Stellungnahme 30/2020 zum Entwurf des Beschlusses der zuständigen Aufsichtsbehörde Österreichs zur Genehmigung der Anforderungen an die Akkreditierung von Zertifizierungsstellen nach Artikel 43 Absatz 3 DSGVO

Angenommen am 7. Dezember 2020

Inhaltsverzeichnis

Der Europäische Datenschutzausschuss –

gestützt auf Artikel 63, Artikel 64 Absatz 1 Buchstabe c, Artikel 64 Absätze 3 bis 8 und Artikel 43 Absatz 3 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, im Folgenden „DSGVO"),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum, 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 10 und Artikel 22 seiner Geschäftsordnung vom 25. Mai 2018,

in Erwägung nachstehender Gründe:

(1) Hauptaufgabe des Ausschusses ist es, die einheitliche Anwendung der Verordnung (EU) 2016/679 (im Folgenden „DSGVO") im gesamten Europäischen Wirtschaftsraum sicherzustellen. Im Einklang mit Artikel 64 Absatz 1 DSGVO gibt der Ausschuss eine Stellungnahme ab, wenn eine Aufsichtsbehörde (AB) beabsichtigt, die Anforderungen an die Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 zu billigen. Mit dieser Stellungnahme soll daher ein harmonisierter Ansatz in Bezug auf die Anforderungen geschaffen werden, die eine Datenschutzaufsichtsbehörde oder die nationale Akkreditierungsstelle an die Akkreditierung einer Zertifizierungsstelle stellt. Die DSGVO gibt zwar keine einheitlichen Anforderungen an die Akkreditierung vor, fördert jedoch Kohärenz. Der Ausschuss ist bestrebt, dieses Ziel mit seinen Stellungnahmen zu erreichen, indem erstens die Aufsichtsbehörden darin bestärkt werden, ihre Anforderungen an die Akkreditierung entsprechend der im Anhang zu den EDSA-Leitlinien über die Akkreditierung von Zertifizierungsstellen vorgegebenen Gliederung zu formulieren, und zweitens die Anforderungen anhand eines vom EDSA erstellten Standardformulars analysiert werden, welches ein Benchmarking der Anforderungen (gemäß ISO 17065 und den EDSA-Leitlinien für die Akkreditierung von Zertifizierungsstellen) ermöglicht.

(2) Nach Artikel 43 DSGVO legen die zuständigen Aufsichtsbehörden die Anforderungen an die Akkreditierung fest. Dabei befolgen sie jedoch das Kohärenzverfahren, um insbesondere durch Festlegung hoher Anforderungen Vertrauen in das Zertifizierungsverfahren zu schaffen.

(3) Dass die Anforderungen an die Akkreditierung dem Kohärenzverfahren unterliegen, bedeutet jedoch nicht, dass die Anforderungen identisch sein sollten. Die zuständigen Aufsichtsbehörden verfügen über einen Ermessensspielraum im Hinblick auf den nationalen oder regionalen Kontext und sollten ihren lokalen Rechtsvorschriften Rechnung tragen. Die Stellungnahme des EDSA soll nicht unionsweit einheitliche Anforderungen herbeiführen, sondern vielmehr erhebliche Inkohärenzen vermeiden, die zum Beispiel das Vertrauen in die Unabhängigkeit oder das Fachwissen akkreditierter Zertifizierungsstellen beeinträchtigen könnten.

[1] Soweit in dieser Stellungnahme auf die „Union" Bezug genommen wird, ist dies als Bezugnahme auf den „EWR" zu verstehen.

(4) Die „Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 der Datenschutz-Grundverordnung (2016/679)“ (im Folgenden „Leitlinien“) und die „Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679“ dienen im Rahmen des Kohärenzverfahrens als Richtschnur.

(5) Wenn ein Mitgliedstaat vorsieht, dass die Zertifizierungsstellen von der Aufsichtsbehörde akkreditiert werden, sollte die Aufsichtsbehörde Akkreditierungsanforderungen festlegen, die u. a. die in Artikel 43 Absatz 2 genannten Anforderungen beinhalten. Verglichen mit den Verpflichtungen, die den nationalen Akkreditierungsstellen im Zusammenhang mit der Akkreditierung von Zertifizierungsstellen zufallen, enthält Artikel 43 weniger genaue Angaben zu den Anforderungen an die von der Aufsichtsbehörde selbst durchgeführte Akkreditierung. Um einen harmonisierten Akkreditierungsansatz zu erreichen, sollten sich die von der Aufsichtsbehörde verwendeten Akkreditierungsanforderungen an der ISO/IEC 17065 orientieren und durch die von der Aufsichtsbehörde gemäß Artikel 43 Absatz 1 Buchstabe b festgelegten zusätzlichen Anforderungen ergänzt werden. Der Europäische Datenschutzausschuss (im Folgenden „EDSA“) stellt fest, dass in Artikel 43 Absatz 2 Buchstaben a bis e die Anforderungen der ISO 17065 wiedergegeben und spezifiziert sind, was zur Einheitlichkeit beiträgt.[2]

(6) Die Stellungnahme des EDSA wird gemäß Artikel 64 Absatz 1 Buchstabe c sowie Artikel 64 Absätze 3 und 8 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 angenommen. Diese Frist kann unter Berücksichtigung der Komplexität der Angelegenheit auf Beschluss des Vorsitzenden um weitere sechs Wochen verlängert werden.

