Stellungnahme des EDSA nach Artikel 64 DSGVO

Stellungnahme 15/2025 zum Entwurf eines Beschlusses der österreichischen Aufsichtsbehörde (AT-AB) betreffend die Zertifizierungskriterien der BDO Consulting GmbH

Angenommen am 8. Juli 2025

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

Inhaltsverzeichnis

1 ZUSAMMENFASSUNG DES SACHVERHALTS 5
2 BEWERTUNG 5
2.1 ALLGEMEINE BEMERKUNGEN 6
2.2 Anwendungsbereich des Zertifizierungsverfahrens und Evaluierungsgegenstand (Target of Evaluation, ToE) 10
2.3 Rechtmäßigkeit der Verarbeitung 10
2.4 Rechtsgrundlage 11
2.5 Grundsätze gemäß Artikel 5 12
2.6 Allgemeine Verpflichtungen der Verantwortlichen und Auftragsverarbeiter 15
2.7 Rechte der betroffenen Personen 17
2.8 Schutz garantierende technische und organisatorische Maßnahmen 17
3 SCHLUSSFOLGERUNGEN/EMPFEHLUNGEN 19
4 SCHLUSSBEMERKUNGEN 22

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“) 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 der DSGVO) oder – im Falle eines Europäischen Datenschutzsiegels – der Genehmigung durch den EDSA (Artikel 42 Absatz 5 und Artikel 70 Absatz 1 Buchstabe o der 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 abzugeben zum Entwurf eines Beschlusses der Aufsichtsbehörde zur Genehmigung der Zertifizierungskriterien.

[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.

(4) Diese Stellungnahme soll sicherstellen, dass die DSGVO in Bezug auf die zu entwickelnden zentralen Elemente von Zertifizierungsverfahren 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 dazugehörigen Addendum „Leitlinien für die Überprüfung und Bewertung von Zertifizierungskriterien“ (im Folgenden „Addendum“).

(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 ordnungsgemäß wiedergeben und zu deren einheitlicher 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 Organisationen einen Mehrwert bieten, indem sie dabei helfen, standardisierte und spezifizierte organisatorische und technische Maßnahmen einzurichten, die die Konformität von Verarbeitungsvorgängen nachweislich erleichtern und verbessern, wobei sektorspezifischen Anforderungen Rechnung getragen wird.

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

(10) Der EDSA erinnert daran, dass Zertifizierungen Instrumente einer freiwilligen Selbstkontrolle sind und dass die Einhaltung eines Zertifizierungsverfahrens weder eine Reduzierung der Verantwortung der Verantwortlichen und der Auftragsverarbeiter für die Einhaltung der DSGVO bewirkt, noch die Aufsichtsbehörden an der Wahrnehmung ihrer sich aus der DSGVO und den einschlägigen nationalen Gesetzen ergebenden Aufgaben und Befugnisse hindert.

(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 abstrakte Informationen über die Bewertungsmethoden anfordern, um die Überprüfbarkeit der im Entwurf vorgesehenen Zertifizierungskriterien im Zusammenhang mit seiner diesbezüglichen Stellungnahme gründlich bewerten zu können, so bedeutet dies nicht, dass Letztere eine Art Genehmigung der betreffenden Bewertungsmethoden beinhaltet –

HAT FOLGENDE STELLUNGNAHME ERLASSEN:

1 ZUSAMMENFASSUNG DES SACHVERHALTS

1. In Übereinstimmung mit Artikel 42 Absatz 5 der DSGVO und den Leitlinien wurden die „ZERTIFIZIERUNGSKRITERIEN FÜR ZERTIFIZIERUNGSVERFAHREN GEMÄSS ARTIKEL 42 DSGVO“ (im Folgenden „Entwurfsfassung der Zertifizierungskriterien“ oder „Zertifizierungskriterien“) von der BDO Consulting GmbH, einer Gesellschaft österreichischen Rechts (217731v), erstellt und der österreichischen Aufsichtsbehörde (im Folgenden „AT-AB“) vorgelegt.

2. Die AT-AB hat einen Entwurf ihres Beschlusses zur Genehmigung der Zertifizierungskriterien vorgelegt und den EDSA am 29. April 2025 gemäß Artikel 64 Absatz 1 Buchstabe c der DSGVO um eine Stellungnahme ersucht. Der Beschluss über die Vollständigkeit des Dossiers erging am 17. Juni 2025.

3. Der Anwendungsbereich der vorliegenden Zertifizierungskriterien ist allgemeiner Natur; die Kriterien beschränken sich nicht auf konkrete Verarbeitungsvorgänge. Eine Zertifizierung der von Verantwortlichen und Auftragsverarbeitern ausgeführten Verarbeitungsvorgänge ist möglich.

4. Die Zertifizierung von gemeinsam Verantwortlichen im Sinne von Artikel 26 der DSGVO ist vom Anwendungsbereich der Zertifizierungskriterien ausgenommen. Darüber hinaus werden keine Zertifizierungen für Unternehmen angeboten, die keine Niederlassung im EWR haben.

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

2 BEWERTUNG

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

2.1 ALLGEMEINE BEMERKUNGEN

7. Der Ausschuss stellt fest, dass Abschnitt 1.1 des Entwurfs der Zertifizierungskriterien („Bewertungsziel“) vorsieht, dass „das Bewertungsziel Prozesse, Verarbeitungsvorgänge und Systeme umfassen kann“. Der Ausschuss hebt hervor, dass ausschließlich Verarbeitungsvorgänge zertifiziert werden können, und empfiehlt der AT-AB daher, den Verfahrensverantwortlichen aufzufordern, im Sinne der Genauigkeit den Verweis auf „Systeme“ zu streichen.

8. In Bezug auf Abschnitt 2.2 des Entwurfs der Zertifizierungskriterien („Struktur der Zertifizierungskriterien“) regt der Ausschuss an, dass die AT-AB den Verfahrensverantwortlichen auffordert, unter dem Unterabschnitt „Zusätzliche Leitlinien“ einen spezifischen Verweis auf „einschlägige Leitlinien des EDSA“, „einschlägige Leitlinien oder Empfehlungen der Artikel-29-Datenschutzgruppe“ und „anwendbares Fallrecht“ hinzuzufügen, denn schließlich müssen diese drei Quellen, in denen Konzepte und Definitionen der Datenschutz-Grundverordnung weiter spezifiziert sind und außerdem festgelegt ist, dass die Definitionen der Datenschutz-Grundverordnung, sofern vorhanden, Vorrang haben, von den Verantwortlichen und/oder Auftragsverarbeitern bei ihren Bemühungen um die Einhaltung der Vorschriften berücksichtigt werden.

9. Ferner hält der Ausschuss fest, dass er auf seiner ersten Plenarsitzung die Leitlinien der WP29 zur DSGVO[4] gebilligt hat. Daher regt der Ausschuss an, dass die AT-AB den Verfahrensverantwortlichen auffordert, ausdrücklich anzugeben, ob die Leitlinien der WP29, auf die im Entwurf der Zertifizierungskriterien Bezug genommen wird, vom EDSA gebilligt wurden.

10. Darüber hinaus regt der Ausschuss an, dass die AT-AB den Verfahrensverantwortlichen auffordert, das Wort „ehemalige“ aus den Verweisen auf die Artikel-29-Datenschutzgruppe zu streichen.

