Zertifizierungsprogramm

AUDITOR Datenschutz-Zertifizierung für Cloud-Anbieter (GDPR CC)

Dokumentenart:	Zertifizierungsprogramm
Kunde:	Zertifizierungsstellen-intern, Interessenten
Autor:	Leitung der Zertifizierungsstelle-DL
Editor:	Sören Scholz
QS:	Stellv. Leitung der Zertifizierungsstelle
Version:	1.0
Status:	Freigegeben
Verschwiegenheit:	ÖFFENTLICH
Verteiler:	Mitarbeiter der Zertifizierungsstelle, Kunden, Interessenten

pwc

Inhaltsverzeichnis

Dokumentenhistorie

Version	Datum	Änderung	Autor/Editor/QS
0.1	22.08.2023	Erstausstellung	Sören Scholz
1.0	27.11.2023	Review	Eva-Maria Weber
1.0	04.12.2023	Review und Freigabe	Ingo Bauer

1 Einleitung

1.1 Zweck

Dieses Dokument beschreibt den Prozess einer AUDITOR Datenschutz-Zertifizierung für Cloud-Anbieter von der Antragstellung bis zur Erteilung durch die Zertifizierungsstelle Dienstleistungen (ZS-DL) der PwC Certification Services GmbH (im Folgenden „Zertifizierungsstelle“ genannt).

Dieses Zertifizierungsprogramm bildet neben den Allgemeinen Geschäftsbedingungen der PwC Certification Services GmbH (im Folgenden „PwC Cert“ oder „Zertifizierungsstelle“) die Grundlage für Cloud-Anbieter, ihre gemäß Art. 42 DS-GVO zertifizierte Cloud-Dienstleistung mit dem Zertifizierungszeichen „AUDITOR“ zu kennzeichnen. Sie dokumentieren damit, dass ihre Cloud-Dienstleistung alle Anforderungen der einschlägigen DS-GVO (Datenschutz-Grundverordnung) erfüllen und sie die Datenverarbeitungsvorgänge im Rahmen einer Auftragsverarbeitung gemäß Art. 28 DS-GVO durchführen.

Gegenüber dem B2B-Kunden des Cloud-Anbieters wird durch das Zertifizierungszeichen „AUDITOR“ das Vertrauen geschaffen, dass eine unabhängige, neutrale und kompetente Stelle die Prüfkriterien sorgfältig untersucht und bewertet hat. Die Fremdüberwachung stellt zudem sicher, dass die Cloud-Dienstleistung auch während des Betriebs aufrecht erhalten bleibt. Der B2B-Kunde erhält somit einen Mehrwert, den er bei der Auswahl des Cloud-Dienstleisters berücksichtigen kann.

Cloud-Anbieter erhalten das Nutzungsrecht für das Zertifizierungszeichen „AUDITOR“ bei Erfüllung der im GDPR CC-Kriterienkatalog aufgeführten Anforderungen nach dem in diesem Zertifizierungsprogramm beschriebenem Verfahren.

Alle Zertifikatinhaber sowie die zertifizierungsrelevanten Informationen können tagesaktuell auf der Internetseite von PwC Cert (www.pwc-cert.com/auditor) abgerufen werden.

1.2 Geltungsbereich

Dieses Zertifizierungsprogramm gilt für Cloud-Anbieter und enthält in Verbindung mit den unten genannten Prüf- und Zertifizierungsgrundlagen alle Anforderungen zur Vergabe des Zertifizierungszeichens „AUDITOR“.

Das vorliegende Zertifizierungsprogramm legt die Anforderungen an die Cloud-Dienstleistung selbst sowie an die Angebotserstellung, Auditzeitkalkulation, Auditierung, Überwachung und Zertifizierung fest.

1.3 Prüf- und Zertifizierungsgrundlagen

Die Grundlagen für die Prüfung und Zertifizierung bilden die nachstehend aufgeführten Dokumente. Bei datierten Verweisen gilt nur die in Bezug genommene Fassung. Bei undatierten Verweisen gilt die jeweils aktuelle Ausgabe des in Bezug genommenen Dokuments einschließlich aller Änderungen.

DIN EN ISO/IEC 17000	Konformitätsbewertung – Begriffe und allgemeine Grundlagen
DIN EN ISO/IEC 17021	Konformitätsbewertung – Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren
DIN EN ISO/IEC 17065	Konformitätsbewertung – Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren

DIN EN ISO 19011	Leitfaden zur Auditierung von Managementsystemen
DIN EN ISO/IEC 27001	Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen
AUDITOR (GDPR CC)	Konformitätsbewertungsprogramm V0.99_b_final (2020-09-28)
AUDITOR (GDPR CC)	Zertifizierungsgegenstand V0.99 (2019-11-26)
AUDITOR (GDPR CC)	Kriterienkatalog V0.99 (2020-01-20)
AUDITOR (GDPR CC)	Schutzklassenkonzept V0.99 (2019-11-27)
AUDITOR (GDPR CC)	Modularitätskonzept V0.99 (2020-01-13)
IAF MD 1:2018	Verbindliches IAF-Dokument für die Auditierung und Zertifizierung von Managementsystemen in Organisationen mit mehreren Standorten
IAF MD 5:2015	Verbindliches IAF-Dokument – Ermittlung von Auditzeiten für die Auditierung von Qualitätsmanagement- (QMS) und Umweltmanagementsystemen (UMS), sowie Managementsystemen für Sicherheit und Gesundheit bei der Arbeit (SGA-MS)
PwC Cert	Antragsformular AUDITOR (GDPR CC)
PwC Cert	Gebührentabelle AUDITOR (GDPR CC)
PwC Cert	AVB Allgemeine Vertragsbedingungen (01.12.2023)
VO (EU) 2016/679	Datenschutz-Grundverordnung (DS-GVO)

1.4 Beginn der Gültigkeit

Dieses Zertifizierungsprogramm gilt ab 2023-12-01.

