in den Zertifizierungskriterien verwendet werden, mit der DSGVO im Einklang stehen, und am Anfang der Kriterien eine Erklärung aufzunehmen, in der erläutert wird, dass in Fällen, in denen die Zertifizierungskriterien Begriffe verwenden, die in der DSGVO definiert sind, diese Begriffe dieselbe Bedeutung haben wie in der DSGVO. Dies gilt insbesondere für folgende Abschnitte:

   - Abschnitt A.1 auf den „Prüfer-Zertifizierungsgegenstand", der dem Evaluierungsgegenstand entspricht; diese Wortwahl wäre verständlicher;
   - in Abschnitt C Kapitel 1 Nummer 1.3 „Art und Zwecke der Datenverarbeitung" heißt es im Entwurf der Zertifizierungskriterien: „In der rechtsverbindlichen Vereinbarung über die in Auftrag gegebene Datenverarbeitung muss im Auftrag die Art und den Zweck der beabsichtigten Datenverarbeitung, die Art der verarbeiteten Daten und die Kategorien betroffener Personen festgelegt werden." In diesem Zusammenhang würde die Verwendung des Begriffs „Art" (type) anstelle von „Wesen" (nature) der verarbeiteten Daten dem Wortlaut von Artikel 28 Absatz 3 DSGVO entsprechen.
   - in Abschnitt C Kapitel 1 Nr. 1.8 „Rückgabe von Datenträgern und Löschung von Daten; Nachweis der Einhaltung der Sorgfaltspflichten bzw. und Beteiligung an und Mitwirkung bei Audits"; ein Verweis auf die Rückgabe aller personenbezogenen Daten, wie in Artikel 28 Absatz 3 Buchstabe g DSGVO vorgesehen, würde für größere Einheitlichkeit sorgen.
   - Abschnitt C Kapitel 2 Nummer 2.4 (4) „Zugriffskontrolle" beinhaltet folgenden Wortlaut: „Gegen vorsätzliche Eingriffe besteht ein Mindestschutz, der diese erschwert." Dies senkt die in Artikel 32 Absatz 1 DSGVO vorgesehenen Garantien, und eine Neufassung wäre angemessen, um die Kohärenz mit der DSGVO zu gewährleisten, auch unter Berücksichtigung des risikobasierten Ansatzes, den das entsprechende Kriterium bereits zu Beginn umfasst, z. B. indem dieser Satz durch folgenden ersetzt wir: „Es wird nachgewiesen, dass die TOM den Schutz vor vorsätzlichen Eingriffen garantieren".
   - In Abschnitt C Kapitel 2 Nummer 2.6 (2) „Nachvollziehbarkeit der Datenverarbeitung" wird sich auf folgende Tatsache bezogen: „Der Cloud-Anbieter sieht einen Mindestschutz gegen vorsätzliche Manipulationen der Maßnahmen zur Nachvollziehbarkeit vor, sodass derartige Manipulationen erschwert werden." Der

Ausschuss ist der Auffassung, dass eine Umformulierung angemessen wäre, um dem in der DSGVO verankerten Schutzniveau besser zu entsprechen, z. B.: „Es ist nachzuweisen, dass die TOM gewährleisten, dass vorsätzliche Manipulationen der Rückverfolgbarkeitsmaßnahmen verhindert werden."

10. Der Ausschuss stellt fest, dass im Kriterium Nr. 9.1 (1) „konzeptionelle Zielsetzung" genannt wird. Der Ausschuss empfiehlt, die Bedeutung dieses Begriffs zu klären.

11. Der Ausschuss ist der Auffassung, dass die Formulierung „unangemessene Risiken" (Kriterium 9.2 und 19.2) unklar ist und weiter ausgearbeitet werden sollte. Ebenso wird der Begriff „unberechtigter Zugriff" in Kriterium 2.4 verwendet, das sich im Einklang mit Artikel 32 Absatz 2 DSGVO stattdessen auf den „unbefugten Zugang" beziehen sollte. Daher empfiehlt der Ausschuss, in den Kriterien genauer zu verdeutlichen, was „unangemessene Risiken" sind, und in Kriterium 2.4 auf die entsprechende Terminologie der DSGVO Bezug zu nehmen.

12. Darüber hinaus stellt der Ausschuss fest, dass sich der Entwurf der Zertifizierungskriterien auf folgende Begriffe bezieht:
    - Abschnitt A Nummer 1 „Inhalts- oder Anwendungsdaten";
    - Abschnitt A, 1 „Geschäft";
    - Abschnitt A, 1 „Verbraucher";
    - Abschnitt A, 1 „B2B";
    - Abschnitt A, 1 „B2C";
    - Abschnitt A Nummer 1 „Nutzungsdaten";
    - Abschnitt A Nummer 1 „Vereinbarung über die in Auftrag gegebene Datenverarbeitung".

    Der Ausschuss begrüßt die Verwendung dieser Begriffe. Um die Lesbarkeit und das Verständnis der Zertifizierungskriterien zu verbessern, empfiehlt der Ausschuss jedoch, die oben genannten Begriffe klar zu definieren, wobei erforderlichenfalls auch andere Rechtsbereiche (z. B. die Richtlinie 93/13/EWG vom 5. April 1993) zu berücksichtigen sind. Zu diesem Zweck regt der Ausschuss an, dass entweder ein neuer Abschnitt „Begriffe und Begriffsbestimmungen" hinzugefügt wird oder dass relevante Begriffe im Rahmen der Kriterien klar definiert werden.

13. In ähnlicher Weise wird in den Kriterien auf den Begriff „Force Majeure" Bezug genommen. Es könnte sinnvoll sein, auf den Begriff „höhere Gewalt" in deutscher Sprache Bezug zu nehmen, um die Übereinstimmung mit dem gemeinschaftlichen Besitzstand zu gewährleisten. Dieser Begriff wird in zahlreichen Instrumenten und Bereichen des europäischen Rechts verwendet, und seine Definition wurde vom EuGH mehrfach in der Rechtsprechung gefestigt (siehe z. B. Rn. 53 in der Rechtssache C-640/15, ECLI:EU:C:2017:39). Um Missverständnisse zu vermeiden, empfiehlt der Ausschuss daher, auf dieses Konzept des EU-Rechts zu verweisen und eine entsprechende Definition vorzulegen.[4]

14. Darüber hinaus stellt der Ausschuss fest, dass auf Seite 7 des Entwurfs der Zertifizierungskriterien auf „Personenbezogene Daten als das zu schützende Gut" Bezug genommen wird. Der Ausschuss ist der Ansicht, dass dieser Begriff weder verständlich noch

[4] Unter ‚höherer Gewalt' sind ungewöhnliche und unvorhersehbare Ereignisse zu verstehen, auf die derjenige, der sich darauf beruft, keinen Einfluss hat und deren Folgen trotz Anwendung der gebotenen Sorgfalt nicht hätten vermieden werden können.

rechtlich fundiert ist. Daher empfiehlt der Ausschuss der deutschen Aufsichtsbehörde, diesen Begriff durch den Begriff „Informationen“ zu ersetzen.