11. Zudem stellt der Ausschuss fest, dass in den Entwürfen der Zertifizierungskriterien sowohl unter A.01.02 („Datenschutzorganisation einschließlich Aufgaben und Zuständigkeiten“ für Verantwortliche) als auch unter B.01.01 („Datenschutzorganisation einschließlich Aufgaben und Zuständigkeiten“ für Auftragsverarbeiter) auf den Begriff „Datenschutzkoordinatoren“ verwiesen wird. Der Ausschuss begrüßt die Verwendung dieses Begriffs. Zur besseren Lesbarkeit und Nachvollziehbarkeit der Zertifizierungskriterien empfiehlt der Ausschuss jedoch, den oben genannten Begriff eindeutig zu definieren. Zu diesem Zweck empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, den Begriff „Datenschutzkoordinatoren“ entweder im Abschnitt „Allgemeine Begriffsbestimmungen“ zu definieren oder in den Kriterien selbst eindeutig zu definieren.

12. In Bezug auf einige der im Entwurf aufgeführten Zertifizierungskriterien stellt der Ausschuss fest, dass ein weiterer Abgleich mit der DSGVO erforderlich ist. Dies gilt insbesondere für die nachstehend aufgeführten Kriterien:

[4] Die vom EDSA gebilligten Leitlinien der WP29 sind hier aufgeführt: https://www.edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en.

- Entwurf des Zertifizierungskriteriums A.02.03 – Maßnahmen zur Umsetzung des Grundsatzes der Datenminimierung: Das Kriterium lautet wie folgt: Der Antragsteller der Zertifizierung stellt sicher, dass der Grundsatz der Datenminimierung gemäß Artikel 5 DSGVO eingehalten wird. Der Antragsteller der Zertifizierung stellt sicher, dass die verarbeiteten personenbezogenen Daten auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden. Artikel 5 Absatz 1 Buchstabe c DSGVO lautet hingegen wie folgt: „Personenbezogene Daten müssen […] dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (‚Datenminimierung')". Demnach fehlt die Tatsache, dass die verarbeiteten personenbezogenen Daten „dem Zweck angemessen und erheblich sowie auf das notwendige Maß beschränkt sind".
- Entwurf des Zertifizierungskriteriums A.02.04 – Maßnahmen zur Umsetzung des Grundsatzes der Richtigkeit: Nach diesem Kriterium muss der Antragsteller der Zertifizierung ein Verfahren zur Aufrechterhaltung der Richtigkeit der personenbezogenen Daten einrichten, bei dem für die zu zertifizierenden Verarbeitungstätigkeiten Folgendes berücksichtigt wird: [...] Maßnahmen zur Überprüfung der verarbeiteten Daten auf Richtigkeit und Aktualität sowie zu ihrer Berichtigung. In Artikel 5 Absatz 1 Buchstabe d DSGVO heißt es jedoch auch: „[E]s sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden". Demnach fehlt der Aspekt, dass die Daten unverzüglich zu löschen sind.
- Entwurf des Zertifizierungskriteriums A.02.10 – Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten: In der DSGVO lautet die entsprechende Bestimmung wie folgt: „[D]ie Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten". In der detaillierten Anforderung fehlt jedoch der Verweis auf die potenzielle weltanschauliche Ausrichtung der Stiftung, Vereinigung oder sonstigen Organisation ohne Gewinnerzielungsabsicht.
- Entwurf des Zertifizierungskriteriums A.02.10 – Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten: In Artikel 9 Absatz 2 Buchstabe b DSGVO heißt es hierzu: „eine[r] Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht". In der detaillierten Anforderung fehlt jedoch der Verweis auf die Aufstellung der Garantien (technische und organisatorische Maßnahmen) zum Schutz der Grundrechte und Interessen der betroffenen Personen und darauf, dass diese Garantien durch ein geeignetes Verfahren auf dem neuesten Stand und risikogerecht zu halten sind (vgl. Kriterium A.06.01).
- Entwurf des Zertifizierungskriteriums A.02.10 – Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten: Artikel 9 Absatz 2 Buchstabe f DSGVO besagt: „[D]ie Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich". In der detaillierten Anforderung fehlt jedoch der Verweis auf „oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit".
- Entwurf des Zertifizierungskriteriums A.03.01 – Verfahren für die Bearbeitung von Anträgen betroffener Personen: Gemäß DSGVO stellt „[d]er Verantwortliche [...] der

betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies [...] erforderlich ist." Diese Fristen fehlen in den Kriterien.

- Entwurf des Zertifizierungskriteriums A.03.01 – Verfahren für die Bearbeitung von Anträgen betroffener Personen: Das Verfahren für die Bearbeitung von Anträgen betroffener Personen umfasst auch einen Punkt zur Bestimmung der Fälle, in denen gemäß Artikel 12 Absatz 5 DSGVO ein angemessenes Entgelt verlangt werden kann, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden. Dieses Element ist in den Kriterien nicht enthalten.
- Entwurf des Zertifizierungskriteriums A.03.04 – Auskunftsrecht der betroffenen Person: Punkt 4 dieses Kriteriums lautet wie folgt: „Der Antragsteller der Zertifizierung muss den Zeitpunkt der Bereitstellung der Daten (Kopie) sowie Einzelheiten zum Auskunftsersuchen dokumentieren." Artikel 15 Absatz 3 DSGVO lautet wie folgt: „Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt." Dieses Element ist in den Kriterien nicht enthalten.
- Entwurf des Zertifizierungskriteriums A.03.11 – Beschränkungen der Rechte betroffener Personen nach Unionsrecht oder nationalem Recht: Gemäß Artikel 23 Absatz 1 DSGVO können „durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, [...] die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt: [...]". In der detaillierten Anforderung dieses Kriteriums werden jedoch nur die Artikel 12 bis 22 DSGVO zitiert. In diesem Kriterium fehlt ein einschlägiger Verweis auf Artikel 34 sowie auf Artikel 5, soweit seine Bestimmungen den Rechten und Pflichten nach den Artikeln 12 bis 22 im Einklang mit Artikel 23 Absatz 1 DSGVO entsprechen. Darüber hinaus wird in der detaillierten Anforderung desselben Kriteriums nicht erwähnt, dass das Wesen der Grundrechte und -freiheiten in der Charta und in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten dargelegt ist.
- Entwurf des Zertifizierungskriteriums A.10.01 – Ernennung eines Datenschutzbeauftragten: Der letzte Satz der detaillierten Anforderung dieses Kriteriums lautet wie folgt: „Hat der Antragsteller der Zertifizierung förmlich einen Datenschutzbeauftragten ernannt, so sind die Kontaktdaten dieses Datenschutzbeauftragten zum einen den Personen innerhalb der Organisation und zum anderen der Aufsichtsbehörde nachweislich mitzuteilen." Artikel 37 Absatz 7 DSGVO schreibt jedoch auch die Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten vor. Dieses Element fehlt in den Kriterien.
- Entwurf des Zertifizierungskriteriums A.10.02 – Stellen- oder Aufgabenbeschreibung des Datenschutzbeauftragten: Der zweite Aufzählungspunkt unter der detaillierten Anforderung lautet: „Überwachung der Einhaltung der DSGVO und Überwachung der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der

Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen“. Dieselbe Aufgabe ist in Artikel 39 Absatz 1 Buchstabe b DSGVO jedoch wie folgt formuliert: „Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen“. Der Verweis auf das österreichische Datenschutzrecht fehlt demnach.

