Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 der Datenschutz-Grundverordnung (2016/679)

Version 3.0

4. Juni 2019

Angenommen

Versionsüberblick

Version 3.0	4. Juni 2019	Hinzufügung von Anhang 1 (Version 2.0 von Anhang 1 wurde im Anschluss an die öffentliche Konsultation am 4. Juni 2019 angenommen)
Version 2.0	4. Dezember 2018	Annahme der Leitlinien im Anschluss an die öffentliche Konsultation; am gleichen Tag wurde Anhang 1 Version 1.0) für die öffentliche Konsultation angenommen
Version 1.0.	6. Februar 2018	Annahme der Leitlinien durch die Artikel 29-Arbeitsgruppe (Version für die öffentliche Konsultation). Die Fassung wurde am 25. Mai 2018 vom Europäischen Datenschutzausschuss verabschiedet.

Inhalt

Der Europäische Datenschutzausschuss —

gestützt auf Artikel 70 Absatz 1 Buchstabe e 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"),

nach Prüfung der Ergebnisse der öffentlichen Konsultation zu den Leitlinien und der öffentlichen Konsultation zu deren Anhang, die gemäß Artikel 70 Absatz 4 im Februar 2018 bzw. zwischen dem 14. Dezember 2018 und dem 1. Februar 2019 stattfand —

HAT FOLGENDE LEITLINIEN ANGENOMMEN

1 EINLEITUNG

1. Die am 25. Mai 2018 in Kraft getretene Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) („DSGVO") setzt einen modernisierten Rahmen für den Datenschutz in Europa, der auf die Einhaltung der Rechenschaftspflicht und der Grundrechte ausgerichtet ist. Den Kern dieses neuen Rahmens bildet eine Reihe von Maßnahmen, die die Einhaltung der Bestimmungen der DSGVO erleichtern. Diese beinhalten sowohl die unter besonderen Umständen (u. a. bei der Ernennung von Datenschutzbeauftragten und der Durchführung von Datenschutz-Folgenabschätzungen) zu beachtenden, zwingenden Anforderungen als auch freiwillige Maßnahmen wie Verhaltensregeln und Zertifizierungsmechanismen.

2. Im Rahmen der Einführung von Zertifizierungsmechanismen sowie Datenschutzsiegeln und -prüfzeichen müssen die Mitgliedstaaten nach Artikel 43 Absatz 1 der DSGVO sicherstellen, dass Zertifizierungsstellen, die eine Zertifizierung gemäß Artikel 42 Absatz 1 erteilen, entweder von der zuständigen Aufsichtsbehörde oder der nationalen Akkreditierungsstelle oder von beiden akkreditiert werden. Wird die Akkreditierung im Einklang mit der ISO/IEC 17065:2012 von der nationalen Akkreditierungsstelle durchgeführt, sind auch die von der zuständigen Aufsichtsbehörde festgelegten zusätzlichen Anforderungen anzuwenden.

3. Aussagekräftige Zertifizierungsmechanismen können die Einhaltung der DSGVO fördern und für die betroffenen Personen und in Business-to-Business-Beziehungen (B2B) – etwa zwischen Verantwortlichen und Auftragsverarbeitern – die Transparenz erhöhen. Der Verantwortliche und der Auftragsverarbeiter können von einer unabhängigen Bescheinigung Dritter profitieren, mit der die Vereinbarkeit ihrer Verarbeitungsvorgänge (mit der DSGVO) nachgewiesen wird[1].

[1] Laut Erwägungsgrund 100 der DSGVO kann die Einführung von Zertifizierungsverfahren die Transparenz erhöhen und die Einhaltung der Verordnung verbessern sowie den betroffenen Personen einen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen.

4. In diesem Zusammenhang hat der Europäische Datenschutzausschuss (EDSA) entschieden, Leitlinien in Bezug auf die Akkreditierung zur Verfügung zu stellen. Der Wert und Zweck der Akkreditierung liegt insbesondere darin, dass damit eine verbindliche Aussage über die Kompetenz der Zertifizierungsstellen getroffen wird, die es ermöglicht, Vertrauen in die Zertifizierungsmechanismen zu schaffen.

5. Ziel dieser Leitlinien ist es, eine Orientierungshilfe für die Auslegung und die Umsetzung der Bestimmungen von Artikel 43 der DSGVO zu geben. Sie sollen Mitgliedstaaten, Aufsichtsbehörden und nationalen Akkreditierungsstellen helfen, eine kohärente und harmonisierte Grundlage für die Akkreditierung von Zertifizierungsstellen , die Zertifizierungen gemäß der DSGVO erteilen, zu schaffen.

2 ANWENDUNGSBEREICH DER LEITLINIEN

6. Diese Leitlinien

- erläutern den Zweck der Akkreditierung im Rahmen der DSGVO;
- beschreiben die Möglichkeiten einer Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 Absatz 1 und legen die wichtigsten dabei zu berücksichtigenden Aspekte dar;
- bilden den Rahmen zur Festlegung zusätzlicher Akkreditierungsanforderungen für den Fall, dass die Akkreditierung von der nationalen Akkreditierungsstelle durchgeführt wird; und
- bilden den Rahmen zur Festlegung von Akkreditierungsanforderungen, wenn die Akkreditierung von der Aufsichtsbehörde durchgeführt wird.

7. Die Leitlinien sind nicht als Handbuch für das Akkreditierungsverfahren von Zertifizierungsstellen gemäß der DSGVO zu verstehen. Es wird darin kein neuer technischer Standard für die Akkreditierung von Zertifizierungsstellen für die Zwecke der DSGVO entwickelt.

8. Die Leitlinien richten sich an:

    - Mitgliedstaaten, die dafür Sorge tragen müssen, dass die Zertifizierungsstellen von der Aufsichtsbehörde und/oder der nationalen Akkreditierungsstelle akkreditiert werden;
    - nationale Akkreditierungsstellen, die die Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 Absatz 1 Buchstabe b durchführen;
    - die zuständige Aufsichtsbehörde, die die „zusätzlichen Anforderungen“ an die in der ISO/IEC 17065:2012[2] benannten Stellen konkretisiert, wenn die Akkreditierung von der nationalen Akkreditierungsstelle gemäß Artikel 43 Absatz 1 Buchstabe b durchgeführt wird;
    - den Europäischen Datenschutzausschuss bei Stellungnahmen zu den Akkreditierungsanforderungen der zuständigen Aufsichtsbehörden und deren Genehmigung gemäß Artikel 43 Absatz 3, Artikel 70 Absatz 1 Buchstabe p und Artikel 64 Absatz 1 Buchstabe c;

[2] Die Internationale Organisation für Normung: Konformitätsbewertung – Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren.

- die zuständige Aufsichtsbehörde, die die Akkreditierungsanforderungen festlegt, wenn die Akkreditierung gemäß Artikel 43 Absatz 1 Buchstabe a von der Aufsichtsbehörde durchgeführt wird;

- andere Interessengruppen, wie etwa potenzielle Zertifizierungsstellen oder Zertifizierungssystemeigner, die Zertifizierungskriterien und -verfahren bereitstellen[3].

9. Begriffsbestimmungen

10. Die folgenden Definitionen zielen darauf ab, ein gemeinsames Verständnis der grundlegenden Elemente des Akkreditierungsprozesses zu fördern. Sie sind als Orientierungspunkte zu verstehen und erheben keinerlei Anspruch darauf, unanfechtbar zu sein. Diese Definitionen basieren auf bestehenden gesetzlichen Rahmenbedingungen und Normen, insbesondere auf den einschlägigen Bestimmungen der DSGVO und der ISO/IEC 17065:2012.

11. Für die Zwecke dieser Leitlinien gelten folgende Begriffsbestimmungen:

12. „*Akkreditierung*" von Zertifizierungsstellen: siehe Abschnitt 3 zur Auslegung der Akkreditierung im Sinne von Artikel 43 der DSGVO;

13. „*Zusätzliche Anforderungen*" sind die von der zuständigen Aufsichtsbehörde festgelegten Anforderungen zur Durchführung einer Akkreditierung[4];

14. „*Zertifizierung*" ist die Beurteilung und unabhängige Bestätigung durch einen Dritten[5], dass die Erfüllung der Zertifizierungskriterien nachgewiesen werden konnte;

15. „*Zertifizierungsstelle*" ist eine[6] Konformitätsbewertungsstelle von dritter Seite[7], die Zertifizierungsmechanismen anwendet[8];

[3] Systemeigner ist eine identifizierbare Organisation, die Zertifizierungskriterien und Anforderungen festgelegt hat, anhand derer die Konformität bewertet werden soll. Die Akkreditierung erfolgt durch die Organisation, die Bewertungen (Artikel 43 Absatz 4) anhand der Anforderungen des Zertifizierungsprogramms durchführt und die Zertifizierungen erteilt (d. h. durch die Zertifizierungsstelle, auch bekannt als Konformitätsbewertungsstelle). Die Organisation, die die Bewertungen durchführt, kann dieselbe Organisation sein, die der Entwickler und Eigentümer des Zertifizierungsprogramms ist. Es kann jedoch auch der Fall sein, dass eine Organisation der Eigentümer des Zertifizierungsprogramms ist und eine (oder mehrere) andere die Bewertungen durchführt.

