Stellungnahme 5/2020 zum Entwurf des Beschlusses der zuständigen Aufsichtsbehörde Luxemburgs zur Genehmigung der Anforderungen an die Akkreditierung von Zertifizierungsstellen nach Artikel 43 Absatz 3 DSGVO

Angenommen am 29. Januar 2020

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

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.

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

(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.

(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 luxemburgische Aufsichtsbehörde (LU AB) hat dem EDSA ihren Entwurf der Anforderungen an die Akkreditierung nach Artikel 43 Absatz 1 Buchstabe a übermittelt. Nach Feststellung der Vollständigkeit des Dossiers wurde es am 25. Oktober 2019 verteilt. Die LU AB wird die Zertifizierungsstellen, die die Zertifizierungen nach den Kriterien der DSGVO vornehmen, akkreditieren.

[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 Entwurf der Anforderungen an die Akkreditierung

Zweck dieser Stellungnahme ist es, die Akkreditierungsanforderungen, die eine Aufsichtsbehörde zusätzlich zu ISO 17065 oder als vollständige Liste von Anforderungen entwickelt hat, zu bewerten, 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. In diesem konkreten Fall stellt der Ausschuss fest, dass die LU AB nach nationalem Recht mit der Akkreditierung von Zertifizierungsstellen betraut ist. Zu diesem Zweck hat die LU AB speziell für die Akkreditierung von Zertifizierungsstellen Anforderungen und dazugehörige Zertifizierungskriterien entwickelt, deren formelle Genehmigung noch aussteht.

Ziel dieser Bewertung der Akkreditierungsanforderungen 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.

Anzumerken ist, dass das Ziel der Richtlinie zur Akkreditierung von Zertifizierungsstellen darin besteht, die Aufsichtsbehörden 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 der Aufsichtsbehörde auf solche Weise festgelegt werden, dass ihre praktische und einheitliche Anwendung in dem von der Aufsichtsbehörde vorgesehenen Zusammenhang möglich ist.

Der Ausschuss hat seine Bewertung gemäß der in Anhang 1 der Leitlinien vorgesehenen Gliederung vorgenommen. Soweit diese Stellungnahme nicht auf einem bestimmten Abschnitt des von der LU AB vorgelegten Entwurfs der Akkreditierungsanforderungen eingeht, ist dies so zu verstehen, dass der Ausschuss dazu nichts anzumerken hat und die LU AB nicht um weitere Maßnahmen ersucht. Der Ausschuss stellt fest, dass die LU AB Informationen bereitgestellt hat, die der Bewertung des Entwurfs der Anforderungen an die Akkreditierung dienen sollen. Die Stellungnahme des Ausschusses befasst sich allerdings nur mit dem Entwurf der Anforderungen an die Akkreditierung.

Darüber hinaus wird in dieser Stellungnahme nicht auf Punkte eingegangen, die außerhalb des Anwendungsbereichs von Artikel 43 Absatz 2 DSGVO liegen, zum Beispiel von der LA AB vorgebrachte Verweise auf nationale Rechtsvorschriften. 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) – dass die Akkreditierungsanforderungen die einheitliche Prüfung der folgenden Punkte 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.

3. 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;

gelangt der Ausschuss zu folgender Stellungnahme:

2.2.1 ALLGEMEINE ANMERKUNGEN

4. Der Ausschuss stellt fest, dass der Entwurf der Anforderungen an die Akkreditierung der im Anhang 1 zu den Leitlinien vorgegebenen Gliederung nicht vollständig entspricht. So fehlen etwa die Abschnitte Anwendungsbereich“ und „Begriffsbestimmungen“. In diesem Zusammenhang merkt der Ausschuss an, dass einige Begriffe, wie „Kunde“ und „Antragsteller“, nicht im gesamten Dokument einheitlich verwendet werden. Um Verwirrung zu vermeiden, sollten die verwendeten Begriffe soweit möglich an die Leitlinien und die Begriffsbestimmungen im Anhang angeglichen und einheitlich verwendet werden. Um die Bewertung zu erleichtern, regt der Ausschuss daher an, dass die LU AB im Entwurf der Anforderungen an die Akkreditierung die im Anhang 1 zu den Leitlinien vorgegebene Gliederung befolgt und die fehlenden Abschnitte hinzufügt.