15. Darüber hinaus nimmt der Ausschuss Abschnitt 2.5 zur „Übertragung von Daten und Transportverschlüsselung“ und Abschnitt 2.7 zur Kenntnis. Der Ausschuss geht davon aus, dass sich der Begriff „Übertragung“ [transfer] auf die Übertragung der Daten bezieht und nicht auf ihre Übermittlung im Sinne der DSGVO, insbesondere in Kapitel V DSGVO. Um Verwirrung zu vermeiden, regt der Ausschuss daher an, den Begriff „transfer“ durch den Begriff „transmission“ zu ersetzen.

16. Darüber hinaus betont der Ausschuss, dass die Kriterien darauf abzielen, ein transparentes Datenschutzniveau festzulegen. Kriterien, die einen „Mindestschutz“ (Kriterium 2.2 (3) und 2.10 (2)) oder „hinreichende Sicherheit“ (Kriterium 2.3 (8)) oder „gleichermaßen angemessene Maßnahmen“ (Kriterium 2.5 und 2.6 (6)) oder die „Erfüllung der aktuellen technischen Empfehlungen (best practices)“ (Kriterium 2.9(4)) erfordern, verfehlen dieses Ziel und könnten zu einer uneinheitlichen Bewertung durch die Zertifizierungsstellen führen. Daher empfiehlt der EDSA, die oben aufgeführten Kriterien zu ändern, um eine klarere Definition des Datenschutzniveaus zu gewährleisten.

2.2 ANWENDUNGSBEREICH DES ZERTIFIZIERUNGSVERFAHRENS UND EVALUIERUNGSGEGENSTAND (EVG)

17. Das Prüfer-Zertifizierungsverfahren steht nur Cloud-Anbietern des privaten Sektors offen, die als Auftragsverarbeiter für Cloud-Nutzer (Organisationen oder natürliche Personen des Privatsektors) als Verantwortliche fungieren. Auch Datenverarbeitungsvorgänge des Cloud-Anbieters, der als Verantwortlicher fungiert und der für die Erbringung seiner Cloud-Dienste für den Cloud-Nutzer erforderlich sind, können im Rahmen des Systems zertifiziert werden.

18. Gemäß der Programmdokumentation umfasst die Prüfer-Zertifizierung „*Datenverarbeitungsvorgänge, die in Produkten oder Diensten oder mithilfe von (auch mehreren) Produkten und Diensten erbracht werden*“. In der Programmdokumentation wird ferner klargestellt, dass das Zertifizierungsverfahren Datenverarbeitungsvorgänge abdeckt, die der Cloud-Anbieter

    (i) als Auftragsverarbeiter „*im Auftrag (Auftragsverarbeitung) nach Art. 28 DSGVO*“;

    (ii) als Verantwortlicher „*um den Vertrag mit dem Cloud-Nutzer über die Bereitstellung des Cloud-Dienstes schließen und diesen durchführen zu können*“; und

    (iii) als Verantwortlicher „*zur Erfüllung rechtlicher Pflichten*“ durchführt.

    In Bezug auf Ziffer ii ist der Ausschuss der Auffassung, dass aus der Regelung nicht klar hervorgeht, welche Verarbeitungsvorgänge unter den Wortlaut *„um den Vertrag mit dem Cloud-Nutzer über die Bereitstellung des Cloud-Dienstes schließen und diesen durchführen zu können“* fallen würden oder nicht. Der Ausschuss empfiehlt daher, den Anwendungsbereich dieser Regelung weiter zu präzisieren, um Folgendes zu erfassen:

    (i) festgelegte, eindeutige und legitime Kategorien von Zwecken der Datenverarbeitung, bei denen der Cloud-Anbieter als Verantwortliche fungiert; und

(ii) Beispiele für Verarbeitungsvorgänge, die

a. im Rahmen der Regelung zertifiziert werden können; und

b. im Rahmen der Regelung nicht zertifiziert werden können.

Diese Klarstellung ist von wesentlicher Bedeutung, um die geeignete Rechtsgrundlage gemäß Artikel 6 DSGVO zu ermitteln und die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten gemäß Artikel 5 DSGVO sicherzustellen.

19. Der Ausschuss erkennt an, dass in Fällen, in denen es sich bei dem Cloud-Nutzer um eine natürliche Person handelt, einige Szenarien auftreten können, in denen die DSGVO nicht für die Verarbeitung personenbezogener Daten durch diese natürliche Person im Rahmen einer rein persönlichen oder familiären Tätigkeit gilt (die in Artikel 2 Absatz 2 Buchstabe c DSGVO vorgesehene sogenannte „Ausnahmeregelung für Haushalte“ oder „persönliche Ausnahme“). In einem solchen Szenario würde die DSGVO weiterhin für den Cloud-Anbieter gelten, der als Auftragsverarbeiter fungiert und die Instrumente für die Verarbeitung bereitstellt (wie in Erwägungsgrund 18 der DSGVO angegeben). Allerdings werden nicht alle Anwendungsfälle im Rahmen einer Beziehung zwischen Unternehmen und Verbrauchern die Anwendbarkeit der Ausnahme für Haushalte/persönliche Zwecke zur Folge haben, und der Ausschuss empfiehlt, in den Kriterien klarzustellen, in welchen Fällen die Ausnahme für den Cloud-Nutzer, der eine natürliche Person ist, nicht gelten würde.