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1 ZUSAMMENFASSUNG DES SACHVERHALTS

1. Die österreichische Aufsichtsbehörde (im Folgenden „AT-AB“) hat dem EDSA ihren Entwurf für die Anforderungen an die Akkreditierung nach Artikel 43 Absatz 1 Buchstabe b vorgelegt. Das Dossier wurde am 9. Oktober 2020 als vollständig erachtet. Die AT-AB wird die Zertifizierungsstellen, die die Zertifizierungen nach den Kriterien der DSGVO vornehmen, akkreditieren.

[2] Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 der Datenschutz-Grundverordnung, Punkt 39. Verfügbar unter: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en.

2 BEWERTUNG

2.1 Allgemeine Ausführungen des EDSA zum vorgelegten Beschlussentwurf

2. Zweck dieser Stellungnahme ist es, die Akkreditierungsanforderungen zu bewerten, die eine Aufsichtsbehörde entweder auf Grundlage von ISO 17065 oder vollständig selbst entwickelt hat, nach denen eine nationale Akkreditierungsstelle oder eine Aufsichtsbehörde gemäß Artikel 43 Absatz 1 DSGVO Zertifizierungsstellen akkreditieren kann, die für die Erteilung und Verlängerung von Zertifizierungen gemäß Artikel 42 DSGVO zuständig sind. Die Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde bleiben davon unberührt. In diesem konkreten Fall stellt der Ausschuss fest, dass die AT-AB nach nationalem Recht mit der Akkreditierung von Zertifizierungsstellen betraut ist. Zu diesem Zweck hat die AT-AB speziell für die Akkreditierung von Zertifizierungsstellen eine Reihe von Anforderungen entwickelt.

3. Bei der Bewertung der Akkreditierungsanforderungen der AT-AB geht es darum, zu untersuchen, inwieweit (durch Ergänzungen oder Streichungen) von den Leitlinien, insbesondere von deren Anhang 1, abgewichen wird. Des Weiteren ist die Stellungnahme des EDSA auf alle Aspekte fokussiert, die einem einheitlichen Ansatz bei der Akkreditierung von Zertifizierungsstellen zuwiderlaufen könnten.

4. Anzumerken ist, dass das Ziel der Leitlinien zur Akkreditierung von Zertifizierungsstellen darin besteht, die Aufsichtsbehörde bei der Festlegung ihrer Anforderungen an die Akkreditierung zu unterstützen. Der Anhang zu den Leitlinien selbst stellt keine Akkreditierungsanforderungen dar. Die Anforderungen an die Akkreditierung von Zertifizierungsstellen müssen von der Aufsichtsbehörde daher auf eine Weise festgelegt werden, die ihre praktische und einheitliche Anwendung in dem von der Aufsichtsbehörde vorgesehenen Zusammenhang ermöglicht.

5. Der Ausschuss anerkennt, dass den nationalen Akkreditierungsstellen auf Grund ihres Fachwissens Spielraum im Hinblick auf die Festlegung der spezifischen Bestimmungen der einschlägigen Akkreditierungsanforderungen gewährt werden sollte. Der Ausschuss hält es jedoch für erforderlich, hervorzuheben, dass etwaige zusätzliche Anforderungen so festzulegen sind, dass diese praktisch und einheitlich angewendet und erforderlichenfalls überprüft werden können.

6. Der Ausschuss merkt an, dass ISO-Normen, insbesondere die ISO 17065, als geistiges Eigentum geschützt sind, weshalb davon abgesehen wird, in dieser Stellungnahme auf den Text des betreffenden Dokuments zu verweisen. Der Ausschuss hat daher beschlossen, ggf. auf einzelne Abschnitte der ISO-Norm zu verweisen, ohne jedoch deren Wortlaut wiederzugeben.

7. Der Ausschuss hat seine Bewertung gemäß der in Anhang 1 der Leitlinien (im Folgenden „Anhang“) vorgesehenen Gliederung vorgenommen. Soweit diese Stellungnahme keine Anmerkungen zu einem bestimmten Abschnitt im von der AT-AB vorgelegten Entwurf der Akkreditierungsanforderungen enthält, ist davon auszugehen, dass der Ausschuss dazu nichts anzumerken hat und die AT-AB nicht um weitere Maßnahmen ersucht.

8. Auf Punkte außerhalb des Anwendungsbereichs von Artikel 43 Absatz 2 DSGVO, zum Beispiel von der AT-AB vorgebrachte Verweise auf nationale Rechtsvorschriften, wird in dieser Stellungnahme nicht eingegangen. Der Ausschuss stellt gleichwohl fest, dass die nationalen Rechtsvorschriften soweit erforderlich mit der DSGVO in Einklang stehen sollten.