1.5 Änderungen

Keine

1.6 Frühere Ausgaben

Keine

2 Antragstellung und Angebotserstellung

Die Angebotserstellung umfasst die Aktivitäten von der Kundenakquise bis hin zur Freigabe und Übermittlung des Angebots an den antragstellenden Cloud-Anbieter. Die Angebotserstellung beinhaltet die folgenden Schritte, die in ihrer Abfolge in der nachstehenden Grafik dargestellt sind.

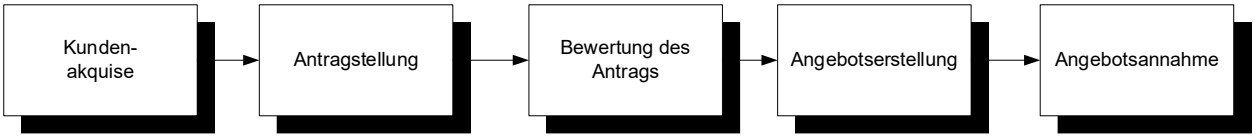

Abbildung 1 Prozess der Angebotserstellung

Im Folgenden wird die detaillierte Vorgehensweise zur Angebotserstellung gemäß den oben genannten Phasen beschrieben.

2.1 Kundenakquise

Die Kundenakquise soll Transparenz und Qualität der Dienstleistungen der Zertifizierungsstelle gewährleisten. Es wird in jedem Fall ein unverbindliches telefonisches Informationsgespräch angeboten, um die Rahmenbedingungen eines Zertifizierungsaudits und einer Zertifizierung zu klären. Auf Wunsch des potentiellen Kunden wird ein persönliches Informationsgespräch – gegebenenfalls auch vor Ort beim potentiellen Kunden – durchgeführt. Das initiale Informationsgespräch muss kostenfrei sein.

Zusätzlich zum Informationsgespräch kann dem potentiellen Kunden ein Readiness-Audit angeboten werden. In diesem Audit wird geprüft, ob die Basiselemente einer Datenschutz-Zertifizierung nach GDPR CC vorhanden sind. Dies kann u. a. die Unterstützung bei der Abgrenzung des Zertifizierungsgegenstandes beinhalten. Das Readiness-Audit ist kostenpflichtig. Durch die Zertifizierungsstelle wird sichergestellt, dass die Unabhängigkeitsanforderungen sowie das Beratungsverbot eingehalten werden.

2.2 Antragstellung durch den Cloud-Anbieter

Für eine konkrete Angebotserstellung ist von dem Cloud-Anbieter ein Zertifizierungsantrag auszufüllen. Antragsberechtigt für eine Zertifizierung nach GDPR CC sind Cloud-Anbieter als Auftragsverarbeiter. Auf Basis des Antrags wird die projektbezogene Unparteilichkeit der Zertifizierungsstelle sichergestellt und die Aufwandskalkulation durchgeführt.

Als Grundlage für den Antrag werden Interessenten der Zertifizierungsantrag (inkl. Stellungnahme) und das Zertifizierungsprogramm durch die Zertifizierungsstelle bereitgestellt. Für den Fall, dass bei der Antragstellung Fragen auftreten, wird dem Cloud-Anbieter mit der Bereitstellung der Unterlagen ein Ansprechpartner der Zertifizierungsstelle benannt, der im Rahmen der Antragstellung unterstützend tätig werden kann. In dem Anschreiben wird durch die Zertifizierungsstelle darauf hingewiesen, dass durch die Antragstellung noch kein verbindliches Vertragsverhältnis entsteht. Der interessierte Cloud-Anbieter hat im Rahmen der Beantragung gemäß diesem Zertifizierungsprogramm und dem GDPR CC-Kriterienkatalog insbesondere die folgenden Informationen bereitzustellen:

- die beantragte Schutzklasse und Wiederherstellbarkeitsklasse;
- Angaben zum Cloud-Anbieter, darunter Name und Anschrift/en der Standorte;

- allgemeine Informationen bezüglich des antragstellenden Cloud-Anbieters, die für den beantragten Zertifizierungsbereich relevant sind, wie z.B. seine Tätigkeiten, personelle und technische Ressourcen, Organigramm, seine Marktausrichtung (national, EU, international, ausgewählte Märkte in Ländern etc.) und ggf. Beziehungen in einer größeren Körperschaft;
- eine umfassende Beschreibung des Zertifizierungsgegenstands gemäß § 5.1.4 GDPR CC;
- eine umfassende Erläuterung zur Nichtanwendbarkeit von Zertifizierungskriterien gemäß § 5.1.5 GDPR CC;
- eine umfassende Erläuterung zur Erfüllung der Zertifizierungskriterien gemäß § 5.1.6 GDPR CC;
- Auskunft über Beratungsleistungen, die durch die Zertifizierungsstelle bezüglich des zu zertifizierenden Datenverarbeitungsvorgangs erbracht (inkl. der Angabe des Zeitraums der Beratung und der beteiligten Personen).

2.3 Bewertung des Antrags

Die Bewertung des Antrags erfolgt dabei durch die Zertifizierungsstelle. Der Antrag wird auf formale Korrektheit geprüft, um gegebenenfalls fehlende Informationen bei dem Antragsteller anzufordern. In Fokus der Bewertung des Antrags stehen:

- Die Beurteilung der Kunden- und Auftragsrisiken (siehe Abschnitt 2.3.1)
- Die Prüfung der projektbezogenen Unparteilichkeit (siehe Abschnitt 2.3.2)
- Die Prüfung von ggf. anzuerkennender bestehender Zertifikate (siehe Abschnitt 2.3.3).
- Das Verständnis des Zertifizierungsgegenstandes sowie der Umsetzung für jedes Zertifizierungskriterium (siehe Abschnitt 2.3.4 und Abschnitt 2.3.6)
- Das Verständnis über die Nichtanwendbarkeit von Zertifizierungskriterien (siehe Abschnitt 2.3.5)