20. Der Ausschuss hebt ferner hervor, dass die Anwendung der Ausnahme für die persönliche Nutzung oder private Haushalte auf den Cloud-Nutzer die sich aus der DSGVO ergebenden Verpflichtungen unberührt lässt, die für den Cloud-Diensteanbieter gelten, wenn dieser in einem solchen Szenario Auftragsverarbeiter ist. Insbesondere in diesem Fall muss der Cloud-Diensteanbieter alle einschlägigen Verpflichtungen erfüllen, die sich aus Artikel 28 DSGVO ergeben. Der Ausschuss empfiehlt daher, das Verfahren zu ändern, um deutlich zu machen, wie die Zertifizierungskriterien anzupassen sind, wenn die Ausnahme für Haushalte/persönliche Ausnahme gegenüber dem Cloud-Nutzer gilt (d. h. zu ermitteln, welche spezifischen Kriterien diese Situation abdecken bzw. welche Kriterien in diesem Fall nicht gelten).

21. Der Ausschuss stellt fest, dass der Kriterienkatalog keine spezifischen Bestimmungen oder Erwägungen in Bezug auf die Verarbeitungstätigkeiten im Zusammenhang mit der technischen Unterstützung und der Wartung von Cloud-Diensten enthält, insbesondere wenn diese Tätigkeiten den Zugang zu personenbezogenen Daten mit sich bringen. Der Ausschuss empfiehlt daher klarzustellen, dass die Verarbeitung personenbezogener Daten im Zuge von Unterstützungs- oder Wartungstätigkeiten im Prüfer-Zertifizierungsverfahren ausdrücklich behandelt wird, sodass die Nutzer ein klares Verständnis und Gewissheit darüber haben, wie personenbezogene Daten bei diesen wesentlichen Aufgaben verarbeitet werden.

22. Aus Gründen der Transparenz sind die Bedingungen, die erfüllt sein müssen, um die Nichtanwendbarkeit eines Kriteriums festzustellen, standardmäßig Bestandteil der Kriterien. Der Ausschuss räumt auch ein, dass einige Kriterien je nach Umständen der Datenverarbeitung möglicherweise nicht relevant sind. Solche Besonderheiten müssen begründet und dokumentiert werden, damit der Cloud-Nutzer über die Gründe informiert wird, aus denen einige Kriterien nicht bewertet werden konnten. Der Ausschuss empfiehlt jedoch, die

folgenden Kriterien weiter auszuführen, wenn die Voraussetzungen für die Nichtanwendbarkeit in der DSGVO festgelegt sind:

— das Kriterium 8.1 dahin gehend, dass Bedingungen festgelegt werden, die erfüllt sein müssen, um zu rechtfertigen, dass kein Datenschutzbeauftragter benannt wurde;

— das Kriterium 8.3 dahin gehend, dass Bedingungen festgelegt werden, die erfüllt sein müssen, um zu rechtfertigen, dass kein Verarbeitungsverzeichnis geführt wird;

— das Kriterium 16 dahin gehend, dass Faktoren festgelegt werden, die bei der Bewertung des Risikos für die Rechte und Freiheiten betroffener Personen zu berücksichtigen sind, wie in den Leitlinien 9/2022 des EDSA für die Meldung von Verletzungen des Schutzes personenbezogener Daten im Rahmen der DSGVO festgelegt.

2.3 VERARBEITUNGSVORGÄNGE NACH ARTIKEL 42 ABSATZ 1 DSGVO

23. In Bezug auf Kriterium 1.5 empfiehlt der EDSA klarzustellen, dass die nach Kriterium 1.5 (Ort der Datenverarbeitung) erforderlichen Informationen auch den Ort der Verarbeitungstätigkeiten umfassen, die von Unterauftragsverarbeitern durchgeführt werden, wenn der Antragsteller einen anderen Auftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten im Namen des Verantwortlichen beauftragt.

2.4 ZULÄSSIGKEIT DER VERARBEITUNG

24. Der Ausschuss stellt fest, dass mit dem Entwurf des Kriteriums 13 Absatz 1 versucht wird, den Anforderungen von Artikel 6 Absatz 1 Buchstabe b DSGVO Rechnung zu tragen, indem Folgendes festgelegt wird: „*Der Cloud-Anbieter* [als Verarbeiter] *darf ausschließlich personenbezogene Daten verarbeiten und Verarbeitungsvorgänge ausführen, solange dies für die Erfüllung eines Vertrags mit dem Cloud-Nutzer oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage des Cloud-Nutzers erfolgen, erforderlich ist*.“ Da der „Cloud-Nutzer“ für das Verfahren jedoch als Verantwortlicher definiert ist, kann es sich bei dem Cloud-Nutzer um eine Organisation oder eine natürliche Person handeln und somit spiegelt dieses Kriterium nicht die Anforderung von Artikel 6 Absatz 1 Buchstabe b wider, wonach ein Verantwortlicher personenbezogene Daten nur dann verarbeiten darf, wenn dies für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Daher empfiehlt der Ausschuss, den Begriff „Cloud-Nutzer“ in Kriterium 13 Absatz 1 durch „betroffene Person“ zu ersetzen und den erläuternden Teil desselben Kriteriums weiter zu ändern.

25. Der Ausschuss stellt fest, dass der Entwurf des Kriteriums 13 Absatz 3 wie folgt lautet: „D*er Cloud-Anbieter* [als Verarbeiter] darf *ausschließlich personenbezogene Daten verarbeiten und Verarbeitungsvorgänge ausführen, solange dies zur Erfüllung des Vertrags mit dem Cloud-Nutzer erforderlich sind und nicht die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person gegen die Verarbeitung überwiegen.*“ Es ist jedoch nicht klar, wie bestimmt wird, ob eine Verarbeitungstätigkeit:

- **sowohl** i) für die Zwecke der berechtigten Interessen des Cloud-Anbieters **als auch** ii) für die Erfüllung des Vertrags mit dem Cloud-Nutzer erforderlich ist und somit Kriterium 13 Absatz 3 erfüllt; oder

- **entweder** i) nur für die Zwecke der berechtigten Interessen des Cloud-Anbieters erforderlich ist **oder** ii) nur für die Erfüllung des Vertrags mit dem Cloud-Nutzer erforderlich ist und somit Kriterium 13 Absatz 3 nicht erfüllt.

Daher empfiehlt der Ausschuss, das Kriterium 13 zu ändern, indem weitere Anforderungen hinzugefügt werden, die es ermöglichen, das Vorstehende zu ermitteln.

