Stellungnahme 15/2020 zum Entwurf des Beschlusses der zuständigen Aufsichtsbehörden Deutschlands zur Genehmigung der Anforderungen an die Akkreditierung von Zertifizierungsstellen nach Artikel 43 Absatz 3 DSGVO

Angenommen am 25. Mai 2020

Angenommen

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 stellen werden. 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 er erstens gegenüber den Aufsichtsbehörden anregt, ihre Anforderungen an die Akkreditierung entsprechend der in Anhang 1 zu den EDSA-Leitlinien 4/2018 über die Akkreditierung von Zertifizierungsstellen vorgegebenen Gliederung zu formulieren, und indem 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 z. B. 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 über die Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 der Datenschutz-Grundverordnung (2016/679)“ (im Folgenden: Leitlinien) und die „Leitlinien 1/2018 über die Zertifizierung und die Festlegung der Zertifizierungskriterien gemäß 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 müssen, 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 beitragen wird.[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 deutschen Aufsichtsbehörden des Bundes und der Länder (im Folgenden: DE-AB) haben dem EDSA ihren Entwurf der Anforderungen an die Akkreditierung nach Artikel 43 Absatz 1 Buchstabe b vorgelegt. Das Dossier wurde am 13. Februar 2020 als vollständig erachtet. Die deutsche nationale Akkreditierungsstelle, die DAkkS, ist die Akkreditierungsstelle, die die Zertifizierungsstellen, welche Zertifizierung nach den Kriterien der DSGVO vornehmen, akkreditieren wird. Das bedeutet, dass die nationale Akkreditierungsstelle die Akkreditierung von Zertifizierungsstellen auf Grundlage der ISO 17065 und der von den DE-AB festgelegten zusätzlichen Anforderungen vornehmen wird, sobald Letztere – nach Stellungnahme des Ausschusses zum Entwurf der Anforderungen – von den DE-AB genehmigt wurden.

[2] Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 der Datenschutz-Grundverordnung, Punkt 39. Abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_de.pdf

2. Gemäß Artikel 10 Absatz 2 der Geschäftsordnung des Ausschusses hat der Vorsitz wegen der Komplexität der Angelegenheit beschlossen, die anfängliche Annahmefrist von acht Wochen um weitere sechs Wochen zu verlängern.

2 BEWERTUNG

2.1 Allgemeine Ausführungen des EDSA zum vorgelegten Beschlussentwurf

3. Zweck dieser Stellungnahme ist es, die Akkreditierungsanforderungen zu bewerten, die eine Aufsichtsbehörde auf Grundlage der ISO 17065 oder vollständig selbst entwickelt hat, nach denen eine nationale Akkreditierungsstelle oder eine Aufsichtsbehörde gemäß Artikel 43 Absatz 1 DSGVO für die Erteilung und Verlängerung von Zertifizierungen gemäß Artikel 42 DSGVO verantwortliche Zertifizierungsstellen akkreditieren kann. Die Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde bleiben unberührt. Im vorliegenden Fall stellt der Ausschuss fest, dass die DE-AB beschlossen haben, für die Erteilung der Akkreditierung auf eine gemeinsame Akkreditierung durch ihre nationale Akkreditierungsstelle, die DAkkS, und die zuständige Aufsichtsbehörde zurückzugreifen, wobei sie im Einklang mit den Leitlinien zusätzliche Anforderungen aufgestellt haben, die bei der Erteilung von Akkreditierungen einzuhalten sind.

4. Ziel dieser Bewertung der zusätzlichen Akkreditierungsanforderungen der DE-AB ist es, zu untersuchen, inwieweit (durch Ergänzungen oder Streichungen) von den Leitlinien, insbesondere von deren Anhang 1, abgewichen wird. Des Weiteren fokussiert sich die Stellungnahme des EDSA auf alle Aspekte, die Einfluss auf einen einheitlichen Ansatz bei der Akkreditierung von Zertifizierungsstellen haben können.

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

6. Der Ausschuss erkennt an, dass ggf. den nationalen Akkreditierungsstellen und den zuständigen Aufsichtsbehörden wegen ihres Fachwissens Spielraum für 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.

7. 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 Wortlaut des betreffenden Dokuments zu verweisen. Der Ausschuss hat daher beschlossen, ggf. auf einzelne Abschnitte der ISO-Norm zu verweisen, ohne jedoch deren Wortlaut wiederzugeben.