Die Prüfung und Bewertung über die Annahme oder Ablehnung des Antrags erfolgt durch die Zertifizierungsstelle und kann grundsätzlich mit Hilfe der Konsultation eines Auditteamleiters erfolgen. Eine Klärung von Differenzen im Verständnis der im Antrag befindlichen Angaben kann durch formlose Rücksprachen erfolgen. Die Begründung der Entscheidung einen Zertifizierungsantrag anzunehmen oder abzulehnen wird dokumentiert und auf dem Fileserver abgelegt. Eine Ablehnung des Antrags ist dem potentiellen Kunden gegenüber schriftlich zu begründen. Grundsätzlich erfolgt die Bewertung des Antrags hinsichtlich der folgenden Punkte:

- die Informationen über die antragstellende Organisation und über den Zertifizierungsgegenstand ausreichend für die Durchführung des Audits sind (siehe oben – Bereitstellung von Informationen),
- die Anforderungen an die Zertifizierung seitens der Zertifizierungsstelle klar definiert und dokumentiert sind und der antragstellenden Organisation bereitgestellt wurden,
- die Zertifizierungsstelle über die Kompetenz und die Fähigkeit verfügt, die Zertifizierungstätigkeiten durchzuführen,
- der Geltungsbereich der angestrebten Zertifizierung, die Standorte der Tätigkeiten der antragstellenden Organisation, die zur Ausführung der Audits erforderliche Zeit sowie alle anderen Aspekte, die die Zertifizierungstätigkeit beeinflussen, berücksichtigt werden (Sprache, Sicherheitsbedingungen, Gefährdungen der Unparteilichkeit und so weiter).

Grundsätzlich wird im Rahmen der Bearbeitung des Antrags sichergestellt, dass die Annahme eines Zertifizierungsantrags weder von der Größe des Cloud-Anbieters oder von der Mitgliedschaft in einer Vereinigung oder Gruppe abhängt noch von der Anzahl der bereits erteilten Zertifizierungen.

Eine Bewertung der Beantragung einer spezifischen Schutzklasse oder Wiederherstellungsklasse erfolgt nicht. Diese Wahl obliegt alleinig dem antragstellenden Cloud-Anbieter.

In Zusammenhang mit der Antragstellung auf Zertifizierung ist durch die Zertifizierungsstelle zu klären, welche Soll-Dokumente (Richtlinien, Anweisungen und ähnliches) und Aufzeichnungen seitens des Kunden gegebenenfalls als vertraulich oder sensibel eingestuft sind und damit vom Auditteam während des Audits möglicherweise nicht ohne weiteres überprüft werden könnten. Sollten derartige Aufzeichnungen für ein effektives Audit unbedingt erforderlich sein, so ist mit dem Kunden durch den Auditteamleiter vor Beginn der Stufe 1 des Verfahrens ein praktikables Zugangsverfahren zu vereinbaren.

Ein angenommener Antrag ist Voraussetzung für den Abschluss einer Zertifizierungsvereinbarung und die Einleitung der Auditaktivitäten.

2.3.1 Beurteilung der Kunden- und Auftragsrisiken

Für jeden geplanten Auftrag wird vor Abgabe eines Angebots bzw. vor Annahme des Auftrags eine Analyse der mit dem Kunden und dem Auftrag verbundenen Risiken vorgenommen. Nachfolgend sind die Pflichten im Rahmen der Angebotsabgabe / Auftragsvereinbarung zusammenfassend dargestellt. Es besteht dabei die Pflicht:

- die Risikoanalyse abzuschließen und zu dokumentieren
- eine Risikoklassifizierung vorzunehmen und gegebenenfalls erforderliche Genehmigungen einzuholen.
- die Anforderungen des Geldwäschegesetzes zu erfüllen.
- zu beurteilen, ob ausreichende qualifizierte personelle Ressourcen zur Durchführung des Auftrags zur Verfügung stehen.
- eine Risikoeinschätzung bei der Verarbeitung von personenbezogenen Daten vorzunehmen
- die notwendigen Konsultationen bei Zweifelsfragen vorzunehmen

und zu dokumentieren.

2.3.2 Prüfung der projektbezogenen Unparteilichkeit

Zur Gewährleistung der Unabhängigkeit ist anhand gegebenenfalls vorhandener vergangener Beziehungen zum potentiellen Kunden und den Angaben auf dem vom Antragsteller ausgefüllten Zertifizierungsantrag vor Abgabe eines Angebots durch die Zertifizierungsstelle zu prüfen, ob:

- inakzeptable Beziehungen des potentiellen Kunden mit der Zertifizierungsstelle oder verbundenen Stellen der Zertifizierungsstelle bestehen (es bestehen keine privaten oder geschäftlichen Verbindungen zwischen Mitarbeitern der Zertifizierungsstelle potentiellen Kunden, die die Unabhängigkeit beeinträchtigen);
- bereits Geschäftsbeziehungen bestanden, die die Unabhängigkeit gefährden (dies ist pauschal anzunehmen, wenn es sich bei dieser Geschäftsbeziehung nicht um die Durchführung eines Drittparteienaudits handelt);
- ob es anhand der Unabhängigkeitserklärungen der Mitglieder des geplanten Auditteams Zweifel an der Unabhängigkeit aller Auditteammitglieder gibt (siehe Abschnitt 2.5.1);
- ob von der Zertifizierungsstelle sonstige wesentliche Gefährdungen der Unabhängigkeit oder Unparteilichkeit erkannt werden.

