Stellungnahme 4/2020 zum Entwurf des Beschlusses der zuständigen Aufsichtsbehörde des Vereinigten Königreichs zur Genehmigung der Anforderungen an die Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 Absatz 3 DSGVO

Angenommen am 29. Januar 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 Artikel 51 Absatz 1 Buchstabe b der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (im Folgenden „Durchsetzungsrichtlinie“),

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 genehmigen. 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 wird. 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

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

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.

(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, 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“) weist darauf hin, 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 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 britische Aufsichtsbehörde hat dem EDSA ihren Entwurf für die Anforderungen an die Akkreditierung nach Artikel 43 Absatz 1 Buchstabe b vorgelegt. Nach Feststellung der Vollständigkeit des Dossiers wurde dieses am 25. Oktober 2019 verteilt. Die UKAS ist die britische nationale Akkreditierungsstelle (NAS), die die Zertifizierungsstellen, die die Zertifizierung nach den Kriterien der DSGVO vornehmen, akkreditieren wird. Das bedeutet, dass die NAS die Akkreditierung von Zertifizierungsstellen auf Grundlage der ISO 17065 und der von der Aufsichtsbehörde festgelegten zusätzlichen Anforderungen vornehmen wird, sobald letztere – nach Stellungnahme des Ausschusses zum Entwurf der Anforderungen – von der Aufsichtsbehörde genehmigt wurden.

[2] Nr. 39 der Leitlinien: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.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, und 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 britische Aufsichtsbehörde beschlossen hat, für die Erteilung der Akkreditierung auf ihre nationale Akkreditierungsstelle (NAS) zurückzugreifen, wobei sie im Einklang mit den Leitlinien zusätzliche Anforderungen aufgestellt hat, die von ihrer NAS bei der Erteilung von Akkreditierungen einzuhalten sind.

4. Ziel dieser Bewertung der zusätzlichen Akkreditierungsanforderungen der britischen Aufsichtsbehörde ist es, zu untersuchen, inwieweit (durch Ergänzungen oder Streichungen) von den Leitlinien, insbesondere von deren Anhang, abgewichen wird. Des Weiteren fokussiert die Stellungnahme des EDSA auf alle Aspekte, die einem einheitlichen Ansatz bezüglich der Akkreditierung von Zertifizierungsstellen zuwiderlaufen könnten.

5. Dabei ist zu beachten, dass die Leitlinien über die Akkreditierung von Zertifizierungsstellen darauf abzielen, die Aufsichtsbehörden bei der Festlegung ihrer Akkreditierungsanforderungen zu unterstützen. Der Anhang zu den Leitlinien selbst stellt allerdings keine Akkreditierungsanforderungen dar. Die Anforderungen an die Akkreditierung von Zertifizierungsstellen müssen von der Aufsichtsbehörde auf solche Weise festgelegt werden, dass ihre praktische und einheitliche Anwendung in dem von der Aufsichtsbehörde vorgesehenen Zusammenhang möglich ist.

6. Der Ausschuss erkennt an, dass den nationalen Akkreditierungsstellen 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 vielmehr beschlossen, ggf. auf einzelne Abschnitte der ISO-Norm zu verweisen, ohne jedoch den Wortlaut wiederzugeben.

8. Der Ausschuss hat seine Bewertung gemäß der in Anhang 1 der Leitlinien vorgesehenen Gliederung vorgenommen. Soweit diese Stellungnahme nicht auf einen bestimmten Abschnitt des von der britischen Aufsichtsbehörde vorgelegten Entwurfs der Akkreditierungsanforderungen eingeht, ist dies so zu verstehen, dass der Ausschuss dazu nichts anzumerken hat und die britische Aufsichtsbehörde nicht um weitere Maßnahmen ersucht.

9. Auf Punkte, die außerhalb des Anwendungsbereichs von Artikel 43 Absatz 2 DSGVO liegen, zum Beispiel auf von der britischen Aufsichtsbehörde vorgebrachte Verweise auf nationale Rechtsvorschriften, wird in dieser Stellungnahme nicht eingegangen. Der Ausschuss stellt gleichwohl fest, dass die nationalen Rechtsvorschriften erforderlichenfalls 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. Interessenskonflikte 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.