- Entwurf des Zertifizierungskriteriums A.04.07 – Überprüfung der Sicherheit der Datenverarbeitung: Unter der detaillierten Anforderung dieses Kriteriums heißt es: „Bei der Bewertung, ob der Auftragsverarbeiter seinen vertraglichen Verpflichtungen nachkommt, insbesondere angemessene technische und organisatorische Maßnahmen zu ergreifen und aufrechtzuerhalten, kann der Antragsteller der Zertifizierung auch die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder ein Zertifizierungsverfahren gemäß Artikel 42 DSGVO heranziehen“. Im Teil „Verweise“ fehlt der Verweis auf Artikel 28 Absatz 5 DSGVO, der die einschlägige Bestimmung enthält.
- Entwurf des Zertifizierungskriteriums A.08.03 – Meldung einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde: Zwar umfasst die detaillierte Anforderung dieses Kriteriums den Wortlaut der Bestimmung nach Artikel 33 Absatz 4 DSGVO, in den Verweisen für dieses Kriterium fehlt jedoch der Verweis auf Artikel 33 Absatz 4 DSGVO.
- Entwurf des Zertifizierungskriteriums A.09.01 – Bewertung und Dokumentation einer Datenschutz-Folgenabschätzung (DSFA): Gemäß Artikel 35 Absatz 1 DSGVO muss der Antragsteller der Zertifizierung bei der Entscheidung, ob eine Datenschutz-Folgenabschätzung erforderlich ist, auch die Umstände der Verarbeitung berücksichtigen. Bei diesem Kriterium werden jedoch nur die Art, der Umfang und die Zwecke der Verarbeitung erwähnt.
- Entwurf des Zertifizierungskriteriums B.08.01 – Meldung von Verletzungen des Schutzes personenbezogener Daten an den Verantwortlichen: Zwar umfasst die detaillierte Anforderung dieses Kriteriums den Wortlaut der Bestimmung nach Artikel 33 Absatz 4 DSGVO, in den Verweisen für dieses Kriterium fehlt jedoch der Verweis auf Artikel 33 Absatz 4 DSGVO.
- Entwurf des Zertifizierungskriteriums B.10.01 – Ernennung eines Datenschutzbeauftragten: Der letzte Satz der detaillierten Anforderung dieses Kriteriums lautet wie folgt: „Hat der Antragsteller der Zertifizierung förmlich einen Datenschutzbeauftragten ernannt, so sind die Kontaktdaten dieses Datenschutzbeauftragten zum einen den Personen innerhalb der Organisation und zum anderen der Aufsichtsbehörde nachweislich mitzuteilen.“ Artikel 37 Absatz 7 DSGVO schreibt jedoch auch die Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten vor. Dieses Element fehlt in den Kriterien.
- Entwurf des Zertifizierungskriteriums A.10.02 – Stellen- oder Aufgabenbeschreibung des Datenschutzbeauftragten: Der zweite Aufzählungspunkt unter der detaillierten Anforderung lautet: „Überwachung der Einhaltung der DSGVO und Überwachung der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen“. Dieselbe Aufgabe ist in Artikel 39

Absatz 1 Buchstabe b DSGVO jedoch wie folgt formuliert: „Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen“. Der Verweis auf das österreichische Datenschutzrecht fehlt demnach.

In Bezug auf alle oben genannten Punkte empfiehlt der Ausschuss der AT-AB daher, den Verfahrensverantwortlichen aufzufordern, die oben genannten Kriterien dahingehend abzuändern, dass sie mit der Datenschutz-Grundverordnung im Einklang stehen.

13. Darüber hinaus stellt der Ausschuss fest, dass sich der Entwurf der Zertifizierungskriterien B.04.04 („Verarbeitung personenbezogener Daten ausschließlich auf der Grundlage einer dokumentierten Weisung des Verantwortlichen“) und B.04.08 („Anforderungen an die Einhaltung der in der Datenverarbeitungsvereinbarung festgelegten Verpflichtungen“) auf den Begriff „Kunde“ bezieht. Zur besseren Lesbarkeit und Nachvollziehbarkeit der Zertifizierungskriterien empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, den oben genannten Begriff im Sinne der Einheitlichkeit und Genauigkeit durch den Begriff „Verantwortlicher“ zu ersetzen.

2.2 Anwendungsbereich des Zertifizierungsverfahrens und Evaluierungsgegenstand (Target of Evaluation, ToE)

14. In Bezug auf Abschnitt 3 des Entwurfs der Zertifizierungskriterien („Nichtanwendbarkeit der Zertifizierungskriterien“) nimmt der Ausschuss zur Kenntnis, dass einige Kriterien je nach den Umständen der Datenverarbeitung möglicherweise nicht relevant sind. Der Ausschuss stellt jedoch fest, dass die Formulierungen „zum Beispiel“ („z. B.“) und „können“ zu Unklarheiten führen und die Überprüfbarkeit der Kriterien beeinträchtigen können. Zu diesem Zweck empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, die Bedingungen aufzunehmen, die erfüllt sein müssen, um die Nichtanwendbarkeit eines Kriteriums standardmäßig als integralen Bestandteil der Kriterien festzustellen, die Formulierung „zum Beispiel“ („z. B.“) zu streichen und das Wort „können“ durch das Wort „müssen“ zu ersetzen.

2.3 Rechtmäßigkeit der Verarbeitung

15. Der Ausschuss nimmt den Entwurf des Zertifizierungskriteriums A.02.09 („Erklärung über die Einwilligung eines Kindes in Diensten der Informationsgesellschaft“) und die Tatsache zur Kenntnis, dass das Kriterium Folgendes vorsieht: „Der Antragsteller der Zertifizierung richtet ein Verfahren für alle Verarbeitungstätigkeiten ein, für die die Zertifizierung gelten soll: die Maßnahmen zur Überprüfung des Alters des Kindes und zur Einholung der Zustimmung des Trägers der elterlichen Verantwortung für das Kind, einschließlich der Überprüfung des Sorgerechts (z. B. kann das Hochladen einer Kopie des Reisepasses und der Geburtsurkunde als Voraussetzung für die Annahme eines Antrags auf Abschluss eines Versicherungsvertrags gelten)“. Auf der Grundlage der Erläuterungen der AT-AB geht der Ausschuss davon aus, dass die Geburtsurkunde nicht in allen Fällen angefordert werden muss, und regt daher an, dass die AT-AB den Verfahrensverantwortlichen auffordert, dieses Kriterium zu ändern, um Missverständnisse zu vermeiden.

16. In Bezug auf den Entwurf des Zertifizierungskriteriums A.02.10 („Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten“) nimmt der Ausschuss zur Kenntnis, dass sich Option c im Einklang mit Artikel 9 Absatz 2 Buchstabe c DSGVO auf die lebenswichtigen Interessen der betroffenen Person oder einer anderen natürlichen Person bezieht (Artikel 9 Absatz 2 Buchstabe c DSGVO). In Unterpunkt b wird jedoch ausdrücklich auf den Schutz des **Lebens** der betroffenen Person als eine der lebenswichtigen Interessen Bezug genommen. Da der Schutz des Lebens nicht die einzige Situation ist, die zu den lebenswichtigen Interessen zählt, und in Artikel 9 Absatz 2 Buchstabe c DSGVO auch auf mögliche lebenswichtige Interessen einer anderen natürlichen Person verwiesen wird, empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, Unterpunkt b dahingehend abzuändern, dass daraus eindeutig die Notwendigkeit hervorgeht, unter Angabe der Gründe zu dokumentieren, warum die Verarbeitung erforderlich ist, um lebenswichtige Interessen (z. B. das Leben) der betroffenen Person oder einer anderen natürlichen Person zu schützen, und warum sie nicht auf eine andere Rechtsgrundlage gestützt werden kann.