[4] Artikel 43 Absatz 1, 3 und 6.

[5] Zu beachten ist, dass gemäß der ISO 17000 die Bestätigung durch eine dritte Seite („Zertifizierung") „auf alle Gegenstände der Konformitätsbewertung anwendbar" (5.5) ist, „mit Ausnahme der Konformitätsbewertungsstellen selbst, für die die Akkreditierung (5.6) gilt."

[6] Nach Abschnitt 2.4 der ISO 17000 ist eine Konformitätsbewertung eine Tätigkeit, die durch eine dritte Seite von einer Person oder Stelle durchgeführt wird, die unabhängig von der Person oder Organisation ist, die den Gegenstand der Konformitätsbewertung anbietet, und von Interessen als Anwender dieses Gegenstands unabhängig ist.

[7] Siehe Abschnitt 2.5, ISO 17000: „Stelle, die Konformitätsbewertungsdienste durchführt"; ISO 17011: „Stelle, die Konformitätsbewertungsdienste durchführt und die Gegenstand der Akkreditierung sein kann"; Abschnitt 3.12, ISO 17065.

[8] Artikel 42 Absatz 1 und Artikel 42 Absatz 5 der DSGVO.

16. „*Zertifizierungsprogramm*“ ist ein Zertifizierungssystem für bestimmte Produkte, Prozesse und Dienstleistungen, für die dieselben festgelegten Anforderungen, spezifischen Regeln und Verfahren gelten[9];

17. „Kriterien“ oder Zertifizierungskriterien sind die Kriterien, anhand derer eine Zertifizierung (Konformitätsbewertung) durchgeführt wird[10];

18. „*Nationale Akkreditierungsstelle*“ ist die einzige Stelle in einem Mitgliedstaat, die gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates benannt wurde und im Auftrag des Staates Akkreditierungen durchführt[11].

3 AUSLEGUNG DER „AKKREDITIERUNG“ ZUR ANWENDUNG VON ARTIKEL 43 DER DSGVO

19. Der Begriff der „Akkreditierung“ wird in der DSGVO nicht definiert. In Artikel 2 Nummer 10 der Verordnung (EG) Nr. 765/2008, der die allgemeinen Anforderungen für die Akkreditierung festlegt, ist die Akkreditierung definiert als

20. „Bestätigung durch eine nationale Akkreditierungsstelle, dass eine Konformitätsbewertungsstelle die in harmonisierten Standards festgelegten Anforderungen und, gegebenenfalls, zusätzliche Anforderungen, einschließlich solcher in relevanten sektoralen Akkreditierungssystemen, erfüllt, um eine spezielle Konformitätsbewertungstätigkeit durchzuführen.“

21. Gemäß EN ISO/IEC 17011:

22. „Akkreditierung bezieht sich auf eine Bestätigung durch eine dritte Seite, die formal darlegt, dass eine Konformitätsbewertungsstelle die Kompetenz besitzt, bestimmte Konformitätsbewertungsaufgaben durchzuführen.“

23. Artikel 43 Absatz 1 besagt:

24. „Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 57 und 58 erteilen oder verlängern Zertifizierungsstellen, die über das geeignete Fachwissen hinsichtlich des Datenschutzes verfügen, nach Unterrichtung der Aufsichtsbehörde – damit diese erforderlichenfalls von ihren Befugnissen gemäß Artikel 58 Absatz 2 Buchstabe h Gebrauch machen kann – die Zertifizierung. Die Mitgliedstaaten stellen sicher, dass diese Zertifizierungsstellen von einer oder beiden der folgenden Stellen akkreditiert werden:

    (a) der gemäß Artikel 55 oder 56 zuständigen Aufsichtsbehörde;
    (b) der nationalen Akkreditierungsstelle, die gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates im Einklang mit der ISO/IEC 17065:2012 und mit den zusätzlichen von der gemäß Artikel 55 oder 56 zuständigen Aufsichtsbehörde festgelegten Anforderungen benannt wurde.“

[9] Siehe Abschnitt 3.9 in Verbindung mit Anhang B der ISO 17065.

[10] Siehe Artikel 42 Absatz 5.

[11] Siehe Artikel 2 Nummer 11 der Verordnung (EG) Nr. 765/2008.

25. In Bezug auf die DSGVO orientieren sich die Akkreditierungsanforderungen an:

- der ISO/IEC 17065:2012 und den „zusätzlichen Anforderungen“, die von der gemäß Artikel 43 Absatz 1 Buchstabe b zuständigen Aufsichtsbehörde festgelegt werden, wenn die Akkreditierung von der nationalen Akkreditierungsstelle durchgeführt wird bzw. von der Aufsichtsbehörde, wenn diese die Akkreditierung selbst vornimmt.

26. In beiden Fällen müssen die konsolidierten Anforderungen die in Artikel 43 Absatz 2 genannten Anforderungen erfüllen.

27. Der Europäische Datenschutzausschuss erkennt an, dass der Zweck der Akkreditierung darin besteht, eine verbindliche Aussage über die Kompetenz einer Stelle für die Durchführung von Zertifizierungen zu geben (Konformitätsbewertungstätigkeiten)[12]. Unter Akkreditierung im Sinne der DSGVO ist Folgendes zu verstehen:

28. Eine Bescheinigung[13] einer nationalen Akkreditierungsstelle und/oder einer Aufsichtsbehörde, dass eine Zertifizierungsstelle[14] zur Durchführung von Zertifizierungen nach den Artikeln 42 und 43 der DSGVO qualifiziert ist, wobei die ISO/IEC 17065:2012 und die von der Aufsichtsbehörde und/oder dem Ausschuss festgelegten zusätzlichen Anforderungen zu berücksichtigen sind.

4 AKKREDITIERUNG GEMÄß ARTIKEL 43 ABSATZ 1 DER DSGVO

29. Artikel 43 Absatz 1 berücksichtigt, dass es für die Akkreditierung von Zertifizierungsstellen mehrere Möglichkeiten gibt. Die DSGVO schreibt vor, dass das Verfahren für die Akkreditierung von Zertifizierungsstellen von den Aufsichtsbehörden und den Mitgliedstaaten festgelegt werden muss. In diesem Abschnitt werden die Akkreditierungswege gemäß Artikel 43 beschrieben.

4.1 Rolle der Mitgliedstaaten

30. Nach Artikel 43 Absatz 1 müssen die Mitgliedstaaten *sicherstellen*, dass die Zertifizierungsstellen akkreditiert sind. Die Mitgliedstaaten können jedoch selbst festlegen, wer für die zur Akkreditierung führende Beurteilung verantwortlich sein soll. Auf der Grundlage von Artikel 43 Absatz 1 gibt es drei Möglichkeiten für die Durchführung der Akkreditierung:

(1) ausschließlich durch die Aufsichtsbehörde auf der Basis ihrer eigenen Anforderungen,
(2) ausschließlich durch die nationale Akkreditierungsstelle, die gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates im Einklang mit der ISO/IEC 17065:2012 und mit zusätzlichen, von der zuständigen Aufsichtsbehörde festgelegten Anforderungen, benannt wurde; oder

[12] Vgl. Erwägungsgrund 15 765/2008/EG.
[13] Vgl. Artikel 2 Nummer 10 der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten.
[14] Vgl. mit der Bestimmung des Begriffs „Akkreditierung“ gemäß der ISO 17011.

(3) durch die Aufsichtsbehörde und die nationale Akkreditierungsstelle (und unter Erfüllung aller oben unter 2 genannten Anforderungen).

31. Es obliegt den einzelnen Mitgliedstaaten zu entscheiden, ob die nationale Akkreditierungsstelle oder die Aufsichtsbehörde oder beide zusammen die Akkreditierungstätigkeiten durchführen werden. In jedem Fall sollte der Mitgliedstaat jedoch sicherstellen, dass dafür angemessene Mittel bereitstehen[15].