8. Der Ausschuss hat seine Bewertung gemäß der in Anhang 1 der Leitlinien (im Folgenden: Anhang) vorgesehenen Gliederung vorgenommen. Soweit diese Stellungnahme nicht auf einen bestimmten Abschnitt des von den DE-AB vorgelegten Entwurfs der Akkreditierungsanforderungen eingeht, ist dies so zu verstehen, dass der Ausschuss dazu nichts anzumerken hat und die DE-AB nicht um weitere Maßnahmen ersucht.

9. Auf Punkte, die außerhalb des Anwendungsbereichs von Artikel 43 Absatz 2 DSGVO liegen, z. B. von den DE-AB vorgebrachte Verweise auf nationale Rechtsvorschriften, wird in dieser Stellungnahme nicht eingegangen. Der Ausschuss stellt gleichwohl fest, dass die nationalen Rechtsvorschriften erforderlichenfalls mit der DSGVO im 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:

1) Regelung aller im Anhang zu den Leitlinien hervorgehobenen Hauptbereiche und Prüfung aller Abweichungen vom Anhang;

2) Unabhängigkeit der Zertifizierungsstelle;

3) Interessenkonflikte der Zertifizierungsstelle;

4) Fachwissen der Zertifizierungsstelle;

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

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

7) transparente Bearbeitung von Beschwerden über Verletzungen der Zertifizierung.

10. Unter Berücksichtigung, dass:

a. in Artikel 43 Absatz 2 DSGVO Akkreditierungsanforderungen aufgeführt 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 abzufassen 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 Billigung 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 über die Akkreditierung von Zertifizierungsstellen Vorschläge für von Datenschutzaufsichtsbehörden aufzustellende Anforderungen an die Akkreditierung von Zertifizierungsstellen durch die nationale Akkreditierungsstelle enthält;

gelangt der Ausschuss zu folgender Stellungnahme:

2.2.1 PRÄFIX

11. Der Ausschuss räumt ein, dass Kooperationsbedingungen, die das Verhältnis einer nationalen Akkreditierungsstelle zu ihrer Datenschutzaufsichtsbehörde regeln, nicht *per se* eine Anforderung an die Akkreditierung von Zertifizierungsstellen darstellen. Im Interesse der Vollständigkeit und Transparenz ist der Ausschuss jedoch der Ansicht, dass solche Kooperationsbedingungen, falls vorhanden, in einer Form zu veröffentlichen sind, die die Aufsichtsbehörde für angemessen hält.

2.2.2 BEGRIFFSBESTIMMUNGEN

12. Der Ausschuss stellt fest, dass in Kapitel 3 („Begriffsbestimmungen“) des Entwurfs der Akkreditierungsanforderungen der DE-AB festgelegt ist, welche Arten von Zertifizierungsprogrammen zulässig sind, wobei bestimmt wird, dass sie die Anforderungen der DIN EN ISO/IEC 17065 erfüllen müssen. In dieser Hinsicht ist darauf hinzuweisen, dass in den Abschnitten 5.1 und 5.2 der EDSA-Leitlinien bereits ausführlich dargelegt ist, was nach der DSGVO zertifiziert werden kann. Daher erkennt der Ausschuss an, dass die DE-AB nicht beabsichtigen, die in den Leitlinien enthaltenen Vorgaben einzuschränken, und dass die Aussagen in Kapitel 3 des Entwurfs der Akkreditierungsanforderungen der DE-AB im Zusammenhang mit diesen Akkreditierungsanforderungen als anwendbar anzusehen sind.

2.2.3 ALLGEMEINE ANMERKUNGEN

13. Der Ausschuss stellt fest, dass im Abschnitt „Allgemeine Anmerkungen“ des Entwurfs der Akkreditierungsanforderungen der DE-AB von „Genehmigung“ der Zertifizierungskriterien durch den EDSA „gemäß Artikel 63, Artikel 64 Absatz 1 Buchstabe c DSGVO“ die Rede ist. Der Ausschuss stellt fest, dass die DSGVO dem EDSA nicht die Befugnis einräumt, Zertifizierungskriterien zu „genehmigen“. Gemäß den oben genannten Artikeln kann der EDSA jedoch Zertifizierungskriterien billigen. Daher empfiehlt der Ausschuss den DE-AB, den Verweis auf die „Genehmigung durch den EDSA“ zu streichen, um den Entwurf mit dem Wortlaut der DSGVO in Einklang zu bringen.