2.4 Rechtsgrundlage

2.4.1 Rechtsgrundlage – Einwilligung

17. Der Ausschuss nimmt zur Kenntnis, dass es zwei verschiedene Entwürfe der Zertifizierungskriterien gibt, was die Einwilligung anbelangt: 02.07.01 („Einwilligung in die Verarbeitung personenbezogener Daten“) und A.02.08 („Form der Einwilligungserklärung“). Der Ausschuss ist der Ansicht, dass sich diese beiden Kriterien überschneiden und dass das Kriterium A.02.08 selbst nicht eindeutig genug ist. Daher regt der Ausschuss an, dass die AT-AB den Verfahrensverantwortlichen auffordert, diese Kriterien zur Vermeidung von Missverständnissen zu ändern und zusammenzuführen.

18. Ebenso empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, der Vollständigkeit halber Artikel 7 DSGVO in die Verweise für dieses Kriterium aufzunehmen.

19. Darüber hinaus sieht der Entwurf des Zertifizierungskriteriums A.02.10 („Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten“) vor, dass die erforderliche Dokumentation eine Aufstellung der Garantien (technische und organisatorische Maßnahmen) zum Schutz der Grundrechte und Interessen der betroffenen Personen enthält und dass diese Garantien durch ein geeignetes Verfahren auf dem neuesten Stand und risikogerecht gehalten werden. Der Ausschuss geht davon aus, dass die in Artikel 9 Absatz 2 DSGVO vorgesehenen „geeigneten Garantien“ in den Kriterien so ausgelegt werden, dass sie sich ausschließlich auf technische und organisatorische Maßnahmen beschränken. Demnach empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, die Formulierung „insbesondere“ hinzuzufügen, um klarzustellen, dass die Aufzählung der Garantien nicht erschöpfend ist und dass auch andere Garantien aufgenommen werden könnten.

2.4.2 Rechtsgrundlage – Verarbeitung personenbezogener Daten zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt

20. Im Entwurf des Zertifizierungskriteriums A.02.07.05 („Verarbeitung personenbezogener Daten zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt“) ist vorgesehen, dass mit dem Zertifizierungsverfahren die Anforderungen bezüglich dieser Rechtsgrundlage festgelegt werden. Der Ausschuss regt an, dass die AT-AB den Verfahrensverantwortlichen auffordert, den Titel dieses Kriteriums zu ändern und in Anlehnung an die Beschreibung dieses Kriteriums und an die Bestimmung nach Artikel 6 Absatz 1 Buchstabe e DSGVO „die dem Antragsteller der Zertifizierung als Verantwortlichen übertragen wurde“ hinzuzufügen.

2.5 Grundsätze gemäß Artikel 5

21. Im Entwurf des Zertifizierungskriteriums A.01.01 („Einhaltung von Artikel 5 DSGVO (Rechenschaftspflicht) durch Umsetzung einer Datenschutzpolitik“) ist vorgesehen, dass mit dem Zertifizierungsverfahren die Themen festgelegt werden, die in der Datenschutzpolitik enthalten sein müssen, einschließlich weiterer Verweise auf die konkreten Kriterien, die für jedes Thema relevant sind. Insbesondere in Bezug auf das Thema „Datenschutzorganisation und Zuständigkeiten (siehe Entwurf des Zertifizierungskriteriums A.01.02)“ kann der allgemeine Verweis auf den Entwurf des Zertifizierungskriteriums A.01.02 zu Unklarheiten führen und die Überprüfbarkeit der Kriterien beeinträchtigen. Daher regt der Ausschuss an, dass die AT-AB den Verfahrensverantwortlichen auffordert, genauer auszuführen, dass in den Maßnahmen zum Schutz personenbezogener Daten die Aufnahme der Identität und der Kontaktdaten des Verantwortlichen, der Kontaktdaten des Datenschutzbeauftragten (falls zutreffend), der Kontaktdaten der Datenschutzkoordinatoren (falls zutreffend), der Rechtsgrundlage für die Verarbeitung(en), des Empfängers oder der Kategorien von Empfängern der personenbezogenen Daten und der Angabe, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für den Abschluss eines Vertrags erforderlich ist, sowie der Angabe, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche Konsequenzen bei einem Versäumnis der Bereitstellung dieser Daten möglich sind, vorgesehen ist.

22. In Bezug auf die Rechenschaftspflicht stellt der Ausschuss fest, dass im Entwurf des Zertifizierungskriteriums A.01.01 („Einhaltung von Artikel 5 DSGVO (Rechenschaftspflicht) durch Umsetzung einer Datenschutzpolitik“) festgelegt ist, dass „[d]er Antragsteller der Zertifizierung [...] in der Lage sein [muss], die Einhaltung der in Artikel 5 DSGVO festgelegten Grundsätze für die Verarbeitung personenbezogener Daten zu gewährleisten und nachzuweisen. Daher muss der Antragsteller der Zertifizierung sicherstellen, dass Maßnahmen festgelegt sind.“ Der Ausschuss stellt fest, dass der Verantwortliche gemäß Artikel 5 Absatz 2 DSGVO[5] nicht nur in der Lage, sondern auch dafür verantwortlich sein muss, die Einhaltung von Artikel 5 Absatz 1 DSGVO nachzuweisen. Daher empfiehlt der Ausschuss der AT-AB, den

[5] Artikel 5 Absatz 2 DSGVO lautet wie folgt: „Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können (‚Rechenschaftspflicht‘).“

Verfahrensverantwortlichen aufzufordern, den Wortlaut dieses Kriteriums am Wortlaut der Bestimmung in Artikel 5 Absatz 2 DSGVO auszurichten.

23. Der Ausschuss begrüßt, dass sich der Entwurf des Zertifizierungskriteriums A.02.01 („Maßnahmen zur Umsetzung des Grundsatzes der Transparenz“) nur auf Artikel 5 Absatz 1 Buchstabe a DSGVO und Erwägungsgrund 39 DSGVO bezieht und dass sich die detaillierte Anforderung desselben Kriteriums auf die Artikel 13 und 14, 15 bis 22 und 34 DSGVO bezieht. Der Ausschuss stellt jedoch fest, dass der Grundsatz der Transparenz auch in Artikel 12 verankert ist[6]. Daher empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, den Verweis auf Artikel 12 DSGVO in die detaillierte Anforderung aufzunehmen, dass der Antragsteller der Zertifizierung über Regeln, einen Mechanismus oder ein Verfahren verfügen muss, um die Transparenzanforderungen der DSGVO sicherzustellen, was bedeutet, dass den betroffenen Personen (gemäß Artikel 13 und 14 DSGVO) Informationen zur Verfügung gestellt werden, um die Vollständigkeit und Einheitlichkeit zu gewährleisten.

24. Darüber hinaus begrüßt der Ausschuss die Tatsache, dass der Entwurf des Zertifizierungskriteriums A.02.01 („Maßnahmen zur Umsetzung des Grundsatzes der Transparenz“) vorschreibt, dass bei der Unterrichtung der betroffenen Personen oder der Kommunikation mit ihnen eine klare und einfache Sprache verwendet wird. Der Ausschuss weist jedoch darauf hin, dass die Verwendung einer klaren und einfachen Sprache bei der Bereitstellung von Informationen nicht nur auf die Kommunikation mit Kindern beschränkt werden darf, sondern bei der Kommunikation mit allen betroffenen Personen sichergestellt werden muss. Daher empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, die Formulierung „(bei der Bereitstellung von Informationen für Kinder)“ im Sinne der Genauigkeit aus den detaillierten Anforderungen des Kriteriums zu streichen.