4.2 Zusammenwirken mit der Verordnung (EG) Nr. 765/2008

32. Der Europäische Datenschutzausschuss weist darauf hin, dass Artikel 2 Nummer 11 der Verordnung (EG) Nr. 765/2008 eine nationale Akkreditierungsstelle definiert als „*einzige* Stelle in einem Mitgliedstaat, die im Auftrag dieses Staates Akkreditierungen durchführt".

33. Artikel 2 Nummer 11 könnte als unvereinbar mit Artikel 43 Absatz 1 der DSGVO betrachtet werden, der die Möglichkeit einräumt, dass die Akkreditierung durch eine andere Stelle als die nationale Akkreditierungsstelle des Mitgliedstaats vorgenommen wird. Der Europäische Datenschutzausschuss gibt zu bedenken, dass hinter der EU-Rechtsvorschrift die Absicht steht, von dem allgemeinen Grundsatz abzuweichen, die Akkreditierung ausschließlich von der nationalen Akkreditierungsbehörde durchführen zu lassen, in dem den Aufsichtsbehörden die gleiche Befugnis hinsichtlich der Akkreditierung von Zertifizierungsstellen eingeräumt wird. Somit ist Artikel 43 Absatz 1 lex specialis gegenüber Artikel 2 Nummer 11 der Verordnung (EG) Nr. 765/2008.

4.3 Die Rolle der nationalen Akkreditierungsstelle

34. Artikel 43 Absatz 1 Buchstabe b sieht vor, dass die nationale Akkreditierungsstelle die Zertifizierungsstellen gemäß ISO/IEC 17065:2012 und den von der zuständigen Aufsichtsbehörde festgelegten zusätzlichen Anforderungen akkreditiert.

35. Aus Gründen der Klarheit hält der Europäische Datenschutzausschuss fest, dass der ausdrückliche Verweis auf „Absatz 1 Buchstabe b" in Artikel 43 Absatz 3 impliziert, dass „diese Anforderungen" auf die zusätzlich von der zuständigen Aufsichtsbehörde gemäß Artikel 43 Absatz 1 Buchstabe b festgelegten Anforderungen verweisen, sowie auf die Anforderungen gemäß Artikel 43 Absatz 2.

36. Die nationalen Akkreditierungsstellen müssen die von den Aufsichtsbehörden zusätzlich festgelegten Anforderungen im Zuge des Akkreditierungsprozesses anwenden.

37. Eine Zertifizierungsstelle mit bereits bestehender Akkreditierung auf der Grundlage der ISO/IEC 17065:2012 für Zertifizierungsprogramme, die nicht mit der DSGVO in Verbindung stehen, die den Geltungsbereich ihrer Akkreditierung auf die gemäß der DSGVO ausgestellten Zertifizierungen ausdehnen möchte, muss die von der Aufsichtsbehörde festgelegten zusätzlichen Anforderungen erfüllen, wenn die Akkreditierung von der nationalen Akkreditierungsstelle durchgeführt wird. Wird die Akkreditierung für die Zertifizierung im Rahmen der DSGVO nur von der zuständigen Aufsichtsbehörde angeboten, muss die zu akkreditierende Zertifizierungsstelle die von der jeweiligen Aufsichtsbehörde festgelegten Anforderungen erfüllen.

4.4 Die Rolle der Aufsichtsbehörde

[15] Siehe Artikel 4 Absatz 9 der Verordnung (EG) Nr. 765/2008.

38. Der Europäische Datenschutzausschuss merkt an, dass nach Artikel 57 Absatz 1 Buchstabe q die Aufsichtsbehörde die Akkreditierung einer Zertifizierungsstelle gemäß Artikel 43 als Aufgabe der Aufsichtsbehörde gemäß Artikel 57 durchzuführen hat, und Artikel 58 Absatz 3 Buchstabe e vorsieht, dass die Aufsichtsbehörde Genehmigungs- und beratende Befugnisse hat, Zertifizierungsstellen gemäß Artikel 43 zu akkreditieren. Der Wortlaut von Artikel 43 Absatz 1 bietet eine gewisse Flexibilität, und die Akkreditierungsbefugnis der Aufsichtsbehörde sollte nur als Aufgabe verstanden werden, wenn sie erforderlich ist. Zur Klärung dieses Punktes kann das nationale Recht der Mitgliedstaaten herangezogen werden. Bei der Akkreditierung durch eine nationale Akkreditierungsstelle muss die Zertifizierungsstelle jedoch gemäß Artikel 43 Absatz 2 Buchstabe a ihre Unabhängigkeit und ihr Fachwissen hinsichtlich des Gegenstandsbereichs des von ihr angebotenen Zertifizierungsmechanismus zur Zufriedenheit der zuständigen Aufsichtsbehörde nachweisen.[16]

39. Wenn ein Mitgliedstaat festlegt, dass die Zertifizierungsstellen von der Aufsichtsbehörde akkreditiert werden sollen, sollte die Aufsichtsbehörde Akkreditierungsanforderungen festlegen, die u.a. die in Artikel 43 Absatz 2 genannten Anforderungen enthalten. Verglichen mit den Verpflichtungen, die den nationalen Akkreditierungsstellen im Zusammenhang mit der Akkreditierung von Zertifizierungsstellen zufallen, sind in Artikel 43 weniger Anforderungen an die Akkreditierung festgelegt, wenn diese von der Aufsichtsbehörde selbst durchgeführt wird. Um einen harmonisierten Ansatz für Akkreditierungen zu erreichen, sollten sich die von der Aufsichtsbehörde verwendeten Akkreditierungskriterien an der ISO/IEC 17065 orientieren und durch die von der Aufsichtsbehörde gemäß Artikel 43 Absatz 1 Buchstabe b zusätzlich festgelegten Anforderungen ergänzt werden. Der Europäische Datenschutzausschuss weist darauf hin, dass Artikel 43 Absatz 2 Buchstaben a bis e Anforderungen der ISO 17065 wiedergeben und festlegen, die zu einer Vereinheitlichung beitragen.

40. Wenn ein Mitgliedstaat festlegt, dass die Zertifizierungsstellen von den nationalen Akkreditierungsstellen zu akkreditieren sind, sollte die Aufsichtsbehörde zusätzliche Anforderungen festlegen, die die bestehenden Akkreditierungsbestimmungen gemäß der Verordnung (EG) Nr. 765/2008 ergänzen (wobei sich die Artikel 3 bis 14 auf die Organisation und Durchführung der Akkreditierung von Konformitätsbewertungsstellen beziehen), sowie die Regeln, in denen die Methoden und Verfahren der Zertifizierungsstellen beschrieben werden. Vor diesem Hintergrund enthält die Verordnung (EG) Nr. 765/2008 weitere Leitlinien: Artikel 2 Nummer 10 definiert die Akkreditierung und verweist auf „harmonisierte Normen“ und „zusätzliche Anforderungen, einschließlich solcher in relevanten sektoralen Akkreditierungssystemen“. Daraus folgt, dass die von der Aufsichtsbehörde zusätzlich festgelegten Anforderungen spezifische Anforderungen enthalten und darauf ausgerichtet sein sollten, unter anderem die Beurteilung der Unabhängigkeit und des Niveaus an datenschutzrechtlichem Fachwissen der Zertifizierungsstellen zu erleichtern, z. B. ihre Fähigkeit, die Verarbeitung personenbezogener Daten durch Verantwortliche und Auftragsverarbeiter gemäß Artikel 42 Absatz 1 zu beurteilen und zu zertifizieren. Dazu gehören auch die für sektorale Akkreditierungssysteme erforderliche Kompetenz sowie Kompetenzen in Bezug auf den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf den Schutz personenbezogener Daten.[17] Der Anhang zu diesen

[16] Die Unabhängigkeit und das Fachwissen sollten in den von der Aufsichtsbehörde gemäß Artikel 43 Absatz 1 Buchstabe b festgelegten zusätzlichen Anforderungen bestimmt werden. Siehe auch Anhang 1 der Leitlinien.
[17] Artikel 1 Absatz 2 der DSGVO.

Leitlinien bietet den zuständigen Aufsichtsbehörden hinsichtlich der „zusätzlich festgelegten Anforderungen“ gemäß Artikel 43 Absatz 1 Buchstabe b und Artikel 43 Absatz 3 weitere Hilfestellungen.

