Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i.V.m. DIN EN ISO/IEC 17065

Version 1.0 (28.08.2018)[1]

Vorwort

Im Folgenden werden die Vorgaben der DIN EN ISO/IEC 17065 aufgrund von Art. 43 Abs. 3 DS-GVO i.V.m. Art. 57 Abs. 1 lit. p DS-GVO durch die deutschen Datenschutz-Aufsichtsbehörden ergänzt und konkretisiert.
Zu berücksichtigen sind die spezifischen datenschutzrechtlichen Vorgaben aus Art. 42, 43 DS-GVO sowie die Anforderungen aus der DIN EN ISO/IEC 17065.

Die DAkkS akkreditiert als Akkreditierungsstelle die Zertifizierungsstellen gemeinsam mit der zuständigen Datenschutzaufsichtsbehörde. Die zuständige Datenschutzaufsichtsbehörde erteilt der Zertifizierungsstelle in einem eigenständigen Verfahren auf Grundlage dieser gemeinsamen Akkreditierung die Befugnis als solche tätig werden zu dürfen.

Der Antrag auf Akkreditierung wird schriftlich bei der DAkkS gestellt. Dort steht ein entsprechendes Formular bereit. Die DAkkS informiert umgehend die zuständige Aufsichtsbehörde über den Antrag und übermittelt ihr die entsprechenden Unterlagen.

Die Zertifizierungsstelle zertifiziert Produkte, Prozesse und Dienstleistungen ihrer Kunden, sofern es sich um Verarbeitungsvorgänge im Sinne der DS-GVO handelt.

Zur Vorbereitung der Akkreditierung muss die Zertifizierungsstelle oder der Programmeigner ein Zertifizierungsprogramm erstellen und durch die DAkkS gemäß DIN EN ISO/IEC 17011 auf Eignung prüfen lassen (vgl. DAkkS-Regel 71 SD 0016). Dieses Zertifizierungsprogramm enthält als wesentlichen Teil die Zertifizierungskriterien zur Umsetzung der datenschutzrechtlichen Anforderungen, die gemäß Art. 57 Abs. 1 lit. n DS-GVO i.V.m. Art. 42 Abs. 5 DS-GVO entweder von der zuständigen Datenschutzaufsichtsbehörde genehmigt werden oder (i.d.R. über die zuständige Aufsichtsbehörde) dem Europäischen Datenschutzausschuss zur Genehmigung bzw. Billigung gemäß Art. 63, 64 Abs. 1 lit. c DS-GVO zu übermitteln sind.

Werden die Kriterien gemäß Art. 57 Abs. 1 lit. n DS-GVO i.V.m. Art. 42 Abs. 5 DS-GVO nur von der zuständigen Datenschutzaufsichtsbehörde genehmigt, so übermittelt sie diese Kriterien gemäß Art. 43 Abs. 6 Satz 2 DS-GVO dem Europäischen Datenschutzausschuss.

Die Zertifizierungsprogramme einschließlich der genehmigten Kriterien nach Art. 42 Abs. 5 DS-GVO werden in der Programmdatenbank auf www.dakks.de veröffentlicht.

[1] Diese Version des Papiers stellt lediglich eine vorläufige Fassung dar. Es steht noch die Stellungnahme des Europäischen Datenschutzausschusses hierzu aus (vgl. Art. 64 Absatz 1 Buchstabe c) DS-GVO).

Hinsichtlich der Vorgaben für diese Kriterien wird auf das Dokument „Guidelines 1/2018 on certification and identifying certification criteria in accordance with Art 42 and 43 of the Regulation 2016/679“ vom 25.05.2018 verwiesen.

Geltungsbereiche der Akkreditierung (Scopes)

Es werden in diesem Dokument keine Geltungsbereiche (Scopes) für die Akkreditierung von Zertifizierungsstellen vorgegeben. Die Zertifizierungsstellen müssen jedoch mit Stellung des Antrags auf Programmprüfung den Anwendungsbereich des Zertifizierungsprogramms festlegen und genau beschreiben. Das Zertifizierungsprogramm legt auch die erforderliche Berufserfahrung und Fachkunde der Auditoren für die festgelegten Anwendungsbereiche fest.

Geltungsdauer der Akkreditierung

Die Akkreditierung wird gemäß Art 43 Abs. 3 DS-GVO auf längstens fünf Jahre befristet.

I. Kapitel 3: Begriffe

Zu 3.4 Produkt, 3.5 Prozess und 3.6 Dienstleistung (Zertifizierungsgegenstand)

Zulässig sind Zertifizierungsprogramme, die als Gegenstand der Zertifizierung Verarbeitungsvorgänge betrachten, die in Produkten, Prozessen und Dienstleistungen oder mit Hilfe von (auch mehreren) Produkten und Dienstleistungen erbracht werden und die dem Verantwortlichen oder dem Auftragsverarbeiter gegenüber die Konformität mit den Vorgaben der DS-GVO unmittelbar oder mittelbar bestätigen.

Der Gegenstand der Zertifizierung muss den Anforderungen der DIN EN ISO/IEC DIN 17065 entsprechen. Damit sind Managementsysteme für die Steuerung von Datenverarbeitungsvorgängen als Gegenstand der Zertifizierung ausgeschlossen. Managementsysteme finden unter den Bedingungen gemäß Kapitel 7, Tz. 7.4, als Teil eines Zertifizierungsmechanismuses Berücksichtigung. Auch muss sich der Zertifizierungsgegenstand auf Datenverarbeitungsvorgänge beziehen.

II. Kapitel 4: Allgemeine Anforderungen

Zu 4.1 Rechtliche und vertragliche Angelegenheiten

Zu 4.1.2.2 Zertifizierungsvereinbarung

Die Mindestanforderungen für eine Zertifizierungsvereinbarung (Vertrag zwischen Zertifizierungsstelle und Kunde) sind um folgende Punkte zu ergänzen:

1. Die Verpflichtung des Kunden, die allgemeinen Zertifizierungsanforderungen im Sinne des 4.1.2.2 lit. a stets zu erfüllen, muss (gleichsam der Regelung für Zertifizierungsstellen des Art. 43 Abs. 2 lit. b i. V. m. Art. 42 Abs. 5 DS-GVO) auch die Zertifizierungskriterien umfassen, die von der zuständigen Datenschutzaufsichtsbehörde oder dem Ausschuss genehmigt bzw. gebilligt wurden.
2. Die Verpflichtung des Kunden, notwendige Vorkehrungen für die Evaluierung und Überwachung im Sinne des 4.1.2.2 lit. c Nr. 1 zu treffen, muss (gleichsam der Regelung für Zertifizierungsstellen des Art. 43 Abs. 2 lit. c DS-GVO) auch Regelungen enthalten, die angemessene Abstände für eine erneute Evaluierung oder Überprüfung festlegen (Regelmäßigkeit).
3. Die Verpflichtung des Kunden, notwendige Vorkehrungen für die Untersuchung von Beschwerden zu treffen im Sinne des 4.1.2.2 lit. c Nr. 2 und lit. j, muss (gleichsam der Regelung für Zertifizierungsstellen des Art. 43 Abs. 2 lit. d DS-GVO) auch konkrete Ausführungen zur Struktur und dem Verfahren für das Beschwerdemanagement enthalten und diese müssen im Management der Zertifizierungsstelle integriert sein.
4. Zusätzlich zu den in 4.1.2.2 genannten Mindestanforderungen sind auch die Folgen der Aussetzung oder Zurückziehung der Akkreditierung in der Verpflichtung zu regeln. Die Folgen der Aussetzung oder der Zurückziehung der Akkreditierung ergeben sich aus Punkt 8.3.2 lit. e der DIN EN ISO/IEC 17011:2004 und Punkt M.8.3.2.1 des IAF/ILAC A5:11/2013. Die Zurückziehung einer Akkreditierung hat Konsequenzen für die Kunden der Zertifizierungsstelle. Deshalb ist in der Zertifizierungsvereinbarung darauf hinzuweisen und verbindlich zu regeln, dass die Zertifizierung des Kunden abhängig von der Akkreditierung der Zertifizierungsstelle ist. Die Aussetzung oder Zurückziehung (Erlöschen bzw. Widerruf) der Akkreditierung führt zur Ungültigkeit der Zertifizierung. Entsprechende Verfahren sind im Management der Zertifizierungsstelle zu integrieren.

   Zusätzlich zu den in 4.1.2.2 genannten Mindestanforderungen ist auch der Transfer von Zertifizierungen bei Erlöschen der Akkreditierung im Sinne der Art. 43 DS-GVO in der Verpflichtung zu regeln.