25. Der Ausschuss begrüßt ferner den Abschnitt „Anwendungsleitlinien“ des Entwurfs des Zertifizierungskriteriums A.02.01 („Maßnahmen zur Umsetzung des Grundsatzes der Transparenz“) und insbesondere den Verweis auf die „Leitlinien für Transparenz gemäß der Verordnung 2016/679 (WP 260 rev.01)“ der ehemaligen Artikel-29-Datenschutzgruppe. Der Ausschuss stellt jedoch fest, dass der EDSA an die Stelle der gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzten Artikel-29-Datenschutzgruppe getreten ist, die mit Inkrafttreten der DSGVO am 25. Mai 2018 aufgehoben wurde, und dass er die Leitlinien 4/2019 zu Artikel 25 über Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen[7] angenommen hat, die von den Verantwortlichen und/oder Auftragsverarbeitern bei ihren Bemühungen um die Einhaltung der Vorschriften berücksichtigt werden müssen. Daher empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, einen Verweis auf

[6] EDSA, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Leitlinien 4/2019 zu Artikel 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen), Version 2.0, angenommen am 20. Oktober 2020, Ziffer 65, abrufbar unter: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

[7] EDSA, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Leitlinien 4/2019 zu Artikel 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen), Version 2.0, angenommen am 20. Oktober, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

die „EDSA-Leitlinien 4/2019 zu Artikel 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Version 2.0, angenommen am 20. Oktober 2020“ aufzunehmen.

26. Der Ausschuss stellt fest, dass es zwar für den Grundsatz der Transparenz ausführliche Kriterien gibt, für den Grundsatz von Treu und Glauben jedoch nicht. In diesem Zusammenhang erklärt der Ausschuss nochmals, dass die Zertifizierungskriterien ein eigenständiges Dokument sein sollen, in dem alle Kriterien so ausführlich und konkret ausgearbeitet sind, dass die Überprüfbarkeit gewährleistet ist. Diesbezüglich weist der Ausschuss darauf hin, dass er in seinen Leitlinien 4/2019 zu Artikel 25 der DSGVO über Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (angenommen am 20. Oktober 2020) mehrere Elemente aufführt, die berücksichtigt werden sollten, 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 Leitlinien 4/2019 zu Artikel 25 der DSGVO über Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (siehe auch Stellungnahme 3/2025 des EDSA) aufgeführt sind.

27. Der Ausschuss begrüßt den Entwurf des Zertifizierungskriteriums A.02.02 („Maßnahmen zur Umsetzung des Grundsatzes der Zweckbindung“) und insbesondere die Anforderung, dass der Antragsteller der Zertifizierung eine Dokumentation für alle zur Zertifizierung vorgesehenen Verarbeitungstätigkeiten erstellen und pflegen muss, die eine Beschreibung der Zwecke der einzelnen zu zertifizierenden Verarbeitungstätigkeit und eine Datenschutzerklärung umfasst, die Auskunft über die Zwecke der zu zertifizierenden Verarbeitungstätigkeiten gibt, für die die personenbezogenen Daten bestimmt sind. Der Ausschuss stellt jedoch fest, dass der Antragsteller der Zertifizierung zwar im Hinblick auf die Grundsätze der Genauigkeit, Integrität und Vertraulichkeit auch die zur Umsetzung dieser Grundsätze ergriffenen Maßnahmen dokumentieren muss, für den Grundsatz der Zweckbindung hingegen nicht. Daher regt der Ausschuss der Vollständigkeit halber an, dass die AT-AB den Verfahrensverantwortlichen auffordert, anzugeben, dass der Antragsteller der Zertifizierung Maßnahmen ergreifen muss, i) bevor er eine Verarbeitung personenbezogener Daten in Erwägung zieht, um die Zwecke der Verarbeitung festzulegen, ii) um festzustellen, ob eine beabsichtigte Änderung der Verarbeitung die Zwecke der Verarbeitung betrifft, und iii) um einem Missbrauch der Zwecke vorzubeugen, und diese Maßnahmen dokumentieren muss.

28. Im Entwurf des Zertifizierungskriteriums A.02.02 („Maßnahmen zur Umsetzung des Grundsatzes der Zweckbindung“) ist vorgesehen, dass mit dem Zertifizierungsverfahren die Anforderungen an den Grundsatz der Zweckbindung festgelegt werden, wobei die Weiterverarbeitung personenbezogener Daten für Zwecke, die mit den festgelegten, eindeutigen und legitimen Zwecken, für die die Daten ursprünglich erhoben wurden, nicht vereinbar sind, durch das Kriterium A.02.07.07 untersagt wird. Der Ausschuss stellt jedoch fest, dass in dem Zertifizierungsverfahren der Ausschluss von Verarbeitungstätigkeiten, die unter die Artikel 85 bis 89 DSGVO fallen, nicht erwähnt wird und dass ein Verweis auf eine solche Verarbeitung in Kriterium A.02.10 enthalten ist. Daher geht der Ausschuss davon aus, dass die relevanten Aspekte der Einhaltung der

DSGVO in Bezug auf die unter diese Artikel fallenden Verarbeitungsvorgänge durch die Zertifizierungskriterien abgedeckt sein sollen. Demzufolge empfiehlt der Ausschuss, klarzustellen, dass eine weitere Verarbeitung für im öffentlichen Interesse liegende Archivierungszwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke nicht per se als mit dem ursprünglichen Zweck (singular) unvereinbar gilt, sofern eine Bewertung der Vereinbarkeit des Zwecks ordnungsgemäß dokumentiert wird, insbesondere im Hinblick auf das Bestehen geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person. Insbesondere ist der Ausschuss der Ansicht, dass die geeigneten Garantien für die Rechte und Freiheiten der betroffenen Personen bei jedem Verarbeitungsvorgang, der für im öffentlichen Interesse liegende Archivierungszwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erfolgt, ebenfalls von der Organisation dokumentiert und im Rahmen der Kompatibilitätsprüfung gemäß Kriterium A.02.07.07 bewertet werden sollten.

2.6 Allgemeine Verpflichtungen der Verantwortlichen und Auftragsverarbeiter

2.6.1 Verpflichtungen der Verantwortlichen und der Auftragsverarbeiter

29. In Bezug auf den Entwurf der Zertifizierungskriterien A.01.03 (für Verantwortliche) und B.01.02 (für Auftragsverarbeiter) („Regelmäßige Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter“) stellt der Ausschuss fest, dass der Antragsteller der Zertifizierung die Mitarbeiter nur über die Datenschutzanforderungen der DSGVO informieren muss, wobei die EU-Datenschutzvorschriften zum einen aus der Datenschutz-Grundverordnung (DSGVO) und zum anderen aus dem österreichischen Datenschutz-Anpassungsgesetz bestehen. Im Sinne der Vollständigkeit und Genauigkeit dieser Kriterien regt der Ausschuss an, dass die AT-AB den Verfahrensverantwortlichen auffordert, auch die Formulierung „Datenschutz-Grundverordnung“ durch „Datenschutzrecht“ zu ersetzen.

30. Darüber hinaus sieht der Entwurf der Zertifizierungskriterien A.10.03 (für Verantwortliche) und B.10.03 (für Auftragsverarbeiter) vor, dass vorgeschrieben wird, dass der Antragsteller einen Nachweis *u. a.* über die Bereitstellung von angemessener zeitlicher, organisatorischer und finanzieller Ressourcen für die ordnungsgemäße Erfüllung aller Aufgaben des Datenschutzbeauftragten erbringt und dass die Zuweisung dieser Ressourcen dokumentiert wird. In Artikel 38 Absatz 2 DSGVO heißt es jedoch: „Der Verantwortliche und der Auftragsverarbeiter unterstützen den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 39, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellen“, was bedeutet, dass auf den allgemeineren Begriff „Ressourcen“ Bezug genommen wird, der auch Zeit, Fortbildungsmaßnahmen und Geräte umfasst. Aus diesem Grund empfiehlt der EDSA der AT-AB, den Verfahrensverantwortlichen aufzufordern, die Kriterien dahingehend anzupassen, dass die dem Datenschutzbeauftragten zugewiesenen Ressourcen nicht nur für die Erfüllung von Aufgaben, sondern auch für die Erhaltung von Fachwissen im Einklang mit Artikel 38 Absatz 2 DSGVO eingesetzt werden können.