41. In Artikel 43 Absatz 6 heißt es: „Die Anforderungen nach Absatz 3 des vorliegenden Artikels und die Kriterien nach Artikel 42 Absatz 5 werden von der Aufsichtsbehörde in leicht zugänglicher Form veröffentlicht.“ Zur Gewährleistung der Transparenz werden daher alle von einer Aufsichtsbehörde genehmigten Kriterien und Anforderungen veröffentlicht. In Bezug auf Qualität und Vertrauen in die Zertifizierungsstellen wäre es wünschenswert, wenn alle Anforderungen an die Akkreditierung für die Öffentlichkeit leicht zugänglich wären.

4.5 Als Zertifizierungsstelle agierende Aufsichtsbehörde

42. Nach Artikel 42 Absatz 5 kann eine Aufsichtsbehörde eine Zertifizierung erteilen. Die DSGVO schreibt jedoch nicht vor, dass sie dafür akkreditiert sein muss, um die Anforderungen der Verordnung (EG) Nr. 765/2008 zu erfüllen. Der Europäische Datenschutzausschuss weist darauf hin, dass Artikel 43 Absatz 1 Buchstabe a und insbesondere Artikel 58 Absatz 2 Buchstabe h sowie Artikel 3 Buchstaben a und e bis f die Aufsichtsbehörden ermächtigen, sowohl Akkreditierungen als auch Zertifizierungen durchzuführen, Empfehlungen abzugeben und gegebenenfalls Zertifizierungen zu widerrufen oder Zertifizierungsstellen anzuweisen, keine Zertifizierungen zu erteilen.

43. Es kann Fälle geben, bei denen eine Trennung der Akkreditierungs- und Zertifizierungsrollen und -pflichten angemessen oder erforderlich ist, beispielsweise wenn eine Aufsichtsbehörde und weitere Zertifizierungsstellen in einem Mitgliedstaat nebeneinander bestehen und beide dasselbe Spektrum an Zertifizierungen erteilen. Die Aufsichtsbehörden sollten daher ausreichende organisatorische Maßnahmen zur Trennung der Aufgaben im Rahmen der DSGVO ergreifen, um Zertifizierungsmechanismen anzubieten und zu ermöglichen. Gleichzeitig haben sie Vorkehrungen zur Vermeidung von Interessenkonflikten zu ergreifen, die sich aus diesen Aufgaben ergeben können. Darüber hinaus sollten die Mitgliedstaaten und die Aufsichtsbehörden den Gedanken der Harmonisierung auf europäischer Ebene berücksichtigen, wenn sie nationale Rechtsvorschriften und Verfahren für die Akkreditierung und Zertifizierung im Einklang mit der DSGVO erstellen.

4.6 Akkreditierungsanforderungen

44. Der Anhang zu diesen Leitlinien enthält Anleitungen zur Bestimmung zusätzlicher Akkreditierungsanforderungen. Neben der Erläuterung der einschlägigen Bestimmungen der DSGVO werden Anforderungen vorgeschlagen, die von den Aufsichtsbehörden und nationalen Akkreditierungsstellen in Betracht gezogen werden sollten, damit die Einhaltung der DSGVO sichergestellt wird.

45. Wie oben ausgeführt, ist die ISO/IEC 17065:2012 die relevante Akkreditierungsnorm, wenn Zertifizierungsstellen von der nationalen Akkreditierungsstelle gemäß der Verordnung (EG) Nr. 765/2008 akkreditiert werden, und sie wird durch die zusätzlichen, von der Aufsichtsbehörde festgelegten Anforderungen ergänzt. Artikel 43 Absatz 2 spiegelt die allgemeinen Bestimmungen der ISO/IEC 17065:2012 vor dem Hintergrund des Schutzes der Grundrechte durch die DSGVO wider. Innerhalb des Anhangs dienen Artikel 43 Absatz 2 und die ISO/IEC 17065:2012 als Grundlage zur Bestimmung der Anforderungen sowie weiterer Kriterien, die sich hinsichtlich der Verarbeitung personenbezogener Daten gemäß der DSGVO auf die Beurteilung des datenschutzrechtlichen Fachwissens der Zertifizierungsstellen und ihre Fähigkeit, die Rechte und Freiheiten natürlicher Personen zu wahren, beziehen. Der

Europäische Datenschutzausschuss hält fest, dass es ihm ein besonderes Anliegen ist, zu gewährleisten, dass die Zertifizierungsstellen über das geeignete Fachwissen hinsichtlich des Datenschutzes gemäß Artikel 43 Absatz 1 verfügen.

46. Die von der Aufsichtsbehörde festgelegten zusätzlichen Akkreditierungsanforderungen gelten für alle Zertifizierungsstellen, die eine Akkreditierung beantragen. Die Akkreditierungsstelle wird beurteilen, ob diese Zertifizierungsstelle über die Kompetenzen zur Durchführung der Zertifizierungstätigkeit im Einklang mit den zusätzlichen Anforderungen und dem Gegenstand der Zertifizierung verfügt. Es soll auf die bestimmten Sektoren oder Zertifizierungsbereiche, für die die Zertifizierungsstelle akkreditiert wurde, Bezug genommen werden.

47. Der Europäische Datenschutzausschuss weist außerdem darauf hin, dass das besondere Fachwissen auf dem Gebiet des Datenschutzes auch über die Anforderungen der ISO/IEC 17065:2012 hinaus erforderlich ist, wenn andere externe Stellen - wie Labore oder Prüfer - Zertifizierungstätigkeiten im Auftrag einer akkreditierten Zertifizierungsstelle für Teile oder Komponenten durchführen. In diesen Fällen ist eine Akkreditierung der externen Stellen unter der DSGVO selbst nicht möglich. Um die Eignung dieser Stellen für ihre Tätigkeit im Auftrag der akkreditierten Zertifizierungsstellen zu gewährleisten, muss die akkreditierte Zertifizierungsstelle jedoch sicherstellen, dass auch das für die akkreditierte Stelle erforderliche datenschutzrechtliche Fachwissen vorhanden ist und durch die externe Stelle in Bezug auf die betreffende Tätigkeit nachgewiesen wird.

48. Der im Anhang zu diesen Leitlinien enthaltene Rahmen für die Bestimmung der zusätzlichen Akkreditierungsanforderungen stellt kein Handbuch für das von der nationalen Akkreditierungsstelle oder der Aufsichtsbehörde durchzuführende Akkreditierungsverfahren dar. Er bietet den Aufsichtsbehörden Leitlinien zur Struktur und Methodik und damit ein Instrument, um die zusätzlichen Anforderungen für die Akkreditierung zu ermitteln.

ANHANG 1

Anhang 1 enthält Anleitungen zur Bestimmung „zusätzlicher" Akkreditierungsanforderungen in Bezug auf die ISO/IEC 17065:2012 und gemäß Artikel 43 Absatz 1 Buchstabe b und Artikel 43 Absatz 3 der DSGVO.

Im Anhang sind Vorschläge für Anforderungen aufgeführt, die die zuständige Datenschutzaufsichtsbehörde erarbeiten soll und die bei der Akkreditierung einer Zertifizierungsstelle durch die nationale Akkreditierungsstelle oder die zuständige Aufsichtsbehörde gelten.[18] Diese zusätzlichen Anforderungen sind dem Europäischen Datenschutzausschuss gemäß Artikel 64 Absatz 1 Buchstabe c vor der Genehmigung zu übermitteln.

Dieser Anhang sollte in Verbindung mit der ISO/IEC 17065:2012 gelesen werden. Die hier verwendeten Abschnitte entsprechen denen der ISO/IEC 17065:2012. Im Falle, dass Aufsichtsbehörden die Akkreditierung gemäß Artikel 43 Absatz 1 Buchstabe a durchführen, wäre ein bewährtes Verfahren, diesen Ansatz, soweit sinnvoll, zu verfolgen. Dies trägt zu einem EU-weit einheitlichen Akkreditierungsverfahren bei.

Unbeschadet der folgenden Leitlinien oder der fehlenden Leitlinien zu jedem beliebigen Punkt der ISO/IEC 17065:2012, kann die zuständige Aufsichtsbehörde weitere zusätzliche Anforderungen betreffend diese Punkte aufstellen, wenn diese im Einklang mit dem innerstaatlichen Recht stehen.

0 PRÄFIX

[Dieser Abschnitt befasst sich mit etwaigen Kooperationsvereinbarungen, , zwischen der nationalen Akkreditierungsstelle und der zuständigen Datenschutzaufsichtsbehörde, beispielsweise mit der Frage, wer für die Entgegennahme von Anträgen zuständig sein soll oder wie die Anerkennung genehmigter Kriterien als Teil des Akkreditierungsverfahrens zu organisieren ist.]