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 bestimmt, 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 bestimmen, 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 bestimmt, 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 (Abschnitt 0 des Entwurfs der zusätzlichen Akkreditierungsanforderungen)

11. Der Ausschuss erkennt an, 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 von der Aufsichtsbehörde für angemessen gehaltener Form zu veröffentlichen sind.

12. Der Ausschuss stellt fest, dass die britische Aufsichtsbehörde solche Bedingungen für die Kooperation mit ihrer nationalen Akkreditierungsstelle aufstellt und dass die endgültige Fassung dieser Kooperationsbedingungen auf der Website der britischen Aufsichtsbehörde abrufbar sein wird.

2.2.2 ALLGEMEINE ANFORDERUNGEN AN DIE AKKREDITIERUNG (Abschnitt 4 des Entwurfs der zusätzlichen Akkreditierungsanforderungen)

13. Hinsichtlich der Anforderungen an die rechtliche Verantwortung (Unterabschnitt 4.1.1) stellt der Ausschuss fest, dass die britische Aufsichtsbehörde verlangt, dass die Zertifizierungsstelle, um deren Akkreditierung es geht, „*im Akkreditierungsverfahren in der Lage sein sollte, Nachweise für die Einhaltung der Vorschriften*“ der DSGVO und des britischen Datenschutzgesetzes von 2018 zu erbringen. Zur Gewährleistung einer angemessenen Prüfung und Durchführung dieser Anforderung regt der Ausschuss an, dass die britische Aufsichtsbehörde die Formulierung „*in der Lage sein sollte, Nachweise … zu erbringen*“ durch „*Nachweise … erbringt*“ ersetzt. Der Ausschuss empfiehlt der britischen Aufsichtsbehörde daher, den Entwurf entsprechend abzuändern.

14. Hinsichtlich der Zertifizierungsvereinbarung (Unterabschnitt 4.1.2) und insbesondere der Anforderung Nummer 8 (Nummer 9 im Anhang) stellt der Ausschuss fest, dass die britische Aufsichtsbehörde einen Teil der in Anhang 1 der Leitlinien vorgesehenen Anforderung neu formuliert hat. Die britische Aufsichtsbehörde hat jedoch einen Hinweis ausgelassen, nämlich dass (gegebenenfalls) „auch alle Folgen für den Kunden zu berücksichtigen sind“. Der Ausschuss empfiehlt der britischen Aufsichtsbehörde daher, den fehlenden Teil der vorgenannten Anforderung hinzuzufügen.

15. Bezüglich der Verwendung von Datenschutzsiegeln und -prüfzeichen (Unterabschnitt 4.1.3), stellt der Ausschuss fest, dass die britische Aufsichtsbehörde verlangt, dass eine Kopie „*des Siegels/Prüfzeichens/Logos dem ICO für seine Akten zugeleitet werden sollte*“. Da Siegel, Prüfzeichen und Logos nicht nur von der Zertifizierungsstelle, sondern auch vom Programmeigner benutzt werden, regt der Ausschuss an, dass die britische Aufsichtsbehörde auf alle Siegel, Prüfzeichen und Logos Bezug nimmt, die in von der britischen Aufsichtsbehörde genehmigten Zertifizierungsprogrammen vorgesehen sind.

2.2.3 ANFORDERUNGEN AN DIE AUSSTATTUNG (Abschnitt 6 des Entwurfs der zusätzlichen Akkreditierungsanforderungen)

16. Hinsichtlich des Personals der Zertifizierungsstelle (Unterabschnitt 6.1), insbesondere Punkt 6, stellt der Ausschuss fest, dass die britische Aufsichtsbehörde vorgesehen hat, dass „*das für Zertifizierungsentscheidungen verantwortliche Personal über erhebliche Berufserfahrung in Bezug auf die Festlegung und Umsetzung von Datenschutzmaßnahmen verfügen muss*“. Der Ausschuss ist allerdings der Ansicht, dass Personal, das Zertifizierungsentscheidungen trifft, möglicherweise nicht selbst „*über erhebliche Berufserfahrung in Bezug auf die Festlegung und Umsetzung von Datenschutzmaßnahmen*“ verfügt, jedoch Zugang zu jemandem mit entsprechender Erfahrung haben sollte, um auf guter Informationsgrundlage zu entscheiden. Erhebliche Berufserfahrung in der Umsetzung solcher Maßnahmen dürfte in diesem Sektor, zumindest in der Anfangszeit, bislang nicht weit verbreitet sein. Der Ausschuss regt daher an, dass die britische Aufsichtsbehörde verlangt, dass die Zertifizierungsstelle die für das Zertifizierungsprogramm erforderliche Berufserfahrung definiert und erklärt.