26. Der Ausschuss nimmt zur Kenntnis, dass Kriterium 13 Absätze 1 und 3 Situationen abdecken, in denen der Cloud-Anbieter als Verantwortlicher personenbezogene Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstaben b und f DSGVO in der vorvertraglichen und nachvertraglichen Phase oder zur Erfüllung eines Vertrags verarbeiten kann. Der EDSA empfiehlt, den Entwurf von Kriterium 13 Absätze 1 und 3 zu ändern, um klarzustellen, welche Verarbeitungsvorgänge in der vor- und nachvertraglichen Phase, für die der Cloud-Anbieter als Verantwortlicher verantwortlich ist, erfasst werden, und dass jeder erläuternde Text entsprechend geändert wird.

27. Darüber hinaus scheinen die Umstände in einem Vertragsverhältnis zwischen Verantwortlichen und Auftragsverarbeitern, unter dem ein Cloud-Anbieter personenbezogene Daten eines Cloud-Nutzers als Verantwortlicher verarbeiten kann, begrenzt zu sein. Dennoch heißt es in dem Entwurf des Kriteriums 13 Absätze 1 und 3, dass der Cloud-Anbieter personenbezogene Daten zur Erfüllung seines Vertrags als Verantwortlicher verarbeiten darf, es werden jedoch keine Beschränkungen der Umstände festgelegt, unter denen ein Cloud-Anbieter dies tun darf. In den Erläuterungen zu den Kriterien (S. 73f) wird klargestellt, dass dies die Behebung von Fehlern, die Einhaltung von Dienstgütevereinbarungen, die direkte Kommunikation mit dem Nutzer und die Analyse des Zugriffsverhaltens usw. umfasst. Obwohl die genannten Verarbeitungsvorgänge möglicherweise vom Cloud-Anbieter als Verantwortlicher vorgenommen werden könnten, scheinen mehrere dieser Verarbeitungsvorgänge in erster Linie vom Cloud-Anbieter als Auftragsverarbeiter vorgenommen zu werden. Daher empfiehlt der EDSA, den Entwurf des Kriteriums 13 Absätze 1 und 3 dahingehend zu ändern, dass klargestellt wird, dass diese Kriterien nicht für Verarbeitungsvorgänge gelten, die unter die Verarbeitungsvereinbarung mit dem Cloud-Nutzer fallen. Darüber hinaus spricht sich der EDSA für die Einführung einer umfassenden Liste der Verarbeitungsvorgänge im Vertragsverhältnis zwischen dem Cloud-Anbieter und dem Cloud-Nutzer aus, die unter den Entwurf des Kriteriums 13 Absätze 1 und 3 fallen.

2.5 ALLGEMEINE PFLICHTEN VON VERANTWORTLICHEN UND AUFTRAGSVERARBEITERN

2.5.1 Pflichten der Verarbeiter

28. Der Ausschuss stellt fest, dass es im Entwurf des Kriteriums 10.1 (1) heißt: *„Zustimmungsbedürftig sind nur solche Subaufträge, bei denen der weitere Auftragsverarbeiter eine Möglichkeit hat, die zu verarbeitenden personenbezogenen Daten zur Kenntnis zu nehmen. Insbesondere darf der Subauftrag nicht dazu führen, dass die Wahrung der Betroffenenrechte erschwert wird.“* Diese Formulierung ist verwirrend und steht offenbar nicht im Einklang mit Artikel 28 Absatz 2 DSGVO. Der Ausschuss empfiehlt, diese Formulierung durch folgenden Wortlaut zu ersetzen: „Im Falle einer allgemeinen schriftlichen Genehmigung unterrichtet der Cloud-Anbieter den Cloud-Nutzer über alle beabsichtigten Änderungen in Bezug auf die Ergänzung oder Ersetzung anderer Verarbeiter, wodurch der Cloud-Nutzer die Möglichkeit erhält, Einwände gegen solche Änderungen zu erheben“.

29. Der Ausschuss stellt fest, dass die Kriterien im Entwurf des Kriteriums 10.1 Absatz 3 nicht die Verpflichtung des Auftragsverarbeiters umfassen, bei der Beauftragung eines Unterauftragsverarbeiters sicherzustellen, dass dem Unterauftragsverarbeiter gemäß Artikel 28 Absatz 4 DSGVO dieselben Verpflichtungen auferlegt werden, wie sie im Vertrag oder in einem anderen Rechtsakt zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind. Daher empfiehlt der Ausschuss, den Entwurf der Zertifizierungskriterien entsprechend umzuformulieren, um diese Verpflichtung aufzunehmen.

30. In demselben Abschnitt wird im Entwurf des Kriteriums 10.1 „Weitere Auftragsverarbeiter des Cloud-Anbieters (Subauftragsverarbeitung)“ erwähnt, dass „der Subauftrag nicht dazu führen [darf], dass die Wahrung der Betroffenenrechte erschwert wird“. Der Ausschuss ist der Ansicht, dass die Art und Weise, wie dieses Kriterium formuliert wird, die in Artikel 28 DSGVO vorgesehenen Garantien verringert, und empfiehlt daher, entweder den Wortlaut dieses Kriteriums so zu ändern, dass er mit der DSGVO in Einklang steht, oder diesen Teil zu streichen.

31. Der Ausschuss stellt fest, dass der Entwurf der Kriterien 9.2 und 19.2 „Datenschutz durch Voreinstellungen“ folgenden Wortlaut enthält: „Der Cloud-Anbieter stellt durch Voreinstellungen sicher, dass personenbezogene Daten nicht ohne Eingreifen der betroffenen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden und hierbei keine Risiken für die betroffenen Personen durch eine zu umfassende Zugänglichmachung von personenbezogenen Daten entstehen.“. Erstens ist der Ausschuss der Auffassung, dass die Formulierungen „Risiken“ und „zu umfassend“ unklar sind und weiter ausgearbeitet werden sollten. Diese Kriterien sollten auch klarstellen, dass die dem Cloud-Anbieter unterstellten Personen nur nach dem Grundsatz „Kenntnis nur, wenn nötig“ auf die Daten zugreifen dürfen. Zweitens hebt der Ausschuss in Bezug auf die Kriterien 9.2 und 19.2 hervor, dass sich die Pflichten der Verantwortlichen gemäß Artikel 25 Absatz 2 DSGVO nicht auf die Zugänglichkeit der Daten beschränken, sondern sich auch auf die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung und die Dauer ihrer Speicherung erstrecken. Daher empfiehlt der Ausschuss, die Kriterien 9.2 und 19.2 entsprechend umzuformulieren.