   Im Falle der Einstellung oder des Verzichts begutachtet die DAkkS bei der aufnehmenden Zertifizierungsstelle, ob der Transfer der Zertifizierung regelkonform abläuft. Auch dieses ist in der Verpflichtung zu regeln.
5. Zusätzlich zu den in 4.1.2.2 genannten Mindestanforderungen ist auch die Einhaltung von Fristen und Verfahrensabläufen zu regeln. In der Zertifizierungsvereinbarung ist zu regeln, dass Fristen und Verfahrensabläufe, die sich beispielsweise aus dem Zertifizierungsprogramm oder anderen Vorschriften ergeben, zwingend zu beachten und einzuhalten sind.
6. Zusätzlich zu den in 4.1.2.2 lit. k genannten Mindestanforderungen ist auch eine Hinweispflicht bei Änderungen der tatsächlichen oder rechtlichen Verhältnisse zu regeln. Es ist zu vereinbaren, dass die Kunden eine Hinweispflicht bei maßgeblichen Änderungen in den tatsächlichen oder rechtlichen Verhältnissen trifft. Die

Zertifizierungsstelle ist bei Hinweisen über solche Änderungen, die Einfluss auf die Konformitätsbewertungsaussage haben könnten verpflichtet, den Sachverhalt innerhalb von 4 Wochen zu ermitteln und geeignete Maßnahmen zu ergreifen.

7. Ergänzend zu Punkt 4.1.2.2 der DIN EN ISO/IEC 17065 wird die erwartete Verfahrensdauer zwischen den Beteiligten abgestimmt und vertraglich festgehalten.

Zu 4.2 Handhabung der Unparteilichkeit

Die Unparteilichkeit der Zertifizierungsstelle ist gemäß 3.13 DIN EN ISO/IEC 17065 nur dann gegeben, wenn Unabhängigkeit und Objektivität gewährleistet sind. Interessenkonflikte dürfen nicht existieren. Andernfalls ist die Durchführung der Tätigkeit nicht möglich.

Die DS-GVO trifft in den Art. 43 Abs. 2 lit. a und e gesonderte Regelungen zum Nachweis über die Unabhängigkeit bzw. das Fehlen von Interessenkonflikten. Die Regeln der DIN EN ISO/IEC DIN 17065 sind, wie folgt, zu ergänzen:

Zu 4.2.1

Unparteilichkeit in diesem Sinne ist nur dann gegeben, wenn die folgenden zusätzlichen Anforderungen erfüllt sind:

1. Im Einklang mit Art. 43 Abs. 2 lit. a DS-GVO sind der zuständigen Datenschutzaufsichtsbehörde gesonderte Nachweise über das Merkmal der Unabhängigkeit vorzulegen. Dies gilt insbesondere für die Nachweise über die Finanzierung der Zertifizierungsstelle, soweit sie die Sicherstellung der Unparteilichkeit betreffen.
2. Entsprechend Art. 43 Abs. 2 lit. e DS-GVO muss die Zertifizierungsstelle der zuständigen Datenschutzaufsichtsbehörde zudem nachgewiesen haben, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen. Solche Konflikte könnten sich z. B. durch eine hohe Umsatzabhängigkeit von Kunden oder sonstigen wirtschaftlichen Druck auf die Zertifizierungsstelle ergeben.
3. Im Einklang mit der DIN EN ISO/IEC 17065 muss die Zertifizierungsstelle darüber hinaus eine dritte Seite im Sinne der DIN EN ISO/IEC DIN 17000:2005 sein. Eine dritte Seite ist eine Stelle, die ein unabhängiger Dritter ist, die den Zertifizierungsgegenstand prüft und von Interessen als Anwender dieses Gegenstandes unabhängig ist. Gemäß Artikel R 17 Abs. 3 S. 1 des Beschlusses Nr. 768/2008/EG muss es sich bei einer Zertifizierungsstelle um einen unabhängigen Dritten handeln, der mit der Einrichtung, die er bewertet, in keinerlei Verbindung steht. Nach Absatz 4 des Artikels R 17 dürfen eine Zertifizierungsstelle, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter nicht Konstrukteur, Hersteller, Lieferant, Installateur, Käufer, Eigentümer, Verwender oder Wartungsbetrieb der zu bewertenden Produkte oder Bevollmächtigter einer dieser Parteien sein, sofern diese Verbindung aufgrund geringer Erheblichkeit die Unparteilichkeit nicht in Frage stellt. Deswegen ist die notwendige Unparteilichkeit und Trennung der beteiligten Stellen sicherzustellen und zu dokumentieren. Keine dritte Seite ist eine Stelle, die Verträge mit den Zertifizierungskunden schließt. Somit können insbesondere Vergabestellen und Auftraggeber sowie deren Organisationen, die Vertragspartner sind oder sein können, nicht selbst Zertifizierungsstelle sein. Bei der Herbeiführung einer rechtlichen Trennung der Zertifizierungsstelle von einer solchen Organisation, gilt der nachfolgende Punkt.

Zu 4.2.7

Gemäß Punkt 4.2.7 der DIN EN ISO/IEC 17065 muss die Zertifizierungsstelle sicherstellen, dass Tätigkeiten rechtlich getrennter juristischer Personen, mit denen die Zertifizierungsstelle oder die juristische Person, der sie angehört, Beziehungen hat, die Unparteilichkeit ihrer Zertifizierungstätigkeiten nicht beeinträchtigen. Eine Zertifizierungsstelle, die einer juristischen Person (z. B. Verband oder eine Körperschaft des öffentlichen Rechts) angehört oder von einer juristischen Person kontrolliert wird oder sonstige Beziehungen zu einer juristischen Person hat, deren Mitglieder oder Anteilseigner Hersteller, Anbieter, Auftragsverarbeiter oder Verantwortliche sind, die von dieser Zertifizierungsstelle zertifiziert werden, kann nur dann als unabhängige dritte Stelle gelten, wenn ihre Unabhängigkeit entsprechend Art. 43 Abs. 2 lit. a DS-GVO bzw. Unparteilichkeiten entsprechend 3.13 der DIN EN ISO/IEC 17065 sowie die Abwesenheit jedweder Interessenkonflikte nachgewiesen ist. Dies kann der Fall sein, wenn

1. die Zertifizierungsstelle rechtlich von der juristischen Person getrennt ist und
2. das Personal der Zertifizierungsstelle und der juristischen Person getrennt sind und in keiner Weise für die Zertifizierungsstelle, insbesondere in Zertifizierungs-,Prüf- und Inspektionsverfahren, tätig wird (siehe nur 4.2.8 der DIN EN ISO/IEC 17065:2013) und
3. die oberste Leitung der Zertifizierungsstelle sich im Gesellschaftervertrag oder in der Satzung der Zertifizierungsstelle im Sinne des Punktes 4.2.5 der DIN EN ISO/IEC 17065 zur Unparteilichkeit verpflichtet und
4. wenn die Satzung oder der Gesellschaftervertrag einen Passus zur Weisungsunabhängigkeit des Geschäftsführers und/oder des Leiters der Zertifizierungsstelle enthält und
5. in Konkretisierung des Punktes 4.2.2 der DIN EN ISO/IEC 17065 kein wirtschaftliches Abhängigkeitsverhältnis zu den Mitgliedern der juristischen Person oder der juristischen Person selbst besteht.

Zu 4.3 Haftung und Finanzierung

In Ergänzung zu den Ausführungen zur Haftung und Finanzierung in 4.3 sind darüber hinaus auch die Anforderungen aus 5.3.2 der DIN EN ISO/IEC 17021 zu beachten:
Die Zertifizierungsstelle muss darlegen können, dass sie die Risiken, die aus ihren Zertifizierungstätigkeiten entstehen, beurteilt hat und dass sie über geeignete Maßnahmen verfügt (z. B. Versicherungen oder Rücklagen), um in den geographischen Regionen, in denen sie tätig ist, die Verbindlichkeiten abzudecken, die aus ihren Tätigkeitsfeldern entstehen. Die Zertifizierungsstelle hat ihre finanzielle Stabilität und Unabhängigkeit nachzuweisen. Die Entscheidung hinsichtlich Auswahl und Benennung dieser Nachweisunterlagen liegt im Ermessen der DAkkS und der zuständigen Datenschutzaufsichtsbehörde. Die Zertifizierungsstelle muss über eine für den Umfang ihrer Tätigkeit angemessene Vermögensschadenshaftpflichtversicherung verfügen. Die Berechnung der notwendigen Deckung hat auf einer Risikobetrachtung der Zertifizierungsstelle zu basieren.