2.2.4 ALLGEMEINE ANFORDERUNGEN AN DIE AKKREDITIERUNG (Kapitel 4 des Entwurfs der Akkreditierungsanforderungen)

14. In Bezug auf die Anforderung der rechtlichen Verantwortung (Abschnitt 4.1 des Entwurfs der Akkreditierungsanforderungen der DE-AB) stellt der Ausschuss fest, dass die DE-AB im Begleitdokument erklären, dass davon ausgegangen werde, dass die Zertifizierungsstelle über die neuesten Verfahren verfüge, und dass es daher nicht notwendig sei, in dieser Hinsicht weitere Anforderungen hinzuzufügen. Der Ausschuss ist jedoch der Auffassung, dass eine bloße Erwartung die Zertifizierungsstellen nicht verpflichtet, über solche Verfahren zu verfügen. Wie in Abschnitt 4.1.1 des Anhangs der Leitlinien festgelegt, müssen Zertifizierungsstellen über die neuesten Verfahren verfügen und 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 persönlichen Daten der Kundenorganisation als Teil des Zertifizierungsprozesses. Daher empfiehlt der Ausschuss den DE-AB, den Entwurf der Anforderungen zu ändern, um ihn mit den Leitlinien in Einklang zu bringen.

15. In Bezug auf Unterabschnitt 4.1.2.2 des Entwurfs der Akkreditierungsanforderungen der DE-AB („Zertifizierungsvereinbarung“) stellt der Ausschuss fest, dass der von den DE-AB vorgelegte Entwurf der Akkreditierungsanforderungen nicht die Verpflichtung enthält, vollständige Transparenz des Zertifizierungsprozesses gegenüber der zuständigen Aufsichtsbehörde zu gewährleisten, einschließlich der vertraulichen Vertragsangelegenheiten. Zudem findet die Verpflichtung des Antragstellers, der Zertifizierungsstelle Zugang zu seinen Datenverarbeitungstätigkeiten zu gewähren, keine Erwähnung. Daher empfiehlt der Ausschuss den DE-AB, die oben genannten Verpflichtungen in ihren Entwurf aufzunehmen.

16. Der Ausschuss stellt fest, dass eine ausdrückliche Bezugnahme auf die Aufgaben und Befugnisse der zuständigen AB (Abschnitt 4.1.2 Nummer 3 des Anhangs) nicht in Unterabschnitt 4.1.2.2 des Entwurfs der Akkreditierungsanforderungen der DE-AB enthalten ist. Der Ausschuss ist der Auffassung, dass dieser Verweis in den Entwurf der Anforderungen aufgenommen werden sollte, und empfiehlt daher den DE-AB, den Entwurf entsprechend zu ändern.

17. Ferner enthält der Entwurf der Anforderungen der DE-AB im Hinblick auf die Zertifizierungsvereinbarung keine Verpflichtung, die es der Zertifizierungsstelle erlaubt, sämtliche Informationen offenzulegen, die gemäß Artikel 42 Absatz 8 und Artikel 43 Absatz 5 DSGVO zur Erteilung der Zertifizierung erforderlich sind (Abschnitt 4.1.2 Nummer 7 des Anhangs). Zwar ist diese Verpflichtung im Abschnitt zum Verfahrensmanagement des von den DE-AB vorgelegten Entwurfs der Akkreditierungsanforderungen enthalten, jedoch sollte sie nach Auffassung des Ausschusses Teil der Zertifizierungsvereinbarung sein, um ihre Verbindlichkeit zu stärken. Daher empfiehlt der Ausschuss den DE-AB, die oben genannte Verpflichtung als Teil der Zertifizierungsvereinbarung aufzunehmen.

18. Gemäß dem Anhang ist der Antragsteller verpflichtet, 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 Entwurf der Akkreditierungsanforderungen der DE-AB enthält Unterabsatz 4.1.2.2, Nummer sechs jedoch lediglich die Verpflichtung, die Zertifizierungsstelle im Falle einer maßgeblichen Änderung der tatsächlichen oder rechtlichen Situation zu informieren, jedoch werden Produkte, Verfahren und Dienstleistungen nicht ausdrücklich erwähnt. Der Ausschuss empfiehlt den DE-AB, einen solchen Verweis im Einklang mit dem Anhang aufzunehmen.