Für jedes Mitglied des geplanten Auditteams ist zu prüfen, ob:

- andere Tätigkeiten als Drittparteienaudits beim potenziellen Kunden durchgeführt wurden (24 Monate rückwirkend). Insbesondere wurden durch Mitglieder des Auditteams in dem genannten Zeitraum keine Beratungsleistungen für die zu prüfende Organisation oder verbundene

Organisationen erbracht, die in Bezug zu dem Prüfungsgegenstand stehen. Solche Beratungsleistungen sind alle Tätigkeiten, die zu Design, Aufbau, Implementierung, Betrieb sowie Verbesserung des Zertifizierungsgegenstandes beitragen;

- private oder geschäftliche Verbindungen zwischen einem Mitglied des Auditteams und dem potentiellen Kunden bestehen, die die Unabhängigkeit beeinträchtigen. Eine Verbindung, die die Unabhängigkeit der Mitglieder eines geplanten Auditteams gefährdet, basiert in der Regel auf Eigentümerschaft, Beherrschung, Leitung, Personal, gemeinsam genutzten Ressourcen, Finanzen, Verträgen, Vermarktung oder Anreizen für die Empfehlung neuer Kunden.

2.3.3 Anerkennung von bestehenden Zertifikaten

Der Cloud-Anbieter kann die Anerkennung bereits bestehender Zertifizierungen (durch eine akkreditierte Zertifizierungsstelle erfolgte Datenschutzzertifizierung nach Art. 42 DS-GVO oder relevante ISO-Zertifizierungen) für Bestandteile seiner Datenverarbeitungsvorgänge des zugrunde liegenden, abgegrenzten Zertifizierungsgegenstandes beantragen (vgl. § 5.1.7 GDPR CC). In diesem Fall wird geprüft, ob und inwieweit eine Anerkennung eines anderen Zertifikats erfolgen kann und im Zertifizierungsprozess als Teilevaluierung anerkannt werden kann.

2.3.3.1 Anforderung der Zertifizierungsgutachten

Damit eine Bewertung zur Anerkennung durchgeführt werden kann, ist es notwendig, das vollständige Zertifizierungsgutachten (z. B. Audit-Report) vom interessierten Cloud-Anbieter anzufragen. Darüber hinaus ist durch den Cloud-Anbieter darzustellen, inwieweit bestehende Zertifizierungsgutachten die GDPR CC-Zertifizierungskriterien erfüllen. Entsprechende Unterlagen werden nach Abstimmung mit dem Cloud-Anbieter durch Mitarbeiter der Zertifizierungsstelle angefordert.

Kann ein Zertifizierungsgutachten nicht durch den Cloud-Anbieter zur Verfügung gestellt werden (z. B., wenn eine Weitergabe aus rechtlichen oder vertraglichen nicht möglich ist) sind ausreichende Informationen bereitzustellen, die eine Bewertung zur Anerkennung ermöglichen. Eine Bewertung der Anerkennung ausschließlich anhand der Zertifizierungsurkunde oder ähnlichem wird nicht durchgeführt und die Anerkennung ist in diesem Fall abzulehnen.

2.3.3.2 Bereitstellung der Zertifizierungsgutachten

Der Cloud-Anbieter stellt die Zertifizierungsgutachten gemäß der Abstimmung mit der Zertifizierungsstelle bereit.

2.3.3.3 Prüfung der Anerkennbarkeit und Bewertung

Die bereitgestellten Dokumente des Cloud-Anbieters zur Bewertung der Anerkennung bereits bestehender Zertifizierungen durch die Zertifizierungsstelle müssen einen genau beschriebenen Zertifizierungsgegenstand sowie eine Darstellung der Schnittstellen bzw. Übergänge zu anderen Systemen und Organisationen enthalten. Darüber hinaus muss der zu zertifizierende Datenverarbeitungsvorgang Bestandteil des Geltungsbereichs der bestehenden Zertifizierung sein (bspw. Datenverarbeitungsvorgang ist Bestandteil des nach DIN EN ISO/IEC 27001 zertifizierten ISMS). Wenn im Folgenden von „Datenverarbeitungsvorgang“ gesprochen wird, sind damit i. d. R. auch mehrere Datenverarbeitungs-vorgänge gemeint, da Zertifizierungsgegenstände von GDPR CC oft nicht nur einen Datenverarbeitungsvorgang umfassen.

Damit eine Prüfung auf Anerkennung grundsätzlich möglich ist, muss es sich um ein Zertifikat der folgenden drei Kategorien handeln:

- Das Zertifikat wurde von einer akkreditierten Zertifizierungsstelle ausgestellt (z. B. ein DIN EN ISO/IEC 27001 Zertifikat durch eine akkreditierte Zertifizierungsstelle);
- Das Zertifikat wurde von einer Stelle ausgestellt, die eine Begutachtung unter Gleichrangigen durchlaufen hat (gem. ISO/IEC 17040:2005);
- Das Zertifikat wurde durch eine staatliche Zertifizierungsstelle auf gesetzlicher Grundlage ausgestellt (z. B. Cyber Security Act).

Andere als die o. g. erteilten Zertifizierungen können im Rahmen einer Zertifizierung gemäß GDPR CC nicht anerkannt werden. Gleichwohl können diese bei Bedarf im Rahmen der Ermittlungstätigkeiten im Sinne einer Dokumentenprüfung mit einbezogen werden, wobei die Einhaltung der Zertifizierungskriterien weiterhin durch weitere geeignete Ermittlungsmethoden vollumfänglich geprüft wird.

Bei der Prüfung der Anerkennung wird die materielle und verfahrensmäßige Gleichwertigkeit der Ergebnisse von Konformitätsbewertungen sichergestellt.

- **Materielle Gleichwertigkeit:**
  Eine materielle Gleichwertigkeit liegt vor, wenn das andere (anzuerkennende) Zertifikat auf Zertifizierungskriterien beruht, die denen des GDPR CC-Kriterienkatalogs im Hinblick auf das Schutzniveau vergleichbar sind oder diese übertreffen. Es wird festgestellt (im Falle einer Anerkennung) mit welcher Schutzklasse und welcher Wiederherstellbarkeitsklasse das Zertifikat anerkannt wird.
- **Verfahrensmäßige Gleichwertigkeit**:
  Eine verfahrensmäßige Gleichwertigkeit liegt vor, wenn das andere Zertifikat in einem akkreditierten Zertifizierungsverfahren erteilt wurde, das eine dieser Verfahrensordnung vergleichbare Gewähr für die ordnungsgemäße Prüfung und Zertifizierung bietet.