5. Der Ausschuss stellt fest, dass in dem Dokument mehrfach auf die Anforderungen „dieses Zertifizierungsverfahrens“ Bezug genommen wird (z. B. Anforderung 4.6.4) oder auf Zertifizierungsstellen, die „gemäß dem … Zertifizierungsverfahren“ akkreditiert sind (z. B. Anforderung 2.2.2). Die Bezugnahme auf das Zertifizierungsverfahren ist offenbar eine Frage der Formulierung. Der Ausschuss legt der LU AB daher nahe, die Bezugnahmen neu zu formulieren, um

der Tatsache Rechnung zu tragen, dass die Zertifizierungsstellen in Übereinstimmung mit den von der Aufsichtsbehörde genehmigten Anforderungen akkreditiert werden.

6. Gleichsam ist die Bezugnahme auf die „in diesem Zertifizierungsverfahren festgelegten Anforderungen“, die im gesamten Dokument verwendet wird (z. B. Anforderung 1.1.1.2), verwirrend. Eine geeignetere Formulierung könnte „die im Zertifizierungsmechanismus festgelegten Kriterien“ lauten. Daher regt der Ausschuss an, dass die LU AB die Bezugnahmen auf „den Zertifizierungsmechanismus“ im gesamten Dokument präzisiert.

7. Der Ausschuss stellt fest, dass mehrere Anforderungen (z. B. 3.2.1.1 und 4.1.2) auf die „einschlägigen internationalen Normen“, die „einschlägigen Normen“ oder die „spezifizierte Norm“ Bezug nehmen. Diese Normen werden allerdings nicht definiert und daher ist unklar, auf welche Normen hier Bezug genommen wird. Somit empfiehlt der Ausschuss der LU AB, klarzustellen, um welche Normen es sich handelt. Dies könnte beispielsweise in den Abschnitten Anwendungsbereich“ oder „Begriffsbestimmungen“ geschehen.

2.2.2 ALLGEMEINE ANFORDERUNGEN AN DIE AKKREDITIERUNG

8. Der Ausschuss stellt fest, dass die Anforderung 1.1.1.1 der LU AB auf eine weitere Norm Bezug nimmt (ISAE 3000), die der Ausschuss nicht bewertet hat. Somit empfiehlt der Ausschuss der LU AB, klarzustellen, dass die Anforderungen nicht durch externe Normen wie die ISAE 3000 außer Kraft gesetzt werden können.

9. Der Ausschuss stellt fest, dass Abschnitt 1.6 der Anforderungen keine Verpflichtung der Zertifizierungsstelle vorsieht, alle Versionen genehmigter Kriterien und alle Zertifizierungsverfahren in leicht zugänglicher Form zu veröffentlichen, so wie dies im Anhang der Leitlinien vorgesehen ist (Abschnitt 4.6). Der Ausschuss stellt fest, dass die LU AB möglicherweise Inhaberin des Zertifizierungssystems ist, ist jedoch der Auffassung, dass es hilfreich wäre, einen geeigneten Hinweis hinzuzufügen, um sicherzustellen, dass die Kriterien auf dem neuesten Stand und über die Zertifizierungsstelle selbst leicht zugänglich sind. In diesem Zusammenhang ist der Ausschuss der Auffassung, dass die LU AB, indem sie die Informationen gemäß Anforderung 1.6.1 nur auf Anfrage zur Verfügung stellt, eine strengere Anforderung festlegt als der Anhang, der vorsieht, dass die Informationen leicht öffentlich zugänglich zu machen sind. Der Ausschuss empfiehlt der LU AB daher, die Anforderung zu ändern, um die Verpflichtung der Zertifizierungsstelle aufzunehmen, alle Versionen der genehmigten Kriterien und alle Zertifizierungsverfahren im Einklang mit dem Anhang der Leitlinien in leicht zugänglicher Form zu veröffentlichen.

10. Der Ausschuss merkt an, dass die Anforderung 1.2.4 auf das „zertifizierte Verfahren“ Bezug nimmt. Der Ausschuss ist der Auffassung, dass eine präzisere Formulierung, die im Einklang mit den Leitlinien steht, verwendet werden könnte, wie etwa die Formulierung „zertifizierte Verarbeitungsvorgänge/-tätigkeiten“. Dies trägt dem weiteren Anwendungsbereich der Zertifizierung Rechnung, der in der DSGVO vorgesehen ist. Der Ausschuss empfiehlt der LU AB daher, den Entwurf der Anforderungen entsprechend zu ändern.

2.2.3 ERFORDERLICHE RESSOURCEN

11. Der Ausschuss merkt an, dass die Anforderung 3.1.1.2 repetitiv und unklar ist, was durch die uneinheitliche Terminologie noch verstärkt wird. So liest sich beispielsweise der dritte Absatz, als würde der Auftragspartner die Entscheidung über die Geeignetheit ausschließlich nach eigenem Ermessen treffen. Der Ausschuss empfiehlt, dass die LU AB einheitliche Terminologie verwendet und die Anforderung so umformuliert, dass sie klarer und verständlicher ist.

