Stellungnahme des EDSA nach Artikel 64 DSGVO

Stellungnahme 18/2024 zum Entwurf eines Beschlusses der Österreichischen Aufsichtsbehörde zu den Zertifizierungskriterien der DSGVO-zt GmbH

Angenommen am 16. Juli 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 das Protokoll 37, in der durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018 geänderten Fassung[1],

gestützt auf Artikel 64 Absatz 1 Buchstabe c der DSGVO und die Artikel 10 und 22 der Geschäftsordnung des Europäischen Datenschutzausschusses

in Erwägung nachstehender Gründe:

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

(2) Die Zertifizierungskriterien sind integraler Bestandteil eines Zertifizierungsverfahrens. Deshalb sieht die DSGVO Genehmigungserfordernisse vor, wobei die Kriterien – im Falle eines nationalen Zertifizierungsverfahrens – der Genehmigung durch die zuständige Aufsichtsbehörde (Artikel 42 Absatz 5 und Artikel 43 Absatz 2 Buchstabe b DSGVO) oder – im Falle eines Europäischen Datenschutzsiegels – der Genehmigung durch den EDSA (Artikel 42 Absatz 5 und Artikel 70 Absatz 1 Buchstabe o DSGVO) bedürfen.

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

[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) Diese Stellungnahme soll sicherstellen, dass die DSGVO in Bezug auf die zu entwickelnden zentralen Elemente von Zertifizierungsverfahren insgesamt sowie von den Aufsichtsbehörden, Verantwortlichen und Auftragsverarbeitern einheitlich angewendet wird. Die Bewertung durch den EDSA erfolgt insbesondere auf 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 dem nachträglich hinzugefügten Anhang „Anleitung für die Überprüfung und Bewertung von Zertifizierungskriterien“ (im Folgenden „Zusatz“), für den die Anhörungsfrist im Rahmen der öffentlichen Konsultation am 26. Mai 2021 ablief.

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

(6) Zertifizierungsmechanismen sollten es den für die Verarbeitung Verantwortlichen und den Auftragsverarbeitern ermöglichen die Einhaltung der DSGVO nachzuweisen; daher sollten die Zertifizierungskriterien die in der DSGVO festgelegten Anforderungen und Grundsätze für den Schutz personenbezogener Daten angemessen widerspiegeln und zu ihrer einheitlichen Anwendung beitragen.

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

(8) Deshalb sollten Zertifizierungen der Organisation einen Mehrwert bieten, indem sie dabei helfen, standardisierte und spezifizierte organisatorische und technische Maßnahmen zu ergreifen, die die Konformität von Verarbeitungsvorgängen nachweislich erleichtern und verbessern, wobei sektorspezifische Anforderungen berücksichtigt werden.

(9) Der EDSA begrüßt die Bemühungen der Verfahrensverantwortlichen, Zertifizierungsverfahren auszuarbeiten, die praktikable und potenziell kosteneffektive Instrumente zur Gewährleistung einer größeren DSGVO-Konformität darstellen und das Recht der betroffenen Personen auf Schutz ihrer Privatsphäre und auf Datenschutz stärken, indem sie für mehr Transparenz sorgen.

(10) Der EDSA erinnert daran, dass Zertifizierungen Instrumente einer freiwilligen Selbstkontrolle sind und dass die Einhaltung eines Zertifizierungsverfahrens weder dazu führt, dass sich die Verantwortung der Verantwortlichen und der Auftragsverarbeiter für die Einhaltung der DSGVO reduziert, noch dazu, dass die Aufsichtsbehörden gehindert wären, ihre sich aus der DSGVO und den einschlägigen nationalen Gesetzen ergebenden Aufgaben und Befugnisse wahrzunehmen.

(11) Die Stellungnahme des EDSA ist gemäß Artikel 64 Absatz 1 Buchstabe c der DSGVO in Verbindung mit Artikel 10 Absatz 2 der Geschäftsordnung des EDSA binnen acht Wochen ab dem ersten Arbeitstag nach dem Beschluss des Vorsitzes und der zuständigen Aufsichtsbehörde über die Vollständigkeit des Dossiers anzunehmen. 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. Sollte der EDSA im Zusammenhang mit seiner diesbezüglichen Stellungnahme abstrakte Informationen über die Bewertungsmethoden anfordern, um die Überprüfbarkeit des Entwurfs von Zertifizierungskriterien gründlich bewerten zu können, so bedeutet dies nicht, dass die Stellungnahme eine Art Genehmigung der betreffenden Bewertungsmethoden beinhaltet –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1 ZUSAMMENFASSUNG DES SACHVERHALTS

1. In Übereinstimmung mit Artikel 42 Absatz 5 der DSGVO und den Leitlinien wurden die „DSGVO-zt GmbH Zertifizierungskriterien“ (im Folgenden „Entwurfsfassung der Zertifizierungskriterien“ oder „Zertifizierungskriterien“) von der DSGVO-zt GmbH, einer Gesellschaft österreichischen Rechts, erstellt und der österreichischen Datenschutzbehörde (im Folgenden „AT-AB“) vorgelegt.