In der Regel liegt eine Gleichwertigkeit bei Zertifikaten vor, welche durch eine akkreditierte Zertifizierungsstelle vergeben werden, und somit insbesondere bei bewilligten Datenschutz-zertifizierungen nach Art. 42 DS-GVO.

2.3.3.4 Entscheidung, Dokumentation und Archivierung der Entscheidung

Die Entscheidung über die Anerkennung von Zertifizierungen erfolgt durch die Zertifizierungsstelle (siehe auch Abschnitt 2.4).

Die Entscheidung über die Anerkennung von Zertifikaten sowie der Schutzklasse und Wiederherstellbarkeitsklasse wird begründet und dokumentiert. Die Dokumentation beinhaltet dabei den Umfang und welche Auswirkungen die Anerkennung auf den verbleibenden Ermittlungsumfang und die Ermittlungsmethoden hat. Weitere Informationen sind im Modularitätskonzept enthalten (siehe “GDPR CC-Modularitätskonzept”).

Hinweis: Anerkannte Zertifizierungen für Bestandteile von Datenverarbeitungsvorgängen müssen im Rahmen der Zertifizierungstätigkeit nicht mehr vollständig bewertet werden. Gleichwohl wird die aktuelle Einhaltung der Kriterien (der vorgelegten, anzuerkennenden Zertifizierung) stichprobenartig geprüft, um die bestehende Zertifizierung zu bewerten (siehe Abschnitt 3.6.6).

2.3.3.5 Information des Cloud-Anbieters

Der Cloud-Anbieter wird über die Entscheidung der Anerkennbarkeit der vorgelegten Zertifizierungen sowie der Anerkennung hinsichtlich der GDPR CC-Kriterien, insbesondere hinsichtlich der Schutz- und Wiederherstellbarkeitsklasse, schriftlich informiert (siehe auch Abschnitt 2.4).

2.3.4 Festlegung des Zertifizierungsgegenstandes

Gegenstand der Bewertung (Zertifizierungsgegenstand, i. S. d. Tz. A.2.2 ISO/IEC 17000:2004, Anhang A) sind Datenverarbeitungsvorgänge mit personenbezogenen Daten i. S. d. Art. 4 Nr. 1 DS-GVO, die in Cloud-Diensten oder mit Hilfe von (auch mehreren) Cloud-Diensten erbracht werden.

Eine Datenverarbeitung ist dabei jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder Vorgangsreihe. Dazu zählen das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten.

Ein Datenverarbeitungsvorgang kann sowohl technische und automatisierte als auch nichttechnische und somit auch organisatorische (bspw. manuelle oder personelle) Vorgangsschritte enthalten, worunter auch Datenschutzkonzepte und -managementsysteme fallen können.

Der gesamte Verarbeitungsvorgang muss den Anforderungen der Datenschutz-Grundverordnung entsprechen. Datenverarbeitungsvorgänge müssen eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen, innerhalb derer die spezifischen Datenschutzrisiken des jeweiligen Cloud-Dienstes vollständig erfasst werden können. Dies bedeutet, dass auch Schnittstellen des zu zertifizierenden Cloud-Dienstes zu anderen Diensten betrachtet werden müssen, um Datenflüsse zu identifizieren, aus denen datenschutzrechtliche Risiken erwachsen können.

Durch den Cloud-Anbieter muss eine detaillierte Beschreibung des Zertifizierungsgegenstandes erstellt werden. Der Zertifizierungsgegenstand wird durch den Antragsteller bei der Beantragung definiert, durch die Zertifizierungsstelle anhand der vorliegenden Informationen abschließend und unter Rücksprache mit dem Antragsteller festgelegt. Dazu ist es notwendig, dass der Antragsteller (Cloud-Anbieter) ausreichend Informationen zur Beurteilung, Abgrenzung und abschließenden Festlegung des Zertifizierungsgegenstandes zur Verfügung stellt. Die Zertifizierungsstelle prüft, ob die Beschreibung des Cloud-Anbieters mindestens die erforderlichen Informationen für eine trennscharfe Abgrenzung des Zertifizierungsgegenstandes umfasst. Dieses beinhaltet:

- Die Benennung und detaillierte (Funktions-)Beschreibung des Datenverarbeitungsvorgangs oder der Datenverarbeitungsvorgänge innerhalb eines entsprechenden Cloud-Dienstes, der zu zertifizieren ist.
- Die detaillierte Beschreibung aller Bestandteile der relevanten Datenverarbeitungsvorgänge, sodass eine abgeschlossene Verfahrensstruktur gewährleistet wird.
- Dokumentation von Verantwortlichkeiten des Cloud-Anbieters im Datenverarbeitungsvorgang.
- Benennung und Informationen zu Standorten bei denen Datenverarbeitungsvorgänge durchgeführt werden (darunter Nennung Zentralstelle sowie weiterer Standorte und Beschreibung der Tätigkeiten, Risiken pro Standort, rechtliche und vertraglichen Regelungen für jeden Standort, den Grad der Zentralisierung der Prozesse/Tätigkeiten, die für alle Standorten erbracht werden, die Schnittstellen zwischen den verschiedenen Standorten).
- Informationen bezüglich aller ausgegliederten Vorgänge, die von dem Cloud-Anbieter im Rahmen des Datenverarbeitungsvorgangs genutzt werden und welche die Konformität mit den Zertifizierungskriterien beeinflussen. Dabei müssen insbesondere Subauftragsverarbeiter und die von ihnen übernommenen Zuständigkeiten und damit verbundenen Aufgaben benannt werden.
- Die Darstellung der Schnittstellen und Übergänge zu anderen Systemen und Organisationen/ Subauftragsverarbeitern (bspw. in Form eines Netzplans). Hierbei sind auch die zugrundeliegenden

Protokolle (bspw. Überwachungsprotokolle, (Muster-)Verträge, Vereinbarungen, Garantien) und sonstige Zusicherungen darzulegen.
- Technische und organisatorische Maßnahmen (TOM) des Cloud-Anbieters i. S. d. Art. 28 DS-GVO.
- Eingesetzte Technik und IT-Landschaft, dazu zählen insbesondere relevante IT-Systeme.
- Organisatorische Prozesse zur Durchführung der Datenverarbeitungsvorgänge.
- Die spezifischen Datenschutzrisiken, die zu zertifizierenden Datenverarbeitungsvorgänge aufweisen.