2.2.4 ANFORDERUNGEN AN DAS VERFAHREN, ARTIKEL 43 ABSATZ 2 BUCHSTABEN C und D (Abschnitt 7 des Entwurfs der zusätzlichen Akkreditierungsanforderungen)

17. Hinsichtlich des allgemeinen Unterabschnitts zu den Verfahrensanforderungen (Unterabschnitt 7.1), insbesondere Absatz 4, stellt der Ausschuss fest, dass eine zusätzliche Anforderung vorgesehen ist, wonach die Akkreditierungsstelle sicherstellen muss, dass die Zertifizierungsstelle eine Untersuchung oder Überprüfung vornimmt, wenn die Einhaltung der Datenschutzvorschriften infrage steht. Der Ausschuss versteht dies so, dass dies die Einhaltung der Datenschutzvorschriften durch den Zertifizierungsinhaber betrifft. Dies sollte jedoch in den Anforderungen deutlicher zum Ausdruck kommen. Des Weiteren ist der Ausschuss der Ansicht, dass die britische Aufsichtsbehörde genau angeben sollte, dass eine solche Untersuchung auf den Gegenstand der Zertifizierung und das Ziel der Beurteilung abstellen sollte. Der Ausschuss empfiehlt daher, dass die britische Aufsichtsbehörde ihre Anforderung entsprechend abändert und klar angibt, dass sich die Einhaltung der Datenschutzvorschriften auf den Zertifizierungsinhaber bezieht und dass die Untersuchung auf den Gegenstand der Zertifizierung und das Ziel der Beurteilung abstellen sollte.

18. Hinsichtlich der Anwendung der Verfahrensanforderungen (Unterabschnitt 7.2) stellt der Ausschuss fest, dass Zertifizierungsstellen angeben müssen, „*ob Auftragsverarbeiter eingesetzt werden, und wenn Auftragsverarbeiter Antragsteller sind, sind deren Verantwortlichkeiten und Aufgaben anzugeben, wobei dem Antrag die relevanten Verträge zwischen dem Verantwortlichen und dem Auftragsverarbeiter beizufügen sind*“. Es wird anerkannt, dass die britische Aufsichtsbehörde den Wortlaut aus Anhang 1 verwendet hat; der Ausschuss regt jedoch an, dass die britische Aufsichtsbehörde prüft, ob in diesem Falle auch gemeinsam für die Verarbeitung Verantwortliche und deren spezifische Vereinbarungen erwähnt werden sollten.

19. Hinsichtlich der Evaluierungsmethoden (Unterabschnitt 7.4) stellt der Ausschuss fest, dass die britische Aufsichtsbehörde eine zusätzliche Anforderung vorsieht: „*Zusätzlich zu Nr. 7.4.5 der ISO 17065 ist vorzusehen, dass bestehende Zertifizierungen, die sich auf denselben Zertifizierungsgegenstand beziehen, im Rahmen einer neuen Evaluierung Berücksichtigung finden können …*“. Diesbezüglich hält es der Ausschuss für erforderlich, genauer klarzustellen, dass in Fällen, in denen bestehende Zertifizierungen im Rahmen einer neuen Evaluierung Berücksichtigung finden,

der Gegenstand der betreffenden Zertifizierung in Bezug auf die Einhaltung der relevanten Zertifizierungskriterien genau zu überprüfen ist. Der Ausschuss empfiehlt daher der britischen Aufsichtsbehörde, den Wortlaut entsprechend klarer zu formulieren.