Zu 4.6 Öffentlich zugängliche Informationen

Die Informationen zum Umgang mit Beschwerden und Einsprüchen im Sinne des 4.6. lit. d sind im Einklang mit Art. 43 Abs. 2 lit. d DS-GVO von der Zertifizierungsstelle generell zu veröffentlichen. Dabei bezieht sich diese Veröffentlichungspflicht nicht nur auf einzelne Vorkommnisse, sondern auch auf die Struktur und Verfahrensweise zur Bearbeitung der Beschwerden durch die Zertifizierungsstelle.

Gemäß Art 42 Abs. 3 DS-GVO sind ergänzend zu 4.6 lit. a neben den Informationen über die von der Zertifizierungsstelle verwendeten Zertifizierungsprogramme, die genehmigten Kriterien im Sinne des Art. 42 Abs. 5 DS-GVO generell unter Angabe des jeweiligen Verwendungszeitraums zu veröffentlichen. Die Form der Veröffentlichung sollte geeignet sein, die Öffentlichkeit möglichst umfassend zu erreichen. Dies ist in der Regel durch die elektronische Form gewährleistet.

III. Kapitel 5: Anforderungen an die Struktur

Die Unparteilichkeit der Zertifizierungsstelle ist gemäß 3.13 DIN EN ISO/IEC 17065 nur dann gegeben, wenn Unabhängigkeit und Objektivität gewährleistet sind. Ergänzend zu Kapitel 5.2 (Kapitel 5.1.1 und 5.2) der DIN EN ISO/IEC 17065, muss die Zertifizierungsstelle zur Zufriedenheit der zuständigen Datenschutzaufsichtsbehörde im Rahmen des Akkreditierungsverfahrens nachweisen, dass der Mechanismus zur Gewährleistung der Unabhängigkeit den Anforderungen des Art. 43 Abs. 2 lit. a und e DS-GVO genügt und deren Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen. Unabhängigkeit bedeutet, dass die betreffende Stelle völlig frei von Weisungen und Druck handeln kann und deren finanzielle Stabilität sichergestellt ist.

IV. Kapitel 6: Anforderungen an Ressourcen

Ergänzend zu Kapitel 6 der DIN EN ISO/IEC 17065 muss die Zertifizierungsstelle das Folgende gemäß der DS-GVO nachweisen können, um als Zertifizierungsstelle akkreditiert zu werden:

1. Geeignetes Fachwissen hinsichtlich des Datenschutzes (Art. 43 Abs. 1 DS-GVO)
2. Unabhängigkeit und Fachwissen hinsichtlich des Zertifizierungsgegenstands (Art. 43 Abs. 2 DS-GVO)

Zu 6.1.2.1 Personalkompetenz

Die Zertifizierungsstelle muss über Ressourcen mit Kenntnissen in folgenden Bereichen verfügen und diese nachweisen können:

1. Kenntnisse der relevanten Normen zur Konformitätsbewertung (insbesondere ISO-Normen, Gesetze etc.)
2. Kenntnisse in den für den Zertifizierungsbereich relevanten Managementsystemen (beispielsweise ISO 9001 /27001 /27017 /27018 / IT-Grundschutz)
3. Kenntnisse im Datenschutzrecht (DS-GVO/BDSG/einschlägige Landesdatenschutzgesetze)
4. Kenntnisse im Telekommunikationsrecht sowie dem Recht der Dienste der Informationsgesellschaft bzw. der ePrivacy-Verordnung
5. Ggf. Kenntnisse in weiteren relevante Datenschutznormen, deren Einschlägigkeit sich aus dem eingesetzten Zertifizierungsprogramm ergibt.

Des Weiteren müssen Kenntnisse und Erfahrungen im technischen und organisatorischen Datenschutz vorhanden und nachgewiesen werden, insbesondere zu den im Anhang 3 genannten Bereichen, soweit sie für das eingesetzte Zertifizierungsprogramm relevant sind.

Das für die Evaluierung und Entscheidung verantwortliche Personal muss ein in der Bundesrepublik Deutschland anerkanntes, einschlägiges Hochschulstudium abgeschlossen haben.

Dabei müssen sowohl die rechtliche als auch technische Fachkunde beim verantwortlichen Personal vorhanden sein, jedoch nicht zwingend in einer Person.

Konkret müssen folgende Voraussetzungen erfüllt sein und nachgewiesen werden:

Technisch (zusätzlich zu Ziffer 1 muss Ziffer 2 oder 3 erfüllt sein):

1. Mindestens achtsemestrige Regelstudienzeit an einer deutschen staatlichen oder staatlich anerkannten Hochschule, welche überwiegend von den Fächern Informatik, Naturwissenschaften, Technik, Mathematik geprägt ist oder entsprechend IT-Prüfungswesen umfasst, und wonach mindestens der akademische Grad des Diploms oder Masters oder eines vergleichbaren Abschlusses getragen werden darf oder wenn durch die zuständige Stelle das Recht verliehen worden ist, die Bezeichnung „Ingenieurin“ oder „Ingenieur“ zu führen.
2. Für Entscheider ist eine Berufserfahrung von mindestens fünf Jahren im technischen Datenschutz erforderlich.
3. Für Evaluatoren sind eine Berufserfahrung von mindestens zwei Jahren im technischen Datenschutz und Kenntnisse und Erfahrungen im Prüfverfahren (z. B. Zertifizierungen/Auditierungen) erforderlich.

Rechtlich (zusätzlich zu Ziffer 1 muss Ziffer 2 oder 3 erfüllt sein):

1. Die juristische Kompetenz besitzt, wer aufgrund eines mindestens achtsemestrigen Studiums an einer deutschen staatlichen oder staatlich anerkannten Hochschule Rechtswissenschaften studiert und den akademischen Grad Master (LL.M.) oder das 1. Juristische Staatsexamen erworben hat.
2. Für Entscheider ist eine Berufserfahrung von mindestens fünf Jahren im Datenschutzrecht erforderlich.
3. Für Evaluatoren sind eine Berufserfahrung von mindestens zwei Jahren im Datenschutzrecht und Kenntnisse sowie Erfahrungen in Prüfverfahren (z. B. Zertifizierungen/Auditierungen) erforderlich.

Um die Kompetenz der zu akkreditierenden Stelle bewerten zu können, wird im Akkreditierungsverfahren zusätzlich zu den schriftlich vorgelegten Unterlagen auf eine begleitende Begutachtung (Witnessing-Model/siehe Anlage 2) zurückgegriffen.

Die Kenntnisse des Personals für Evaluierung und Entscheidung müssen auf aktuellem Stand gehalten werden. Ein Nachweis der Kenntnisse kann durch Fortbildungsbescheinigungen, einschlägige Arbeitserfahrung (z. B. durchgeführte Zertifizierungsverfahren) oder auf eine andere Art zur Zufriedenheit der zuständigen Datenschutzaufsichtsbehörde im Akkreditierungsverfahren bzw. den Überwachungsbegutachtungen der akkreditierten Zertifizierungsstelle nachgewiesen werden.

Für die Bewertung der Gleichwertigkeit ausländischer Abschlüsse sind die Nachweise gemäß der Richtlinie 2013/55/EU über die Anerkennung von Berufsqualifikationen (ABl. L 354 vom 28.12.2013, S. 132-170) in Verbindung mit der Richtlinie 2006/100/EG vom 20.11.2006 maßgeblich.

Zu 6.2.2

Werden Evaluierungstätigkeiten an externe Stellen ausgegliedert, so gelten für diese Stellen die gleichen Voraussetzungen wie für die Zertifizierungsstelle. Insbesondere sind diese datenschutzspezifischen Anforderungen durch die unterbeauftragte Stelle zu beachten.

V. Kapitel 7: Anforderungen an Prozesse

Zu 7.1 Allgemeines

Die Zertifizierungskriterien sind Teil des Zertifizierungsprogramms.

Das genehmigte Zertifizierungsprogramm muss die geplanten Evaluationsmethoden (siehe Ausführungen zu 7.4) enthalten. Es wird hierzu auf Kapitel 3.9 der DIN EN ISO/IEC 17065 verwiesen.