2.6 RISIKEN FÜR DIE RECHTE UND FREIHEITEN NATÜRLICHER PERSONEN

32. Der EDSA stellt fest, dass der Cloud-Anbieter gemäß dem Kriterium 2.1 (1) verpflichtet ist, eine Risikoanalyse in Bezug auf die Datensicherheit durchzuführen. Darüber hinaus wird im Kriterium 2.1 (5) vorgesehen, dass der Cloud-Anbieter die Maßnahmen zur Datensicherheit zur Minderung der von ihm ermittelten Risiken festlegt.

    Weitere Kriterien sind im Abschnitt „Gewährleistung der Datensicherheit durch geeignete TOM nach dem Stand der Technik“ des Kriterienkatalogs festgelegt. Ferner werden die Anforderungen an TOM in Bezug auf verschiedene Sicherheitsaspekte wie Sicherheitsbereich und Zutrittskontrolle (2.2), Zugangskontrolle (2.3) und Zugriffskontrolle (2.4) festgelegt. Aus Gründen der Klarheit empfiehlt der EDSA, die Kriterien stärker zu differenzieren, indem der Cloud-Anbieter

- ein spezifisches Risikoszenario bei der Durchführung einer Risikoanalyse in Bezug auf die Datensicherheit berücksichtigt (z. B. 2.2 (1) „*Der Cloud-Anbieter stellt durch risikoangemessene TOM sicher, dass Räume und Anlagen gegen Schädigung durch Naturereignisse gesichert werden [...]*“),

- verbindliche TOM einführt (z. B. 2.2 (2) „*Der Cloud-Anbieter überprüft den Zutritt zu Räumen und Datenverarbeitungsanlagen durch eine Zwei-Faktor-Authentifizierung*.“).

2.7 TECHNISCHE UND ORGANISATORISCHE SCHUTZVORKEHRUNGEN

33. Der Ausschuss stellt fest, dass sich Kriterium 16 im Zusammenhang mit der Meldung von Verletzungen des Schutzes personenbezogener Daten nicht auf die Pflichten des Verantwortlichen gemäß Artikel 33 Absatz 1 DSGVO bezieht, insbesondere in Bezug auf die Frist von 72 Stunden. Darüber hinaus heißt es in Kriterium 16: „Der Cloud-Anbieter meldet der Aufsichtsbehörde Datenschutzverletzungen, **wenn sie voraussichtlich** nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führen.“, wobei die DSGVO folgenden Wortlaut hat: „es sei denn, dass die Verletzung des Schutzes personenbezogener Daten [...]“. Daher empfiehlt der Ausschuss, diese Kriterien zu ändern, um sicherzustellen, dass sie mit der DSGVO im Einklang stehen.

34. In Bezug auf Abschnitt 2.5 Absatz 2 des Entwurfs der Zertifizierungskriterien „*Übertragung von Daten und Transportverschlüsselung*“ begrüßt der Ausschuss die Aufnahme des Kriteriums „*Bei verschlüsselter Übertragung sind die Kodierungsschlüssel sicher aufzubewahren.*“. Der Ausschuss ist der Auffassung, dass mit dem Kriterium weiter klargestellt werden soll, wie die Kodierungsschlüssel als sicher aufbewahrt angesehen werden können. Der Ausschuss hält es für wichtig, dass konkrete und überprüfbare Kriterien für die getroffenen Sicherheitsmaßnahmen vorhanden sind. Der Ausschuss empfiehlt daher, dieses Kriterium entsprechend zu ändern.

35. Darüber hinaus stellt der Ausschuss in Abschnitt 2.7 Absatz 1 zur „Pseudonymisierung“ fest, dass der Cloud-Anbieter es dem Cloud-Nutzer ermöglichen muss, die in pseudonymisierter Form übertragenen Daten zu verarbeiten. Der Ausschuss betont, dass dieses Kriterium den Eindruck erweckt, dass sich die Pseudonymisierung auf übertragene oder übermittelte personenbezogene Daten beschränkt. Der Ausschuss ist jedoch der Auffassung, dass dies nicht mit Artikel 32 im Einklang steht, der die Pseudonymisierung nicht auf diese beiden Situationen beschränkt. Daher empfiehlt der Ausschuss, dieses Kriterium entsprechend zu ändern.

36. In Bezug auf Abschnitt 2.8 Absatz 1 „Anonymisierung“ empfiehlt der Ausschuss aus Gründen der Genauigkeit, dass das Kriterium in Bezug auf den Cloud-Anbieter, mit dem sichergestellt wird, dass die Anonymisierung nicht aufgehoben werden kann, geändert wird und dass auf die Einrichtung von TOM Bezug genommen wird, um sicherzustellen, dass die Anonymisierung nicht rückgängig gemacht werden kann.

5 In Bezug auf Abschnitt 2.9 „Verschlüsselung gespeicherter Daten“ empfiehlt der Ausschuss klarzustellen, dass die Speicherung auch Backups der gespeicherten Daten umfasst. Darüber hinaus ist der Ausschuss in Bezug auf die „Schutzkategorie 1“ der Auffassung, dass das Kriterium unklar ist, was möglicherweise zu unterschiedlichen Auslegungen führen kann. Gilt das Kriterium nur für Daten, die vom Cloud-Nutzer verschlüsselt wurden, bevor sie in der Cloud gespeichert werden, empfiehlt der Ausschuss, den Satz so umzuformulieren, dass nur diese Bedeutung erfasst wird (z. B.: „Der Cloud-Anbieter muss es dem Cloud-Nutzer ermöglichen, vom Cloud-Nutzer verschlüsselte Daten zu speichern“). Bietet der Cloud-Anbieter dem Cloud-Nutzer jedoch Verschlüsselungsinstrumente an, verwaltet der Cloud-Anbieter die kryptografischen Schlüssel für die Verschlüsselung/Entschlüsselung. Der

Ausschuss empfiehlt daher, klarzustellen, dass der Antragsteller die „Schutzkategorie 1“ nicht auswählen kann, wenn sein Angebot Verschlüsselungsinstrumente für den Cloud-Nutzer enthält, da dieses Schutzniveau kein sicheres Schlüsselmanagement abdeckt.