Die Festlegung und Dokumentation des Zertifizierungsgegenstandes erfolgt abschließend durch die Zertifizierungsstelle, wobei Rückfragen oder Unklarheiten in Zusammenarbeit mit dem Cloud-Anbieter geklärt werden. Der festgelegte Zertifizierungsgegenstand wird dem Antragsteller (Cloud-Anbieter) zur Gegenprüfung zur Verfügung gestellt.

Hinweis: Festlegung des Zertifizierungsgegenstandes im praktischen Vorgehen:

Die Festlegung des Zertifizierungsgegenstandes ist in der Praxis ein komplexer Vorgang, da die spezifischen Verarbeitungsvorgänge, die in dem jeweiligen Cloud-Dienst erbracht werden, identifiziert werden müssen. Dabei ist zwischen Datenverarbeitungsvorgängen, die als Auftragsverarbeiter erbracht werden und solchen, die als Verantwortlicher durchgeführt werden, zu unterscheiden. Wie weit oder eng ein Verarbeitungsvorgang gefasst wird, hängt von dem jeweiligen Zweck der Verarbeitung ab. Dieser bestimmt letztlich die Grenzen des Verarbeitungsvorgangs. Mehrere Zwecke oder. Zweckänderungen können beispielsweise auf unterschiedliche Verarbeitungsvorgänge hindeuten

Im Rahmen der Festlegung und Abgrenzung des Zertifizierungsobjekts ist zu berücksichtigen, dass:

- Einzelne Verarbeitungsvorgänge innerhalb eines Dienstes können nur zertifiziert werden, wenn sie keine direkte Verbindung zu anderen Verarbeitungsvorgängen haben
- klar und vollständig beschrieben werden (einschließlich der Schnittstellen)
- Ein „Rosinenpicken“ unkritischer Teile und ihre Zertifizierung nicht möglich ist.
- Die Zertifizierung nach Art. 42 und Art. 43 DS-GVO eine **Vollbestätigung** vorsieht
- Der Zertifizierungsgegenstand ist so zu bestimmen, dass er eine **in sich geschlossene Verfahrensstruktur** aufweist.

Nutzen verschiedene Dienste die gleichen Verarbeitungsvorgänge, zum Beispiel für das User Access Management, so könnte es sich ergeben, dass eine einmalige, horizontal modularisierte Zertifizierung eines solchen Verarbeitungsvorgangs für mehrere Dienste genutzt werden kann. Dies vermeidet die mehrfache Prüfung eines einzelnen Verarbeitungsvorgangs. Inwieweit die Definition solcher weiter ausgelegten Verarbeitungsvorgänge sinnvoll und möglich ist, ist individuell mit dem jeweiligen Antragsteller zu überprüfen.

Im Rahmen der Erstellung des Angebotes kann es sinnvoll sein, dem Antragsteller im Rahmen eines Workshops die Grundlagen und Grenzen der Definition des Zertifizierungsgegenstandes näher zu bringen. Dabei können dem Antragsteller die Anforderungen an den Zertifizierungsgegenstand sowie die Vorgehensweise zur Identifikation der relevanten Verarbeitungsvorgänge erläutert werden.

Die Vorlage einer vollständigen Datenflussanalyse des jeweiligen Dienstes durch den Antragsteller und deren Diskussion mit den an der Verarbeitung beteiligten Akteuren sollten dabei im Zentrum der Identifikation der Verarbeitungsvorgänge stehen. Dies umfasst insbesondere:

- die weiteren Auftragsverarbeiter (Subauftragsverarbeiter) und
- die Darlegung der Zugriffsmöglichkeiten der Cloud-Nutzer und des Cloud-Anbieters in den jeweiligen Datenverarbeitungsvorgang.

2.3.5 Nichtanwendbarkeit von Zertifizierungskriterien

Im Rahmen des Antrags hat der Antragsteller eine Erläuterung zur Nichtanwendbarkeit von Zertifizierungskriterien darzustellen. Die Erläuterung muss eine detaillierte Darstellung beinhalten, welche Zertifizierungskriterien abhängig vom jeweiligen Zertifizierungsgegenstand anwendbar bzw. nicht anwendbar sind. Die Einschätzung der Nichtanwendbarkeit von Zertifizierungskriterien wird entsprechend durch den Antragsteller dokumentiert und der Zertifizierungsstelle im Rahmen des Antrags mitgeteilt. Die Dokumentation muss dabei mindestens die folgenden Angaben beinhalten:

- Eine Auflistung der Kriterien, die nicht anwendbar sind.
- Eine ausführliche Begründung pro Kriterium, warum dieses für den konkreten Zertifizierungsgegenstand nicht anwendbar ist.

Die Zertifizierungsstelle prüft die vom Antragsteller bereitgestellte Dokumentation zur Nichtanwendbarkeit auf Korrektheit und Vollständigkeit und dokumentiert diese entsprechend. Dabei wird sichergestellt, dass bei vergleichbaren Zertifizierungsverfahren und Sachverhalten die gleiche Entscheidung hinsichtlich der Nichtanwendbarkeit getroffen wird, um eine mögliche Willkür bei der Bewertung auszuschließen.

