Version 1.0 (15.03.2019)

Akkreditierungsprozess für den Bereich „Datenschutz“ gemäß Art. 42, 43 DS-GVO[1]

Programmprüfung

Akkreditierung

1. Antragsphase Programmprüfung

Antragstellung und -prüfung

- Antrag Programmprüfung und Genehmigung der Zertifizierungskriterien (46 FB 001)
- Liste einzureichender Unterlagen (46 FB 002)
- Kombinierte Checkliste (46 FB 003)
- DAkkS prüft Antrag auf Vollständigkeit

Einbeziehung der zuständigen Aufsichtsbehörde

zuständige Aufsichtsbehörde erhält Information über Eingang eines Antrags und alle eingereichten Unterlagen

2. Programmprüfung und Genehmigung der Kriterien

System-Programmprüfung

- Systembegutachter der DAkkS prüft Erfüllung der Normanforderungen (ISO/IEC 17065 und ISO/IEC 17067)
- Regel DAkkS zur Prüfung von Programmen (71 SD 0 016)

Fach-Programmprüfung

Die zuständige Aufsichtsbehörde prüft Erfüllung der Normanforderungen aus ISO/IEC 17065 und hierzu ergänzende Anforderungen.

Genehmigung der Kriterien

Nach erfolgreicher Fachprüfung des Programms, erfolgt eine Genehmigung der Zertifizierungskriterien durch die zuständige Aufsichtsbehörde.

Feststellung der Akkreditierungsfähigkeit

Feststellung der Akkreditierungsfähigkeit des Zertifizierungsprogramms durch den Programmausschuss nach der Genehmigung der Kriterien

3. Antragsphase Akkreditierung / Befugniserteilung

Antragstellung und -prüfung

- Antrag auf Akkreditierung und Befugniserteilung (72 FB 001.1)
- Anlage: Auskunft zur Information der Befugnis erteilenden Behörde (72 FB 002)
- Liste einzureichender Unterlagen (72 FB 004.6_17065)

Einbeziehung der zuständigen Aufsichtsbehörde

zuständige Aufsichtsbehörde erhält Information über Eingang eines Antrags und alle eingereichten Unterlagen

4. Begutachtungsphase

Auswahl der Begutachter

- Systembegutachter DAkkS
- Fachbegutachter der zuständigen Aufsichtsbehörde

Planung

- Beauftragung der Begutachter/ Terminabstimmung
- Erstellung eines Begutachtungsplans (75 FB 001)

Dokumentenprüfung

- Prüfung aller eingereichten Unterlagen
- Bericht (75 FB 009)

Begehung der Zertifizierungsstelle

- Feststellung von Abweichungen durch System- und Fachbegutachter
- Abarbeitung der Feststellungen durch Zertifizierungsstelle
- Bewertung der Abarbeitung durch System- und Fachbegutachter

Witnessing

- Witnessaudit
- Witnessbericht

5. Akkreditierungsphase / Befugniserteilung

AKA Entscheidung

- Prüfung aller Unterlagen und Bewertung der Berichte der System- und Fachbegutachter
- Entscheidung durch DAkkS und zuständige Aufsichtsbehörde

Akkreditierungsurkunde

- Erstellung der Urkunde (Gültigkeit: maximal 5 Jahre)
- Übermittlung an Zertifizierungsstelle und zuständige Aufsichtsbehörde

Befugniserteilung

Zuständige Aufsichtsbehörde erteilt der akkreditierten Stelle die Befugnis, als Zertifizierungsstelle tätig zu sein.

Verzeichnis akkreditierter Stellen

Aufnahme in das Verzeichnis der DAkkS

6. Überwachungsphase

Akkreditierung | Zertifizierung

Überwachung

- Regelmäßige Wiederholungs-begutachtung der Zertifizierungsstelle
- Anzahl der Wiederholungs-begutachtung wird nach einem risikobasierten Ansatz festgelegt

Reakkreditierung

Die Zertifizierungsstelle kann einen Antrag auf Reakkreditierung stellen

Zertifizierung

Die zuständige Aufsichtsbehörde wird vor der Erteilung, Verlängerung, sowie beim Widerruf von Zertifizierungen unter der Angabe von Gründen benachrichtigt. Des Weiteren werden die erteilten Zertifizierungen überprüft.