1 ANWENDUNGSBEREICH[19]

Der Anwendungsbereich der ISO/IEC 17065:2012 ist im Einklang mit der DSGVO auszulegen. Weitere Informationen finden sich in den Leitlinien zur Akkreditierung und Zertifizierung. Die nationale Akkreditierungsstelle und die zuständige Aufsichtsbehörde sollten während des Akkreditierungsprozesses den Anwendungsbereich eines Zertifizierungsmechanismus (beispielsweise die Zertifizierung von Datenverarbeitungen eines Cloud-Dienstes) in die Beurteilung einbeziehen, insbesondere in Bezug auf Kriterien, Fachwissen und Evaluierungsmethoden. Durch den breiten Anwendungsbereich der ISO/IEC 17065:2012, der Produkte, Prozesse und Dienstleistungen umfasst, dürfen die Anforderungen der DSGVO nicht herabgestuft oder außer Kraft gesetzt werden. Beispielsweise darf ein Regelungsmechanismus nicht das einzige Element eines Zertifizierungsverfahrens sein, da die Zertifizierung die Verarbeitung von personenbezogenen Daten – d. h. die Verarbeitungsvorgänge – beinhalten muss. Gemäß Artikel 42 Absatz 1 ist eine Zertifizierung

[18] Für Informationen zum Genehmigungsprozess von Zertifizierungskriterien siehe Abschnitt 4 der Zertifizierungsleitlinien.

[19] Die Nummerierung bezieht sich auf die ISO/IEC 17065:2012.

nach der DSGVO nur auf die Verarbeitungsvorgänge von Verantwortlichen und Auftragsverarbeitern anwendbar.

2 NORMATIVE VERWEISUNGEN

Die DSGVO hat Vorrang vor der ISO/IEC 17065:2012. Falls in den zusätzlichen Anforderungen oder im Zertifizierungsmechanismus Bezug auf andere ISO-Normen genommen wird, müssen diese im Einklang mit den in der DSGVO festgelegten Anforderungen ausgelegt werden.

3 BEGRIFFE

Im Rahmen dieses Anhangs gelten die Begriffe und Begriffsbestimmungen der Leitlinien zur Akkreditierung (WP 261) und Zertifizierung (EDPB 1/2018) und sie haben Vorrang vor den Begriffen der ISO-Normen.

4 ALLGEMEINE ANFORDERUNGEN

4.1 Rechtliche und vertragliche Angelegenheiten

4.1.1 Rechtliche Verantwortung

Eine Zertifizierungsstelle sollte der nationalen Akkreditierungsstelle und der zuständigen Aufsichtsbehörde (immer) nachweisen können, dass sie über die neuesten Verfahren verfügt und diese mit den in den Akkreditierungsbedingungen festgelegten rechtlichen Zuständigkeiten – einschließlich der zusätzlichen Anforderungen bei Anwendung der Verordnung (EU) 2016/679 – im Einklang stehen. Da eine Zertifizierungsstelle selbst Verantwortlicher/Auftragsverarbeiter ist, muss sie nachweisen können, dass sie über mit der Verordnung (EU) 2016/679 vereinbare Verfahren und Maßnahmen verfügt, insbesondere für die Kontrolle von und den Umgang mit personenbezogenen Daten der Kundenorganisation als Teil des Zertifizierungsprozesses.

Die zuständige Aufsichtsbehörde kann gegebenenfalls weitere Anforderungen und Verfahren hinzufügen, um die DSGVO-Konformität der Zertifizierungsstellen vor der Akkreditierung zu überprüfen.

4.1.2 Zertifizierungsvereinbarung

Die Mindestanforderungen für eine Zertifizierungsvereinbarung werden durch folgende Punkte vervollständigt:

Die Zertifizierungsstelle muss ergänzend zu den Anforderungen der ISO/IEC 17065:2012 nachweisen, dass ihre Zertifizierungsvereinbarungen:

1. den Antragsteller verpflichten, stets sowohl die allgemeinen Zertifizierungsanforderungen im Sinne von Abschnitt 4.1.2.2 Buchstabe a der ISO/IEC 17065:2012 als auch die von der zuständigen Aufsichtsbehörde oder dem Europäischen Datenschutzausschuss genehmigten Kriterien im Einklang mit Artikel 43 Absatz 2 Buchstabe b und Artikel 42 Absatz 5 einzuhalten;
2. den Antragsteller verpflichten, vollständige Transparenz des Zertifizierungsprozesses gegenüber der zuständigen Aufsichtsbehörde zu gewährleisten, einschließlich der vertraulichen Vertragsangelegenheiten in Zusammenhang mit der Einhaltung von

Datenschutzbestimmungen gemäß Artikel 42 Absatz 7 und Artikel 58 Absatz 1 Buchstabe c;

3. nicht die Verantwortung des Antragstellers für die Einhaltung der Verordnung (EU) 2016/679 verringern und nicht die Aufgaben und Befugnisse der im Einklang mit Artikel 42 Absatz 5 zuständigen Aufsichtsbehörden berühren;
4. den Antragsteller verpflichten, der Zertifizierungsstelle sämtliche Informationen bereitzustellen und ihr Zugang zu seinen Datenverarbeitungstätigkeiten zu gewähren, welche für den Zertifizierungsprozess gemäß Artikel 42 Absatz 6 erforderlich sind;
5. den Antragsteller verpflichten, geltende Fristen und Abläufe einzuhalten. In der Zertifizierungsvereinbarung ist festzulegen, dass Fristen und Abläufe, die sich beispielsweise aus dem Zertifizierungsprogramm oder anderen Verordnungen ergeben, zu beachten und einzuhalten sind;
6. im Hinblick auf Abschnitt 4.1.2.2 Buchstabe c Nr. 1 der ISO/IEC 17065:2012 Vorschriften zu Gültigkeit, Erneuerung und Widerruf gemäß Artikel 42 Absatz 7 und Artikel 43 Absatz 4 festlegen, einschließlich Vorschriften über angemessene Zeitabstände für die Neubeurteilung oder Prüfung (Ordnungsmäßigkeit) im Einklang mit Artikel 42 Absatz 7;
7. es der Zertifizierungsstelle erlauben, sämtliche Information offenzulegen, die gemäß Artikel 42 Absatz 8 und Artikel 43 Absatz 5 zur Erteilung der Zertifizierung erforderlich sind;
8. Regeln zu den notwendigen Vorkehrungen für die Untersuchung von Beschwerden im Sinne von Ansatz 4.1.2.2 Buchstabe c Nr. 2 enthalten, darüber hinaus werden in Buchstabe j eindeutige Aussagen zur Struktur und Verfahren der Beschwerdeabwicklung gemäß Artikel 43 Absatz 2 Buchstabe d festgelegt;
9. falls sich ein Widerruf oder eine Aussetzung der Akkreditierung der Zertifizierungsstelle auf den Kunden auswirkt, sollten, ergänzend zu den in Abschnitt 4.1.2.2 der ISO/IEC 17065:2012 genannten Mindestanforderungen, auch sämtliche Konsequenzen für den Kunden thematisiert werden;
10. den Antragsteller verpflichten, 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.

4.1.3 Verwendung von Datenschutzsiegeln und -prüfzeichen

Zertifikate, Siegel und Prüfzeichen dürfen nur unter Einhaltung der Artikel 42 und 43 und der Leitlinien zur Akkreditierung und Zertifizierung verwendet werden.

4.2 Handhabung der Unparteilichkeit

Die Akkreditierungsstelle muss sicherstellen, dass ergänzend zur Anforderung in Abschnitt 4.2 der ISO/IEC 17065:2012

1. die Zertifizierungsstelle den zusätzlichen Anforderungen der zuständigen Aufsichtsbehörde (gemäß Artikel 43 Absatz 1 Buchstabe b) entspricht

    a. und im Einklang mit Artikel 43 Absatz 2 Buchstabe a einen eigenen Nachweis über ihre Unabhängigkeit erbringt. Dies gilt insbesondere für Nachweise, die die Finanzierung der Zertifizierungsstelle betreffen, insofern sie die Gewährleistung der Unparteilichkeit betreffen;

    b. und ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt gemäß Artikel 43 Absatz 2 Buchstabe e führen;

2. die Zertifizierungsstelle keine relevante Verbindung zu dem Kunden hat, den sie beurteilt.