2.2 Schwerpunkte der Bewertung (Artikel 43 Absatz 2 DSGVO und Anhang 1 zu den EDSA-Leitlinien), die die Akkreditierungsanforderungen für eine einheitliche Prüfung vorsehen:

a. Regelung aller im Anhang zu den Leitlinien hervorgehobenen Hauptbereiche und Prüfung aller Abweichungen vom Anhang;

b. Unabhängigkeit der Zertifizierungsstelle;

c. Interessenkonflikte der Zertifizierungsstelle;

d. Fachwissen der Zertifizierungsstelle;

e. geeignete Garantien, die sicherstellen, dass die DSGVO-Zertifizierungskriterien von der Zertifizierungsstelle ordnungsgemäß angewendet werden;

f. Verfahren für die Erteilung, die regelmäßige Überprüfung und den Widerruf der DSGVO-Zertifizierung; sowie

g. transparente Bearbeitung von Beschwerden über Verletzungen der Zertifizierung.

9. Unter Berücksichtigung, dass:

a. in Artikel 43 Absatz 2 DSGVO Akkreditierungsanforderungen angeführt sind, die eine Zertifizierungsstelle erfüllen muss, um akkreditiert werden zu können;

b. Artikel 43 Absatz 3 DSGVO vorsieht, dass die Anforderungen an die Akkreditierung von Zertifizierungsstellen der Genehmigung durch die zuständige Aufsichtsbehörde bedürfen;

c. Artikel 57 Absatz 1 Buchstaben p und q DSGVO vorsehen, dass die Anforderungen an die Akkreditierung von Zertifizierungsstellen von einer zuständigen Aufsichtsbehörde zu formulieren und zu veröffentlichen sind, wobei diese beschließen kann, die Akkreditierung von Zertifizierungsstellen selbst vorzunehmen;

d. Artikel 64 Absatz 1 Buchstabe c DSGVO vorsieht, dass der Ausschuss eine Stellungnahme abgibt, wenn eine Aufsichtsbehörde die Genehmigung der Anforderungen an die Akkreditierung einer Zertifizierungsstelle nach Artikel 43 Absatz 3 beabsichtigt;

e. falls die nationale Akkreditierungsstelle die Akkreditierung nach der ISO/IEC 17065/2012 durchführt, auch die von der zuständigen Aufsichtsbehörde aufgestellten zusätzlichen Anforderungen zu erfüllen sind;

f. Anhang 1 der Leitlinien zur Akkreditierung von Zertifizierungsstellen Vorschläge für von Datenschutzaufsichtsbehörden festzulegende Anforderungen an die Akkreditierung von Zertifizierungsstellen durch die nationale Akkreditierungsstelle enthält;

gelangt der Ausschuss zu folgender Stellungnahme:

2.2.1 ALLGEMEINE ANMERKUNGEN

10. Der Ausschuss anerkennt, dass der Entwurf der Anforderungen der AT-AB, wie von der AT-AB erläutert, im Einklang mit den Verfahrensvorschriften des österreichischen Rechts erstellt wurde.

Dennoch empfiehlt der Ausschuss der AT-AB, sich nach dem Aufbau und den Titeln des Anhangs zu richten, soweit dies nach nationalem Recht möglich ist.

11. Der Ausschuss anerkennt, dass der Entwurf der Akkreditierungsanforderungen der AT-AB einen Abschnitt über Begriffe und Begriffsbestimmungen enthält. Einige der Begriffe werden jedoch nicht konsistent im gesamten Dokument verwendet (z. B. „Konformitätsbewertung“ anstelle von „Zertifizierung“ in Abschnitt 7.1.2; „die mit dem Zertifizierungsverfahren betrauten Personen“ anstelle von „Bewerter“ in Abschnitt 7.5; der Verweis auf „Datenschutzbehörde“ anstelle von „AT-AB“ usw.). Der Ausschuss fordert die AT-AB auf, eine konsistente Verwendung der Begriffe sicherzustellen.

12. Der Ausschuss stellt fest, dass die Anforderungen präskriptiv formuliert werden sollten. In den Anforderungen ist daher das Wort „sollen“ zu vermeiden und stattdessen das Wort „müssen“ zu verwenden. Der EDSA fordert die AT-AB auf, diesbezüglich die erforderlichen Änderungen vorzunehmen (z. B. in Abschnitt 10(1)).

13. Der Ausschuss erkennt die Besonderheit der von der AT-AB vorgelegten Erläuterungen an. Er ist jedoch der Auffassung, dass einige der Erläuterungen eher in den Text der Verordnung aufgenommen werden sollten. Insbesondere empfiehlt der Ausschuss der AT-AB, diesbezüglich die folgenden Änderungen vorzunehmen: Aufnahme des Verweises auf die Aufgaben und Befugnisse der AB in Abschnitt 9(2)(7); Aufnahme der Verweise auf das EU-Siegel in Abschnitt 8(2); hinsichtlich Abschnitt 9.3.1 des Anhangs sollte die Verordnung die in den Erläuterungen hinzugefügten Pflichten in Bezug auf die Kommunikation mit den Antragstellern und Inhabern einer Zertifizierung enthalten; in die Verordnung sollten auch die Informationen bezüglich Abschnitt 9.3.4 des Anhangs aufgenommen werden; Abschnitt 19 sollte einen klaren Hinweis auf die Verpflichtung der Zertifizierungsstelle enthalten, die Management-Prinzipien und ihre dokumentierte Umsetzung gegenüber der AB offenzulegen; Abschnitt 11 sollte Informationen in Bezug auf eine frühere Zertifizierung enthalten (Seite 6, Absatz 2 der Erläuterungen).