Zu 7.2 Antrag

Ergänzend zu Punkt 7.2 der DIN EN ISO/IEC 17065 muss der Kunde im Antrag den Zertifizierungsgegenstand genau beschreiben. Dies beinhaltet auch die Darstellung der Schnittstellen bzw. Übergänge zu anderen Systemen und Organisationen. Hierbei sind auch die zugrundeliegenden Protokolle und sonstige Zusicherungen darzulegen. Werden Auftragsverarbeiter zur Abwicklung der Datenverarbeitungsvorgänge des Zertifizierungsgegenstandes eingesetzt, so sind diese im Antrag inkl. der von ihnen übernommenen Zuständigkeiten und damit verbundenen Aufgaben zu benennen.

Antragsberechtigt für eine Zertifizierung sind der für die Datenverarbeitung Verantwortliche und der Auftragsverarbeiter.

Zu 7.3 Antragsbewertung

Ergänzend zu Punkt 7.3.1 lit. b der DIN EN ISO/IEC 17065 werden im Rahmen der Antragsbewertung zwischen dem Antragsteller und der Zertifizierungsstelle die geplanten Evaluationsmethoden unter Berücksichtigung des auf den Kunden anwendbaren Datenschutzrechts vertraglich in der Zertifizierungsvereinbarung festgehalten.

Die Überwachung der Verträge nach 4.1.2.2 muss Bestandteil des Managements der Zertifizierungsstelle sein.

Der Zeitraum zwischen dem Abschluss der letzten Evaluierung und der Zertifizierungsentscheidung darf nur in berechtigten Ausnahmefällen die Dauer von 3 Monaten überschreiten.

Ergänzend zu Punkt 7.3.3 der DIN EN ISO/IEC 17065 muss die Zertifizierungsstelle darlegen, dass trotz fehlender Erfahrung mit dem Zertifizierungsgegenstand, dem Geltungsbereich oder dem Kundentyp sowohl eine technische als auch rechtliche Kompetenz in angemessenem Umfang für die Zertifizierungstätigkeiten des Einzelauftrages besteht

Zu 7.4 Evaluierung

Ergänzend zu Punkt 7.4.1 der DIN EN ISO/IEC 17065 werden die im Zertifizierungsprogramm festgehaltenen Evaluationsmethoden von der Zertifizierungsstelle im Rahmen der Zertifizierung umgesetzt.

Die geeigneten Evaluationsmethoden müssen insbesondere folgende Bereiche abdecken:

1. eine Methode zur Bewertung der Notwendigkeit und Verhältnismäßigkeit von Verarbeitungsvorgängen in Bezug auf ihren Zweck,

2. eine Methode zur Bewertung der Zusammenstellung und Einschätzung aller Risiken, die von dem Verantwortlichen und ggf. Auftragnehmer betrachtet werden im Hinblick auf Art. 5 DS-GVO, die Rechtsfolgen nach Art. 30, 32, 35 und 36 DS-GVO sowie die Festlegung von technischen und organisatorischen Maßnahmen gemäß Art. 24, 25, und 32 DS-GVO, soweit die genannten gesetzlichen Normen auf den Zertifizierungsgegenstand Anwendung finden, und
3. eine Methode zur Bewertung der Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten im Rahmen der dem Zertifizierungsgegenstand zuzurechnenden Verarbeitungen sichergestellt und der Nachweis erbracht wird, dass die gesetzlichen Anforderungen erfüllt werden.

Die Zertifizierungsstelle hat sicherzustellen, dass diese Evaluationsmethoden validiert sind. Das heißt, dass in vergleichbaren Verfahren auch vergleichbare Evaluationsmethoden Anwendung finden und zu vergleichbaren Ergebnissen führen. Dieser Nachweis ist innerhalb der Programmprüfung bei der Akkreditierungsstelle zu führen.

Ergänzend zu Punkt 7.4.4 der DIN EN ISO/IEC 17065 kann die Evaluierung durch zuvor von der Zertifizierungsstelle anerkannte entsprechend fachkundige externe Evaluatoren erfolgen.

Für die rechtlichen und tatsächlichen Verhältnisse dieser externen Evaluatoren zur Zertifizierungsstelle gelten die Regelungen von Kapitel 6 der DIN EN ISO/IEC 17065 unter Beachtung der o.g. Regelungen.

Ergänzend zu Punkt 7.4.3 der DIN EN ISO/IEC 17065 kann die Zertifizierungsstelle im Verlaufe des Zertifizierungsverfahrens weitere, aus ihrer Sicht für die Zertifizierung notwendige Informationen und/oder Dokumentationen anfordern. Die Zertifizierungsstelle hat das Recht, das Zertifizierungsverfahren abzubrechen, sofern der Antragssteller der Pflicht zur Beibringung dieser Informationen und/oder Dokumentationen nicht nachkommt.

Ergänzend zu Punkt 7.4.5 der DIN EN ISO/IEC 17065 hat die Zertifizierungsstelle im Rahmen ihrer Kriterien zu definieren, welchen Stellenwert andere Zertifizierungen des Kunden (z. B. IT-Grundschutz, DIN EN ISO/IEC 27001/27002) für ihre Evaluierung einnehmen. Es ist darzulegen, welche Zertifizierungen als Evaluierung berücksichtigt werden können, wie und in welchem Umfang dies der Fall ist und welche Auswirkungen dies konkret auf den verbleibenden Evaluationsumfang und die Evaluationsmethoden hat. Gemäß 7.4.5. müssen diese Evaluierungen vor Antragstellung des Kunden abgeschlossen sein und durch eine Konformitätsbewertungsstelle durchgeführt worden sein, welche die Anforderungen an die Gleichwertigkeit nach Tz. 6.2.2.1 DIN EN ISO/IEC 17065 erfüllt.

Bestehende Zertifizierungen können insbesondere, wie folgt, Berücksichtigung finden:

1. Eine erfolgte Datenschutzzertifizierung nach Art. 42 DS-GVO durch eine akkreditierte Zertifizierungsstelle, die bereits einen Teil des Zertifizierungsgegenstands abdeckt, kann als Teilevaluierung berücksichtigt werden.
2. Erfolgte Datenschutzzertifizierungen nach Art. 42 DS-GVO sind jedoch nicht ausreichend, um (Teil-)Evaluationen vollständig zu ersetzen. Die Zertifizierungsstelle ist weiterhin verpflichtet die aktuelle Einhaltung der Anforderungen (der vorgelegten Zertifizierung) zumindest stichprobenartig zu überprüfen und bestehende Zertifizierungen zu bewerten. Auswirkungen auf die Gültigkeitsdauer der eingebrachten Zertifizierung ergeben sich nicht.
3. Andere durch eine akkreditierte Zertifizierungsstelle erteilte Zertifizierungen als solche nach Art. 42 DS-GVO (z. B. ISO Zertifizierungen) können ebenfalls einen Faktor für

die Konformität darstellen und als solche im Rahmen der Zertifizierung beachtet werden. Sie sind jedoch nicht ausreichend, um (Teil-)Evaluationen vollständig zu ersetzen. Die Zertifizierungsstelle ist auch hier weiterhin verpflichtet, die Einhaltung der Anforderungen anhand der Verifizierung des Prüfungsberichtes und zumindest stichprobenartig zu überprüfen sowie die bestehende Zertifizierungen auf Eignung zu bewerten.

4. Die Befristung der berücksichtigten Zertifikate ist zu notieren und für 7.7 (7.7.2) vorzuhalten. Die Gültigkeitsdauer des Zertifikats wird auf das Ablaufdatum des kürzest laufenden berücksichtigte Zertifizierungen reduziert. Bei der Rezertifizierung der Zertifizierung wird die Ablauffrist des Zertifikats auf die Laufzeit des berücksichtigten Zertifikats verlängert, jedoch maximal auf die Standardlaufzeit eines Zertifikats oder bei weiteren berücksichtigten Fremdzertifikaten auf die kürzeste Laufzeit (s.o.). Wird keine Rezertifizierung durchgeführt, muss mindestens der ursprünglich abgedeckte Bereich erneut geprüft werden.

Notwendig für eine solche Beachtung ist das Vorliegen eines vollständigen Zertifizierungsgutachtens oder von Informationen, die eine Bewertung der Zertifizierungstätigkeit und -ergebnisse ermöglicht. Eine Zertifizierungsurkunde oder ähnliche Bescheinigungen über eine Zertifizierung sind hierbei nicht ausreichend. Ergeben sich bei einer solchen Prüfung Abweichungen von den Anforderungen, oder sonstige Unregelmäßigkeiten, so ist die Evaluation im Rahmen des laufenden Zertifizierungsverfahrens zu erweitern und ggf. auf den gesamten, bereits zertifizierten Gegenstand auszudehnen.