4.3 Haftung und Finanzierung

Die Akkreditierungsstelle muss ergänzend zur Anforderung in Abschnitt 4.3.1 der ISO/IEC 17065:2012 regelmäßig sicherstellen, dass die Zertifizierungsstelle über geeignete Vorkehrungen verfügt (z. B. Versicherungen oder Rücklagen), um ihre Verbindlichkeiten in den geografischen Regionen, in denen sie operiert, decken zu können.

4.4 Nicht diskriminierende Bedingungen

Die Aufsichtsbehörde kann zusätzliche Anforderungen formulieren, wenn diese im Einklang mit dem innerstaatlichen Recht stehen.

4.5 Vertraulichkeit

Die Aufsichtsbehörde kann zusätzliche Anforderungen formulieren, wenn diese im Einklang mit dem innerstaatlichen Recht stehen.

4.6 Öffentlich zugängliche Informationen

Ergänzend zur Anforderung in Abschnitt 4.6 ISO/IEC 17065:2012 muss die Akkreditierungsstelle von der Zertifizierungsstelle verlangen, dass zumindest

1. alle Versionen (die aktuelle und frühere) der im Sinne von Artikel 42 Absatz 5 verwendeten, genehmigten Kriterien veröffentlicht werden und leicht zugänglich sind, sowie auch alle Zertifizierungsverfahren, wobei die jeweilige Gültigkeitsdauer zu nennen ist.
2. Informationen zu Verfahren und Einsprüchen zur Bearbeitung von Beschwerden gemäß Artikel 43 Absatz 2 Buchstabe d veröffentlicht werden.

5 ANFORDERUNGEN AN DIE STRUKTUR, ARTIKEL 43 ABSATZ 4 [„ANGEMESSENE“ BEURTEILUNG]

5.1 Organisationsstruktur und oberste Leitung

Die Aufsichtsbehörde kann zusätzliche Anforderungen formulieren.

5.2 Mechanismen zur Sicherung der Unparteilichkeit

Die Aufsichtsbehörde kann zusätzliche Anforderungen formulieren.

6 ANFORDERUNGEN AN RESSOURCEN

6.1 Personal der Zertifizierungsstelle

Die Akkreditierungsstelle muss ergänzend zur Anforderung in Abschnitt 6 der ISO/IEC 17065:2012 für jede Zertifizierungsstelle sicherstellen, dass deren Personal:

1. angemessene und aktuelle Fachkunde (Wissen und Erfahrung) hinsichtlich des Datenschutzes gemäß Artikel 43 Absatz 1 nachweist;
2. über unabhängiges und aktuelles Fachwissen im Hinblick auf den Gegenstand der Zertifizierung gemäß Artikel 43 Absatz 2 Buchstabe a verfügt und kein Interessenkonflikt gemäß Artikel 43 Absatz 2 Buchstabe e besteht;

3. sich dazu verpflichtet, die in Artikel 42 Absatz 5 genannten Kriterien gemäß Artikel 43 Absatz 2 Buchstabe b zu respektieren;
4. über einschlägige und angemessene Kenntnisse und Erfahrungen in der Anwendung von Datenschutzvorschriften verfügt;
5. über relevantes und angemessenes Wissen und einschlägige Erfahrung im Bereich technischer und organisatorischer Datenschutzmaßnahmen verfügt;
6. Erfahrung in den in den zusätzlichen Anforderungen 6.1.1, 6.1.4 und 6.1.5 genannten Bereichen nachweisen kann, insbesondere

Für Personal mit technischer Fachkunde:

- relevantes technisches Fachwissen mit einer Qualifikation, die mindestens dem Niveau 6 des EQR[20] entspricht oder einen anerkannten geschützten Titel (z. B. Dipl.-Ing.) in dem relevanten reglementierten Beruf oder über umfangreiche Berufserfahrung.
- *Für Zertifizierungsmaßnahmen verantwortliches Personal* muss über umfangreiche Erfahrung bei der Ermittlung und Umsetzung von Datenschutzmaßnahmen verfügen.
- *Für Evaluierungen verantwortliches Personal* muss über Berufserfahrung im technischen Datenschutz und Wissen und Erfahrung in ähnlichen Verfahren (z. B. Zertifizierungen/Audits) verfügen und gegebenenfalls registriert sein.

Das Personal muss nachweisen, dass es durch kontinuierliche Weiterbildung sein spezielles Wissen in den Bereichen Technik und Audit pflegt.

Für Personal mit rechtlicher Fachkunde:

- Studium der Rechtswissenschaften an einer EU-Universität oder staatlich anerkannten Universität mit einer Mindestdauer von acht Semestern und dem akademischen Grad Master (LL.M.) bzw. einem vergleichbaren Grad oder umfangreiche Berufserfahrung;
- *Für Zertifizierungsentscheidungen verantwortliches* Personal muss umfangreiche Berufserfahrungen im Datenschutzrecht nachweisen und, falls vom Mitgliedstaat verlangt, registriert sein;
- *Für Evaluierungen verantwortliches Personal* muss mindestens zwei Jahre Berufserfahrung im Datenschutzrecht und Wissen und Erfahrung in ähnlichen Verfahren (z. B. Zertifizierungen/Audits) nachweisen können sowie, falls vom Mitgliedstaat verlangt, registriert sein.
    - Das Personal muss nachweisen, dass es durch kontinuierliche Weiterbildung sein spezielles Wissen in den Bereichen Technik und Audit pflegt.

6.2 Ressourcen für die Evaluierung

Die Aufsichtsbehörde kann im Einklang mit innerstaatlichem Recht zusätzliche Anforderungen formulieren

7 ANFORDERUNGEN AN PROZESSE, ARTIKEL 43 ABSATZ 2 BUCHSTABEN C UND D

7.1 Allgemeines

[20] Siehe Vergleichswerkzeug des Qualifikationsrahmens: https://ec.europa.eu/ploteus/en/compare?

Ergänzend zu der Anforderung in Abschnitt 7.1 der ISO/IEC 17065:2012 muss die Akkreditierungsstelle Folgendes sicherstellen:

1. Die Zertifizierungsstellen erfüllen bei Antragstellung die zusätzlichen Anforderungen der zuständigen Aufsichtsbehörde (gemäß Artikel 43 Absatz 1 Buchstabe b), sodass Aufgaben und Pflichten nicht zu einem Interessenkonflikt gemäß Artikel 43 Absatz 2 Buchstabe b führen.
2. Die zuständigen Aufsichtsbehörden werden benachrichtigt, wenn eine Zertifizierungsstelle ein genehmigtes Europäisches Datenschutzsiegel in einem neuen Mitgliedstaat von einer Außenstelle aus in Betrieb nimmt.

7.2 Antrag

Ergänzend zu Abschnitt 7.2 der ISO/IEC 17065:2012 sollte verlangt werden, dass:

1. der Zertifizierungsgegenstand (Evaluierungsgegenstand, EVG) im Antrag genau beschrieben werden muss. Dies beinhaltet auch Schnittstellen und Übergänge zu anderen Systemen und Organisationen, Protokolle und andere Nachweise;
2. im Antrag festgelegt wird, ob Auftragsverarbeiter eingesetzt werden und falls Auftragsverarbeiter gleichzeitig Antragsteller sind, müssen deren Verantwortlichkeiten und Aufgaben beschrieben werden und der Antrag muss den/die relevanten Vertrag/Verträge (Verantwortlicher/Auftragsverarbeiter) enthalten.

7.3 Antragsbeurteilung

Ergänzend zu Abschnitt 7.3 der ISO/IEC 17065:2012 sollte verlangt werden, dass:

1. in der Zertifizierungsvereinbarung verbindliche Beurteilungsverfahren in Bezug auf den Evaluierungsgegenstand (EVG) festgelegt werden;
2. bei der in Abschnitt 7.3 Buchstabe e beschriebenen Beurteilung der Kompetenz berücksichtigt wird, ob in ausreichendem Maße technisches und rechtliches Fachwissen über den Datenschutz vorhanden ist.