2.6.2 Verpflichtungen der Verantwortlichen

31. Der Entwurf des Zertifizierungskriteriums A.01.03 („Regelmäßige Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter“) und die darin enthaltenen Kriterien werden vom Ausschuss begrüßt. Der Ausschuss stellt hingegen fest, dass der Entwurf der Zertifizierungskriterien zwar ausführliche Kriterien für die Auftragsverarbeiter enthält, in den Bereichen, in denen mithilfe von Schulungsmaßnahmen das Bewusstsein geschärft werden soll, jedoch kein Bezug auf die Beziehung zu den Auftragsverarbeitern genommen wird. Daher regt der Ausschuss an, dass die AT-AB den Verfahrensverantwortlichen auffordert, dieses Kriterium entsprechend zu ändern und eine Darstellung der Beziehungen zu den Auftragsverarbeitern in den Bereichen aufzunehmen, in denen mithilfe von Schulungsmaßnahmen das Bewusstsein der Mitarbeiter geschärft werden soll.

2.6.3 Verpflichtungen der Auftragsverarbeiter

32. In Bezug auf den Entwurf des Zertifizierungskriteriums A.04.05 („Datenverarbeitungsvereinbarungen mit Datenverarbeitern, die alle Anforderungen von Artikel 28 DSGVO erfüllen“) begrüßt der Ausschuss die Aufnahme der Verpflichtung des Datenverarbeiters, dafür Sorge zu tragen, dass nur dann ein anderer Auftragsverarbeiter in Anspruch genommen wird, wenn eine gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen vorliegt. Der Ausschuss stellt ferner fest, dass der Antragsteller der Zertifizierung gemäß dem Kriterium A.04.06 („Recht auf Widerspruch gegen weitere Unterauftragsverarbeiter“) dafür Sorge tragen muss, dass die beauftragten Datenverarbeiter keine weiteren Unterauftragsverarbeiter in Anspruch nehmen, es sei denn, es liegt eine schriftliche Genehmigung des Verantwortlichen gemäß Artikel 28 Absatz 2 DSGVO vor. Der Ausschuss regt an, dass die AT-AB den Verfahrensverantwortlichen auffordert, in das Kriterium A.04.05 der Vollständigkeit halber einen Verweis auf das Kriterium A.04.06 aufzunehmen.

33. Der Entwurf des Zertifizierungskriteriums B.07.09 („Verfahren für die Pseudonymisierung oder Anonymisierung von Daten“) und die darin enthaltenen Kriterien werden vom Ausschuss begrüßt. Der Ausschuss stellt jedoch fest, dass nach dem Entwurf des ähnlichen Zertifizierungskriteriums A.07.09, der für Verantwortliche gilt, verlangt wird, dass die Dokumentation der für die Pseudonymisierung und Anonymisierung verwendeten Maßnahmen – falls möglich – auch einen Nachweis / eine Begründung der Wirksamkeit des Verfahrens enthält. Daher regt der Ausschuss an, dass die AT-AB den Verfahrensverantwortlichen auffordert, dieses Kriterium im Sinne der Einheitlichkeit entsprechend zu ändern.

34. Der Entwurf des Zertifizierungskriteriums B.08.01 („Meldung von Verletzungen des Schutzes personenbezogener Daten an den Verantwortlichen“) sieht vor, dass der Auftragsverarbeiter den Verantwortlichen unverzüglich und nach Möglichkeit innerhalb von 72 Stunden über die Verletzung des Datenschutzes unterrichtet. Nach Ansicht des Ausschusses wird durch die Verpflichtung, den Verantwortlichen innerhalb von 72 Stunden zu benachrichtigen, der in der DSGVO festgelegte Standard herabgesetzt, der vorsieht, dass der Auftragsverarbeiter den Verantwortlichen unverzüglich benachrichtigen muss. Demzufolge empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, dieses Kriterium zu ändern und die Frist von 72 Stunden zu streichen.

2.7 Rechte der betroffenen Personen

35. Der Ausschuss begrüßt die Tatsache, dass in Abschnitt 4.8 des Entwurfs der Zertifizierungskriterien („Rechte der betroffenen Personen“) darauf hingewiesen wird, dass der Antragsteller der Zertifizierung ein Verfahren einrichten muss, mit dem die Bearbeitung von Anfragen der betroffenen Personen (Artikel 12 bis 22 DSGVO) und deren Beantwortung „unverzüglich und in jedem Fall innerhalb eines Monats“ sichergestellt werden. Der Ausschuss stellt jedoch fest, dass hinsichtlich des Auskunftsrechts in Abschnitt A.03.04 der Zertifizierungskriterien der Hinweis auf die Frist für die Beantwortung des Antrags der betroffenen Person fehlt. Daher empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, dieses Kriterium entsprechend zu ändern und einen Hinweis auf die Frist aufzunehmen, um die Vollständigkeit und Einheitlichkeit zu gewährleisten.

36. Der Ausschuss begrüßt ferner, dass in demselben Abschnitt des Entwurfs der Zertifizierungskriterien die Anforderung enthalten ist, die Identität der betroffenen Person zu überprüfen und die im Zuge dieser Überprüfung unternommenen Schritte zu dokumentieren, wenn der Antragsteller der Zertifizierung begründete Zweifel an der Identität der natürlichen Person hat, die den Antrag stellt. Der Ausschuss empfiehlt der AT-AB jedoch, den Verfahrensverantwortlichen aufzufordern, auch anzugeben, auf welche Weise der Identitätsnachweis von der betroffenen Person erbracht werden kann.

2.8 Schutz garantierende technische und organisatorische Maßnahmen

37. Der Entwurf des Zertifizierungskriteriums A.04.01 („Datenschutz durch Technikgestaltung“) und die darin enthaltenen Kriterien werden vom Ausschuss begrüßt. Der Ausschuss stellt jedoch fest, dass in dem Entwurf der Kriterien nicht erwähnt wird, dass die Entscheidung darüber, wie die Datenschutzgrundsätze anzuwenden sind, nach Artikel 25 DSGVO zu einem sehr frühen Zeitpunkt getroffen werden muss. Im Sinne der Vollständigkeit und Genauigkeit empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, dieses Kriterium mit der DSGVO in Einklang zu bringen.

38. Ebenso weist der Ausschuss darauf hin, dass der Verweis auf das sehr frühe Stadium der Verarbeitung auch in den einschlägigen Kriterien zur „Unterstützung bei der Umsetzung des Datenschutzes durch Technikgestaltung“ im Entwurf des Zertifizierungskriteriums B.04.01.1 fehlt. Daher empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, auch dieses Kriterium entsprechend zu ändern.