2.2.4 ANFORDERUNGEN AN DAS VERFAHREN

12. Der Ausschuss stellt fest, dass die Anforderung 4.2.1 mehrere Beispiele für erforderliche Informationen enthält. Im Einklang mit Abschnitt 7.2 des Anhangs 1 der Leitlinien sollten jedoch die ersten beiden Beispiele jeweils eine eigene Anforderung darstellen. Der Ausschuss empfiehlt der LU AB daher, die Formulierung zu ändern und die vorstehenden Beispiele in Form von Anforderungen aufzunehmen.

13. Im Hinblick auf Abschnitt 4.4 (Evaluierung) der Anforderungen an die Akkreditierung der LU AB ist der Ausschuss der Ansicht, dass die Anforderungen an die Akkreditierung die Verpflichtung der Zertifizierungsstelle enthalten sollten, sicherzustellen, dass Evaluierungsmethoden vorhanden sind, und dass diese Evaluierungsmethoden, die im Zertifizierungsverfahren beschrieben sind, standardisiert und allgemein anwendbar sind. Damit wäre sichergestellt, dass vergleichbare Evaluierungsmethoden für vergleichbare Evaluierungsgegenstände verwendet werden. Abweichungen von diesen Evaluierungsmethoden müssten von der Zertifizierungsstelle gerechtfertigt werden. Daher empfiehlt der Ausschuss der LU AB, den Entwurf zu ändern, um die vorstehend genannte Verpflichtung der Zertifizierungsstelle aufzunehmen.

14. Des Weiteren stellt der Ausschuss fest, dass nach der Anforderung 4.4.2 zwar Outsourcing nicht gestattet ist, die Zertifizierungsstelle in bestimmten Bereichen jedoch externe Sachverständige einsetzen darf. Diesbezüglich ist es wichtig, klarzustellen, dass die Zertifizierungsstelle auch dann für die Entscheidung verantwortlich bleibt, wenn sie externe Sachverständige einsetzt. Der Ausschuss empfiehlt der LU AB daher, die Formulierung in der Anforderung 4.4.2 entsprechend zu ändern.

15. Der Ausschuss stellt fest, dass in Abschnitt 4.7 der Anforderungen an die Akkreditierung der LU AB („Dokumentation über die Zertifizierung“) nicht auf die im Anhang enthaltene Anforderung zur Dokumentierung des Überwachungszeitraums eingegangen wird (Abschnitt 7.9). Daher regt der Ausschuss an, dass die LU AB den Überwachungszeitraum im Sinne von Abschnitt 7.9 über die Überwachung in die Anforderungen aufnimmt.

16. In Bezug auf Abschnitt 4.8 („Verzeichnis der zertifizierten Verarbeitungstätigkeiten“) der Anforderungen an die Akkreditierung der LU AB legt die Anforderung 4.8.1 fest, dass die Informationen der Öffentlichkeit „auf Anfrage“ zur Verfügung gestellt werden. Der Ausschuss ist der Auffassung, dass die in Abschnitt 7.8 des Anhangs 1 festgelegte Verpflichtung zur Transparenz besser erfüllt wäre, wenn die Zertifizierungsstelle die Informationen der Öffentlichkeit von sich aus zur Verfügung stellen würde. Der Ausschuss empfiehlt der LU AB daher, den Entwurf dahin zu ändern, dass er vorsieht, dass die Zertifizierungsstelle die in Abschnitt 7.8 des Anhangs 1 der Leitlinien aufgeführten Informationen veröffentlicht.

17. Der Ausschuss merkt an, dass Abschnitt 4.8 eine Überschrift zur Überwachung beinhaltet, die keine Anforderungen vorsieht. Der Ausschuss empfiehlt der LU AB, klarzustellen, wie die Überwachung durchgeführt werden wird.

18. Was Beendigung, Einschränkung, Aussetzung oder Widerruf der Zertifizierung betrifft (Unterabschnitt 4.10), so merkt der Ausschuss an, dass ein Hinweis darauf fehlt, dass die Zertifizierungsstelle verpflichtet ist, Entscheidungen und Anweisungen der zuständigen Aufsichtsbehörde, die Zertifizierung eines Kunden (Antragsteller) zu widerrufen oder diese nicht zu erteilen, falls die Voraussetzungen für eine Zertifizierung nicht mehr erfüllt werden, zu akzeptieren. Diese Verpflichtung ist sowohl in Artikel 58 Absatz 2 Buchstabe h der DSGVO als auch in Abschnitt 7.11

des Anhangs 1 vorgesehen. Daher empfiehlt der Ausschuss der LU AB, die Anforderungen an die Akkreditierung dahingehend zu ändern, dass Bestimmungen zu Beendigung, Einschränkung, Aussetzung oder Widerruf der Zertifizierung festgelegt werden.