2. Die AT-AB hat ihren Entwurf eines Beschlusses zur Genehmigung der Zertifizierungskriterien vorgelegt und den EDSA am 11. April 2024 um eine Stellungnahme gemäß Artikel 64 Absatz 1 Buchstabe c der DSGVO ersucht. Der Beschluss über die Vollständigkeit des Dossiers wurde am 29. Mai 2024 gefasst.

2 BEWERTUNG

3. Der Ausschuss hat seine Bewertung gemäß der in Anhang 2 der Leitlinien (im Folgenden „Anhang“) und dem entsprechenden Zusatz vorgesehenen Gliederung vorgenommen. Soweit diese Stellungnahme keine Anmerkungen zu einem bestimmten Abschnitt der Entwurfsfassung der Zertifizierungskriterien enthält, ist davon auszugehen, dass der Ausschuss dazu nichts anzumerken hat und die AT-AB nicht um weitere Maßnahmen ersucht.

4. Bei diesen Zertifizierungskriterien handelt es sich um nationale Kriterien gemäß Artikel 42 Absatz 5 der DSGVO und nicht um ein EU-Datenschutzsiegel.

5. Die vorliegende Zertifizierung ist keine Zertifizierung gemäß Artikel 46 Absatz 2 Buchstabe f der DSGVO, die für die Übermittlung personenbezogener Daten ins Ausland vorgesehen ist, und sie enthält deshalb keine geeigneten Garantien im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen gemäß Artikel 46 Absatz 2 Buchstabe f0. Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation ist nämlich nur zulässig, wenn die Bestimmungen von Kapitel V der DSGVO eingehalten werden.

2.1 ALLGEMEINE BEMERKUNGEN

6. In Bezug auf Abschnitt 2.4 der Entwurfsfassung der Zertifizierungskriterien stellt der Ausschuss fest, dass sich diese auf die DSGVO-Zertifizierung gemäß Artikel 42 Absatz 1 der DSGVO beziehen, die es einem für die Verarbeitung Verantwortlichen oder einem Auftragsverarbeiter ermöglichen soll, nachzuweisen, dass die zertifizierte Verarbeitung personenbezogener Daten in strikter Übereinstimmung mit der DSGVO erfolgt. Der Ausschuss geht jedoch davon aus, dass diese Zertifizierungskriterien nur für Verantwortliche und nicht für Auftragsverarbeiter relevant sind. Daher empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen zu verpflichten, diesen Abschnitt aus Gründen der Klarheit entsprechend zu ändern.

7. Darüber hinaus stellt der Ausschuss fest, dass sich die Entwurfsfassung der Zertifizierungskriterien in Abschnitt 4 über „normative Verweise“ auf den „Prüfumfang“ der

vorliegenden Zertifizierungskriterien bezieht. Der Ausschuss ist mit dem Konzept des „Prüfumfangs“ nicht vertraut, und empfiehlt der AT-AB daher, vom Verfahrensverantwortlichen zu verlangen, dass er in den Kriterien klarstellt, was dieser Begriff bedeutet.

8. Darüber hinaus stellt der Ausschuss in demselben Abschnitt fest, dass der Verweis auf die nationalen Akkreditierungsanforderungen fehlt, und empfiehlt der AT-AB daher, den Verfahrensverantwortlichen zu verpflichten, diesen Abschnitt der Kriterien entsprechend zu ändern.

9. Der Ausschuss stellt ferner fest, dass in der gesamten Entwurfsfassung der Zertifizierungskriterien auf den Inhalt der Bestimmungen der DSGVO verwiesen wird. In diesem Zusammenhang stellt der Ausschuss auch fest, dass einige Verweise auf einschlägige Artikel der DSGVO fehlen. So findet sich beispielsweise in Abschnitt 2.7 der Entwurfsfassung der Zertifizierungskriterien ein Verweis auf Erwägungsgrund 100 der DSGVO, der nicht vollständig dem Wortlaut des relevanten Erwägungsgrundes übereinstimmt. Ebenso sind die Begriffsbestimmungen in den Abschnitten 5.2.5 und 5.2.20 der Entwurfsfassung der Zertifizierungskriterien für die Begriffe „betroffene Person“ und „Datenschutzfolgenabschätzung“ – welche sich nach Auffassung des Ausschusses auf das Konzept der Datenschutz-Folgenabschätzung in der DSGVO bezieht – nicht vollständig an die Begriffsbestimmungen der DSGVO angeglichen. Aus Gründen der Kohärenz empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, bei der Verwendung von Definitionen der DSGVO sicherzustellen, dass diese einheitlich verwendet werden und die entsprechenden Verweise auf die DSGVO-Bestimmungen aufgenommen werden.