39. In Bezug auf den Entwurf des Kriteriums A.01.04, („Laufende Überwachung der Einhaltung der Datenschutzanforderungen“) begrüßt der Ausschuss die Aufnahme der Angabe, dass „der Antragsteller der Zertifizierung über einen Überwachungsplan verfügen muss, der alle Datenschutzaktivitäten abdeckt, die über einen festgelegten Zeitraum risikoorientiert gemäß einer ‚Risikokarte‘ des Unternehmens oder der Organisation zu überwachen sind“. In Anbetracht der Tatsache, dass der Begriff „Überwachungsplan“ zu Unklarheiten führen und die Überprüfbarkeit dieses Kriteriums beeinträchtigen kann, empfiehlt der Ausschuss der AT-AB jedoch, den Verfahrensverantwortlichen aufzufordern, dieses Kriterium dahingehend zu ändern,

dass darin auch vorgegeben wird, dass der Antragsteller ein Überwachungsverfahren einrichten muss, mit dem eine Analyse aller Datenschutzaktivitäten ermöglicht wird.

40. In dem Entwurf des Zertifizierungskriteriums A.06.03 (für Verantwortliche) („Regelmäßige Überprüfung der Risikoanalyse“) ist vorgesehen, dass „[d]ie vom Antragsteller der Zertifizierung durchgeführte Risikoanalyse [...] regelmäßig überprüft“ wird. In diesem Zusammenhang stellt der Ausschuss fest, dass der Begriff „regelmäßig“ recht weit gefasst sein, zu Unklarheiten führen und die Überprüfbarkeit dieses Kriteriums beeinträchtigen kann. Zu diesem Zweck empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, die Regelmäßigkeit der Überprüfungen näher zu erläutern und die betreffenden Kriterien dahingehend anzupassen, dass Antragsteller verpflichtet werden, Risikomanagementverfahren einzuführen, auf deren Grundlage die zur Erfüllung dieses Kriteriums getroffenen Maßnahmen kontinuierlich angepasst werden.

41. Analog dazu empfiehlt der Ausschuss der AT-AB in Bezug auf den Entwurf der Zertifizierungskriterien (für Auftragsverarbeiter) B.06.03 („Regelmäßige Überprüfung der Risikoanalyse“), den Verfahrensverantwortlichen aufzufordern, die Regelmäßigkeit der Überprüfungen näher zu erläutern und die betreffenden Kriterien dahingehend anzupassen, dass Antragsteller verpflichtet werden, Risikomanagementverfahren einzuführen, auf deren Grundlage die zur Erfüllung dieses Kriteriums getroffenen Maßnahmen kontinuierlich angepasst werden.

42. Darüber hinaus begrüßt der Ausschuss den Entwurf der Zertifizierungskriterien A.07.21 (für Verantwortliche) und B.07.21 (für Auftragsverarbeiter) („Leitlinien für Mitarbeiter zum Umgang mit Wechseldatenträgern“) und die Anforderung, dass ein themenspezifisches Konzept vorliegen muss. Der Ausschuss stellt jedoch fest, dass dieses themenspezifische Konzept vom Risikomanagementverfahren unabhängig zu sein scheint. Daher empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, diese Kriterien dahingehend abzuändern, dass sie eine Anforderung zum Abgleich dieses Konzepts mit dem allgemeinen Risikomanagementverfahren enthalten.

43. Der Ausschuss nimmt den Entwurf der Zertifizierungskriterien A.07.24 (für Verantwortliche) und B.07.24 (für Auftragsverarbeiter) („Prüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen“) zur Kenntnis, in denen vorgegeben wird, dass „[d]er Antragsteller der Zertifizierung [...] regelmäßige Kontrollen [durchführt], um die Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen sicherzustellen“. In diesem Zusammenhang stellt der Ausschuss fest, dass der Begriff „regelmäßig“ recht weit gefasst sein, zu Unklarheiten führen und die Überprüfbarkeit dieses Kriteriums beeinträchtigen kann. Daher empfiehlt der Ausschuss, dass genauer angegeben und erläutert wird, welche Kontrollen als „regelmäßige“ Kontrollen gelten, um die Überprüfbarkeit dieses Kriteriums zu verbessern.

44. Der Ausschuss begrüßt den Entwurf der Zertifizierungskriterien A.07.02 (für Verantwortliche) und B.07.02 (für Auftragsverarbeiter), die sich auf „Malware-Schutz und Updates“ beziehen. Der Ausschuss ist jedoch der Auffassung, dass die Anforderungen nicht weitreichend genug sind, dass in den Kriterien Strategien/Verfahren für die Ergebnisse des Risikomanagements enthalten sein sollten und dass die Kriterien nicht als losgelöste Anforderungen an den Malware-Schutz sowohl

für die Überprüfbarkeit als auch für die Wirksamkeit zu betrachten sind. Daher empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen aufzufordern, derartige Strategien zu entwickeln und sie in die Kriterien aufzunehmen.

45. Darüber hinaus ist der Ausschuss der Ansicht, dass die Kriterien A.07.02 sowie A.06.01 und A.06.02 (für Verantwortliche) in Bezug auf die Dokumentation eines Risikomanagementverfahrens bzw. in Bezug auf risikoorientierte Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung (Risiko-Kontroll-Matrix) aufeinander abgestimmt werden müssen. Was für das Kriterium A.07.02 gilt, gilt auch für die Kriterien A.07.03 bis A.07.10 sowie A.07.14 bis A.07.18 (d. h. der derzeitige Inhalt scheint nicht ausreichend zu sein). Demnach scheinen die entsprechenden Kriterien für Auftragsverarbeiter, nämlich die Kriterien B.06.01 und B.06.02, ebenso wenig ausreichend zu sein. Der Vollständigkeit halber empfiehlt der Ausschuss der AT-AB daher, den Verfahrensverantwortlichen aufzufordern, diese Kriterien abzuändern.

3 SCHLUSSFOLGERUNGEN/EMPFEHLUNGEN

46. Abschließend hält der EDSA fest, dass die derzeitigen Zertifizierungskriterien seiner Auffassung nach zu einer uneinheitlichen Anwendung der DSGVO führen können und dass die folgenden Änderungen vorgenommen werden müssen, um die Anforderungen nach Artikel 42 DSGVO unter Berücksichtigung der Leitlinien und des Addendums zu erfüllen:

47. Betreffend den Abschnitt „Allgemeine Bemerkungen“ empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen zu Folgendem aufzufordern:

    1. im Sinne der Genauigkeit den Verweis auf „Systeme“ in Abschnitt 1.1 „Bewertungsziel“ zu streichen;

    2. zur besseren Lesbarkeit und Nachvollziehbarkeit der Kriterien den Begriff „Datenschutzkoordinatoren“ entweder im Abschnitt „Allgemeine Begriffsbestimmungen“ zu definieren oder in den Kriterien selbst eindeutig zu definieren;

    3. die in Ziffer 12 dieser Stellungnahme aufgeführten Kriterien dahingehend abzuändern, dass sie mit der Datenschutz-Grundverordnung im Einklang stehen;

    4. den Begriff „Kunde“ in den Kriterien B.04.04 („Verarbeitung personenbezogener Daten ausschließlich auf der Grundlage einer dokumentierten Weisung des Verantwortlichen“) und B.04.08 („Anforderungen an die Einhaltung der in der Datenverarbeitungsvereinbarung festgelegten Verpflichtungen“) im Sinne der Einheitlichkeit und Genauigkeit durch den Begriff „Verantwortlicher“ zu ersetzen.

48. Betreffend den Abschnitt „Anwendungsbereich des Zertifizierungsverfahrens und Evaluierungsgegenstand (Target of Evaluation, ToE)“ empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen zu Folgendem aufzufordern:

    1. die Bedingungen aufzunehmen, die erfüllt sein müssen, um die Nichtanwendbarkeit eines Kriteriums standardmäßig als integralen Bestandteil der Kriterien festzustellen, die Formulierung „zum Beispiel“ („z. B.“) zu streichen und das Wort „können“ durch das Wort „müssen“ zu ersetzen.