2.2.2 ALLGEMEINE ANFORDERUNGEN AN DIE AKKREDITIERUNG

14. In Bezug auf das Erfordernis der rechtlichen Verantwortung stellt der Ausschuss fest, dass die AT-AB im Begleitdokument erläutert, dass sich die Verpflichtung der Zertifizierungsstelle zur Einhaltung der DSGVO aus der DSGVO selbst ergebe und die Aufnahme weiterer diesbezüglicher Anforderungen daher nicht erforderlich sei. Der Ausschuss vertritt jedoch die Ansicht, dass die Verpflichtung der Zertifizierungsstelle zur Einhaltung der DSGVO und der Akkreditierungsanforderungen in die Verordnung aufgenommen werden sollte. Wie in Abschnitt 4.1.1 des Anhangs der Leitlinien festgelegt, muss die Zertifizierungsstelle nachweisen können, dass sie über die neuesten Verfahren verfügt und dass diese mit den in den Akkreditierungsbedingungen festgelegten rechtlichen Zuständigkeiten im Einklang stehen. Ferner muss die Zertifizierungsstelle nachweisen können, dass sie über mit der DSGVO vereinbare Verfahren und Maßnahmen verfügt, insbesondere für die Kontrolle von und den Umgang mit personenbezogenen Daten der Kundenorganisation als Teil des Zertifizierungsprozesses. Daher empfiehlt der Ausschuss der AT-AB, den Entwurf der Anforderungen zu überarbeiten und mit den Leitlinien in Einklang zu bringen.

15. In Bezug auf die Handhabung der Unparteilichkeit ist eine Zertifizierungsstelle gemäß Abschnitt 5.2 des Entwurfs der Anforderungen der AT-AB nicht unparteiisch, „wenn zwischen der Zertifizierungsstelle und dem Zertifizierungswerber oder -inhaber ein Vertragsverhältnis im Sinne des Art. 26 Abs. 1 zweiter Satz oder Art. 28 Abs. 3 DSGVO besteht“. Nach Auffassung des Ausschusses werden andere Situationen, in denen die Unabhängigkeit der Zertifizierungsstelle beeinträchtigt

werden kann, von dieser Formulierung nicht erfasst. In diesem Zusammenhang stellt der Ausschuss fest, dass jede Art von wirtschaftlicher oder organisatorischer Beziehung zwischen der Zertifizierungsstelle und der juristischen Person, abhängig von ihren Merkmalen, die Unparteilichkeit der Zertifizierungstätigkeiten beeinträchtigen kann. Beispielsweise sollte die Zertifizierungsstelle weder derselben Unternehmensgruppe angehören noch in irgendeiner Weise von dem Kunden gesteuert werden, den sie beurteilt. Daher empfiehlt der Ausschuss der AT-AB, den Entwurf der Anforderungen zu überarbeiten und klarzustellen, dass jede Art von wirtschaftlicher Beziehung zwischen der Zertifizierungsstelle und der juristischen Person, abhängig von ihren Merkmalen, die Unparteilichkeit der Zertifizierungstätigkeiten beeinträchtigen kann.

16. In Bezug auf Abschnitt 8(7) der Verordnung der AT-AB ist der Ausschuss der Ansicht, dass die öffentlich zugänglichen Informationen auch alle Versionen der Kriterien gemäß Artikel 42 Absatz 5 DSGVO umfassen sollten, und fordert die AT-AB auf, eine solche Klarstellung vorzunehmen.

17. Nach Auffassung des Ausschusses deckt Abschnitt 9 („Zertifizierungsvereinbarung“) der Verordnung der AT-AB nicht alle in Abschnitt 4.1.2 des Anhangs angeführten Punkte ab. Der Ausschuss stellt fest, dass konkret die folgenden im Anhang genannten Punkte fehlen: Nummer 2 (den Antragsteller verpflichten, vollständige Transparenz des Zertifizierungsprozesses gegenüber der zuständigen Aufsichtsbehörde zu gewährleisten, einschließlich der vertraulichen Vertragsangelegenheiten) und Nummer 7 (es der Zertifizierungsstelle erlauben, [der AB] sämtliche Information offenzulegen, die gemäß Artikel 42 Absatz 8 und Artikel 43 Absatz 5 zur Erteilung der Zertifizierung erforderlich sind). Der EDSA empfiehlt der AT-AB deshalb, die oben genannten Punkte aufzunehmen.

18. Der Ausschuss stellt fest, dass die Bezugnahme auf die Fristen im Abschnitt 9(2)(1) auf die „in den Zertifizierungsanforderungen vorgesehenen Fristen“ beschränkt ist, während Abschnitt 4.1.2 Nummer 5 des Anhangs weiter gefasst ist und auch die Verpflichtung zur Einhaltung von Abläufen umfasst. Daher fordert der EDSA die AT-AB auf, den Wortlaut so umzuformulieren, dass allgemeiner auf Fristen Bezug genommen wird, und entsprechend dem Anhang einen Verweis auf geltende Abläufe aufzunehmen.