10. Der Ausschuss stellt fest, dass bei einigen Kriterien nicht ganz klar ist, was genau zu prüfen ist. Der Ausschuss unterstreicht, dass dies in den Kriterien selbst deutlich gemacht werden sollte. In diesem Zusammenhang stellt der Ausschuss fest, dass in den Entwürfen der Zertifizierungskriterien nicht immer die Elemente definiert werden, auf deren Grundlage die Bewertung durchgeführt werden soll, um deutlich zu machen, was vom Antragsteller nachgewiesen und von der Zertifizierungsstelle geprüft werden soll. So wird beispielsweise in Abschnitt 2.11 der Entwurfsfassung der Zertifizierungskriterien auf „geeignete Maßnahmen“ verwiesen, die sich „wirksam“ auf das jeweilige Schutzniveau auswirken müssen. Der Ausschuss weist in diesem Zusammenhang darauf hin, dass in der Entwurfsfassung der Zertifizierungskriterien die für die Einstufung der Maßnahmen als „angemessen“ und deren „wirksame“ Wirkung zu berücksichtigenden Faktoren fehlen, was die Durchführung der Prüfung durch die Zertifizierungsstelle gefährden kann. Ebenso wird in Abschnitt 2.12 der Entwurfsfassung der Zertifizierungskriterien auf „angemessene“ Maßnahmen verwiesen. Schließlich werden die zu berücksichtigenden relevanten Faktoren nicht durch die Kriterien festgelegt. Unter Berücksichtigung der vorstehenden Ausführungen empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen zu verpflichten, diese Zertifizierungskriterien zu ändern, indem er die Faktoren näher erläutert, die bei der Durchführung der einschlägigen Bewertungen zu berücksichtigen sind.

11. In Bezug auf Abschnitt 3 der Entwurfsfassung der Zertifizierungskriterien zum „Anwendungsbereich“ geht der Ausschuss davon aus, dass sich dies auf den Evaluierungsgegenstand (Target of Evaluation) bezieht, und empfiehlt der AT-AB daher, vom Verfahrensverantwortlichen zu verlangen, den Titel dieses Abschnitts zu ändern, indem er aus Gründen der Klarheit entsprechend umbenannt wird.

12. In Bezug auf Abschnitt 5.1 der Entwurfsfassung der Zertifizierungskriterien fordert der Ausschuss die AT-AB auf, vom Verfahrensverantwortlichen zu verlangen, dass er klarstellt, dass die Begriffsbestimmungen der DSGVO – soweit vorhanden – Vorrang haben. Ebenso fordert der Ausschuss die AT-AB auf, vom Verfahrensverantwortlichen zu verlangen, in Abschnitt 5 der Entwurfsfassung der Zertifizierungskriterien einen Verweis auf „EDSA-relevante Leitlinien“ und „geltende Rechtsprechung“ aufzunehmen, da diese beiden Quellen von den Verantwortlichen bei ihren Compliance-Bemühungen berücksichtigt werden müssen, denn sie führen die Konzepte und Definitionen der DSGVO weiter aus.

13. In Bezug auf Abschnitt 2.11.3 der Anlage zu Anhang I fordert der Ausschuss die AT-AB auf, vom Verfahrensverantwortlichen zu verlangen, dass er klarstellt, dass „der beabsichtigte Transportweg festgelegt und dokumentiert“ wird.

2.2 ANWENDUNGSBEREICH DES ZERTIFIZIERUNGSVERFAHRENS UND EVALUIERUNGSGEGENSTAND (TARGET OF EVALUATION, TOE)

14. Der Ausschuss begrüßt die in Abschnitt 2.3 der Entwurfsfassung der Zertifizierungskriterien enthaltenen Erläuterungen zu der Tatsache, dass die Kriterien keinen Mechanismus darstellen, mit dem das Vorhandensein angemessener Garantien gemäß Artikel 42 Absatz 2 und Artikel 46 Absatz 2 Buchstabe f der DSGVO für die internationale Übermittlung personenbezogener Daten nachgewiesen wird. Der Vollständigkeit halber fordert der Ausschuss die AT-AB auf, den Verfahrensverantwortlichen zu verpflichten, diesen Punkt auch in Abschnitt 3 zum „Anwendungsbereich“ aufzunehmen.

15. In Bezug auf Abschnitt 3.1 der Entwurfsfassung der Zertifizierungskriterien über den „Anwendungsbereich“ empfiehlt der Ausschuss, den Verweis auf die „Zertifizierung eines Produkts oder einer Dienstleistung“ zu streichen, da nur Verarbeitungsvorgänge gemäß der DSGVO zertifiziert werden können.

16. In Bezug auf Abschnitt 3.2 der Entwurfsfassung der Zertifizierungskriterien fordert der Ausschuss die AT-AB auf, den Verfahrensverantwortlichen zu verpflichten, zu ergänzen, dass die Beschreibung des Evaluierungsgegenstands nicht nur „ausführlich“, sondern auch „vollständig“ sein muss.

17. In demselben Abschnitt (d. h. 3.2) der Entwurfsfassung der Zertifizierungskriterien stellt der Ausschuss fest, dass sich die Kriterien auf eine Liste von „Partnern“ beziehen. Dem Ausschuss ist nicht ganz klar, was der Begriff „Partner“ bedeutet, weshalb er die AT-AB auffordert, den Verfahrensverantwortlichen zu verpflichten, dies in den Kriterien zu präzisieren.