Bei Unklarheiten bzw. Zweifeln an der Nichtanwendbarkeit eines Kriteriums durch die Zertifizierungsstelle wird eine Klärung mit dem Antragsteller herbeigeführt. Dazu werden je nach Notwendigkeit unter anderem weitere Dokumente und Erläuterungen vom Antragsteller angefordert oder es werden entsprechende Ermittlungsmethoden (vgl. GDPR CC § 5.2.4) durch die Zertifizierungsstelle angewandt.

Wird die Nichtanwendbarkeit eines Kriteriums durch die Zertifizierungsstelle bestätigt, wird dieses Kriterium im Rahmen der Ermittlung nicht geprüft. Die nachweislichen Gründe, Entscheidungsregeln, sowie der Umfang der Nichtanwendbarkeit und die Ergebnisse der Bewertung werden durch die Zertifizierungsstelle nachvollziehbar dokumentiert (siehe auch Abschnitt 2.5.3).

Nicht anwendbar sind Kriterien insbesondere dann (vgl. GDPR CC § 5.1.5 (5)), wenn:

- der Cloud-Anbieter diese nicht erfüllen kann, weil sie außerhalb seines Verantwortungsbereichs liegen. So wird der Cloud-Anbieter bspw. nach dem Zertifizierungskriterium Nr. 6.2 zur Unterstützung des Cloud-Nutzers bei der Auskunftserteilung verpflichtet. Das Kriterium ist jedoch auf die Datenverarbeitungsvorgänge des Cloud-Anbieters nicht anwendbar und der Cloud-Anbieter somit von der Auskunftserteilung entbunden, wenn der Verantwortungsbereich für die betreffenden Daten beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt (bspw. im Falle einer Infrastructure-as-a-Service Cloud-Dienstleistung). Das Gleiche gilt, wenn nicht der Cloud-Anbieter, sondern Subauftragsverarbeiter für den Zugang zu Datenverarbeitungssystemen nach dem Zertifizierungskriterium Nr. 2.3 verantwortlich sind. In diesem Fall ist das Zertifizierungskriterium Nr. 2.3 auf den Cloud-Anbieter nicht anwendbar. Der Cloud-Anbieter muss sich jedoch davon überzeugen, dass die Subauftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten (siehe Zertifizierungskriterium Nr. 10.4) und somit ihrerseits das Zertifizierungskriterium Nr. 2.3 erfüllen.
- die Erfüllung des Kriteriums verhindert, einen legitimen Datenverarbeitungszweck zu erreichen. So kann beispielsweise ein Anbieter eines E-Mail-Dienstes die Mailheader nicht anonymisieren, da ansonsten die Zustellung von E-Mails nicht mehr ordnungsgemäß gewährleistet werden kann, sodass er zu einer solchen Anonymisierung auch nicht verpflichtet werden kann.
- der Cloud-Anbieter die in den Zertifizierungskriterien adressierten Handlungen nicht vornimmt. Setzt der Cloud-Anbieter bspw. keine Subauftragsverarbeiter ein oder findet keine Datenverarbeitung außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums statt, sind die Zertifizierungskriterien aus Abschnitt V und VI des GDPR CC Kriterienkatalogs nicht anwendbar.

- die Datenschutz-Grundverordnung oder die sie konkretisierenden Gesetze die Anwendbarkeit nicht absolut fordern, sondern von gewissen Voraussetzungen oder „Schwellen“ abhängig machen, welche vom Cloud-Anbieter nicht erfüllt werden. Dies ist beispielsweise bei der Benennung eines Datenschutzbeauftragten (Art. 37 Abs. 1 und 4 DS-GVO i. V. m. § 38 BDSG) oder beim Führen eines Verarbeitungsverzeichnisses der Fall (Art. 30 Abs. 5 DS-GVO).

Darüber hinaus ist es möglich, dass der Cloud-Anbieter oder die Zertifizierungsstelle – z. B. im Rahmen der Festlegung des Zertifizierungsgegenstandes oder der Ermittlungs- und Bewertungstätigkeiten – eine Nichtanwendbarkeit von Zertifizierungskriterien aufgrund besonderer Umstände und Eigenschaften des Datenverarbeitungsvorgangs feststellen. Im Falle einer Feststellung der Nichtanwendbarkeit wird diese entsprechend begründet und dargelegt. Die Beurteilung und die Ergebnisse müssen durch die Zertifizierungsstelle nachvollziehbar dokumentiert werden (siehe auch Abschnitt 2.5.3).

2.3.6 Stellungnahme des Cloud-Anbieters zur Erfüllung von Zertifizierungskriterien

Im Rahmen des Antrags reicht der Antragsteller bei der Zertifizierungsstelle eine detaillierte Stellungnahme zur Erfüllung der Zertifizierungskriterien ein. Diese ist unter anderem die Grundlage für die Erstellung des Angebots sowie die Planung (Vorbereitung und Durchführung) der Ermittlung.

Durch die Zertifizierungsstelle wird dem Antragsteller eine Vorlage “FBL Stellungnahme zur Erfüllung von Zertifizierungskriterien” im Rahmen des Antrags-Prozesses bereitgestellt. Die Vorlage kann durch den Antragsteller genutzt werden, um die Umsetzung des Cloud-Anbieters dediziert für jedes Zertifizierungskriterium korrekt und vollständig darzustellen. Die Darstellung erfolgt dabei differenziert für die Unterpunkte des jeweiligen Kriteriums (bspw. Erläuterung zu Kriterium Nr. 2.2 (2)) und referenziert zur entsprechenden Dokumentation (bspw. Prozessdokumentation, Logs, Intranet, etc.) oder relevanter Systeme. Durch die Abgabe der Stellungnahme versichert der Antragsteller gegenüber der Zertifizierungsstelle, dass die in der Stellungnahme genannten Maßnahmen vollständig umgesetzt sind.

Die Zertifizierungsstelle bewertet alle vorliegenden Informationen und entscheidet über die Annahme oder Ablehnung des Antrags.