2.8 KRITERIEN FÜR DEN NACHWEIS DES VORHANDENSEINS GEEIGNETER GARANTIEN FÜR DIE ÜBERMITTLUNG PERSÖNLICHER DATEN

37. Der Ausschuss begrüßt den Entwurf des Kriteriums 11 „Datenübermittlung“. Der Ausschuss stellt jedoch fest, dass die Begriffsbestimmungen, die sich auf „Datenimporteur“ und „Datenexporteur“ beziehen, weder denen entsprechen, die der Ausschuss in seinen Leitlinien 05/2021 über das Zusammenspiel zwischen der Anwendung des Artikels 3 und der Bestimmungen über internationale Übermittlungen nach Kapitel V DSGVO noch von der Europäischen Kommission in den Standardvertragsklauseln für internationale Übermittlungen bereitgestellt hat. Aus Gründen der Kohärenz empfiehlt der Ausschuss daher, diese Begriffsbestimmungen entsprechend zu überarbeiten.

38. Der Ausschuss konnte keine spezifischen Kriterien für Übermittlungen feststellen, die anwendbar wären, wenn der Cloud-Anbieter als Verantwortlicher auftritt. Der Ausschuss empfiehlt, spezielle Kriterien hinzuzufügen, um diese Situationen abzudecken.

39. Angesichts der vorstehenden Erwägungen geht der Ausschuss davon aus, dass die im System enthaltenen Kriterien für Übermittlungen nur für Cloud-Anbieter gelten, die als Auftragsverarbeiter fungieren. In diesem Zusammenhang stellt der Ausschuss fest, dass der Entwurf der Kriterien neben einem allgemeinen Verweis auf die „Vereinbarung über die in Auftrag gegebene Datenverarbeitung“ mit dem Verantwortlichen offenbar den Auftragsverarbeiter in vollem Umfang für die Bewertung der zu verwendenden Übermittlungsinstrumente, der Rechtsvorschriften des Drittlands sowie gegebenenfalls der zu ergreifenden ergänzenden Maßnahmen verantwortlich hält. Vielmehr ist gemäß Artikel 28 Absatz 3 Buchstabe a DSGVO daran zu erinnern, dass der Auftragsverarbeiter als Datenexporteur im Namen des Verantwortlichen handelt und sicherstellen muss, dass die Bestimmungen des Kapitels V bei der betreffenden Übermittlung gemäß den Anweisungen des Verantwortlichen eingehalten werden, einschließlich der Verwendung eines geeigneten Übermittlungsinstruments. 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.[5]

40. Daher empfiehlt der Ausschuss, insbesondere in den Punkten 3 und 4 des Entwurfs des Kriteriums 11.1 sowie in den Erläuterungen, den Umsetzungsleitlinien und dem Abschnitt über die wesentlichen europäischen Garantien (insbesondere in Bezug auf den Verweis auf ergänzende Maßnahmen im Absatz über wirksame Rechtsbehelfe[6]) darauf hinzuweisen, dass

[5] Siehe Leitlinien 5/2021 über das Zusammenspiel zwischen der Anwendung des Artikels 3 und der Bestimmungen über internationale Übermittlungen nach Kapitel V DSGVO, Nummer 19.

[6] In diesem Zusammenhang sollte der Verantwortliche gemäß Artikel 28 Absatz 3 Buchstabe a DSGVO in der Lage sein, den Auftragsverarbeiter aufzufordern, die in Bezug auf das Recht und die Praxis des Drittlands durchgeführte Bewertung vorzulegen, um zu überprüfen, ob die vom Auftragsverarbeiter ergriffenen

der Auftragsverarbeiter „im Einklang mit den Anweisungen des für die Verarbeitung Verantwortlichen“ handeln muss.

41. Was den Zugang zu den von Behörden von Drittländern übermittelten Daten betrifft, so schreibt der Entwurf des Kriteriums 11.1 in Punkt 5 vor, dass der Cloud-Anbieter personenbezogene Daten nur dann offenlegt, wenn die Offenlegung auf einem geltenden internationalen Abkommen zwischen dem ersuchenden Drittland und der EU oder Deutschland beruht. In einem solchen Fall betont der Ausschuss, dass der Auftragsverarbeiter im Einklang mit Artikel 28 Absatz 3 Buchstabe a DSGVO den Verantwortlichen vor jeder Offenlegung über diese rechtliche Anforderung unterrichtet, es sei denn, das Gesetz verbietet diese Unterrichtung aus Gründen eines wichtigen öffentlichen Interesses, die im Unionsrecht oder im deutschen Recht verankert sind, und empfiehlt, den Entwurf des Kriteriums entsprechend zu ändern.

42. Darüber hinaus bezieht sich der Entwurf des Kriteriums 11.2 auf Cloud-Anbieter ohne Niederlassung in der EU oder im EWR, die jedoch gemäß Artikel 3 Absatz 2 der DSGVO unterliegen. Folglich geht der Ausschuss davon aus, dass das Zertifizierungsverfahren für Zertifizierungskunden gilt, die außerhalb der EU oder des EWR ansässig sind. Da dies bedeuten könnte, dass ein solcher Auftragsverarbeiter mit Sitz außerhalb der EU/des EWR auch personenbezogene Daten außerhalb der EU/des EWR verarbeiten könnte, empfiehlt der Ausschuss, im Entwurf des Kriteriums 11.1 klarzustellen, dass immer dann, wenn eine „Übermittlung“ im Sinne von Artikel 44 DSGVO an einen Auftragsverarbeiter mit Sitz außerhalb der EU oder des EWR erfolgt, die in Kapitel V DSGVO festgelegten Verpflichtungen in vollem Umfang eingehalten werden. Darüber hinaus empfiehlt der Ausschuss, klarzustellen, dass der Antragsteller nicht berechtigt ist, die Zertifizierung in einer Weise zu nutzen, die den Eindruck erwecken könnte, dass es sich bei der Zertifizierung selbst um ein Übermittlungsinstrument gemäß Artikel 46 Absatz 2 Buchstabe f DSGVO handelt. Die Verantwortlichen sollten ungeachtet des Vorliegens der Zertifizierung dennoch eine Bewertung der Rechtsvorschriften des Empfängerlands vornehmen, bevor sie Daten an den zertifizierten Auftragsverarbeiter außerhalb der EU übermitteln. Für den Fall, dass die Rechtsvorschriften kein angemessenes Schutzniveau vorsehen, sollten zusätzliche Maßnahmen ergriffen werden. Ein Auftragsverarbeiter sollte von der Beantragung einer Zertifizierung absehen, wenn ihm bekannt ist, dass seine Rechtsvorschriften ihn daran hindern würden, die im Zertifizierungssystem verankerten Grundsätze der DSGVO einzuhalten[7].