19. In Bezug auf Unterabschnitt 4.2.7 des Entwurfs der Akkreditierungsanforderungen der DE-AB („Handhabung von Unparteilichkeit“) empfiehlt der Ausschuss, die Kriterien für Zertifizierungsstellen, die einer separaten Rechtsperson angehören oder von dieser kontrolliert werden, strenger zu gestalten, um zu berücksichtigen, dass jede Art wirtschaftlicher Beziehung zwischen der Zertifizierungsstelle und der Rechtsperson je nach den Merkmalen der Beziehung die Unparteilichkeit ihrer Zertifizierungstätigkeiten beeinträchtigen kann.

20. In Bezug auf Abschnitt 4.6 des Entwurfs der Akkreditierungsanforderungen der DE-AB („öffentlich zugängliche Informationen“) stellt der Ausschuss fest, dass kein Verweis auf die Veröffentlichung aller Fassungen der genehmigten Kriterien und der Zertifizierungsprozesse enthalten ist. Daher regt der Ausschuss an, den Entwurf der Akkreditierungsanforderungen zu ändern, um ausdrücklich hervorzuheben, dass die Veröffentlichung alle Fassungen der genehmigten Kriterien und der Zertifizierungsverfahren umfasst. Darüber hinaus stellt der Ausschuss fest, dass in Abschnitt 4.6 Absatz 2 festgelegt ist, dass „die von der Zertifizierungsstelle verwendeten Zertifizierungssysteme die gemäß Artikel 42 Absatz 5 DSGVO genehmigten Kriterien die Angabe der genehmigten Gültigkeitsdauer … *allgemein zu veröffentlichen [sind]*.“ Um Unklarheiten zu vermeiden, regt der

Ausschuss an, das Wort „allgemein“ zu streichen und das Wort „und“ zwischen „Zertifizierungssysteme“ und „die gemäß Artikel 42 Absatz 5 DSGVO genehmigten Kriterien“ einzufügen.

2.2.5 ANFORDERUNGEN AN RESSOURCEN (Kapitel 6 des Entwurfs der Akkreditierungsanforderungen)

21. Bezüglich der Anforderungen an Fachwissen und insbesondere Unterabschnitt 6.1.2.1 des Entwurfs der Akkreditierungsanforderungen der DE-AB („Personalkompetenz“), stellt der Ausschuss fest, dass das für die aufgeführten Bereiche geforderte Wissen nicht voraussetzt, dass dieses Wissen relevant und angemessen sein muss. Um zu gewährleisten, dass das im Anhang geforderte Niveau an Fachwissen vorhanden ist, empfiehlt der Ausschuss den DE-AB, den Wortlaut an die Leitlinien anzupassen, indem verlangt wird, dass das Wissen relevant und angemessen sein muss.

22. Ferner stellt der Ausschuss fest, dass bei Personal mit technischem Fachwissen, das für Entscheidungen zuständig ist, je nach Bildungsniveau mindestens sieben Jahre Berufserfahrung oder fünf Jahre Berufserfahrung im technischen Datenschutz verlangt wird, während das für die Bewertungen zuständige Personal je nach Bildungsniveau vier Jahre Berufserfahrung oder zwei Jahre Berufserfahrung im technischen Datenschutz und Erfahrung im Prüfverfahren haben sollte. In ähnlicher Weise müssen Mitarbeiter mit juristischen Fachkenntnissen, die Entscheidungen treffen, über mindestens fünf Jahre Berufserfahrung im Datenschutzrecht verfügen, während die mit der Bewertung betrauten Personen mindestens zwei Jahre Berufserfahrung im Datenschutzrecht und in Auditverfahren haben müssen. Der Ausschuss stellt fest, dass zwischen der verlangten Mindestdauer an Berufserfahrung von mit Entscheidungen betrautem Personal und von mit der Bewertung betrautem Personal ein erheblicher Unterschied besteht. In diesem Zusammenhang ist der Ausschuss der Auffassung, dass sich die Anforderungen an die Kompetenz der Gutachter und Entscheider nach den verschiedenen von ihnen wahrgenommenen Aufgaben richten sollte und nicht nach der Anzahl der Jahre an Berufserfahrung. Nach Auffassung des Ausschusses sollten die Gutachter über mehr Fachwissen und Berufserfahrung im Bereich der technischen Verfahren (z. B. Audits und Zertifizierungen) verfügen, während die Entscheider über ein allgemeineres und umfassenderes Fachwissen und Berufserfahrung im Bereich des Datenschutzes verfügen sollten. Vor diesem Hintergrund regt der Ausschuss an, den Schwerpunkt stärker auf die unterschiedlichen inhaltlichen Kenntnisse und/oder Erfahrung von Gutachtern und Entscheidern zu legen und die Unterschiede bei den für sie erforderlichen Jahren an Berufserfahrung zu verringern.