18. Ebenso stellt der Ausschuss fest, dass sich die Kriterien in diesem Abschnitt nicht auf „Auftragsverarbeiter“, sondern nur auf „Unterauftragsverarbeiter“ beziehen. Daher fordert er die AT-AB auf, den Verfahrensverantwortlichen aufzufordern, auch „Auftragsverarbeiter“ hinzuzufügen.

2.3 ZERTIFIZIERUNGSKRITERIEN

19. Der Ausschuss versteht den ergänzenden Charakter des Anhangs I (technische und organisatorische Maßnahmen) zu den zentralen Zertifizierungskriterien auf der Grundlage von Abschnitt 8 der Entwurfsfassung der Zertifizierungskriterien so, dass „falls bestimmte Maßnahmen des Anhangs I nicht implementiert werden, weil sie auf den spezifischen Kontext

der Datenverarbeitung nicht anwendbar sind oder sich die Implementierung dieser Maßnahmen nicht auf die Restrisiken der Datenverarbeitung auswirken würde, der Antragsteller der Zertifizierungsstelle eine angemessene und ausführliche Dokumentation zur Begründung dieser Entscheidungen vorzulegen hat. Die Nicht-Implementierung von Sicherheitsmaßnahmen darf nicht auf der Entscheidung des Antragstellers beruhen, dass er ein höheres Restrisiko akzeptiert. Auf Verlangen der Zertifizierungsstelle muss der Antragsteller eine Liste der Maßnahmen des Anhangs I vorlegen, die nicht implementiert wurden." Der Ausschuss nimmt dies zur Kenntnis, empfiehlt der AT-AB jedoch, vom Verfahrensverantwortlichen zu verlangen, dass er klarstellt, in welchen Fällen die Nichtanwendbarkeit der in Anhang I aufgeführten Maßnahmen gegeben sein wird, und genauer zu erläutern, wie diese Nichtanwendbarkeit vom Antragsteller begründet wird. So sollte beispielsweise in Abschnitt 2.8.15 der Anlage zu Anhang I in Bezug auf die „E-Mail-Verschlüsselung" näher klargestellt werden, i) unter welchen Umständen und ii) welche Art von Begründung der Antragsteller liefern müsste, um von der Anwendung dieser Maßnahme abzuweichen.

2.4 RECHTMÄßIGKEIT DER VERARBEITUNG

20. Der Ausschuss stellt fest, dass in Abschnitt 7.1.2.2 Buchstabe b der Entwurfsfassung der Zertifizierungskriterien Folgendes ausgeführt wird: „Richtet sich das Ersuchen um Zustimmung durch einen Dienst der Informationsgesellschaft an einen Minderjährigen, der nach den Bestimmungen des Mitgliedstaats eine solche Zustimmung nur mit Zustimmung des Trägers der elterlichen Verantwortung wirksam erteilen kann, so umfasst das Verfahren die Einholung der Zustimmung oder des Einverständnisses des Trägers der elterlichen Verantwortung". Der Ausschuss geht davon aus, dass sich der Verweis auf die Bestimmungen der Mitgliedstaaten auf die nach nationalem Recht geltenden Bestimmungen bezieht. Daher fordert der Vorstand die AT-AB auf, den Verfahrensverantwortlichen aufzufordern, dieses Kriterium entsprechend zu ändern.

2.5 GRUNDSÄTZE GEMÄß ARTIKEL 5

21. Der Ausschuss stellt fest, dass Abschnitt 6 der Entwurfsfassung der Zertifizierungskriterien, der sich auf die Rechenschaftspflicht bezieht, Kriterien im Zusammenhang mit a) der Datenschutz-Folgenabschätzung, b) der Beteiligung von Auftragsverarbeitern, c) Verzeichnissen von Verarbeitungstätigkeiten und d) Verletzungen des Schutzes personenbezogener Daten enthält. Der Ausschuss weist in diesem Zusammenhang darauf hin, dass der Grundsatz der Rechenschaftspflicht gemäß Artikel 5 Absatz 2 der DSGVO ein übergeordneter Grundsatz ist, der horizontal für alle Pflichten der für die Verarbeitung Verantwortlichen gilt. Aus Gründen der Klarheit und Kohärenz empfiehlt der Ausschuss der AT-AB daher, den Verfahrensverantwortlichen zu verpflichten, in den Zertifizierungskriterien klarzustellen, dass der Grundsatz der Rechenschaftspflicht alle Kriterien und nicht nur die in Abschnitt 6 genannten Kriterien umfasst (z. B. durch Änderung der Überschrift).