3 SCHLUSSFOLGERUNGEN UND EMPFEHLUNGEN

43. Abschließend vertritt der EDSA folgende Meinung:

44. in Bezug auf die „allgemeinen Bemerkungen“ empfiehlt der Ausschuss, dass die deutsche Aufsichtsbehörde ihren Beschlussentwurf zur Genehmigung der Prüfer-Zertifizierungskriterien für die Datenschutz-Zertifizierung von EU-Cloud-Diensten wie folgt ändert:

zusätzlichen Maßnahmen tatsächlich ein angemessenes Schutzniveau für die in dem Drittland übermittelten personenbezogenen Daten gewährleisten.

[7] Siehe Stellungnahme 25/2022 des EDSA zu den Zertifizierungskriterien für das Europäische Datenschutzsiegel (EuroPriSe) für die Zertifizierung von Verarbeitungsvorgängen durch Auftragsverarbeiter (Nummer 9-11).

1. In den Kriterien 9.2 und 19.2 ist zu verdeutlichen, was der Begriff „unangemessene Risiken“ umfasst, und Verweis auf die entsprechende Terminologie der DSGVO.
2. In den Kriterien sind die Begriffe „Inhalts- oder Anwendungsdaten“, „Unternehmen“, „Verbraucher“, „B2B“, „B2C“, „Nutzungsdaten“ und „Vereinbarung über die in Auftrag gegebene Datenverarbeitung“ zu definieren.
3. Bei der Bezugnahme auf „personenbezogene Daten als zu schützendes Gut“ ist der Begriff „Gut“ durch den Begriff „Informationen“ zu ersetzen.
4. Die Kriterien 2.2(3), 2.9.(4), 2.10(2), 2.5, 2.6(6) sind zu ändern, da darin kein transparentes Datenschutzniveau festgelegt wird.

45. In Bezug auf den „Anwendungsbereich des Zertifizierungsverfahrens und den Evaluierungsgegenstand“ empfiehlt der Ausschuss, dass die deutsche Aufsichtsbehörde ihren Entwurf eines Beschlusses zur Genehmigung der Prüfer-Zertifizierungskriterien für die Datenschutz-Zertifizierung von EU-Cloud-Diensten wie folgt ändert:

    1. der Anwendungsbereich des Verfahrens weiter präzisiert wird auf i) festgelegte, explizite und rechtmäßige Kategorien von Datenverarbeitungsvorgängen, bei denen der Cloud-Anbieter als Verantwortlicher fungiert, und ii) Beispiele für Verarbeitungsvorgänge, die im Rahmen des Verfahrens zertifiziert bzw. nicht zertifiziert werden können;
    2. in den Kriterien klargestellt wird, in welchen Fällen die Ausnahme für Haushalte/persönliche Ausnahme nicht für den Cloud-Nutzer gilt, bei dem es sich um eine natürliche Person handelt;
    3. das Verfahren geändert wird, um deutlich zu machen, welche Anpassungen an den Zertifizierungskriterien erforderlich sind, wenn die Ausnahme für Haushalte/persönliche Ausnahme gegenüber dem Cloud-Nutzer gilt (d. h. es ist zu ermitteln, welche spezifischen Kriterien für diese Situation gelten bzw. welche Kriterien in diesem Fall nicht gelten);
    4. die Kriterien 8.1, 8.3 und 16 sind weiter auszuführen, um die Bedingungen für die Nichtanwendbarkeit nach Maßgabe der DSGVO aufzunehmen.

46. in Bezug auf die „Rechtmäßigkeit der Verarbeitung“ empfiehlt der Ausschuss, dass die deutsche Aufsichtsbehörde ihren Beschlussentwurf zur Genehmigung der Prüfer-Zertifizierungskriterien für die Datenschutz-Zertifizierung von EU-Cloud-Diensten wie folgt ändert:

    1. der Begriff „Cloud-Nutzer“ in Kriterium 13 Absatz 1 ist durch den Begriff „betroffene Person“ zu ersetzen und der erläuternde Teil dieser Kriterien ist weiter ändern;
    2. in Kriterium 13 sind weitere Anforderungen hinzuzufügen, um festzulegen, wann eine Verarbeitungstätigkeit sowohl für (i) Zwecke des berechtigten Interesses des Cloud-Anbieters als auch (ii) die Erfüllung des Vertrags mit dem Cloud-Nutzer erforderlich ist und somit Kriterium 13 Absatz 3 erfüllt oder nur für einen dieser beiden Zwecke erforderlich ist;
    3. die Kriterien 13 Absätze 1 und 3 sind zu ändern, um klarzustellen, welche Verarbeitungsvorgänge in der vor- und nachvertraglichen Phase erfasst werden, für die der Cloud-Anbieter als Verantwortlicher verantwortlich ist; jeder erläuternde Text ist entsprechend zu ändern;
    4. die Kriterien 13 Absätze 1 und 3 sind zu ändern, um klarzustellen, dass diese Kriterien nicht für Verarbeitungsvorgänge gelten, die unter die Verarbeitungsvereinbarung mit dem Cloud-Nutzer fallen.

47. in Bezug auf die „allgemeinen Pflichten der Verantwortlichen und der Auftragsverarbeiter“ empfiehlt der Ausschuss, dass die deutsche Aufsichtsbehörde ihren Entwurf eines Beschlusses zur Genehmigung der Prüfer-Zertifizierungskriterien für die Datenschutz-Zertifizierung von EU-Cloud-Diensten wie folgt ändert:

    1. das Kriterium 10.1 Absatz 1 ist in Bezug auf die Nutzung von Unterauftragnehmern durch den Cloud-Nutzer zu ändern, um es mit Artikel 28 Absatz 2 DSGVO in Einklang zu bringen;
    2. das Kriterium 10.1 Absatz 3 ist dahingehend zu ändern, dass eine Verpflichtung des Auftragsverarbeiters ergänzt wird, bei der Beauftragung eines Unterauftragsverarbeiters sicherzustellen, dass dem Unterauftragsverarbeiter gemäß Artikel 28 Absatz 4 DSGVO dieselben Verpflichtungen auferlegt werden, wie sie im Vertrag oder in einem anderen Rechtsakt zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind;
    3. der Verweis im Kriterium 10.1 darauf, dass „der Subauftrag nicht dazu führen darf, dass die Wahrung der Rechte der betroffenen Personen erschwert wird“ geändert oder gestrichen wird, da damit die Garantien nach Artikel 28 beeinträchtigt werden;
    4. die Kriterien 9 Absatz 2 und 19 Absatz 2 sind dahingehend zu ändern, dass die Begriffe „unangemessene Risiken“, „zu umfassend“ erläutert werden, dass die Personen handeln, bis die Behörde des Cloud-Diensteanbieters auf die Daten nur nach dem Grundsatz „Kenntnis nur, wenn nötig“ zugreifen kann, und dass gemäß Artikel 25 Absatz 2 DSGVO die Pflichten des Verantwortlichen keine eingeschränkte Zugänglichkeit der Daten darstellen.