Ergänzend zu Punkt 7.4.6 der DIN EN ISO/IEC 17065 hat die Zertifizierungsstelle in ihren Zertifizierungskriterien detailliert darzulegen, wie die in Punkt 7.4.6 geforderte Unterrichtung des Kunden über Abweichungen gegenüber einem Zertifizierungsprogramm erfolgt. Hierbei sind zumindest die Form und die zeitlichen Umstände einer solchen Unterrichtung zu definieren.

Ergänzend zu Punkt 7.4.9 der DIN EN ISO/IEC 17065 hat die Zertifizierungsstelle in ihren Kriterien darzulegen, wie diese Dokumentation erfolgt. Die Form und die Inhalte der Dokumentation sind so zu gestalten, dass sowohl die Evaluation als solches, als auch nachfolgend die Bewertungsergebnisse vollständig und nachvollziehbar sind.

Die Dokumentation ist im Akkreditierungsverfahren und jederzeit auf Wunsch der Datenschutzaufsichtsbehörde vollumfänglich zugänglich zu machen.

Zu 7.5 Bewertung

Ergänzend zu Punkt 7.5.1 der DIN EN ISO/IEC 17065 hat die Zertifizierungsstelle im Zertifizierungsprogramm und innerhalb des Managementsystems gemäß Tz. 8.1. DIN EN ISO/IEC 17065 - darzulegen, wie sichergestellt wird, dass die mit der Bewertung beauftragte(n) Person(en) weder direkt noch indirekt in den Evaluationsprozess involviert war(en). Die Anwendung dieser Kriterien und deren Ergebnisse sind im Rahmen der Bewertung zu dokumentieren.

Zu 7.6. Zertifizierungsentscheidung

Die Zertifizierungsstelle muss gemäß der Tz. 7.8 DIN EN ISO/IEC 17065 ein öffentliches Kurzgutachten über das Ergebnis der Zertifizierung veröffentlichen.

Die Zertifizierungsstelle unterrichtet die zuständige Datenschutzaufsichtsbehörde über die Zertifizierung schriftlich mindestens eine Woche vor Erteilung der Zertifizierung. Diese

Unterrichtung muss den Namen des Kunden, die Beschreibung des Zertifizierungsgegenstands und das öffentliche Kurzgutachten enthalten.

Ergänzend zu Punkt 7.6.1 der DIN EN ISO/IEC 17065 hat die Zertifizierungsstelle in ihren Kriterien detailliert darzulegen, wie ihre Unabhängigkeit und Verantwortlichkeit im Hinblick auf die Zertifizierungsentscheidungen sichergestellt wird.

Ergänzend zu Punkt 7.6.2 der DIN EN ISO/IEC 17065 muss die Entscheidung über die Zertifizierung durch den bzw. die Leiter(in) der Zertifizierungsstelle oder einen direkt von ihm bzw. ihr beauftragte qualifizierte Person erfolgen. DIN EN ISO/IEC 17065 Tz.7.6.3 ist zu beachten. Die Evaluierung kann, wie in Ergänzung zu 7.4.2 dargestellt, durch zuvor von der Zertifizierungsstelle anerkannte Sachverständige erfolgen.

Ergänzend zu Punkt 7.6.6 der DIN EN ISO/IEC 17065 hat die Zertifizierungsstelle in ihren Kriterien darzulegen, wie der Kunde über eine Entscheidung, die Zertifizierung nicht zu gewähren, informiert wird. Sie hat ferner darzulegen, welche Widerspruchsmöglichkeiten der Kunde gegenüber der Zertifizierungsstelle in diesen Fällen hat sowie welche Form und Frist hierbei einzuhalten ist.

Zu 7.7 Zertifizierungsdokumentation

Ergänzend zu Punkt 7.7.1. e) der DIN EN ISO/IEC 17065 und in Übereinstimmung mit Art 42 Abs. 7 DS-GVO ist die Gültigkeitsdauer von Zertifizierungen auf höchstens drei Jahre zu befristen.

Ergänzend zu Punkt 7.7.1. e) der DIN EN ISO/IEC 17065 ist der Zeitraum der vorgesehenen Überwachung im Sinne des Kapitels 7.9 ebenfalls zu dokumentieren.

Ergänzend zu Punkt 7.7.1 f) der DIN EN ISO/IEC 17065 hat die Zertifizierungsstelle dem Kunden im Rahmen der Zertifizierungsdokumentation den Zertifizierungsgegenstand (ggf. unter Angabe des Versionsstandes oder ähnlicher Kennzeichen) zu benennen.

Zu 7.8 Verzeichnis zertifizierter Produkte, Prozesse und Dienstleistungen

Ergänzend zu Punkt 7.8 der DIN EN ISO/IEC 17065 muss die Zertifizierungsstelle die Informationen zu zertifizierten Produkten, Prozessen und Dienstleistungen intern vorhalten und über das Internet allgemein abrufbar halten. Die intern vorzuhaltenden Informationen und das öffentliche Verzeichnis müssen ergänzend zu Punkt 7.8 der DIN EN ISO/IEC 17065 enthalten:

Ein Kurzgutachten bzgl. des jeweiligen Zertifizierungsergebnisses,

1. aus dem sich der genaue Zertifizierungsgegenstand (inklusive Versions- oder Funktionsstand),
2. das Prüfverfahren (inklusive der Zertifizierung zugrundliegender Kriterien (ggf. mit Versionsangabe)) und
3. das Prüfergebnis ableiten lassen.

Des Weiteren muss das Verzeichnis

1. Kontaktdaten des Antragstellers (juristische oder natürliche Person),
2. eine Registriernummer,
3. das Zertifizierungsdatum und das Ablaufdatum der Zertifizierung,
4. Informationen über die Erst- bzw. Re-Zertifizierung,
5. Angaben zu möglichen Überwachungstätigkeiten zur Aufrechterhaltung der Zertifizierung sowie

6. über die eventuelle Einbindung externer Evaluatoren enthalten.

Ergänzend zu Punkt 7.8 der DIN EN ISO/IEC 17065 und Punkt 8.3 der DIN EN ISO/IEC 17021, sowie gemäß Art. 43 Abs. 5 DS-GVO teilen die Zertifizierungsstellen den zuständigen Datenschutzaufsichtsbehörden die Gründe für die Erteilung oder den Widerruf der beantragten Zertifizierung mit.

Zu 7.9 Überwachung

Ergänzend zu Punkt 7.9.1, 7.9.2, 7.9.3 und 7.9.4 der DIN EN ISO/IEC 17065, 8.3. der DIN EN ISO/IEC 17021 und gemäß Art. 43 Abs. 2 lit. c DS-GVO sind zur Aufrechterhaltung der Zertifizierung während des Überwachungszeitraums Überwachungsmaßnahmen erforderlich.

Im Zertifizierungszyklus sind mindestens zwei Überwachungen durchzuführen. Diese sich systematisch wiederholenden Konformitätsbewertungstätigkeiten umfassen in der Regel folgende Arten der Überwachung:

1. Turnusmäßige anlasslose Überwachungen inklusive Betriebsbegehungen,
2. Anlassbezogene Überwachungen, als Ergebnis einer entsprechenden Risikoanalyse, inklusive Betriebsbegehungen.

Der Turnus für anlasslose Überwachungen ist im Zertifizierungsprogramm festzulegen. Darüber hinaus ist die Art der Überwachung zu definieren und darzulegen, wie den typischen datenschutzrechtlichen Risiken angemessen begegnet wird.

Anlassbezogene Überwachungen erfolgen bei Auffälligkeiten, die eine Nichteinhaltung der Zertifizierungsanforderungen befürchten lassen. Das Verfahren und die notwendige Zertifizierungsvereinbarung mit dem Kunden sind im Akkreditierungsverfahren und auf Wunsch der Datenschutzaufsichtsbehörden jederzeit nachzuweisen.

Zu 7.10 Änderungen, die sich auf die Zertifizierung auswirken

Ergänzend zu Punkt 7.10.1 und 7.10.2 der DIN EN ISO/IEC 17065 hat die Zertifizierungsstelle in ihrem Zertifizierungsprogramm Prozesse zu definieren, die sicherstellen, dass dem Kunden Änderungen der rechtlichen Rahmenbedingungen, die sich durch Gesetzesnovellierungen, den Erlass delegierter Rechtsakte der Europäischen Kommission, Entscheidungen des Europäischen Datenschutzausschusses und Gerichtsentscheidungen ergeben, sowie Fortentwicklungen des Stands der Technik (soweit relevant für die künftige Zertifizierung und Überwachung), die ihn betreffen, zeitnah mitgeteilt werden. Dies muss in das Managementsystem im Sinne von Kapitel 8 aufgenommen werden.