19. Außerdem weist der Ausschuss darauf hin, dass der Antragsteller gemäß dem Anhang verpflichtet ist, die Zertifizierungsstelle zu informieren, falls sich seine tatsächliche oder rechtliche Situation maßgeblich ändert oder Änderungen seiner Produkte, Verfahren und Dienstleistungen eintreten, die von der Zertifizierung betroffen sind (Abschnitt 4.1.2 Nummer 10 des Anhangs). Im Abschnitt 9(2)(4) des Entwurfs der Anforderungen verweist die AT-AB zudem nur auf wesentliche Änderungen, ohne diese näher auszuführen. Der Ausschuss empfiehlt der AT-AB, zu präzisieren, dass sich die wesentlichen Änderungen auf „ihre tatsächliche oder rechtliche Situation und auf ihre von der Zertifizierung betroffenen Produkte, Verfahren und Dienstleistungen beziehen“.

20. Der EDSA weist darauf hin, dass die Zertifizierungsvereinbarung gemäß Abschnitt 4.1.2 Nummer 6 des Anhangs Vorschriften zu Gültigkeit, Erneuerung und Widerruf sowie Vorschriften über angemessene Zeitabstände für die Neubeurteilung oder Prüfung enthalten sollte. Abschnitt 9(2)(5) der Verordnung der AT-AB enthält einen Hinweis auf die diesbezüglichen Verpflichtungen des Kunden, nicht aber auf die oben genannten Vorschriften. Der Ausschuss empfiehlt der AT-AB daher, einen solchen Verweis im Einklang mit dem Anhang aufzunehmen.

21. Der Ausschuss anerkennt, dass Abschnitt 9(2)(7) offenbar die in Abschnitt 4.1.2 Nummer 3 des Anhangs niedergelegte Anforderung hinsichtlich der Verantwortung des Antragstellers für die Einhaltung der DSGVO widerspiegelt. Einige Klarstellungen wären jedoch von Vorteil. Daher regt der Ausschuss an, den Wortlaut klarer zu formulieren und an den Anhang anzupassen.

Angenommen

22. Der EDSA stellt fest, dass in Abschnitt 14(2) der Verordnung die im Anhang angegebene Verpflichtung fehlt, dass Zertifikate, Siegel und Prüfzeichen nur unter Einhaltung der Artikel 42 und 43 und der Leitlinien zur Akkreditierung und Zertifizierung verwendet werden dürfen. Der Ausschuss empfiehlt der AT-AB, den Entwurf entsprechend zu ändern.

2.2.3 ANFORDERUNGEN AN RESSOURCEN

23. Die Erläuterungen zum Fachwissen der Zertifizierungsstelle (Abschnitt 7 des Entwurfs der Akkreditierungsanforderungen der AT-AB) decken nach Auffassung des Ausschusses die Nummern 2 und 3 in Abschnitt 6.1 des Anhangs nicht ab. Daher empfiehlt der Ausschuss der AT-AB, den Entwurf entsprechend zu ändern und die fehlenden Punkte aufzunehmen.

24. Im Hinblick auf die Ausbildungsanforderungen muss Personal mit technischer Fachkunde laut Anhang „relevantes technisches Fachwissen mit einer Qualifikation, die mindestens dem Niveau 6 des EQR entspricht oder einen anerkannten geschützten Titel (z. B. Dipl.-Ing.) in dem relevanten reglementierten Beruf“ nachweisen. Abschnitt 7(3) des Entwurfs der Akkreditierungsanforderungen der AT-AB nimmt jedoch nicht auf den unterstrichenen Teil Bezug. Angesichts der Vielfalt der Bildungssysteme empfiehlt der Ausschuss der AT-AB, den Entwurf der Anforderungen an den Wortlaut des Anhangs anzupassen und dabei das spezifische Bildungssystem und die im nationalen Recht verankerten Anforderungen zu berücksichtigen. Beispielsweise könnte in den Anforderungen der Nachweis „einer gleichwertigen Berufsausbildung, für welchen in dem Mitgliedsstaat, in dem er erfolgte, ein anerkannter geschützter Titel oder eine solche Berufsbezeichnung verliehen wird“ gefordert werden.

25. Darüber hinaus ist der Ausschuss der Auffassung, dass die Liste der Fachgebiete bereits auf das im Anhang geforderte technische Fachwissen zugeschnitten ist. Daher regt der Ausschuss an, im Hinblick auf die Ausbildungsanforderungen des technischen Personals den Verweis auf „Naturwissenschaften“ aus der Liste der Fachgebiete zu streichen.

26. In Abschnitt 7.6 ist festgelegt, dass Entscheider über Erfahrung mit den Vorschriften des technischen Datenschutzes verfügen sollten. Dieser spezifische Verweis eignet sich eher für Bewerter als für Entscheidungsträger. Der Ausschuss ist vielmehr der Ansicht, dass die Anforderungen an das Fachwissen von Bewertern und Entscheidungsträgern auf ihre unterschiedlichen Aufgaben abgestimmt sein sollten. Nach Auffassung des Ausschusses sollten Bewerter speziellere Fachkenntnisse und Berufserfahrung im Bereich der technischen Verfahren (z. B. Audits und Zertifizierungen) mitbringen, während Entscheidungsträger über allgemeinere und umfassendere Fachkenntnisse und Berufserfahrung im Bereich des Datenschutzes verfügen sollten. Daher rät der Ausschuss der AT-AB, die Anforderungen unter Berücksichtigung der unterschiedlichen Anforderungen an die Fachkenntnisse und/oder Erfahrung von Bewertern und Entscheidungsträgern zu überarbeiten.