23. Zudem ist der Ausschuss der Auffassung, dass die Kenntnisse der für den Zertifizierungsbereich relevanten Managementsysteme auf die ISO/IEC 27701:2019 – Sicherheitstechniken – Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz – Anforderungen und Leitfaden – ausgeweitet werden sollten, und regt an, einen diesbezüglichen Verweis aufzunehmen.

24. Was schließlich die Ausbildungsanforderungen an das technische Personal angeht, so 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 Hochschulausbildung des technischen Personals den Verweis auf „Naturwissenschaften“ aus der Liste der Fachgebiete zu streichen.

2.2.6 ANFORDERUNGEN AN PROZESSE (Kapitel 7 des Entwurfs der Akkreditierungsanforderungen)

25. Der Ausschuss stellt fest, dass in Kapitel 7 des Entwurfs der Akkreditierungsanforderungen der DE-AB mehrfach auf den Begriff „ihre Kriterien“ Bezug genommen wird (z. B. in den Abschnitten 7.4, 7.6, 7.11 und 7.13). Um Unklarheiten zu vermeiden, regt der Ausschuss an, die Bedeutung dieses Begriffs klarzustellen, indem beispielsweise in Anhang 1 (Glossar) eine Erläuterung eingefügt wird.

26. In Bezug auf Abschnitt 7.1 des Entwurfs der Akkreditierungsanforderungen der DE-AB („Allgemeine Informationen“) stellt der Ausschuss fest, dass kein ausdrücklicher Verweis auf die Verpflichtung der Zertifizierungsstelle vorhanden ist, die zusätzlichen Anforderungen zu erfüllen. Zwar könnte eine solche Verpflichtung aus dem Wortlaut des Entwurfs der Anforderungen abgeleitet werden, jedoch ist der Ausschuss der Auffassung, dass ein ausdrücklicher Verweis auf diese Verpflichtung aufgenommen werden sollte. Daher empfiehlt der Ausschuss den DE-AB, den Entwurf entsprechend zu ändern.

27. Der Ausschuss stellt fest, dass der Entwurf der zusätzlichen Anforderungen der DE-AB keinen Verweis auf den Betrieb eines genehmigten Europäischen Datenschutzsiegels gemäß Abschnitt 7.1.2 des Anhangs enthält. Der Ausschuss ist der Auffassung, dass dieser Verweis aufgenommen werden sollte, insbesondere angesichts der Tatsache, dass die Akkreditierung einer Zertifizierungsstelle, die Europäische Datenschutzsiegel erteilt, möglicherweise in jedem Mitgliedstaat, in dem die Zertifizierungsstelle niedergelassen ist, durchgeführt werden muss.[3] Daher empfiehlt der Ausschuss den DE-AB, diesen Verweis aufzunehmen. So könnte beispielsweise in dem Entwurf der Anforderungen Folgendes festgelegt werden: *„Die zuständige Aufsichtsbehörde wird benachrichtigt, wenn eine Zertifizierungsstelle ein genehmigtes Europäisches Datenschutzsiegel in einem neuen Mitgliedstaat von einer Niederlassung aus in Betrieb nimmt.“*

28. Der Ausschuss stellt fest, dass der Entwurf der Akkreditierungsanforderungen der DE-AB in Abschnitt 7.2 („Antrag“) die Situation regelt, in der zur Durchführung von Datenverarbeitungsvorgängen im Einklang mit dem Anhang der Leitlinien Auftragsverarbeiter eingesetzt werden. Der Ausschuss stellt jedoch fest, dass der Antrag – wenn Auftragsverarbeiter eingesetzt werden – den/die relevanten Vertrag/Verträge (Verantwortlicher/Auftragsverarbeiter) enthalten muss, wie im Anhang ausgeführt. Daher empfiehlt der Ausschuss den DE-AB, den Wortlaut den Leitlinien anzupassen und den Verweis auf den/die Vertrag/Verträge (Verantwortlicher/Auftragsverarbeiter) aufzunehmen. Darüber hinaus regt der Ausschuss an, zu prüfen, ob in diesem Fall auch auf gemeinsam Verantwortliche und deren spezifische Regelungen Bezug genommen werden sollte.