Ergänzend zu Punkt 7.10.1 der DIN EN ISO/IEC 17065 hat die Zertifizierungsstelle in ihrem Zertifizierungsprogramm zu definieren,

1. welches die Änderungen sind, die eine Mitteilung und ggf. eine Umsetzung beim Kunden erforderlich machen,
2. welche Evaluationsmethoden in einem solchen Fall durch die Zertifizierungsstelle vorzunehmen sind,
3. welche Fristen es für die Umsetzung der Maßnahmen gibt, um die bestehende Zertifizierung aufrecht zu erhalten.

Die Zertifizierungsstelle hat darüber hinaus zu definieren, wie sie sicherstellt, dass in vergleichbaren Zertifizierungsverfahren (auch im Fall einer Änderung der Zertifizierungsanforderungen) vergleichbare Prüfungen durchgeführt werden.

Ferner ist durch die Zertifizierungsstelle zu definieren, welche Maßnahmen und Prozesse einzuleiten sind, falls die Prüfung zu dem Ergebnis führt, dass die Zertifizierung nicht aufrechterhalten werden kann. Die entsprechenden Maßnahmen und dazugehörigen Prozesse sind umzusetzen und mittels des Managements der Zertifizierungsstelle vorzuhalten.

Ergänzend zu Punkt 7.10.2 der DIN EN ISO/IEC 17065 hat die Zertifizierungsstelle in ihrem Zertifizierungsprogramm zu definieren, in welchen Fällen und in welcher Art eine Information der Zertifizierungsstelle durch den Kunden (bei durch ihn ausgelösten Änderungen) zu erfolgen hat. Dies ist zumindest immer dann der Fall, wenn sich der Zertifizierungsgegenstand hinsichtlich der Verarbeitung personenbezogener Daten, die Einsatzumgebung und/oder der Anwendungskontext oder sonstige Rahmenbedingungen geändert haben, die relevant für die Zertifizierungsaussage sind. Dies betrifft insbesondere durch ihn festgestellte Änderungen der für den Zertifizierungsgegenstand einschlägigen Rechtsnormen sowie des Standes der Technik. Ferner sind die ggf. durch die Meldung ausgelösten Maßnahmen auf Seiten der Zertifizierungsstelle und des Kunden zu definieren. Die Zertifizierungsstelle hat darüber hinaus zu definieren, wie sichergestellt wird, dass in vergleichbaren Fällen vergleichbare Maßnahmen ergriffen werden. Ferner sind auch hier die entsprechenden Maßnahmen und dazugehörigen Prozesse umzusetzen und mittels des Managements der Zertifizierungsstelle vorzuhalten.

Zu 7.11 Beendigung, Einschränkung, Aussetzung oder Zurückziehung der Zertifizierung

Ergänzend zu Kapitel 7.11.1 der DIN EN ISO/IEC 17065 ist die zuständige Datenschutzaufsichtsbehörde über ergriffene Maßnahmen und über Weiterführungen, Einschränkungen, Aussetzen und Zurückziehen der Zertifizierung umgehend schriftlich zu informieren.

Ferner hat die Zertifizierungsstelle im Rahmen ihrer Kriterien zu definieren, welche Maßnahmen in welchen Fällen der Feststellung einer Nichtkonformität zu ergreifen sind.

Zu 7.12. Aufzeichnungen

Sämtliche Dokumentation der Zertifizierungsstelle muss vollständig, nachvollziehbar, aktuell und revisionssicher sein. Dies gilt sowohl für abgeschlossene und ohne positive Entscheidung beendete, als auch laufende Zertifizierungsverfahren. Für laufende Zertifizierungsverfahren muss zu erkennen sein, welche Zertifizierungskriterien erfüllt sind und welche noch nicht. Außerdem muss die Zertifizierungsstelle eine Statistik über abgeschlossene und abgebrochene Verfahren führen.

Ergänzend zu Kapitel 7.12.1 sind alle Aufzeichnungen zum Zertifizierungsverfahren während der Gültigkeit der Zertifizierung und nach Beendigung der Zertifizierungsvereinbarung darüber hinaus drei Jahre aufzubewahren. Diese Frist kann sich im Falle von Auseinandersetzungen zwischen der Zertifizierungsstelle und dem Kunden oder dem Kunden und der zuständigen Aufsichtsbehörde über die Gültigkeit der Zertifizierung hinaus bis zum Abschluss dieses Verfahrens verlängern.

Zu 7.13 Beschwerden und Einsprüche

Ergänzend zu Punkt 7.13.1 der DIN EN ISO/IEC 17065 hat die Zertifizierungsstelle im Rahmen ihrer Kriterien zu definieren,

1. wer Beschwerden oder Einsprüche einreichen kann,
2. wer diese auf Seiten der Zertifizierungsstelle bearbeitet,
3. welche Überprüfungen in diesem Zusammenhang stattfinden und
4. welche Möglichkeiten der Anhörung für die Beteiligten bestehen.

Ferner hat die Zertifizierungsstelle Fristen für die Beteiligten zu definieren, um den Prozess der Bearbeitung von Beschwerden und Einsprüchen zeitlich zu kontrollieren.

Ergänzend zu Punkt 7.13.2 der DIN EN ISO/IEC 17065 hat die Zertifizierungsstelle im Rahmen ihrer Kriterien zu definieren,

1. wie und wem gegenüber diese Bestätigung abzugeben ist,
2. welche Fristen hierfür gelten und
3. welche Prozesse im Anschluss daran zu initiieren sind.

Ergänzend zu Punkt 7.13.1 der DIN EN ISO/IEC 17065 hat die Zertifizierungsstelle im Rahmen ihrer Kriterien zu definieren, wie die personelle Trennung zwischen Zertifizierungstätigkeit und der Bearbeitung von Einsprüchen und Beschwerden sichergestellt wird. Gem. Punkt 7.13.5 der DIN EN ISO/IEC 17065 muss die Entscheidung, die die Beschwerde oder den Einspruch klärt, durch Personen erfolgen oder bewertet und genehmigt werden, die nicht in die Zertifizierungstätigkeiten, die sich auf die Beschwerde oder den Einspruch beziehen, einbezogen sind.

VI. Kapitel 8: Managementsystemanforderungen

Generelle Anmerkungen

Generelle Voraussetzung des Managementsystems gemäß Kapitel 8 der DIN EN ISO/IEC 17065 ist, dass die Umsetzung aller Anforderungen aus den vorherigen Kapiteln im Rahmen der Anwendung des Zertifizierungsmechanismus durch die akkreditierte Zertifizierungsstelle dokumentiert, evaluiert, kontrolliert und selbstverantwortlich überwacht werden.

Das grundlegende Prinzip eines Managements ist es, eine Systematik vorzugeben, nach der effektiv und effizient die gesetzten Ziele – hier: Durchführung der Umsetzung der Zertifizierungsleistungen – durch geeignete Vorgaben erreicht werden. Dies erfordert die Nachvollziehbarkeit und Prüffähigkeit von erbrachten Umsetzungen der Akkreditierungsanforderungen durch die Zertifizierungsstelle und deren dauerhafter Aufrechterhaltung.

Dazu muss das Managementsystem eine Methodik vorgeben, wie diese Vorgaben datenschutzkonform erreicht, kontrolliert, auch fortwährend bei der akkreditierten Stelle selbst geprüft werden können.

Diese Managementprinzipien und deren dokumentierte Umsetzung müssen im Akkreditierungsverfahren und danach jederzeit auf Wunsch der Datenschutzaufsichtsbehörde von der akkreditierten Zertifizierungsstelle u.a. während einer Untersuchung in Form von Datenschutzüberprüfungen (Art. 58 Abs. 1 lit. b DS-GVO) oder einer Überprüfung der nach Art. 42 Abs. 7 DS-GVO erteilten Zertifizierungen (Art. 58 Abs. 1 lit. c DS-GVO) nachvollziehbar sein und offengelegt werden (Art. 58 DS-GVO).

Insbesondere muss die akkreditierte Zertifizierungsstelle dauerhaft und fortwährend öffentlich machen, welche Zertifizierungen auf welcher Basis (bzw. Zertifizierungsprogrammen) durchgeführt wurden, wie lange die Zertifizierungen unter welchen Rahmenbedingungen Gültigkeit besitzen (ErwG 100).