2.2.4 ANFORDERUNGEN AN PROZESSE

27. Der Ausschuss stellt fest, dass der Antrag auf Zertifizierung gemäß Abschnitt 8(1)(2) („Zertifizierungsverfahren“) der Verordnung „Angaben zur beantragten Zertifizierung“ enthalten muss. Nach Auffassung des EDSA sollte dieser Wortlaut entsprechend dem Anhang um die Angaben ergänzt werden, die enthalten sein sollten. In diesem Zusammenhang bezieht sich Abschnitt 7.2

Nummer 1 des Anhangs auf den Zertifizierungsgegenstand (Evaluierungsgegenstand, EVG), der auch „Schnittstellen und Übergänge zu anderen Systemen und Organisationen, Protokolle und andere Nachweise“ beinhaltet. Der Ausschuss empfiehlt der AT-AB daher, die im Anhang genannten Angaben aufzunehmen.

28. Der Ausschuss stellt fest, dass in Abschnitt 8(1)(3) der Verordnung auf die gemeinsame Verantwortlichkeit und den Einsatz von Auftragsverarbeitern Bezug genommen wird. In diesem Zusammenhang sollte die AT-AB nach Ansicht der EDSA angeben, dass die Informationen über die Auftragsverarbeiter/gemeinsam Verantwortlichen eine Beschreibung ihrer Verantwortlichkeiten und Aufgaben beinhalten sollten und dass der Antrag die relevanten Verträge oder Vereinbarungen enthalten muss.

29. In Bezug auf das Erfordernis gemäß Abschnitt 7.3 Nummer 1 des Anhangs, in der Zertifizierungsvereinbarung verbindliche Beurteilungsverfahren in Bezug auf den Evaluierungsgegenstand (EVG) festzulegen, stellt der Ausschuss fest, dass Abschnitt 9(2)(10) der Verordnung nur auf „Bewertungsmethoden“ verweist. Der Ausschuss regt an, dass die AT-AB deren Verbindlichkeit eindeutig klarstellt.

30. Nach Ansicht des Ausschusses geht aus Abschnitt 10 der Verordnung („Änderung von Zertifizierungsvereinbarungen“) nicht klar genug hervor, welche Art von Änderungen gemeint ist. Aufgrund weiterer Erläuterungen der AT-AB geht der Ausschuss davon aus, dass es sich um Änderungen handelt, die sich auf die Zertifizierung auswirken könnten. Angesichts der Notwendigkeit, die Unparteilichkeit der Zertifizierungsstelle zu wahren, regt der Ausschuss daher an, dass die AT-AB die Anforderungen umformuliert, um klarzustellen, dass es sich um Änderungen handelt, die sich auf die Zertifizierung auswirken könnten, und, um klarzustellen, dass der Kunde rechtzeitig allgemeine Informationen über Änderungen erhält, die sich auf seine Zertifizierung auswirken könnten.

31. Darüber hinaus stellt der Ausschuss fest, dass es keinen Verweis auf die in Abschnitt 7.10 des Anhangs zu vereinbarenden Änderungsverfahren gibt. Der Ausschuss regt an, einen solchen Verweis aufzunehmen und einige Verfahren zu nennen, die eingeführt werden könnten (z. B. Übergangszeiträume, Genehmigungsprozesse der zuständigen Aufsichtsbehörde usw.). Darüber hinaus ist der Ausschuss der Auffassung, dass Änderungen des Stands der Technik ebenfalls relevant sind und sich auf die Zertifizierung auswirken könnten. Daher empfiehlt der Ausschuss der AT-AB, diese Möglichkeit in die Liste der Änderungen aufzunehmen, die sich auf die Zertifizierung auswirken.

32. Der Ausschuss stellt fest, dass in Abschnitt 11 der Verordnung („Evaluierung“) einige der in Abschnitt 7.4 des Anhangs genannten Punkte nicht enthalten sind. Insbesondere ist der Ausschuss der Auffassung, dass der Entwurf der Anforderungen der AT-AB die Verpflichtung der Zertifizierungsstelle enthalten sollte, in ihrem Zertifizierungsmechanismus detailliert darzulegen, wie die in Abschnitt 7.4.6 der ISO/IEC 17065:2012 geforderten Informationen den Antragsteller über Nichtkonformitäten mit einem Zertifizierungsmechanismus unterrichten (Abschnitt 7.4 Absatz 5 des Anhangs). Der Ausschuss empfiehlt der AT-AB daher, eine solche Verpflichtung in den Entwurf aufzunehmen.

33. Darüber hinaus ist der Ausschuss der Ansicht, dass Abschnitt 11(1) nicht nur auf Abschnitt 7.4 der ISO/IEC 17065:2012 verweisen sollte. Beispielsweise könnte die Anforderung lauten: „Ergänzend zu Abschnitt 7.4 der ISO/IEC 17065:2012 …“. Darüber hinaus sollten die Erläuterungen nach Auffassung des Ausschusses alle Punkte aus Abschnitt 7.4 des Anhangs abdecken. Der Ausschuss fordert die AT AB daher auf, den Entwurf entsprechend zu ändern.