Gemeinsamer Prozessschritt

Prozessschritt DAkkS

Prozessschritt Aufsichtsbehörde

[1] Diese allgemeine Darstellung betrifft ausschließlich einen nationalen Akkreditierungsprozess und ist nicht als abschließend zu betrachten.

Beschreibung des Akkreditierungsprozesses für den Bereich Datenschutz gemäß Art. 42, 43 DS-GVO

Wie verläuft der Akkreditierungsprozess?

Gemäß Art. 43 Datenschutz-Grundverordnung (DS-GVO) und § 39 Bundesdatenschutzgesetz (BDSG) werden Stellen, die im Datenschutzbereich zertifizieren möchten, durch die Deutsche Akkreditierungsstelle (DAkkS) zusammen mit der Befugnis erteilenden, zuständigen Datenschutz-Aufsichtsbehörde (Aufsichtsbehörde) akkreditiert. Interessierte Stellen müssen dabei sowohl die Anforderungen aus der EN-ISO/IEC 17065/2012 erfüllen, als auch ergänzende Anforderungen aus dem Datenschutzbereich.

Zur Durchführung von Akkreditierungen sind insgesamt sechs Phasen vorgesehen. Diese Phasen werden im Nachfolgenden gemäß der Abbildung beschrieben. Die Abbildung und folgende Beschreibung geben einen ersten, nicht abschließenden Überblick über den Ablauf eines reibungslosen Akkreditierungsprozesses.

1. Antragsphase Programmprüfung

Der eigentlichen Akkreditierung ist eine Programmprüfung vorgeschaltet.

Der Programmprüfungsprozess beginnt mit der Einsendung des Antrags auf Programmprüfung und Genehmigung der Zertifizierungskriterien (46 FB 001), sowie der fachspezifischen Anlagen an die Prüfstelle für neue Konformitätsbewertungsprogramme der DAkkS. Die Einbeziehung der zuständigen Aufsichtsbehörde erfolgt durch die DAkkS.

2. Programmprüfung und Genehmigung der Kriterien

Die Programmprüfung bei der DAkkS erfolgt gemäß der Regel zur Prüfung der Feststellung der Akkreditierungsfähigkeit neuer privater Konformitätsbewertungsprogramme (71 SD 0 016).

- Im ersten Schritt erfolgt eine Rechts-, Formal- und Systemprüfung des Konformitätsbewertungsprogramms durch die Programmprüfstelle der DAkkS.
- Anschließend erfolgt eine Fachprüfung des Konformitätsbewertungsprogramms und der entsprechenden Zertifizierungskriterien durch die zuständige Aufsichtsbehörde.
- Erfolgreich abgeschlossen wird die Fachprüfung der Aufsichtsbehörde mit der Genehmigung der Zertifizierungskriterien gem. Art. 57 Abs. 1 lit. n DS-GVO i.V.m. Art. 42 Abs. 5 DS-GVO.
- Erfolgt die Genehmigung der Zertifizierungskriterien (und ggf. die Beseitigung von Abweichungen), wird das Programmprüfungsverfahren durch einen feststellenden Bescheid des Programmausschusses der DAkkS abgeschlossen.

Ergänzungsinformation: Die Zertifizierungskriterien sind zwar separat genehmigungsbedürftig, die Genehmigung erfolgt jedoch im Kontext eines zugehörigen Zertifizierungsprogramms, da das Programm nur als Ganzes eine Akkreditierungsfähigkeit besitzen kann.

3. Antragsphase Akkreditierung/Befugniserteilung

Die eigentliche Akkreditierung beginnt mit der Einsendung des Akkreditierungsantrages (72 FB 001.1) und der fachspezifischen Anlagen an die Zentrale Antragsbearbeitung (ZAB) der DAkkS.

Die ZAB überprüft den Antrag in Abstimmung mit der zuständigen Fachabteilung der DAkkS. Dabei wird auch die zuständige Aufsichtsbehörde, als Befugnis erteilende Behörde, in das Akkreditierungsverfahren eingebunden.