22. Der Ausschuss begrüßt die Aufnahme des Grundsatzes der Verarbeitung nach Treu und Glauben in Abschnitt 7.2 der Entwurfsfassung der Zertifizierungskriterien zusammen mit dem Verweis auf die EDSA-Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen. Der Ausschuss möchte jedoch betonen, dass die Zertifizierungskriterien ein „eigenständiges" Dokument sein sollen, in dem alle Kriterien

ausreichend und spezifisch ausgearbeitet sind, um überprüfbare Kriterien zu haben. In diesem Zusammenhang stellt der Ausschuss fest, dass der Ausschuss in seinen Leitlinien 4/2019 zu Artikel 25 über Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen mehrere Elemente aufführt, die berücksichtigt werden müssen, um dem Grundsatz von Treu und Glauben Genüge zu tun. Um die Vollständigkeit und Überprüfbarkeit der Kriterien zu gewährleisten, empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, weitere spezifische, präzise und überprüfbare Kriterien zu entwickeln, sofern diese nicht bereits in anderen Teilen der Kriterien enthalten sind. Grundlage hierfür sollten alle Elemente bilden, die in Ziffer 70 der am 20. Oktober 2020 angenommenen Leitlinien 4/2019 zu Artikel 25 über Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen aufgeführt sind.

2.6 ALLGEMEINE VERPFLICHTUNGEN DER VERANTWORTLICHEN UND AUFTRAGSVERARBEITER

23. Der Ausschuss empfiehlt, bei der Definition des Evaluierungsgegenstands die Anforderungen an die Vereinbarung zwischen dem Antragsteller und den potenziellen gemeinsam Verantwortlichen, die am Evaluierungsgegenstand beteiligt sind, im Hinblick auf ihre jeweiligen Verantwortlichkeiten für die Einhaltung der Zertifizierungskriterien zu definieren.

24. Darüber hinaus empfiehlt der Ausschuss, Kriterien zur Umsetzung von Artikel 26 Absatz 3 der DSGVO aufzunehmen.

25. Der Ausschuss stellt fest, dass Abschnitt 6.2.3 der Entwurfsfassung der Zertifizierungskriterien nicht mit dem Wortlaut von Artikel 28 Absatz 2 DSGVO vereinbar ist, in dem es heißt: „Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. [...]“. Insbesondere empfiehlt der Ausschuss der AT-AB, vom Verfahrensverantwortlichen zu verlangen, Abschnitt 6.2.3 anzupassen und die Wörter „schriftlich“ und „allgemein“ so zu verwenden, dass nicht der irreführende Eindruck erweckt wird, dass nur die „allgemeine Genehmigung“ schriftlich sein muss [sondern auch die gesonderte Genehmigung].

26. Der Ausschuss stellt fest, dass in Abschnitt 6.1.1 Buchstabe d der Entwurfsfassung der Zertifizierungskriterien nicht auf Artikel 35 Absatz 4 der DSGVO Bezug genommen wird. Er empfiehlt der AT-AB, vom Verfahrensverantwortlichen zu verlangen, einen Verweis auf diese Bestimmung und die Liste der Arten von Verarbeitungsvorgängen aufzunehmen, für die eine Datenschutz-Folgenabschätzung gemäß Artikel 35 Absatz 1 der DSGVO erforderlich ist.

27. In Bezug auf Abschnitt 6.1.6 der Entwurfsfassung der Zertifizierungskriterien zur kontinuierlichen Evaluierung stellt der Ausschuss fest, dass sich die Kriterien (in Fußnote 9) zu einer „anerkannten Evaluierungsmethode“ auf zwei Dokumente beziehen, die von der Agentur der Europäischen Union für Cybersicherheit (ENISA) herausgegeben wurden. Der Ausschuss fordert die AT-AB auf, den Verfahrensverantwortlichen zu verpflichten, klarzustellen, dass diese Dokumente lediglich ein Beispiel für anerkannte Evaluierungsmethoden sind, und in den Kriterien weiter zu präzisieren, dass in diesem Zusammenhang die neueste Fassung der einschlägigen Standards zu berücksichtigen ist.

28. In diesem Sinne fordert der Ausschuss die AT-AB auf, den Verfahrensverantwortlichen zu verpflichten, näher zu erläutern, worauf sich die ENISA-Dokumente beziehen, und die

Verwendung von Links in den Kriterien zu vermeiden, um den Zugang zu den einschlägigen Dokumenten in Zukunft zu gewährleisten.

29. Der Ausschuss stellt fest, dass es in Abschnitt 6.3 der Entwurfsfassung der Zertifizierungskriterien heißt: „Zweck des Verzeichnisses von Verarbeitungstätigkeiten gemäß Artikel 30 der DSGVO ist es, einen Überblick über die Verarbeitungstätigkeiten und die damit verbundenen Risiken für die Rechte und Freiheiten der betroffenen Personen sowie die ergriffenen Abhilfemaßnahmen zu geben“. Der Ausschuss hebt hervor, dass die damit verbundenen Risiken und die Abhilfemaßnahmen zusätzlich zu den Informationen gelten, die in den Verzeichnissen von Verarbeitungstätigkeiten gemäß Artikel 30 der DSGVO enthalten sein müssen. Daher fordert der Ausschuss die AT-AB auf, vom Verfahrensverantwortliche zu verlangen, diese Anforderung entweder zu ändern, um nicht den Eindruck zu erwecken, dass die DSGVO verlangt, die Risiken und Abhilfemaßnahmen in das Verzeichnis der Verarbeitung aufzunehmen, oder in den Kriterien zu erläutern, dass die Aufnahme dieser Informationen in die Verzeichnisse von Verarbeitungstätigkeiten gemäß Artikel 30 der DSGVO nicht obligatorisch ist.