Konkrete Ergänzungen:

Zu 8.1 Allgemeines

Sowohl bei Option A als auch bei Option B müssen zusätzlich die Ergänzungen dieses Dokuments zur Anwendung kommen. In beiden Fällen, aber besonders bei Nutzung von Option B, muss gewährleistet sein, dass die Anwendung der Ergänzungen explizit auf den Anwendungsbereich zugeschnitten ist, damit diese erkennbar und prüfbar sind. Der Bezug zur Anwendung der Ergänzungen muss nachweisbar sein.

Zu 8.1.1:

Beispielsweise müssen Prozesse entsprechend der vorherigen Kapitel im eigenen Management der Zertifizierungsstelle umgesetzt werden. Dazu gehören:

1. Verwaltung der Zertifizierungskriterien und entsprechender Genehmigungsverfahren
2. Überwachung, Kontrolle, Evaluierung und Verbesserung der Struktur der internen Abläufe der Zertifizierungsstelle mit Fortschreibung der entsprechenden intern geführten Nachweise,
3. Verwaltung des Beschwerdemanagements,
4. Aussetzung und Zurückziehung der Zertifizierung und Dokumentation der Gründe,

5. Vertragsmanagement,
6. Sicherstellung der Unabhängigkeit (Unparteilichkeit/finanzielle Stabilität) und Management der entsprechenden Nachweise,
7. Veröffentlichung von Zertifizierungskriterien/Zertifizierungsentscheidungen etc.,
8. Ressourcen (Personalkompetenz und externe Ressourcen),
9. Antragsmanagement,
10. Überwachung von Änderungen mit Auswirkungen auf Zertifizierungen und
11. Überwachung der Verwendung von Zertifizierungen.

Ergänzend zu Kapitel 8 der ISO 17065 sind folgende weitere neue Punkte zu erfüllen:

8.9 Fortschreibung der Evaluationsmethoden

8.9.1 Die Zertifizierungsstelle muss Verfahren zur Lenkung der Fortschreibung der Evaluationsmethoden zur Anwendung im Rahmen der Evaluierung in Punkt 7.4 festlegen. Die Fortschreibung hat im Zuge der Änderung der rechtlichen Rahmenbedingungen, der relevanten Risikoquellen, des Stands der Technik und der Implementierungskosten von technischen und organisatorischen Maßnahmen zu erfolgen.

8.9.2 Die Verfahren müssen die erforderlichen Lenkungsmaßnahmen festlegen, um sicherzustellen, dass:

1. alle relevanten Änderungen der rechtlichen Rahmenbedingungen (gemäß Punkt 7.4 und den dazugehörigen Erweiterungen in diesem Text),
2. Vertragsbestandteile zwischen Kunde und Zertifizierungsstelle,
3. alle relevanten neu auftretenden (Kategorien von) Risikoquellen und Schwachstellen der Informationstechnik, Geräte und Sicherheitstechnik sowie
4. der Fortschritt des Stands der Technik in Bezug auf Verarbeitungstätigkeiten und technische und organisatorische Maßnahmen, die zur Sicherstellung der Einhaltung der gesetzlichen Anforderungen, insbesondere im Hinblick auf die Umsetzung der Datenschutzgrundsätze und die Sicherheit der Verarbeitung angewandt werden können,

erfasst, dokumentiert und bewertet sowie in den Evaluationsmethoden abgebildet werden.

Daneben ist sicherzustellen, dass im Rahmen des Managementsystems Änderungen von Anforderungen der Datenschutzaufsichtsbehörden und des Datenschutzausschusses an Kriterienkatalogen und Zertifizierungsverfahren überwacht werden und diese Änderungen umgehend in die eigenen Verfahren der Zertifizierungsstelle integriert werden. Die Akkreditierungsstelle und die zuständige Datenschutzaufsichtsbehörde sind über Änderungen zu informieren.

Auch muss durch die Zertifizierungsstelle sichergestellt werden, dass Rechtsakte bzw. anderen Vorgaben von dem Datenschutzausschuss oder Datenschutzaufsichtsbehörden zeitnah zur Kenntnis genommen werden und die umgehende Umsetzung veranlasst wird. Die Akkreditierungsstelle und die zuständigen Datenschutzaufsichtsbehörden müssen hierüber informiert werden.

8.10 Aufrechterhaltung der Fachkunde

Die Zertifizierungsstellen müssen Verfahren zur Lenkung der Fortbildung ihrer Beschäftigten im Hinblick auf die Aktualisierung ihrer Fachkunde unter Berücksichtigung der unter Punkt 8.9.2 aufgeführten Entwicklungen einrichten.

8.11 Verantwortlichkeiten und Zuständigkeiten

8.11.1 Verhältnis zwischen Zertifizierungsstelle und ihren Kunden

Folgende Punkte sind zur Umsetzung entsprechender Verfahren und geeigneter Kommunikationsstrukturen zwischen der Zertifizierungsstelle und Kunden herzustellen:

1. Vorhalten eines Geschäftsverteilungsplans der akkreditierten Zertifizierungsstelle,
    a. um Auskunfts- oder Informationsersuchen oder
    b. einen Kontakt bei einer Beschwerde zu einer erteilten Zertifizierung zu ermöglichen.
2. Vorhalten des Prozesses der Antragsstellung:
    a. Status der Antragsbewertung bei eingereichtem Antrag zur Zertifizierung
    b. Bewertungen durch die zuständigen Datenschutzaufsichtsbehörde
        i. Rückmeldungen durch die zuständige Datenschutzaufsichtsbehörde (mit Tagesdatum)
        ii. Entscheidungen der zuständigen Datenschutzaufsichtsbehörde (mit Tagesdatum).

8.11.2 Konformitätsbewertungstätigkeiten und ihre Abläufe

Im Fokus müssen die Konformitätsbewertungstätigkeiten und ihre Abläufe sein. Dazu gehören

1. Offenlegung von Konformitätsbewertungstätigkeiten, um Änderungen bzw. Änderungsprozesse bei akkreditierten Zertifizierungsstellen nachvollziehen zu können; darin ist festzuhalten
    a. auf welcher Basis ein Konformitätsprogramm erstellt wurde, ggf. unter Angabe entsprechender Referenzen, z. B. der technischen Normen DIN EN ISO/IEC 17000 und DIN EN ISO/IEC 17011 und weiterer Quellen, wie Spezialgesetzen und ebenso spezifischerer technischer Normen, die abhängig von der Anwendung zum Einsatz kommen;
    b. der Einsatz von ggf. spezifischen Methoden in Prüfkonzepten und -verfahren zur Konformitätsbewertung, so dass darin enthaltene Maßstäbe für Soll- Ist-Vergleich erreicht, kontrolliert und fortwährend geprüft und verbessert werden;
    c. die Dokumentation von Kontrollen, Prüfungen und Verbesserungen der Maßstäbe unter Angabe des Zeitpunkt und der Gründe für die jeweilige Anpassung (entsprechend Punkt 7.10).
2. Nachverfolgung der Konformitätsbewertung (durch eine dritte Stelle, Delegation der Aufgaben im Zertifizierungsprozess)
3. Dokumentation und Nachverfolgung von Verpflichtungen zur Unparteilichkeit (entsprechend Punkt 4.2.3)
4. Versionierungen im Rahmen eines Publikationsmanagements; d.h. als Konsequenzen aus der Umsetzung von Punkten 4.1.2.2, 4.6 und 7.8.
    a. von Zertifizierungsprogrammen;
    b. von Maßstäben zur Konformitätsbewertung in Zertifizierungsprogrammen
    c. Mindestanforderungen an die Zertifizierungsvereinbarungen
5. Nachverfolgung der konkreten Zertifizierungen und ihrer dazugehörigen Veröffentlichungen (entsprechend Punkt 7.8) und ggf. spezifische Beschwerden zu einer Zertifizierung, falls diese entsprechend Punkt 4.6 vorliegen.

8.11.3 Beschwerdemanagement

Ein Beschwerdemanagementsystem ist als integraler Bestandteil im Managementsystem zu etablieren; dieses muss insbesondere die Anforderungen aus den Punkten 4.1.2.2 lit. c, 4.1.2.2 lit. j, 4.6 lit. d und 7.13 DIN EN ISO/IEC 17065 realisieren.
Konsequenzen sind, dass

1. bei größeren Änderungen eine neue Risikobewertung erfolgt.
2. Eine solche Risikobewertung kann direkten Einfluss auf die eingesetzten Zertifizierungsgegenstände haben.