Die Befugniserteilung (siehe Phase 5) ist gegenüber dem Akkreditierungsverfahren ein gesondertes Verwaltungsverfahren. Die DAkkS nimmt den Antrag auf Befugniserteilung im Rahmen des Akkreditierungsverfahrens entgegen und leitet ihn an die zuständige Aufsichtsbehörde weiter.

Ergänzungsinformation: optional können sich Zertifizierungsstellen vorab in einem Vorgespräch mit der zuständigen Fachabteilung der DAkkS über ihre angestrebte Akkreditierung oder das Akkreditierungsverfahren im konkreten Fall informieren.

4. Begutachtungsphase

Die DAkkS begutachtet gemeinsam mit der zuständigen Aufsichtsbehörde (Begutachterteam) die Erfüllung der Anforderungen der ISO/IEC 17065/2012 und der ergänzenden Anforderungen der Aufsichtsbehörden.

- Zunächst prüft das Begutachterteam die eingereichten Dokumente und vereinbart anschließend einen oder mehrere Termine für die Begehung der Zertifizierungsstelle.
- Neben der Vor-Ort Begehung finden ein oder mehrere Witness-Audits statt. Die Erstakkreditierung erfolgt unter der Auflage der Durchführung eines Witness-Audits beim ersten Kunden der Zertifizierungsstelle.
- Die Ergebnisse werden in einem Begutachtungsbericht dokumentiert. Festgestellte Abweichungen kann die Zertifizierungsstelle durch entsprechende Korrekturmaßnahmen im Anschluss an die Begutachtungstermine beheben. Diese werden durch das Begutachterteam nochmals überprüft und bewertet.

Ergänzungsinformation: der Umfang und die Dauer der Begutachtung sind von der Größe der Zertifizierungsstelle, dem Geltungsbereich der Akkreditierung und der Komplexität des Verfahrens abhängig.

5. Akkreditierungsphase/Befugniserteilung

In dieser Phase bewertet ein Akkreditierungsausschuss (AKA – Zusammensetzung: 1/3 DAkkS und 2/3 zuständige Aufsichtsbehörde) die Begutachtungsergebnisse und entscheidet über die Erteilung der Akkreditierung. Eine positive Entscheidung muss einstimmig erfolgen.

Die DAkkS bescheinigt den erfolgreichen Abschluss der Akkreditierungsphase durch den Akkreditierungsbescheid und die Akkreditierungsurkunde. Die Akkreditierung wird anschließend im Verzeichnis der akkreditierten Stellen der DAkkS gelistet. Die Akkreditierung wird gemäß Art 43 Abs. 3 DS-GVO auf längstens fünf Jahre befristet. Vor Ablauf der Akkreditierung kann eine Zertifizierungsstelle einen Antrag auf Reakkreditierung stellen.

Auf Grundlage der erfolgreichen Akkreditierung kann die zuständige Aufsichtsbehörde der Zertifizierungsstelle die Befugnis erteilen, im Rahmen des akkreditierten Programms tätig zu sein.

6. Überwachungsphase

Akkreditierung: Die Kompetenz einer Stelle wird auch nach einer erteilten Akkreditierung in regelmäßigen Abständen durch die DAkkS und die zuständige Aufsichtsbehörde überwacht. Die Anzahl der Wiederholungsbegutachtungen wird nach einem risikobasierten Ansatz der DAkkS festgelegt. Auf diesem Weg wird sichergestellt, dass die Zertifizierungsstelle die jeweiligen Akkreditierungsanforderungen dauerhaft erfüllt und als kompetent eingestuft werden kann.

Werden bei den Überwachungsbegutachtungen Abweichungen festgestellt, kann dies zur Einschränkung, Aussetzung oder Aufhebung der Akkreditierung führen mit möglichen Auswirkungen auf bereits erteilte Zertifizierungen.

Zertifizierung: Jeder Aufsichtsbehörde obliegt in ihrem Hoheitsgebiet gem. Art. 57 Abs. 1 lit. o DS-GVO die Pflicht, die nach Art. 42 Abs. 7 DS-GVO erteilten Zertifizierungen regelmäßig zu überprüfen. Hierzu informieren die akkreditierten Zertifizierungsstellen die zuständige Aufsichtsbehörde vor Erteilung, Verlängerung oder Widerruf von Zertifizierungen, unter Nennung der entsprechenden Gründe.