19. Der Ausschuss merkt an, dass Abschnitt 9 des Anhangs allgemeine Überschriften beinhaltet, für die keine Anforderungen vorgesehen werden. So wird etwa Abschnitt 9.3.4 über die Aussetzung oder den Widerruf der Akkreditierung nicht behandelt. Dies sind wichtige Bereiche, die Querverweise zu den entsprechenden Abschnitten oder Anforderungen erfordern, die hinzugefügt werden. Der Ausschuss empfiehlt der LU AB daher, klarzustellen, wo die Anforderungen behandelt werden.

3 SCHLUSSFOLGERUNGEN/EMPFEHLUNGEN

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

21. Allgemein empfiehlt der Ausschuss der LU AB:

    1. die Bedeutung des Begriffs „Norm“ klarzustellen, der in mehreren Anforderungen enthalten ist (z. B. in Anforderung 3.2.1.1 und Anforderung 4.1.2). Dies könnte beispielsweise in den Abschnitten „Anwendungsbereich“ oder „Begriffsbestimmungen“ geschehen.

22. In Bezug auf „allgemeine Anforderungen an die Akkreditierung“ empfiehlt der Ausschuss, dass die LU AB

    1. klarstellt, dass die Anforderungen nicht durch externe Normen und Standards wie zum Beispiel ISAE 3000 außer Kraft gesetzt werden können;

    2. die Anforderungen in Abschnitt 1.6 dahingehend ändert, dass die Verpflichtung der Zertifizierungsstelle, alle Versionen der genehmigten Kriterien und alle Zertifizierungsverfahren in leicht zugänglicher Form zu veröffentlichen, entsprechend dem Anhang der Leitlinien aufgenommen wird.

23. In Bezug auf „erforderliche Ressourcen“ empfiehlt der Ausschuss, dass die LU AB

    1. einheitliche Terminologie verwendet und die Anforderung 3.1.1.2 so umformuliert, dass sie klarer und verständlicher ist.

24. In Bezug auf „Anforderungen an das Verfahren“ empfiehlt der Ausschuss, dass die LU AB:

    1. Abschnitt 4.4 des Entwurfs der Anforderungen dahin ändert, dass er die Verpflichtung der Zertifizierungsstelle enthält, sicherzustellen, dass Evaluierungsmethoden vorhanden sind, und dass diese Evaluierungsmethoden, die im Zertifizierungsverfahren beschrieben sind, standardisiert und allgemein anwendbar sind; vorsieht, dass Abweichungen von den Evaluierungsmethoden von der Zertifizierungsstelle begründet werden müssen;

    2. die Formulierung in der Anforderung 4.4.2 ändert, um klarzustellen, dass die Zertifizierungsstelle auch dann für die Entscheidung verantwortlich bleibt, wenn sie externe Sachverständige einsetzt;

3. Abschnitt 4.8 des Entwurfs dahingehend ändert, dass er vorsieht, dass die Zertifizierungsstelle die in Abschnitt 7.8 der Leitlinien des Anhangs 1 aufgeführten Informationen veröffentlicht;
4. in Abschnitt 4.8 klarstellt, wie die Überwachung durchgeführt wird;
5. Unterabschnitt 4.10 dahingehend ändert, dass Bestimmungen über die Beendigung, Einschränkung, Aussetzung oder den Widerruf der Zertifizierung festgelegt werden.

4 SCHLUSSBEMERKUNGEN

25. Diese Stellungnahme richtet sich an die LU AB und wird gemäß Artikel 64 Absatz 5 Buchstabe b der DSGVO veröffentlicht.

26. Nach Artikel 64 Absätze 7 und 8 der DSGVO muss die Aufsichtsbehörde dem Vorsitz binnen zwei Wochen nach Eingang der Stellungnahme mitteilen, ob sie den Entwurf ihrer Aufstellung beibehalten oder ändern wird. Innerhalb derselben Frist übermittelt sie den geänderten Entwurf der Aufstellung oder gibt, wenn sie nicht beabsichtigt, der Stellungnahme des Ausschusses zu folgen, die maßgeblichen Gründe an, aus denen sie nicht beabsichtigt, dieser Stellungnahme ganz oder teilweise zu folgen.

Für den Europäischen Datenschutzausschuss

Vorsitzende

(Andrea Jelinek)