48. in Bezug auf die „technischen und organisatorischen Schutzvorkehrungen“ empfiehlt der Ausschuss, dass die deutsche Aufsichtsbehörde ihren Entwurf eines Beschlusses zur Genehmigung der Prüfer-Zertifizierungskriterien für die Datenschutz-Zertifizierung von EU-Cloud-Diensten wie folgt ändert:

    1. das Kriterium 16 ist dahingehend zu ändern, dass die Verpflichtung des Verantwortlichen aufgenommen wird, die Aufsichtsbehörde innerhalb von 72 Stunden zu unterrichten, und dass der Begriff „wenn“ durch „es sei denn“ ersetzt wird, wenn auf eine Verletzung des Schutzes personenbezogener Daten Bezug genommen wird, die wahrscheinlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führen wird, Bezug genommen wird, um dieses Kriterium mit Artikel 33 DSGVO in Einklang zu bringen;
    2. das Kriterium 2.5 Absatz 2 ist weiter zu präzisieren, um zu erläutern, wie die Kodierungsschlüssel als sicher gespeichert angesehen werden können;
    3. das Kriterium 2.8 Absatz 1 ist zu ändern, indem hinzugefügt wird, dass die Anonymisierung nicht widerrufen werden kann, und indem auf die Einrichtung von TOM verwiesen wird, um sicherzustellen, dass die Anonymisierung nicht rückgängig gemacht werden kann;
    4. das Kriterium 2.9 ist zu ändern und darin ist aufzunehmen, dass die Cloud-Bereitstellung es dem Cloud-Nutzer ermöglichen muss, von ihm verschlüsselte Daten zu speichern.

49. in Bezug auf die „geeigneten Garantien im Rahmen der Übermittlung personenbezogener Daten“ empfiehlt der Ausschuss der deutschen Aufsichtsbehörde, ihren Entwurf eines Beschlusses zur Genehmigung der Prüfer-Zertifizierungskriterien für die Datenschutz-Zertifizierung von EU-Cloud-Diensten wie folgt zu ändern:

    1. Angleichung der Definitionen der Begriffe „Datenimporteur“ und „Datenexporteur“ entweder an die Definitionen der Leitlinien des EDSA über das Zusammenspiel zwischen

der Anwendung des Artikels 3 und der Bestimmungen über internationale Übermittlungen nach Kapitel V DSGVO oder an die der Europäischen Kommission in den Standardvertragsklauseln für internationale Übermittlungen genannten.
2. Aufnahme eines Verweises auf die Notwendigkeit, dass der Auftragsverarbeiter „im Einklang mit den Anweisungen des für die Verarbeitung Verantwortlichen“ handeln muss, insbesondere in den Punkten 3 und 4 des Entwurfs des Kriteriums 11.1 sowie in der Erläuterung, den Leitlinien für die Umsetzung und in dem Abschnitt über die wesentlichen europäischen Garantien (insbesondere im Hinblick auf den Verweis auf ergänzende Maßnahmen im Absatz über wirksame Rechtsbehelfe).
3. Änderung des Kriteriums 11.1 Absatz 5, einschließlich der Tatsache, dass der Auftragsverarbeiter den Verantwortlichen über jede Offenlegung personenbezogener Daten über diese rechtliche Anforderung unterrichtet, es sei denn, das Gesetz verbietet solche Mitteilungen aus Gründen des wichtigen öffentlichen Interesses, die im Unionsrecht oder im deutschen Recht verankert sind.
4. im Entwurf des Kriteriums 11.1 ist klarzustellen, dass immer dann, wenn eine „Übermittlung“ im Sinne von Artikel 44 DSGVO an einen Auftragsverarbeiter mit Sitz außerhalb der EU oder des EWR erfolgt, die in Kapitel V DSGVO festgelegten Verpflichtungen in vollem Umfang einzuhalten sind;
5. es muss deutlich gemacht werden, dass der Antragsteller nicht berechtigt ist, die Zertifizierung in einer Weise zu nutzen, die den Eindruck erwecken könnte, dass es sich bei der Zertifizierung selbst um ein Übermittlungsinstrument nach Artikel 46 Absatz 2 Buchstabe f DSGVO handelt.

4 ABSCHLIESSENDE BEMERKUNGEN

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

Gemäß Artikel 64 Absätze 7 und 8 DSGVO hat die deutsche Aufsichtsbehörde dem Vorsitz binnen zwei Wochen nach Eingang der Stellungnahme auf elektronischem Wege mitzuteilen, ob sie ihren Beschlussentwurf beibehalten oder ändern wird. Innerhalb derselben Frist übermittelt sie den geänderten Beschlussentwurf oder gibt, wenn sie nicht beabsichtigt, der Stellungnahme des EDSA zu folgen, die maßgeblichen Gründe an, aus denen sie nicht beabsichtigt, dieser Stellungnahme ganz oder teilweise zu folgen.

Die deutsche Aufsichtsbehörde muss dem EDSA ihren endgültigen Beschluss mitteilen, damit diesen im Register der Beschlüsse in Bezug auf Fragen, die im Rahmen des Kohärenzverfahrens behandelt wurden, gemäß Artikel 70 Absatz 1 Buchstabe y DSGVO erfassen kann.

Der EDSA weist darauf hin, dass die deutsche Aufsichtsbehörde gemäß Artikel 43 Absatz 6 DSGVO die Prüfer-Zertifizierungskriterien in leicht zugänglicher Form veröffentlichen und dem Ausschuss zur Aufnahme in das öffentliche Register der Zertifizierungsverfahren und Datenschutzsiegel gemäß Artikel 42 Absatz 8 DSGVO übermitteln muss.

Für den Europäischen Datenschutzausschuss
Die Vorsitzende

(Anu Talus)