2.7 RECHTE BETROFFENER PERSONEN

Der Ausschuss nimmt zur Kenntnis, dass in Abschnitt 6.4.1 Buchstabe d der Entwurfsfassung der Zertifizierungskriterien auf eine „anerkannte Methode zur Beurteilung, ob wahrscheinlich ein Risiko oder ein hohes Risiko besteht“ verwiesen wird. Der Ausschuss empfiehlt, die Verbindung zwischen dem hohen Risiko und den Grundrechten und Grundfreiheiten betroffener Personen hinzuzufügen, um dieses Kriterium an den Wortlaut der DSGVO anzugleichen.

2.8 SCHUTZ GARANTIERENDE TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

30. Der Ausschuss nimmt zur Kenntnis, dass die grundlegenden Zertifizierungskriterien durch zwei Dokumente ergänzt werden: „Anhang I“, in dem die wichtigsten technischen und organisatorischen Maßnahmen dargelegt sind, und „Anlage zu Anhang I“, in der diese weiter spezifiziert werden. Der Ausschuss geht davon aus, dass diese beiden Dokumente vollständig Teil der Kriterien sind und dass alle Kriterien obligatorisch zu überprüfen sind, während lediglich bestimmte technische und organisatorische Maßnahmen ausgeschlossen werden können, indem der Zertifizierungsstelle eine dokumentierte Begründung dafür vorgelegt wird, dass sie für die betreffende Verarbeitungstätigkeit nicht relevant sind. Der Ausschuss ist sich auch darüber im Klaren, dass die Zertifizierungsstelle immer eine Bewertung der Nichtanwendbarkeit bestimmter Kriterien vornehmen wird.

31. Darüber hinaus stellt der Ausschuss fest, dass in der Anlage zu Anhang I, Absätze 2.2.1, 2.2.2 und 2.2.3, einige Begriffe nicht objektiv bewertet werden können (z. B. „insbesondere“, „leicht zu überwachen“, „wenn alle Mitarbeiter einander kennen“). Der Ausschuss empfiehlt der AT-AB, vom Verfahrensverantwortlichen die Streichung dieser Verweise zu verlangen, um Unklarheiten in den Kriterien zu vermeiden.

32. Ebenso ist der Ausschuss der Auffassung, dass die Aussage in der Anlage zu Anhang I Abschnitt 2.2.8, dass „das Risiko der Wiederherstellung je nach den jeweiligen Schutzanforderungen durch Einhaltung gemeinsamer Normen und Standards minimiert werden muss“, nicht hinreichend präzise ist. Daher empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen zu verpflichten, spezifischere Leitlinien zu formulieren und

aufzunehmen (z. B. durch Festlegung von Musternormen oder -standards und durch Bezugnahme auf den „Stand der Technik“).

33. Der Ausschuss stellt fest, dass in der Anlage zu Anhang I, Abschnitt 2.8.15, auf die Verschlüsselung von E-Mails Bezug genommen wird: „E-Mails, die personenbezogene Daten enthalten, müssen vor unbefugtem Zugriff geschützt werden. Je nach Inhalt muss hierfür eine Transport- oder End-to-End-Verschlüsselung verwendet werden. Grundsätzlich gilt, dass die Transportverschlüsselung unabhängig vom Inhalt umzusetzen ist, für besondere Kategorien von Daten sollte die End-to-End-Verschlüsselung zumindest im Verlauf der geplanten Geschäftsprozesse obligatorisch sein.“ Der Ausschuss fordert die AT-AB auf, vom Verfahrensverantwortlichen zu verlangen, diese Ausnahme entweder zu streichen, da sie nicht nur für die E-Mail-Verschlüsselung relevant ist, oder diese Kriterien zur Vermeidung von Missverständnissen in einen anderen Teil der Kriterien (d. h. in Anhang I Abschnitt 3) zu verschieben.

34. Darüber hinaus ermutigt der Ausschuss die Aufsichtsbehörde, den Verfahrensverantwortlichen aufzufordern, den außergewöhnlichen Charakter dieser Maßnahme zu verdeutlichen und hervorzuheben und auf Artikel 9 Absatz 2 Buchstabe c der DSGVO zu verweisen.

35. In Abschnitt 6.2.1 der Entwurfsfassung der Zertifizierungskriterien ist die Rede von „Verfahren, mit denen sichergestellt wird, dass nur Auftragsverarbeiter eingesetzt werden, die insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so implementiert werden, dass die Verarbeitung diesen Zertifizierungskriterien entspricht“. Der Ausschuss stellt fest, dass die technischen und organisatorischen Maßnahmen für den für die Verarbeitung Verantwortlichen im Einklang mit den Kriterien in Abschnitt 8 der Zertifizierungskriterien aufgeführt sind. Zur besseren Lesbarkeit und Genauigkeit von Abschnitt 6.2.1 fordert der Ausschuss die AT-AB daher auf, vom Verfahrensverantwortlichen zu verlangen, dass er auf Abschnitt 8 der Entwurfsfassung der Zertifizierungskriterien verweist.