49. Betreffend den Abschnitt „Rechtmäßigkeit der Verarbeitung“ empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen zu Folgendem aufzufordern:

    1. Unterpunkt b des Kriteriums A.02.10 dahingehend abzuändern, dass daraus eindeutig die Notwendigkeit hervorgeht, unter Angabe der Gründe zu dokumentieren, warum die Verarbeitung erforderlich ist, um lebenswichtige Interessen (z. B. das Leben) der betroffenen Person oder einer anderen natürlichen Person zu schützen, und warum sie nicht auf eine andere Rechtsgrundlage gestützt werden kann.

50. Betreffend den Abschnitt „Rechtsgrundlage“ empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen zu Folgendem aufzufordern:

    1. der Vollständigkeit halber Artikel 7 DSGVO in die Verweise für das Einwilligungskriterium aufzunehmen;

    2. die Formulierung „insbesondere“ hinzuzufügen, um klarzustellen, dass auch andere Garantien in die gemäß Kriterium A.02.10 erforderliche Dokumentation aufgenommen werden könnten.

51. Betreffend den Abschnitt „Grundsätze des Artikels 5“ empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen zu Folgendem aufzufordern:

    1. den Wortlaut des Kriteriums A.01.01 am Wortlaut der Bestimmung in Artikel 5 Absatz 2 DSGVO auszurichten;

    2. den Verweis auf Artikel 12 DSGVO in die detaillierte Anforderung des Kriteriums A.02.01 aufzunehmen, dass der Antragsteller der Zertifizierung über Regeln, einen Mechanismus oder ein Verfahren verfügen muss, um die Transparenzanforderungen der DSGVO sicherzustellen, was bedeutet, dass den betroffenen Personen (gemäß Artikel 13 und 14 DSGVO) Informationen zur Verfügung gestellt werden, um die Vollständigkeit und Einheitlichkeit zu gewährleisten;

    3. die Formulierung „(bei der Bereitstellung von Informationen für Kinder)“ im Sinne der Genauigkeit aus den detaillierten Anforderungen des Kriteriums zu streichen;

    4. im Abschnitt „Anwendungsleitlinien“ des Kriteriums A.02.01 einen Verweis auf die „EDSA-Leitlinien 4/2019 zu Artikel 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Version 2.0, angenommen am 20. Oktober 2020“ aufzunehmen;

    5. für den Grundsatz von Treu und Glauben 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 Leitlinien 4/2019 zu Artikel 25 der DSGVO über Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (siehe auch Stellungnahme 3/2025 des EDSA) aufgeführt sind;

    6. in Kriterium A.02.07.07 klarzustellen, dass eine weitere Verarbeitung für im öffentlichen Interesse liegende Archivierungszwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke nicht per se als mit dem ursprünglichen Zweck (singular) unvereinbar gilt, sofern eine Bewertung der Vereinbarkeit des Zwecks ordnungsgemäß dokumentiert wird, insbesondere im

Hinblick auf das Bestehen geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person.

52. Betreffend den Abschnitt „Allgemeine Verpflichtungen der Verantwortlichen und Auftragsverarbeiter“ empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen zu Folgendem aufzufordern:

    1. die Kriterien A.10.03 (für Verantwortliche) und B.10.03 (für Auftragsverarbeiter) dahingehend anzupassen, dass die dem Datenschutzbeauftragten zugewiesenen Ressourcen nicht nur für die Erfüllung von Aufgaben, sondern auch für die Erhaltung von Fachwissen im Einklang mit Artikel 38 Absatz 2 DSGVO eingesetzt werden können;

    2. Kriterium B.08.01 zu ändern und die Frist von 72 Stunden zu streichen.

53. Betreffend den Abschnitt „Rechte der betroffenen Personen“ empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen zu Folgendem aufzufordern:

    1. Kriterium A.03.04 zu ändern und einen Hinweis auf die Frist aufzunehmen, um die Vollständigkeit und Einheitlichkeit zu gewährleisten;

    2. anzugeben, auf welche Weise der Identitätsnachweis von der betroffenen Person erbracht werden kann.

54. Betreffend den Abschnitt „Schutz garantierende technische und organisatorische Maßnahmen“ empfiehlt der Ausschuss der AT-AB, den Verfahrensverantwortlichen zu Folgendem aufzufordern:

    1. Kriterium A.04.01 im Sinne der Vollständigkeit und Genauigkeit mit der DSGVO in Einklang zu bringen;

    2. Kriterium B.04.01.1 zu ändern und einen Hinweis auf das sehr frühe Stadium der Verarbeitung aufzunehmen;

    3. Kriterium A.01.04 dahingehend zu ändern, dass darin auch vorgegeben wird, dass der Antragsteller ein Überwachungsverfahren einrichten muss, mit dem eine Analyse aller Datenschutzaktivitäten ermöglicht wird;

    4. die Regelmäßigkeit der Überprüfungen näher zu erläutern und Kriterium A.06.03 dahingehend anzupassen, dass Antragsteller verpflichtet werden, Risikomanagementverfahren einzuführen, auf deren Grundlage die zur Erfüllung dieses Kriteriums getroffenen Maßnahmen kontinuierlich angepasst werden;

    5. die Regelmäßigkeit der Überprüfungen näher zu erläutern und Kriterium B.06.03 dahingehend anzupassen, dass Antragsteller verpflichtet werden, Risikomanagementverfahren einzuführen, auf deren Grundlage die zur Erfüllung dieses Kriteriums getroffenen Maßnahmen kontinuierlich angepasst werden

    6. die Kriterien A.07.21 (für Verantwortliche) und B.07.21 (für Auftragsverarbeiter) dahingehend abzuändern, dass sie eine Anforderung zum Abgleich dieses Konzepts mit dem allgemeinen Risikomanagementverfahren enthalten;

7. genauer anzugeben und zu erläutern, welche Kontrollen als „regelmäßige“ Kontrollen gelten, um die Überprüfbarkeit der Kriterien A.07.24 (für Verantwortliche) und B.07.24 (für Auftragsverarbeiter) zu verbessern;

8. Strategien für die Ergebnisse des Risikomanagements zu entwickeln und sie in die Kriterien A.07.02 (für Verantwortliche) und B.07.02 (für Auftragsverarbeiter) aufzunehmen;

9. der Vollständigkeit halber Kriterium A.07.02 auf die Kriterien A.06.01 und A.06.02 (für Verantwortliche) und Kriterium B.06.01 auf das Kriterium B.06.02 (für Verarbeiter) abzustimmen.

55. Schließlich erinnert der EDSA im Einklang mit den Leitlinien auch daran, dass die AT-AB im Falle von Änderungen der Zertifizierungskriterien der BDO Consulting GmbH, die wesentliche Änderungen mit sich bringen,[8] dem EDSA die geänderte Fassung gemäß Artikel 42 Absatz 5 und Artikel 43 Absatz 2 Buchstabe b der DSGVO vorlegen muss.

4 SCHLUSSBEMERKUNGEN

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

57. 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 Entwurf ihres Beschlusses beibehalten oder ändern wird. Innerhalb derselben Frist übermittelt sie den geänderten Entwurf oder teilt unter Angabe der maßgeblichen Gründe mit, dass sie beabsichtigt, der Stellungnahme des Ausschusses insgesamt oder teilweise nicht zu folgen.

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

59. Der EDSA erinnert daran, dass die AT-AB gemäß Artikel 43 Absatz 6 der DSGVO die Zertifizierungskriterien GDPR-CARPA 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
Der Vorsitz

(Anu Talus)

[8] 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.