20. Hinsichtlich des Satzes „*Der vollständige Evaluierungsbericht oder Informationen, die die Evaluierung der vorherigen Zertifizierungstätigkeit und ihrer Ergebnisse ermöglichen, können berücksichtigt werden*“, empfiehlt der Ausschuss der britischen Aufsichtsbehörde, das Wort „können [berücksichtigt werden]“ zu streichen, sodass deutlich wird, dass bestehende Zertifizierungen von der Zertifizierungsstelle zu berücksichtigen sind. Außerdem ist der Ausschuss der Meinung, dass es klarer wäre, einfach von „Zertifizierung“ statt von „Zertifizierungstätigkeit“ zu sprechen, weshalb er der britischen Aufsichtsbehörde empfiehlt, den Entwurf entsprechend zu ändern. Darüber hinaus könnte die Formulierung „vorherige Zertifizierung“ irreführend sein, da nicht klar auf die bestehende Zertifizierung, die die Zertifizierungsstelle im Rahmen ihrer eigenen Evaluierung berücksichtigen will, Bezug genommen wird. Der Ausschuss regt an, dass die britische Aufsichtsbehörde den Wortlaut ändert, um klarzustellen, dass dies eine Bezugnahme auf die bestehende Zertifizierung ist. Abschließend stellt der Ausschuss fest, dass die Zertifizierungsstelle den Evaluierungsbericht und jegliche sonstigen relevanten Informationen, die eine Evaluierung der Zertifizierungstätigkeit ermöglichen, einsehen können sollte, um ihre Entscheidung auf einer guten Informationsgrundlage treffen zu können. Der Ausschuss empfiehlt daher der britischen Aufsichtsbehörde, den Wortlaut entsprechend klarzustellen.

21. Des Weiteren ist der Ausschuss der Ansicht, dass die britische Aufsichtsbehörde, in dem Absatz, der mit „*zusätzlich zu Nr. 7.4.6 der ISO 17065“* beginnt, auf „ihren Zertifizierungsmechanismus“ Bezug nimmt, eigentlich wohl „das Zertifizierungsprogramm“ meint. Der Ausschuss empfiehlt der britischen Aufsichtsbehörde daher, den Wortlaut entsprechend zu ersetzen.

22. Hinsichtlich der die Zertifizierung betreffenden Änderungen (Unterabschnitt 7.10), insbesondere Aufzählungspunkt 4 („Beschlüsse des Europäischen Datenschutzausschusses“) nimmt der Ausschuss zur Kenntnis, dass die britische Aufsichtsbehörde den in Anhang 1 vorgesehenen Wortlaut verwendet hat. Um jedoch sicherzustellen, dass klar verstanden wird, was unter „Beschlüsse des Europäischen Datenschutzausschusses“ zu verstehen ist, regt der Ausschuss an, dass die britische Aufsichtsbehörde diese Bezugnahme verdeutlicht. Hier könnte man etwa die Formulierung „vom Europäischen Datenschutzausschuss angenommene Dokumente“ verwenden.

3 SCHLUSSFOLGERUNGEN/EMPFEHLUNGEN

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

24. In Bezug auf die „Allgemeinen Anforderungen an die Akkreditierung“ empfiehlt der Ausschuss der britischen Aufsichtsbehörde:

    1. in Unterabschnitt 4.1.1 die Formulierung „in der Lage sein sollte, Nachweise … zu erbringen“ durch „Nachweise … erbringt“ zu ersetzen;

    2. in Unterabschnitt 4.1.2 den fehlenden Teil der Anforderung einzufügen, sodass diese mit dem Text in Anhang 1 der Leitlinien in Einklang steht.

25. In Bezug auf die „Verfahrensanforderungen“ empfiehlt der Ausschuss der britischen Aufsichtsbehörde:

    1. Unterabschnitt 7.1 abzuändern, um klar anzugeben, dass sich die Einhaltung der Datenschutzvorschriften auf den Zertifizierungsinhaber bezieht und dass die Untersuchung auf den Gegenstand der Zertifizierung und das Ziel der Beurteilung abstellen sollte;

    2. Unterabschnitt 7.4 zu ändern, indem das Wort „können“ gestrichen wird, sodass es heißt, dass bestehende Zertifizierungen berücksichtigt werden, sowie „Zertifizierungstätigkeit“ durch „Zertifizierung“ zu ersetzen;

    3. das Wort „Zertifizierungsmechanismus“ durch „Zertifizierungsprogramm“ zu ersetzen.

4 ABSCHLIESSENDE BEMERKUNGEN

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

27. Nach Artikel 64 Absätze 7 und 8 DSGVO teilt die Aufsichtsbehörde dem Vorsitz binnen zwei Wochen nach Eingang der Stellungnahme auf elektronischem Wege mit, ob sie ihren Entwurf ändern oder beibehalten 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.

Für den Europäischen Datenschutzausschuss

Vorsitzende

(Andrea Jelinek)

Angenommen