2.9 KRITERIEN FÜR DEN NACHWEIS DES VORHANDENSEINS GEEIGNETER GARANTIEN FÜR DIE ÜBERMITTLUNG PERSONENBEZOGENER DATEN

36. Der Ausschuss konnte keine spezifischen Kriterien im Zusammenhang mit Artikel 48 der DSGVO („Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung“) ermitteln. In diesem Zusammenhang empfiehlt der Ausschuss der AT-AB, vom Verfahrensverantwortliche zu verlangen, ein Kriterium hinzuzufügen, wonach der Antrag eines Drittlands auf Übermittlung oder Offenlegung personenbezogener Daten als solcher einer Übermittlung oder Offenlegung keine Rechtmäßigkeit gemäß Artikel 48 der DSGVO verleiht.

3 SCHLUSSFOLGERUNGEN/EMPFEHLUNGEN

Der EDSA gelangt zu folgenden Schlussfolgerungen und Empfehlungen:

37. In Bezug auf die „allgemeinen Bemerkungen“ empfiehlt der Ausschuss der AT-AB, vom Verfahrensverantwortlichen Folgendes zu verlangen:

1. Abschnitt 2.4 zu ändern, um klarzustellen, dass die Zertifizierungskriterien nur für Verantwortliche und nicht für Auftragsverarbeiter relevant sind;
2. in Abschnitt 4 der Zertifizierungskriterien den Begriff „Prüfumfang“ präzisieren;
3. in Abschnitt 4 der Zertifizierungskriterien den fehlenden Verweis auf die Akkreditierungsanforderungen zu ergänzen;
4. in den gesamten Zertifizierungskriterien sicherstellen, dass die Begriffsbestimmungen der DSGVO in Übereinstimmung mit der DSGVO verwendet werden und die entsprechenden Verweise auf die Bestimmungen der DSGVO enthalten sind;
5. die Abschnitte 2.11 und 2.12 der Zertifizierungskriterien zu ändern, indem die Faktoren, die bei der Durchführung der entsprechenden Bewertungen zu berücksichtigen sind, ausführlicher beschrieben werden;
6. Abschnitt 3 der Zertifizierungskriterien bezüglich des „Anwendungsbereichs“ aus Gründen der Klarheit umzubenennen.

38. In Bezug auf den „Anwendungsbereich des Zertifizierungsverfahrens und Evaluierungsgegenstand (Target of Evaluation, ToE)“ empfiehlt der Ausschuss, dass die AT-AB vom Verfahrensverantwortlichen Folgendes verlangt:

    1. In Abschnitt 3.1 der Zertifizierungskriterien den Verweis auf die „Zertifizierung eines Produkts oder einer Dienstleistung“ zu streichen, da nur Verarbeitungsvorgänge gemäß der DSGVO zertifiziert werden können.

39. In Bezug auf die „Zertifizierungskriterien “ empfiehlt der Ausschuss, dass die AT-AB vom Verfahrensverantwortlichen Folgendes verlangt:

    1. klarzustellen, in welchen Fällen die Nichtanwendbarkeit der in Anhang I aufgeführten Maßnahmen gegeben sein wird, und genauer zu erläutern, wie diese Nichtanwendbarkeit vom Antragsteller begründet wird. So sollte beispielsweise in Abschnitt 2.8.15 der Anlage zu Anhang I in Bezug auf die „E-Mail-Verschlüsselung“ näher klargestellt werden, i) unter welchen Umständen und ii) welche Art von Begründung der Antragsteller liefern müsste, um von der Anwendung dieser Maßnahme abzuweichen.

40. In Bezug auf die „Grundsätze des Artikels 5“ empfiehlt der Ausschuss, dass die AT-AB vom Verfahrensverantwortlichen Folgendes verlangt:

    1. In den Zertifizierungskriterien klarzustellen, dass der Grundsatz der Rechenschaftspflicht gemäß Artikel 5 Absatz 2 der DSGVO alle Kriterien abdeckt und nicht nur die in Abschnitt 6 der Zertifizierungskriterien genannten Kriterien (d. h. a) Datenschutz-Folgenabschätzungen, b) Beteiligung von Auftragsverarbeitern, c) Verzeichnisse von Verarbeitungstätigkeiten und d) Verletzungen des Schutzes personenbezogener Daten);
    2. in Abschnitt 7.2 der Zertifizierungskriterien weitere spezifische, präzise und überprüfbare Kriterien zu entwickeln, sofern diese nicht bereits in anderen Teilen der Kriterien enthalten sind. Grundlage hierfür sollten alle Elemente bilden, die in den Leitlinien 4/2019 zu Artikel 25 über Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen aufgeführt sind;

41. in Bezug auf die „allgemeinen Verpflichtungen der Verantwortlichen und Auftragsverarbeiter“ empfiehlt der Ausschuss, dass die AT-AB vom Verfahrensverantwortlichen Folgendes verlangt:

    1. bei der Definition des Evaluierungsgegenstands die Anforderungen an die Vereinbarung zwischen dem Antragsteller und den potenziellen gemeinsam