Im Fall begründeter Beschwerden ist die zuständige Datenschutzaufsichtsbehörde zu informieren.

8.12 Weitere Verfahren

Die Verfahren für den Fall der Aussetzung oder Zurückziehung (Erlöschen bzw. Widerruf) der Akkreditierung sind in das Managementsystem der Zertifizierungsstelle zu integrieren. Dies beinhaltet Verfahren zur Behandlung der damit verbundenen Zertifizierungen.

Wird die Zertifizierungsstelle von der Datenschutzaufsichtsbehörde angewiesen, eine erteilte Zertifizierung gemäß Art. 58 Abs. 2 lit. h DS-GVO zu widerrufen, oder keine Zertifizierung zu erteilen, so muss die Zertifizierungsstelle im Rahmen ihres Managementsystems sicher stellen, dass der entsprechende Kunde hierüber und die Folgen daraus informiert wird, entsprechende Registereinträge angepasst werden und die Datenschutzaufsichtsbehörde hierüber in Kenntnis gesetzt wird.

Anhang 1 Abkürzungsverzeichnis / Glossar

Sofern sich aus dem Kontext nichts anderes ergibt, kommen die folgenden Definitionen zur Anwendung:

Anforderungen	Bezeichnet die datenschutzspezifischen Ergänzungen der gesetzlichen und normativen Anforderungen zur Akkreditierung gemäß VO (EG) 765/2008 i.V.m. DIN EN ISO/IEC 17065 gemäß Art. 43 Abs. 1 lit. b DS-GVO.
Akkreditierung	Akkreditierung ist die Bestätigung durch eine nationale Akkreditierungsstelle, dass eine Zertifizierungsstelle die in Normen festgelegten Anforderungen und, gegebenenfalls, zusätzliche Anforderungen, einschließlich solcher in relevanten sektoralen Akkreditierungssystemen, erfüllt, um eine spezielle Konformitätsbewertungstätigkeit durchzuführen.
Akkreditierungsausschuss (AKA)	Der AKA ist ein internes Verfahrensbezogenes Entscheidungsgremium der DAkkS, dass die Akkreditierungsentscheidung auf Basis der Begutachtungsergebnisse und weiterer Erkenntnisse trifft (Verwaltungsakt). Der AKA besteht aus drei Mitgliedern. Zwei Mitglieder werden von den Datenschutzbehörden benannt. Eine positive Akkreditierungsentscheidung kann nur Einstimmig erfolgen. Für eine negative Entscheidung genügt ein negatives Votum.
AKA-Mitglied	AKA-Mitglieder sind sach- und fachkundige Personen, die an der Akkreditierungsentscheidung mitwirken dürfen und nicht an der Begutachtung beteiligt waren, über die der AKA im konkreten Verfahren entscheiden soll.
Begutachter(in)	Begutachter(in), ist eine sach- und fachkundige Person, die Begutachtungen im Rahmen der Akkreditierung erbringt.

(Genehmigte) Kriterien	Genehmigte Zertifizierungskriterien im Sinne der DS-GVO sind Kriterien, die durch die Datenschutzaufsicht nach Art 57 Abs. 1 DS-GVO als Teil von durch die DAkkS gemäß 4.6.3 auf Eignung geprüften Zertifizierungs-programmen gebilligt worden sind.
Kunde	Verantwortlicher oder Auftragsverarbeiter, der die von ihm durchgeführte Verarbeitung dem Zertifizierungsverfahren unterwirft (Art. 42 Abs. 6 S. 1 DS-GVO)
Programmeigner	Hält die Rechte an einem Zertifizierungsprogramm und überwacht dieses.
Zertifizierungsmechanismus	Entspricht dem Zertifizierungsprogramm und seinem Management
Zertifizierungsprogramm	Zertifizierungsprogramm ist ein Dokument einer Zertifizierungsstelle oder eines unabhängigen privaten oder öffentlichen Programmeigners, das für die Zertifizierungsstellen die spezifischen Anforderungen, Regeln sowie Prüf- und Inspektionsverfahren beschreibt, die zur Konformitätsbewertung eines Produkts, Verfahrens oder einer Dienstleistung (siehe I. Kapitel 3: Begriffe) verwendet werden müssen, um die mit dem Konformitätsbewertungsnachweis (z. B. Laborwert, Analyse, Inspektionsbericht, Versuch, Zertifizierung, usw.) verbundene Aussage, auf wissenschaftlich nachvollziehbare und systematische Weise treffen zu können. Auf Antrag wird die Akkreditierungsfähigkeit eines Zertifizierungsprogramms durch feststellenden Verwaltungsakt durch die DAkkS bestätigt. Teil des Zertifizierungsprogramms sind die genehmigten Kriterien.
Zertifizierungsstelle	Entspricht der Konformitätsbewertungsstelle als dritte, die ein Zertifizierungsprogramm betreibt.
Zertifizierungstätigkeiten	Alle Aktivitäten einer Zertifizierungsstelle gemäß DIN EN ISO/IEC 17065.

Anhang 2: Witnessing-Modell

Das Witnessing (ausgeführt durch Mitarbeiter der Datenschutzaufsichtsbehörde oder von der Beauftragten und der Akkreditierungsstelle) findet grundsätzlich an dem Ort statt, an dem die Tätigkeit im Zertifizierungsprozess ausgeführt wird. Dies ist in der Regel beim Kunden der Zertifizierungsstelle oder deren Auftragsverarbeiter der Fall; kann je nach Zertifizierungsprogramm, aber auch in den Räumlichkeiten der Zertifizierungsstelle oder an anderen Orten, an denen Tätigkeiten im Rahmen der Evaluierung erfolgen durchgeführt werden. Die DAkkS (in Abstimmung mit der zuständigen Datenschutzaufsichtsbehörde) behält sich dabei vor, festzulegen, welches Personal bzw. welche Tätigkeiten im Zertifizierungsprozess einem Witnessing zu unterziehen sind. Der Umfang des erforderlichen Witnessing im Rahmen des Begutachtungsverfahrens wird durch die DAkkS (zusammen mit der zuständigen Datenschutzaufsichtsbehörde) nach folgenden Grundsätzen festgelegt:

1. Für die Erstakkreditierung einer Zertifizierungsstelle muss je Geltungsbereich des Zertifizierungsprogramms mindestens ein Witnessaudit durchgeführt werden;
2. Es ist zulässig die Durchführung von ausstehenden Witnessaudits in einem angemessenen Zeitraum entsprechend ISO 17011 nachzuholen und die Akkreditierung unter Auflage der Durchführung des ausstehenden Witnessaudits zu erteilen,
3. bei der anschließenden Überwachung der Akkreditierung entsprechend ISO 17011 ist für mindestens einen Anwendungsbereich aus allen Programmen der Zertifizierungsstelle ein Witnessaudit durchzuführen; im Akkreditierungszyklus müssen mindestens 50% aller Geltungsbereiche aus allen Programmen durch ein Witnessaudit abgedeckt werden,
4. Witnessaudits dürfen in Abhängigkeit von weiteren Befunden und risikoorientierter Betrachtung jederzeit außerplanmäßig angeordnet werden.

Die Anzahl kann begrenzt werden, wenn die Akkreditierungsstelle das ausreichende Vertrauen in die Arbeit der Zertifizierungsstelle begründen kann. Will die Zerifizierungsstelle ein neues Zertifizierungsprorgramm einsetzen, so ist hierfür ein erneutes Witnessing erforderlich.

Anhang 3: Kenntnisse und Erfahrungen im technischen und organisatorischen Datenschutz

1. Angewandte Kryptographie (z. B. Verschlüsselungsverfahren, Hashverfahren, PKI)
2. Pseudonymisierung/Anonymisierung
3. Datenschutzfördernde Technologien (Privacy Enhancing Technologies)
4. Identitätsmanagement und Rollen-/Rechtekonzepte
5. Protokollierung und Transparenz
6. Risikobasierter Ansatz nach DS-GVO (beispielweise Artikel 5 Abs. 1 DS-GVO und entsprechende ISO Normen)
7. Verfahren zur Durchführung einer Datenschutz-Folgenabschätzung (z. B. Standard-Datenschutzmodell, ISO 29134)
8. Informations- und Cybersicherheit (mit Blick auf Rechte und Freiheiten natürlicher Personen)
9. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
10. Verfahren zum Löschen personenbezogener Daten / Löschkonzepte
11. Datenschutzmanagementsysteme und Governance