7.4 Evaluierung

Ergänzend zu Abschnitt 7.4 der ISO/IEC 17065:2012 müssen Zertifizierungsmechanismen angemessene Evaluierungsverfahren beschreiben, mit denen beurteilt wird, ob die Verarbeitungsvorgänge mit den Zertifizierungskriterien übereinstimmen, wie beispielsweise:

1. eine Methode, mit der die Notwendigkeit und Angemessenheit von Verarbeitungsvorgängen im Verhältnis zu deren Zweck und den betreffenden Personen beurteilt wird;
2. eine Methode, mit der die Abdeckung, die Zusammensetzung und die Evaluierung sämtlicher von Verantwortlichen und Auftragsverarbeitern berücksichtigter Risiken hinsichtlich der rechtlichen Folgen gemäß den Artikeln 30, 32, 35 und 36 der DSGVO und hinsichtlich der Definition von technischen und organisatorischen Maßnahmen gemäß den Artikeln 24, 25 und 32 der DSGVO beurteilt werden, insofern die vorgenannten Artikel auf den Zertifizierungsgegenstand anzuwenden sind, und
3. eine Methode, mit der Rechtsbehelfe, einschließlich Garantien, Sicherheiten und Verfahren zur Sicherstellung des Schutzes persönlicher Daten im Rahmen der Verarbeitung, die dem Zertifizierungsgegenstand zuzuschreiben ist, beurteilt werden und mit der nachgewiesen wird, dass die in den Kriterien festgelegten rechtlichen Anforderungen eingehalten werden; und
4. Dokumentation über Methoden und Ergebnisse.

Von der Zertifizierungsstelle sollte verlangt werden, sicherzustellen, dass diese Evaluationsmethoden standardisiert und allgemein anwendbar sind. Das bedeutet, dass für vergleichbare Zertifizierungsgegenstände (engl. Targets of Evaluation, ToE) vergleichbare Evaluierungsmethoden angewendet werden. Jegliche Abweichungen von dieser Verfahrensweise sind von der Zertifizierungsstelle zu begründen.

Ergänzend zu Abschnitt 7.4.2 der ISO/IEC 17065:2012 sollte es zulässig sein, dass die Evaluierung von externen, von der Zertifizierungsstelle anerkannten Sachverständigen durchgeführt wird.

Ergänzend zu Punkt 7.4.5 der ISO/IEC 17065:2012 sollte verlangt werden, dass eine datenschutzspezifische Zertifizierung im Einklang mit den Artikeln 42 und 43 der DSGVO, die schon einen Teil eines Zertifizierungsgegenstandes abdeckt, in eine laufende Zertifizierung einbezogen werden kann. Trotzdem genügt es nicht, (Teil-)Evaluierungen vollständig zu übernehmen. Die Zertifizierungsstelle ist verpflichtet, die Einhaltung der Kriterien zu überprüfen. Eine Anerkennung erfordert in jedem Fall einen vollständigen Evaluierungsbericht oder Informationen, durch die eine Beurteilung der früheren Zertifizierungstätigkeiten und deren Ergebnisse ermöglicht werden. Eine Zertifizierungsaussage oder ähnliche Zertifizierungsbescheinigungen sollten nicht als ausreichend angesehen werden, einen Bericht zu ersetzen.

Ergänzend zu Abschnitt 7.4.6 der ISO/IEC 17065:2012 sollte festgelegt werden, dass die Zertifizierungsstelle in ihrem Zertifizierungsmechanismus genau darlegen muss, wie der Kunde (Antragsteller auf Zertifizierung) durch die Informationen, die in Abschnitt 7.4.6 verlangt werden, über Nichtkonformitäten mit einem Zertifizierungsmechanismus informiert wird. In diesem Rahmen sollten zumindest die Art der Informationen und der Zeitpunkt festgelegt werden.

Ergänzend zu Abschnitt 7.4.9 der ISO/IEC 17065:2012 sollte festgelegt werden, dass die Dokumentation der Aufsichtsbehörde für Datenschutz auf Anfrage vollständig zugänglich gemacht werden muss.

7.5 Überprüfung (Review)

Ergänzend zu Abschnitt 7.5 der ISO/IEC 17065:2012 werden Verfahren für die Erteilung, die regelmäßige Überprüfung und den Widerruf der jeweiligen Zertifizierungen gemäß Artikel 43 Absatz 2 und Artikel 43 Absatz 3 verlangt.

7.6 Zertifizierungsentscheidung

Ergänzend zu Abschnitt 7.6.1 der ISO/IEC 17065:2012 sollte die Zertifizierungsstelle verpflichtet werden, in ihren Verfahren genau darzulegen, wie ihre Unabhängigkeit und ihre Zuständigkeit in Bezug auf individuelle Zertifizierungsentscheidungen sichergestellt sind.

7.7 Zertifizierungsdokumentation

Ergänzend zu Abschnitt 7.7.1.e der ISO/IEC 17065:2012 und im Einklang mit Artikel 42 Absatz 7 der DSGVO sollte festgelegt werden, dass Zertifizierungen für eine Höchstdauer von drei Jahren erteilt werden.

Ergänzend zu Abschnitt 7.7.1.e der ISO/IEC 17065:2012 sollte festgelegt werden, dass der Zeitraum der beabsichtigten Überwachung im Sinne von Abschnitt 7.9 auch dokumentiert wird.

Ergänzend zu Abschnitt 7.7.1.f der ISO/IEC 17065:2012 sollte die Zertifizierungsstelle den Zertifizierungsgegenstand in der Zertifizierungsdokumentation benennen (falls zutreffend unter Angabe des Versionsstandes oder ähnlicher Kennzeichen).

7.8 Verzeichnis zertifizierter Produkte

Ergänzend zu Abschnitt 7.8 der ISO/IEC 17065:2012 sollte die Zertifizierungsstelle sicherstellen, dass Informationen zu zertifizierten Produkten, Prozessen und Dienstleistungen intern verfügbar und öffentlich zugänglich bleiben. Die Zertifizierungsstelle wird eine Zusammenfassung des Evaluierungsberichts veröffentlichen. Diese Zusammenfassung soll Transparenz im Hinblick auf das, was zertifiziert wurde und wie es beurteilt wurde, schaffen. Darin wird beispielsweise Folgendes erklärt:

(a) der Geltungsbereich der Zertifizierung und eine aussagekräftige Beschreibung des Evaluierungsgegenstandes (EVG),

(b) die jeweiligen Zertifizierungskriterien (einschließlich Versionsstand oder Funktionsstatus),

(c) die Evaluierungsmethoden und durchgeführten Tests und

(d) das/die Ergebnis/se.

Ergänzend zu Abschnitt 7.8 der ISO/IEC 17065:2012 und gemäß Artikel 43 Absatz 5 der DSGVO muss die Zertifizierungsstelle der zuständigen Aufsichtsbehörde die Gründe für die Erteilung oder den Widerruf der beantragten Zertifizierung mitteilen.

7.9 Überwachung

Ergänzend zu den Abschnitten 7.9.1, 7.9.2 und 7.9.3 der ISO/IEC 17065:2012 und gemäß Artikel 43 Absatz 2 Buchstabe c der DSGVO sind zur Aufrechterhaltung der Zertifizierung regelmäßige Überwachungsmaßnahmen während des Überwachungszeitraums Pflicht.

7.10 Änderungen, die sich auf die Zertifizierung auswirken

Ergänzend zu den Abschnitten 7.10.1 und 7.10.2 der ISO/IEC 17065:2012 gehören zu den die Zertifizierung betreffenden Änderungen, die die Zertifizierungsstelle berücksichtigen muss: Änderungen von Rechtsvorschriften zum Datenschutz, die Annahme delegierter Rechtsakte der Europäischen Kommission im Einklang mit Artikel 43 Absätze 8 und 9, Beschlüsse des Europäischen Datenschutzausschusses und Gerichtsentscheidungen auf dem Gebiet des Datenschutzes. Die Änderungsverfahren, auf die sich geeinigt werden muss, können folgende Punkte beinhalten: Übergangszeiträume, Genehmigungsprozesse der zuständigen Aufsichtsbehörde, Neubeurteilung des jeweiligen Zertifizierungsgegenstandes und angemessene Maßnahmen, um die Zertifizierung zu entziehen, falls die zertifizierten Verarbeitungsvorgänge nicht mehr mit den aktualisierten Kriterien konform sind.

7.11 Beendigung, Einschränkung, Aussetzung oder Zurückziehung der Zertifizierung

Ergänzend zu Abschnitt 7.11.1 der ISO/IEC 17065:2012 sollte die Zertifizierungsstelle verpflichtet sein, die zuständige Aufsichtsbehörde und die nationale Akkreditierungsstelle gegebenenfalls sofort schriftlich über ergriffene Maßnahmen und über Fortführung, Einschränkung, Aussetzung und Widerruf einer Zertifizierung zu informieren.