Verantwortlichen, die an dem Evaluierungsgegenstand beteiligt sind, im Hinblick auf ihre jeweiligen Verantwortlichkeiten für die Einhaltung der Zertifizierungskriterien zu definieren;

2. Kriterien aufzunehmen, mit denen die Bestimmungen von Artikel 26 Absatz 3 der DSGVO umgesetzt werden;
3. Abschnitt 6.2.3 der Zertifizierungskriterien anzupassen und die Wörter „schriftlich“ und „allgemein“ so zu verwenden, dass nicht der irreführende Eindruck erweckt wird, dass nur die „allgemeine Genehmigung“ schriftlich sein muss [sondern auch die gesonderte Genehmigung];
4. einen Verweis auf Artikel 35 Absatz 4 der DSGVO und auf die Liste der Arten von Verarbeitungsvorgängen aufzunehmen, für die eine Datenschutz-Folgenabschätzung gemäß Artikel 35 Absatz 1 der DSGVO erforderlich ist;

42. in Bezug auf die „Rechte betroffener Personen“ empfiehlt der Ausschuss, dass die AT-AB vom Verfahrensverantwortlichen Folgendes verlangt:

    1. in Abschnitt 6.4.1 Buchstaben d die Verbindung zwischen dem hohen Risiko und den Grundrechten und Grundfreiheiten betroffener Personen hinzuzufügen, um dieses Kriterium an den Wortlaut der DSGVO anzugleichen;

43. in Bezug auf die „Schutz garantierende technische und organisatorische Maßnahmen“ empfiehlt der Ausschuss, dass die AT-AB vom Verfahrensverantwortlichen Folgendes verlangt:

    1. in der Anlage zu Anhang I Abschnitte 2.2.1, 2.2.2 und 2.2.3, einige Begriffe zu streichen, die nicht objektiv bewertet werden können z. B. „insbesondere“, „leicht zu überwachen“, „wenn alle Mitarbeiter einander kennen“), um Unklarheiten bei den Kriterien zu vermeiden;
    2. in Abschnitt 2.2.8 der Anlage zu Anhang I spezifischere Leitlinien zu formulieren und aufzunehmen (z. B. durch Festlegung von Musternormen oder -standards und durch Bezugnahme auf den „Stand der Technik“);

44. In Bezug auf die „Kriterien für den Nachweis des Vorhandenseins geeigneter Garantien für die Übermittlung personenbezogener Daten“ empfiehlt der Ausschuss, dass die AT-AB vom Verfahrensverantwortlichen Folgendes verlangt:

    1. ein Kriterium hinzuzufügen, wonach der Antrag eines Drittlands auf Übermittlung oder Offenlegung personenbezogener Daten als solcher einer Übermittlung oder Offenlegung keine Rechtmäßigkeit gemäß Artikel 48 der DSGVO verleiht.

45. Schließlich erinnert der EDSA im Einklang mit den Leitlinien auch daran, dass die AT-AB im Falle von Änderungen der Zertifizierungskriterien der DSGVO-zt GmbH, die wesentliche Änderungen mit sich bringen,[4] dem EDSA die geänderte Fassung gemäß Artikel 42 Absatz 5 und Artikel 43 Absatz 2 Buchstabe b der DSGVO vorlegen muss.

[4] Siehe Abschnitt 9 des Zusatzes zu den Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung mit „Leitlinien für die Überprüfung und Bewertung von Zertifizierungskriterien“, für den die Frist für die öffentliche Konsultation am 26. Mai 2021 endete.

4 SCHLUSSBEMERKUNGEN

46. Diese Stellungnahme richtet sich an die AT-AB und wird gemäß Artikel 64 Absatz 5 Buchstabe b DSGVO veröffentlicht.

47. Nach Artikel 64 Absätze 7 und 8 der DSGVO muss die AT-AB dem Vorsitz binnen zwei Wochen nach Eingang der Stellungnahme auf elektronischem Weg mitteilen, ob sie den Beschlussentwurf beibehalten oder ändern wird. Innerhalb derselben Frist übermittelt sie den geänderten Beschlussentwurf oder gibt, wenn sie nicht beabsichtigt, der Stellungnahme des Ausschusses zu folgen, die maßgeblichen Gründe an, aus denen sie beabsichtigt, dieser Stellungnahme insgesamt oder teilweise nicht zu folgen.

48. Gemäß Artikel 70 Absatz 1 Buchstabe y der DSGVO teilt die federführende Aufsichtsbehörde dem EDSA den endgültigen Beschluss zwecks Aufnahme in das Register der Beschlüsse mit, die Gegenstand des Kohärenzverfahrens waren.

49. Der EDSA erinnert daran, dass die AT-AB gemäß Artikel 43 Absatz 6 der DSGVO die Zertifizierungskriterien der DSGVO-zt GmbH in leicht zugänglicher Form veröffentlichen und sie dem Ausschuss zur Aufnahme in das öffentliche Register der Zertifizierungsverfahren und Datenschutzsiegel gemäß Artikel 42 Absatz 8 der DSGVO übermitteln muss.

Für den Europäischen Datenschutzausschuss
Die Vorsitzende

(Anu Talus)