Angenommen

34. Der Ausschuss stellt fest, dass die Verpflichtung, Verfahren für die Erteilung, die regelmäßige Überprüfung und den Widerruf der jeweiligen Zertifizierungen gemäß Artikel 43 Absatz 2 und Artikel 43 Absatz 3 (Abschnitt 7.5 des Anhangs) vorzusehen, im Entwurf der Anforderungen der AT-AB nicht enthalten ist. Der EDSA empfiehlt der AT-AB deshalb die Aufnahme dieser Verpflichtung.

35. Außerdem empfiehlt der EDSA der AT-AB, in Abschnitt 13(1) einen Verweis auf die DSGVO und die von einer Aufsichtsbehörde genehmigten Zertifizierungskriterien aufzunehmen.

36. Im Hinblick auf Abschnitt 13.4 („Zertifizierungsentscheidung“) stellt der Ausschuss fest, dass die ersten beiden Punkte von Abschnitt 7.7 des Anhangs in der Verordnung nicht berücksichtigt sind, obwohl in der Erläuterung zu Abschnitt 9.2.3 festgelegt ist, dass die Zertifizierung für eine Höchstdauer von drei Jahren erteilt werden kann. Der Ausschuss ist der Auffassung, dass diese Anforderungen im Text der Verordnung enthalten sein sollten, und empfiehlt der AT-AB, diese Informationen in den Entwurf der Verordnung aufzunehmen.

37. Der Ausschuss anerkennt, dass Abschnitt 15(1) („Verzeichnis zertifizierter Produkte“) die Verpflichtung der Zertifizierungsstelle enthält, ein Verzeichnis zertifizierter Produkte zu führen. Wie jedoch in Abschnitt 7.8 des Anhangs dargelegt, ist sicherzustellen, dass die Informationen zu zertifizierten Produkten, Prozessen und Dienstleistungen intern verfügbar und öffentlich zugänglich bleiben. Der Ausschuss empfiehlt der AT-AB, den Entwurf entsprechend zu ändern.

38. Der Ausschuss stellt ferner fest, dass in Abschnitt 15(3) festgelegt ist, dass die Zertifizierungsstelle der Aufsichtsbehörde auf Anfrage das vollständige Verzeichnis zur Verfügung stellt. Die Anforderungen sollten jedoch auch die Verpflichtung enthalten, dass die Zertifizierungsstelle der zuständigen Aufsichtsbehörde die Gründe für die Erteilung oder den Widerruf der beantragten Zertifizierung mitteilen muss. Der Ausschuss empfiehlt der AT-AB, den Entwurf entsprechend zu ändern.

39. In Bezug auf die Verpflichtung, die Aufsichtsbehörde über die Gründe für die Beendigung, Einschränkung, Aussetzung oder den Widerruf einer Zertifizierung zu informieren (Abschnitt 17(2) der Verordnung), sollte die AT-AB nach Ansicht des Ausschusses klarstellen, dass die Unterrichtung schriftlich erfolgen sollte.

40. In Bezug auf Abschnitt 18(2)(2) der Verordnung erkennt der Ausschuss an, dass Angaben in Bezug auf „allfällige Unvereinbarkeitsregelungen“ aufgenommen wurden. Der Ausschuss geht davon aus, dass sich dieser Verweis darauf bezieht, dass die Zertifizierungsstelle festlegen muss, wie eine Trennung zwischen Zertifizierungstätigkeiten und der Bearbeitung von Widersprüchen und Beschwerden gewährleistet wird (Abschnitt 7.13 des Anhangs). Der Ausschuss hält den Wortlaut des Anhangs jedoch für klarer und regt an, dass die AT-AB den Wortlaut entsprechend anpasst.

2.2.5 MANAGEMENTSYSTEMANFORDERUNGEN

41. In Bezug auf Abschnitt 9(2)(9)(a) der Verordnung nimmt der Ausschuss den Verweis auf einen Maßnahmenkatalog für die Behandlung von Beschwerden zur Kenntnis. Nach Ansicht des Ausschusses ist der Wortlaut des Anhangs (Abschnitt 4.1.2 Nummer 8) vollständiger, da er Struktur und Verfahren der Beschwerdeabwicklung berücksichtigt. Der Ausschuss fordert die AT AB daher auf, den Entwurf entsprechend zu ändern.

2.2.6 WEITERE ZUSÄTZLICHE ANFORDERUNGEN

42. Der Ausschuss ist der Auffassung, dass einige in den Abschnitten 9.3.1 und 9.3.3 des Anhangs aufgeführte Punkte fehlen. Insbesondere sollten die folgenden Informationen ergänzt werden: Hinsichtlich Abschnitt 9.3.1 des Anhangs sollte die Verordnung die Verfahren zur Gewährleistung angemessener Abläufe und Kommunikationsstrukturen enthalten, vor allem die Verpflichtung eine Dokumentation über Aufgaben und Zuständigkeiten durch die Zertifizierungsstelle zu führen und ein Antragsverfahren zum Zweck der Evaluierungen durch die zuständige Aufsichtsbehörde zu pflegen. Zudem verweist Abschnitt 9(2)(11) der Verordnung nur auf *Kommunikationsstrukturen* und nicht auf *Kommunikationsstrukturen und Abläufe*, wie im Anhang gefordert. Hinsichtlich Abschnitt 9.3.3 des Anhangs sollte die Verordnung darauf hinweisen, dass die Zertifizierungsstelle der Aufsichtsbehörde relevante Beschwerden und Einsprüche mitteilen muss. Der Ausschuss empfiehlt der AT-AB, den Entwurf der Anforderungen entsprechend zu ändern.