29. Der Ausschuss stellt fest, dass in Abschnitt 7.2 des Entwurfs der von den DE-AB vorgelegten Akkreditierungsanforderungen festgelegt ist, dass „der Verantwortliche und der Auftragsverarbeiter … berechtigt [sind], eine Zertifizierung zu beantragen“. Die Möglichkeit für Auftragsverarbeiter, eine Zertifizierung zu beantragen, wird von dem spezifischen Zertifizierungssystem abhängen. Um Verwirrung zu vermeiden, regt der Ausschuss daher an, den oben genannten Verweis zu streichen oder klarzustellen, dass die Möglichkeit, dass Auftragsverarbeiter zertifiziert werden, vom Geltungsbereich des Zertifizierungssystems abhängt.

[3] Siehe hierzu die Leitlinien 1/2018, Rn. 44.

30. In Bezug auf Abschnitt 7.3 des Entwurfs der Akkreditierungsanforderungen der DE-AB („Bewertungsanträge“) stellt der Ausschuss fest, dass der Entwurf der Akkreditierungsanforderungen der DE-AB besagt, dass „die geplanten Bewertungsmethoden … vertraglich festgelegt [werden] …“. Um klarzustellen, dass es sich hierbei um eine Anforderung handelt, regt der Ausschuss an, den ersten Absatz neu zu formulieren, um klarzustellen, dass die Bewertungsmethoden in die Zertifizierungsvereinbarung aufzunehmen sind, d. h. die Anforderung dahingehend zu formulieren, dass „die geplanten Bewertungsmethoden … vertraglich [festzulegen sind]“. Darüber hinaus regt der Ausschuss an, den Verweis auf Abschnitt 7.3.1.b der ISO-Norm 17065 durch Abschnitt 7.3 der ISO-Norm 17065 zu ersetzen, um den Wortlaut mit dem Anhang in Einklang zu bringen. Ferner stellt der Ausschuss fest, dass im vierten Absatz auf angemessene technische und rechtliche Kompetenzen Bezug genommen wird. Um der Klarheit willen regt der Ausschuss an, „auf dem Gebiet des Datenschutzes“ hinzuzufügen.

31. Der Ausschuss stellt fest, dass in Abschnitt 7.4 des Entwurfs der Akkreditierungsanforderungen der DE-AB („Bewertungsmethoden“) keine Verpflichtung der Zertifizierungsstelle vorgesehen ist, angemessene Bewertungsmethoden zu beschreiben, mit denen beurteilt wird, ob die Verarbeitungsvorgänge mit den Zertifizierungskriterien übereinstimmen. Der Ausschuss empfiehlt den DE-AB, den Entwurf der Anforderungen dahingehend zu ändern, dass eine solche Verpflichtung aufgenommen wird. Es könnte beispielsweise Folgendes hinzugefügt werden: „*Die Zertifizierungsstelle stellt sicher, dass die für die Erteilung der Zertifizierung verwendeten Verfahren angemessene Evaluierungsverfahren beschreiben, mit denen bewertet wird, ob die Verarbeitungsvorgänge mit den Zertifizierungskriterien übereinstimmen*.“ Darüber hinaus ist der Ausschuss im Hinblick auf den ersten Bereich, der Gegenstand der Bewertungsmethoden sein soll, der Auffassung, dass die Notwendigkeit und Verhältnismäßigkeit ggf. auch in Bezug auf die betroffenen Personen zu bewerten ist. Schließlich stellt der Ausschuss fest, dass kein Verweis auf die Dokumentation über Methoden und Ergebnisse vorhanden ist. Daher regt der Ausschuss an, den Entwurf zu ändern und solche Verweise ausdrücklich aufzunehmen.

32. Im Hinblick auf bestehende Zertifizierungen (Abschnitt 7.4 des Entwurfs der Akkreditierungsanforderungen der DE-AB) ist der Ausschuss der Auffassung, dass Nummer vier auf Seite 13 zu Verwirrung führt, da unklar ist, wie die Gültigkeitsdauer der derzeitigen Zertifizierung mit jener der vorherigen Zertifizierung zusammenhängt und wie sie miteinander vereinbar wären. Darüber hinaus scheint es nicht möglich zu sein, die Gültigkeit einer zuvor von einer anderen akkreditierten Zertifizierungsstelle erteilten Zertifizierung in Frage zu stellen. Zusammenfassend lässt sich sagen, dass dem Absatz mehr Klarheit in Bezug auf das Verhältnis zwischen den verschiedenen genannten Elementen zugutekäme. Der Ausschuss empfiehlt den DE-AB, den Entwurf zu ändern, indem insbesondere klargestellt wird, dass die Gültigkeitsdauer der DSGVO-Zertifizierung nicht von der Gültigkeit anderer Arten von Zertifizierungen abhängig sein darf.