Gemäß Artikel 58 Absatz 2 Buchstabe h muss die Zertifizierungsstelle Entscheidungen der zuständigen Aufsichtsbehörde akzeptieren, eine Zertifizierung zu widerrufen oder einem Kunden (Antragsteller) keine Zertifizierung zu erteilen, falls die Anforderungen für eine Zertifizierung nicht bzw. nicht mehr erfüllt werden.

7.12 Aufzeichnungen

Die Zertifizierungsstelle sollte sicherstellen, dass die gesamte Dokumentation vollständig, verständlich, auf dem neuesten Stand und prüfungstauglich ist.

7.13 Beschwerden und Einsprüche, Artikel 43 Absatz 2 Buchstabe d

Ergänzend zu Abschnitt 7.13.1 der ISO/IEC 17065:2012 sollte die Zertifizierungsstelle festlegen,

(a) wer Beschwerde oder Widerspruch einlegen kann,

(b) wer diese, seitens der Zertifizierungsstelle, bearbeitet,

(c) welche Überprüfungen in diesem Rahmen stattfinden; und

(d) welche Möglichkeiten der Beratung für die beteiligten Parteien bestehen.

Ergänzend zu Abschnitt 7.13.2 der ISO/IEC 17065:2012 sollte die Zertifizierungsstelle festlegen,

(a) wie und wem eine solche Bestätigung erteilt wird,

(b) welche Fristen hierfür gelten und

(c) welche Maßnahmen danach eingeleitet werden.

Ergänzend zu Abschnitt 7.13.1 der ISO/IEC 17065:2012 muss die Zertifizierungsstelle festlegen, wie eine Trennung zwischen Zertifizierungstätigkeiten und der Bearbeitung von Widersprüchen und Beschwerden gewährleistet wird.

8 MANAGEMENTSYSTEMANFORDERUNGEN

Eine generelle Anforderung des Managementsystems gemäß Abschnitt 8 der ISO/IEC 17065:2012 ist, dass die Umsetzung aller Anforderungen nach Maßgabe der vorgenannten Abschnitte innerhalb des Anwendungsbereichs des Zertifizierungsmechanismus durch die akkreditierte Zertifizierungsstelle unabhängig dokumentiert, evaluiert, gesteuert und überwacht wird.

Das Grundprinzip des Managements ist es, ein System zu definieren, nach dem seine Ziele effektiv und effizient gesetzt werden, nämlich: die Umsetzung der Zertifizierungsdienste - durch geeignete Vorgaben. Dies erfordert Transparenz und Überprüfbarkeit der Umsetzung der Akkreditierungsanforderungen durch die Zertifizierungsstelle und deren permanente Einhaltung.

Dazu muss das Managementsystem eine Methodik für die Einhaltung und Steuerung der Anforderungen im Einklang mit Rechtsvorschriften zum Datenschutz sowie für die kontinuierliche Überprüfung der akkreditierten Stelle festlegen.

Diese Management-Prinzipien und ihre dokumentierte Umsetzung müssen transparent sein und von der akkreditierten Zertifizierungsstelle gemäß Artikel 58 während des Akkreditierungsverfahrens und anschließend jederzeit auf Verlangen der zuständigen Aufsichtsbehörde für Datenschutz während einer Untersuchung in Form von Datenschutzüberprüfungen und gemäß Artikel 58 Absatz 1 Buchstabe b oder einer Prüfung der im Einklang mit Artikel 42 Absatz 7 und gemäß Artikel 58 Absatz 1 Buchstabe c erteilten Zertifizierungen offengelegt werden.

Insbesondere muss die akkreditierte Zertifizierungsstelle dauerhaft und kontinuierlich bekannt geben, welche Zertifizierungen auf welcher Grundlage (oder Zertifizierungsmechanismen oder Zertifizierungssysteme), durchgeführt wurden und wie lange die Zertifizierungen unter welchen Rahmenbedingungen (Erwägungsgrund 100) gültig sind.

8.1 Optionen

Die zuständige Aufsichtsbehörde kann weitere zusätzliche Anforderungen festlegen und hinzufügen, wenn diese im Einklang mit innerstaatlichem Recht stehen.

8.2 Allgemeine Managementsystem-Dokumentation

Die zuständige Aufsichtsbehörde kann weitere zusätzliche Anforderungen festlegen und hinzufügen, wenn diese im Einklang mit innerstaatlichem Recht stehen.

8.3 Lenkung von Dokumenten

Die zuständige Aufsichtsbehörde kann weitere zusätzliche Anforderungen festlegen und hinzufügen, wenn diese im Einklang mit innerstaatlichem Recht stehen.

8.4 Lenkung von Aufzeichnungen

Die zuständige Aufsichtsbehörde kann weitere zusätzliche Anforderungen festlegen und hinzufügen, wenn diese im Einklang mit innerstaatlichem Recht stehen.

8.5 Managementprüfung

Die zuständige Aufsichtsbehörde kann weitere zusätzliche Anforderungen festlegen und hinzufügen, wenn diese im Einklang mit innerstaatlichem Recht stehen.

8.6 Interne Audits

Die zuständige Aufsichtsbehörde kann weitere zusätzliche Anforderungen festlegen und hinzufügen, wenn diese im Einklang mit innerstaatlichem Recht stehen.

8.7 Korrekturmaßnahmen

Die zuständige Aufsichtsbehörde kann weitere zusätzliche Anforderungen festlegen und hinzufügen, wenn diese im Einklang mit innerstaatlichem Recht stehen.

8.8 Vorbeugende Maßnahmen

Die zuständige Aufsichtsbehörde kann weitere zusätzliche Anforderungen festlegen und hinzufügen, wenn diese im Einklang mit innerstaatlichem Recht stehen.

9 WEITERE ZUSÄTZLICHE ANFORDERUNGEN21

9.1 Aktualisierung von Evaluierungsmethoden

Die Zertifizierungsstelle muss Verfahren festlegen, die die Aktualisierung von Evaluierungsmethoden für die Evaluierung nach Maßgabe von Abschnitt 7.4 vorgeben. Die Aktualisierung muss im Zuge von Änderungen des Rechtsrahmens, der relevanten Risiken, des Stands der Technik und der Kosten für die Umsetzung von technischen und organisatorischen Maßnahmen stattfinden.

9.2 Fachwissen pflegen

Zertifizierungsstellen müssen Verfahren entwickeln, um die dauerhafte Schulung ihrer Angestellten zu gewährleisten, damit deren Fähigkeiten auf dem neuesten Stand bleiben, wobei die in Abschnitt 9.1 aufgeführten Entwicklungen zu berücksichtigen sind.

9.3 Pflichten und Kompetenzen

9.3.1 Kommunikation zwischen der Zertifizierungsstelle und deren Kunden

Entsprechende Verfahren müssen angemessene Abläufe und Kommunikationsstrukturen zwischen der Zertifizierungsstelle und deren Kunden gewährleisten. Dazu gehören

[21] Die zuständige Aufsichtsbehörde kann weitere zusätzliche Anforderungen festlegen und hinzufügen, wenn diese im Einklang mit innerstaatlichem Recht stehen.

1. die Pflege der Dokumentation über Aufgaben und Zuständigkeiten durch die akkreditierte Zertifizierungsstelle zum Zwecke von
    a. Informationsanfragen oder
    b. zur Kontaktaufnahme im Falle einer Beschwerde gegen eine Zertifizierung;
2. die Pflege des Antragsverfahrens im Hinblick auf
    a. die Information über den aktuellen Stand des Antrags;
    b. Evaluierungen durch die zuständige Aufsichtsbehörde auf der Grundlage von
        i. Rückmeldungen;
        ii. Entscheidungen der zuständigen Aufsichtsbehörde.

9.3.2 Dokumentation der Evaluierungstätigkeiten

Die Aufsichtsbehörde kann zusätzliche Anforderungen formulieren.

9.3.3 Bearbeitung von Beschwerden

Fester Bestandteil des Managementsystems sollte ein Beschwerdeverfahren sein, mit dem insbesondere die Anforderungen der Abschnitte 4.1.2.2 Buchstabe c, 4.1.2.2 Buchstabe j, 4.6 Buchstabe d und 7.13 der ISO/IEC 17065:2012 umgesetzt werden.

Beschwerden und Einsprüche sollten der zuständigen Aufsichtsbehörde mitgeteilt werden.

9.3.4 Widerrufsbearbeitung

Die Vorgehensweise im Falle einer Aussetzung oder eines Widerrufs der Akkreditierung muss in das Managementsystem der Zertifizierungsstelle integriert werden, einschließlich der Mitteilungen an Kunden.