3 SCHLUSSFOLGERUNGEN/EMPFEHLUNGEN

43. Da der Entwurf der Akkreditierungsanforderungen der österreichischen Aufsichtsbehörde zu einer inkohärenten Praxis der Akkreditierung von Zertifizierungsstellen führen könnte, sind folgende Änderungen vorzunehmen:

44. In Bezug auf „Allgemeine Anmerkungen“ empfiehlt der Ausschuss der AT AB,

    1) die erforderlichen Änderungen vorzunehmen und einige der Erläuterungen in den Text der Verordnung aufzunehmen, wie in Ziffer 13 dieser Stellungnahme ausgeführt.

45. In Bezug auf „Allgemeine Anforderungen an die Akkreditierung“ empfiehlt der Ausschuss der AT-AB,

    2) den Entwurf der Anforderungen zu überarbeiten und in die Verordnung aufzunehmen, dass die Zertifizierungsstelle zur Einhaltung der DSGVO und der Akkreditierungsanforderungen verpflichtet ist und nachweisen muss, dass sie über mit der DSGVO vereinbare Verfahren und Maßnahmen verfügt, insbesondere für die Kontrolle von und den Umgang mit personenbezogenen Daten der Kundenorganisation als Teil des Zertifizierungsprozesses;

    3) klarzustellen, dass jede Art von wirtschaftlicher Beziehung zwischen der Zertifizierungsstelle und der juristischen Person, abhängig von bestimmten Merkamlen, die Unparteilichkeit der Zertifizierungstätigkeiten beeinträchtigen kann;

    4) in Abschnitt 9 alle in Abschnitt 4.1.2 (insbesondere Nummern 2 und 7) des Anhangs aufgeführten Punkte aufzunehmen;

    5) in die Zertifizierungsvereinbarung Vorschriften zu Gültigkeit, Erneuerung und Widerruf sowie Vorschriften über angemessene Zeitabstände für die Neubeurteilung oder Prüfung aufzunehmen;

    6) in Abschnitt 14(2) die im Anhang angegebene Verpflichtung zu ergänzen, dass Zertifikate, Siegel und Prüfzeichen nur unter Einhaltung der Artikel 42 und 43 und der Leitlinien zur Akkreditierung und Zertifizierung verwendet werden dürfen.

46. In Bezug auf „Anforderungen an Ressourcen“ empfiehlt der Ausschuss der AT-AB,

1) die Verpflichtungen aus Abschnitt 6.1 Nummern 2 und 3 des Anhangs aufzunehmen;

2) den Wortlaut im Hinblick auf die Ausbildungsanforderungen an Personal mit technischer Fachkunde an den Anhang anzupassen und dabei das spezifische Bildungssystem und die im nationalen Recht verankerten Anforderungen zu berücksichtigen.

47. In Bezug auf „Anforderungen an Prozesse“ empfiehlt der Ausschuss der AT-AB,

1) die fehlenden Punkte aus Abschnitt 7.4 des Anhangs aufzunehmen, insbesondere die Verpflichtung der Zertifizierungsstelle, in ihrem Zertifizierungsmechanismus detailliert darzulegen, wie die in Abschnitt 7.4.6 der ISO/IEC 17065:2012 geforderten Informationen den Antragsteller über Nichtkonformitäten aus einem Zertifizierungsverfahren unterrichten;

2) die Verpflichtung aufzunehmen, Verfahren für die Erteilung, die regelmäßige Überprüfung und den Widerruf der jeweiligen Zertifizierungen gemäß Artikel 43 Absatz 2 und Artikel 43 Absatz 3 (Abschnitt 7.5 des Anhangs) vorzusehen;

3) die ersten beiden Punkte des Abschnitts 7.7 des Anhangs in die Verordnung aufzunehmen;

4) in Abschnitt 15(1) darzulegen, dass die Informationen zu zertifizierten Produkten, Prozessen und Dienstleistungen intern verfügbar und öffentlich zugänglich bleiben müssen;

5) die Verpflichtung aufzunehmen, dass die Zertifizierungsstelle der zuständigen Aufsichtsbehörde die Gründe für die Erteilung oder den Widerruf der beantragten Zertifizierung mitteilen muss.

48. In Bezug auf „Weitere zusätzliche Anforderungen“ empfiehlt der Ausschuss der AT-AB,

1) die fehlenden Punkte der Abschnitte 9.3.1 und 9.3.3 des Anhangs aufzunehmen.

4 SCHLUSSBEMERKUNGEN

49. Diese Stellungnahme richtet sich an die österreichische Aufsichtsbehörde und wird gemäß Artikel 64 Absatz 5 Buchstabe b DSGVO veröffentlicht.

50. Nach Artikel 64 Absätze 7 und 8 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.

51. Die AT-AB übermittelt dem Ausschuss den endgültigen Beschluss zur Aufnahme in das nach Artikel 70 Absatz 1 Buchstabe y DSGVO vorgesehene Register der Beschlüsse, die Gegenstand des Kohärenzverfahrens waren.

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

(Andrea Jelinek)

Angenommen