33. Betreffend Abschnitt 7.5 („Beurteilung“) des Entwurfs der Akkreditierungsanforderungen der DE-AB regt der Ausschuss an, die Überschrift des Abschnitts in „Überprüfung“ umzuändern.

34. In Bezug auf die Änderungen, die sich auf die Zertifizierung auswirken (Abschnitt 7.10 des Entwurfs der Akkreditierungsanforderungen der DE-AB) stellt der Ausschuss fest, dass im Entwurf der Akkreditierungsanforderungen der DE-AB festgelegt ist, dass „der Kunde … rechtzeitig über Änderungen des Rechtsrahmens, die Auswirkungen auf ihn haben, unterrichtet [wird]“. Angesichts der Notwendigkeit, die Unparteilichkeit der Zertifizierungsstelle zu wahren, regt der Ausschuss an, den Satz umzuformulieren, um deutlich zu machen, dass der Kunde rechtzeitig allgemeine Informationen über Änderungen erhält, die Auswirkungen auf ihn haben könnten. Damit klar wird,

was unter „Beschlüsse des Europäischen Datenschutzausschusses“ zu verstehen ist, regt der Ausschuss außerdem an, dass die DE-AB diesen Verweis näher erläutern. Man könnte beispielsweise die Formulierung „vom Europäischen Datenschutzausschuss angenommene Dokumente“ verwenden.

35. Der Ausschuss stellt fest, dass Abschnitt 7.11 des Entwurfs der Akkreditierungsanforderungen der DE-AB („Beendigung, Beschränkung, Aussetzung oder Widerruf der Zertifizierung“) nicht die Verpflichtung der Zertifizierungsstelle enthält, Entscheidungen der DE-AB zu akzeptieren, eine Zertifizierung zu widerrufen oder einem Antragsteller keine Zertifizierung zu erteilen, falls die Anforderungen für eine Zertifizierung nicht bzw. nicht mehr erfüllt werden. Der Ausschuss empfiehlt den DE-AB daher, eine solche Verpflichtung in den Entwurf aufzunehmen. Darüber hinaus regt der Ausschuss an, in der Überschrift des Abschnitts im Einklang mit dem Anhang der Leitlinien das Wort „Beschränkung“ durch das Wort „Einschränkung“ zu ersetzen.

2.2.7 WEITERE ZUSÄTZLICHE ANFORDERUNGEN

36. In Bezug auf Unterabschnitt 8.11.3 der Akkreditierungsanforderungen der DE-AB („Beschwerdeabwicklung“) regt der Ausschuss an, den Verweis auf „gerechtfertigte Beschwerden“ durch „begründete Beschwerden“ zu ersetzen, um mehr Klarheit zu schaffen.

3 SCHLUSSFOLGERUNGEN / EMPFEHLUNGEN

37. Da der Entwurf der Akkreditierungsanforderungen der deutschen Aufsichtsbehörden des Bundes und der Länder zu einer inkohärenten Praxis der Akkreditierung von Zertifizierungsstellen führen könnte, sind folgende Änderungen vorzunehmen:

38. In Bezug auf „Allgemeine Anmerkungen“ empfiehlt der Ausschuss, dass die DE-AB:

    1) die Bezugnahme auf „Genehmigung durch den EDSA“ streicht, um den Entwurf mit dem Wortlaut der DSGVO in Einklang zu bringen.

39. In Bezug auf „Allgemeine Anforderungen an die Akkreditierung“ empfiehlt der Ausschuss, dass die DE-AB:

    1) die Anforderungen in Bezug auf die rechtliche Verantwortung (Unterabschnitt 4.1) ändern, um sie an die Leitlinien anzupassen;

    2) Unterabschnitt 4.1.2.2 dahin gehend ändern, dass in die Zertifizierungsvereinbarung die Verpflichtung aufgenommen wird, vollständige Transparenz des Zertifizierungsprozesses gegenüber den DE-AB zu gewährleisten und der Zertifizierungsstelle Zugang zu den Datenverarbeitungstätigkeiten des Antragstellers zu gewähren;

    3) in Unterabschnitt 4.1.2.2 ausdrücklich auf die Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde gemäß dem Anhang Bezug nehmen;

    4) in die Bestandteile der Zertifizierungsvereinbarung die Verpflichtung aufnehmen, die es der Zertifizierungsstelle erlaubt, sämtliche Informationen offenzulegen, die gemäß Artikel 42 Absatz 8 und Artikel 43 Absatz 5 DSGVO zur Erteilung der Zertifizierung erforderlich sind;

5) in Unterabschnitt 4.1.2.2, Nummer sechs, ausdrücklich auf „von der Zertifizierung betroffene Produkte, Verfahren und Dienstleistungen“ Bezug nehmen;

6) in Unterabschnitt 4.2.7 die Kriterien strenger gestalten, die für Zertifizierungsstellen gelten, die einer separaten Rechtsperson angehören oder von dieser kontrolliert werden, und zu berücksichtigen, dass jede Art wirtschaftlicher Beziehung zwischen der Zertifizierungsstelle und der Rechtsperson je nach ihren Merkmalen die Unparteilichkeit ihrer Zertifizierungstätigkeiten beeinträchtigen kann.

40. In Bezug auf „Anforderungen an Ressourcen“ empfiehlt der Ausschuss, dass die DE-AB:

1) den Wortlaut von Unterabschnitt 6.1.2.1 an die Leitlinien anpassen, indem verlangt wird, dass das Wissen relevant und angemessen sein muss.

41. In Bezug auf „Anforderungen an Prozesse“ empfiehlt der Ausschuss, dass die DE-AB:

1) Abschnitt 7.1 dahin ändern, dass ein ausdrücklicher Verweis auf die Verpflichtung der Zertifizierungsstelle vorhanden ist, die zusätzlichen Anforderungen zu erfüllen;

2) einen Verweis auf den Betrieb eines genehmigten Europäischen Datenschutzsiegels aufnehmen;

3) den Wortlaut in Abschnitt 7.2 durch Aufnahme eines Verweises auf den/die Vertrag/Verträge (Verantwortlicher/Auftragsverarbeiter) an die Leitlinien anpassen;

4) in Abschnitt 7.4 die Verpflichtung der Zertifizierungsstelle aufnehmen, angemessene Bewertungsmethoden zu beschreiben, mit denen bewertet wird, ob die Verarbeitungsvorgänge mit den Zertifizierungskriterien übereinstimmen;

5) in Abschnitt 7.4 klarstellen, dass die Gültigkeitsdauer der DSGVO-Zertifizierung nicht von der Gültigkeit anderer Arten von Zertifizierungen abhängig sein darf;

6) in Abschnitt 7.11 die Verpflichtung der Zertifizierungsstelle aufnehmen, Entscheidungen und Anordnungen der DE-AB zu akzeptieren, einem Antragsteller die Zertifizierung zu entziehen oder nicht auszustellen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt sind.

4 ABSCHLIESSENDE BEMERKUNGEN

42. Diese Stellungnahme richtet sich an die deutschen Aufsichtsbehörden des Bundes und der Länder und wird gemäß Artikel 64 Absatz 5 Buchstabe b DSGVO veröffentlicht.

43. Nach Artikel 64 Absätze 7 und 8 DSGVO teilen die DE-AB dem Vorsitz binnen zwei Wochen nach Eingang der Stellungnahme auf elektronischem Wege mit, ob sie ihren Beschlussentwurf ändern oder beibehalten werden. Innerhalb derselben Frist übermitteln sie den geänderten Beschlussentwurf oder geben, wenn sie beabsichtigen, der Stellungnahme des Ausschusses nicht zu folgen, die maßgeblichen Gründe an, weshalb sie beabsichtigen, dieser Stellungnahme insgesamt oder teilweise nicht zu folgen.

44. Die DE-AB übermitteln dem Ausschuss den endgültigen Beschluss für die Aufnahme in das Register der Beschlüsse, die Gegenstand des Kohärenzverfahrens waren, nach Artikel 70 Absatz 1 Buchstabe y DSGVO.

Für den Europäischen Datenschutzausschuss

Vorsitz

(Andrea Jelinek)

Angenommen