2.4 Entscheidung über die Antragsprüfung und Dokumentation

Auf Grundlage der Bewertung entscheidet die Zertifizierungsstelle über die Annahme oder Ablehnung des Antrags sowie die Berücksichtigung bestehender Zertifizierungen.

Im Falle einer negativen Prüfung des Zertifizierungsantrags durch die Zertifizierungsstelle wird der Cloud-Anbieter über die Ablehnung des Antrags schriftlich informiert. Mögliche Gründe für eine Ablehnung des Antrags können bspw. sein:

- der Cloud-Anbieter ist an illegalen Aktivitäten beteiligt;
- der Cloud-Anbieter hat wiederholt gegen die GDPR CC-Zertifizierungskriterien verstoßen;
- ähnliche auf den Cloud-Anbieter bezogene Probleme wie z. B. öffentlich bekannte Datenschutzverstöße oder entsprechende Ermittlungen der Behörden.

Darüber hinaus müssen Anträge abgelehnt werden, wenn der Zertifizierungsstelle

- die Kompetenz oder Fähigkeit für die Zertifizierungstätigkeiten, die sie ausführen muss, fehlen,
- die Mittel zur Durchführung aller Auswahl- und Ermittlungstätigkeiten fehlen oder
- die Unparteilichkeit gefährdet ist.

2.5 Angebotserstellung

Nachdem der Antrag des interessierten Cloud-Anbieters durch die Zertifizierungsstelle geprüft und positiv bewertet wurde, erfolgt die Zusammenstellung des voraussichtlichen Auditteams, die Bestätigung der Unparteilichkeit der Teammitglieder sowie die Erstellung der Zertifizierungsvereinbarung (Angebot). Eine geschlossene Vertragsbeziehung und formelle Beauftragung zwischen der Zertifizierungsstelle und dem Cloud-Anbieter ist die notwendige Voraussetzung für ein Zertifizierungsaudit. Der Prozess gliedert sich in die nachfolgenden Schritte.

2.5.1 Erstellen der Auditzeit-Kalkulation

Die Basis für die Auditzeit-Kalkulation bilden die im Rahmen des Antrags zur Zertifizierung bereitgestellten Informationen des Cloud-Anbieters. Bei Bedarf werden von dem Cloud-Anbieter weitere Informationen angefragt oder Unklarheiten in Rücksprache mit dem Cloud-Anbieter geklärt.

2.5.2 Zusammenstellung des Auditteams

Die Zusammenstellung eines für die Zertifizierung geeigneten Auditteams obliegt der Zertifizierungsstelle. Dies schließt auch die Sicherstellung einer geeigneten Auswahl von Auditoren ein (u. a. Auditteamleiter und weiteren Personen), die zur Durchführung von Auswahl- und/oder Ermittlungstätigkeiten nach GDPR CC beauftragt werden (der Begriff „Auditor“ ist Synonym für den Begriff „Evaluator“, welcher vom GDPR CC-Konformitätsbewertungsprogramm verwendet wird).

Eine Auswahl durch den Antragsteller ist dabei ausgeschlossen. Ein Einspruch des Kunden gegen den Einsatz einer bestimmten Person im Auditteam wird im Rahmen des Beschwerdemanagements behandelt.

Bei der Entscheidung über die angemessenen Kenntnisse und Fähigkeiten des Auditteams muss Folgendes berücksichtigt werden:

- Die Größe, Art und Komplexität der zu auditierenden Organisation.
- Die Ziele und der Umfang des Auditprogramms.
- Erfordernisse der Zertifizierung, Registrierung und Akkreditierung.
- Die Rolle des Auditprozesses beim Management der zu auditierenden Organisation.
- Das Vertrauensniveau, das im Auditprogramm erforderlich ist.
- Die Komplexität des zu zertifizierenden Zertifizierungsgegenstandes (vgl. dazu Abschnitt 2.3.4).
- Berücksichtigung von individuellen Ausprägungen von Technologien, Dienstleistungen, Prozessen sowie gesetzlicher und vertraglicher Anforderungen und Rahmenbedingungen.

Es ist sicherzustellen, dass mindestens einer Person im Auditteam über die jeweiligen erforderlichen Qualifikationen und Fähigkeiten verfügt.

Weiter muss bei der Größe und Zusammensetzung des Auditteams berücksichtigt werden und ob die designierten Mitglieder des Auditteams den Zertifizierungsgegenstand des Kunden zuvor bereits auditiert haben.

Die Qualifikationen sind durch Berufserfahrung abzustützen. Wichtig ist die Fähigkeit von identifizierten Sicherheitsvorfällen auf Schwachstellen z.B. im Managementsystem schlussfolgern zu können sowie die unterschiedlichen Aktivitäten und Risiken einer Organisation zu verstehen, um vernünftige Bewertungen vornehmen zu können.

Es ist möglich, dass während eines Audits weiterer technischer Sachverstand benötigt wird. In diesem Fall werden weitere Fachexperten involviert. Zur fortlaufenden Verbesserung können neue Kenntnisse auch externe Erklärungen aus der Forschung von Universitäten, aus Kontakten zu Mitgliedern des

Unparteilichkeitsausschusses sowie von spezialisierten Organisationen erworben werden. Dabei erfolgt keine Bearbeitung eines konkreten Vorfalls beim Kunden, sondern ein reiner Wissenstransfer in Richtung Zertifizierungsstelle.

Bei der Erstellung eines Angebots wird von der Zertifizierungsstelle die Unparteilichkeit der Mitglieder des Prüfungsteams gegenüber dem zu prüfenden Kunden sichergestellt. Eine ausführliche Beschreibung der auftragsbezogenen Unparteilichkeitsprüfung ist in Abschnitt 2.3.2 dargestellt.

Die Prüfung der projektbezogenen Unparteilichkeit muss vor Abgabe eines Angebots abgeschlossen werden. Dieses beinhaltet die Bestätigung der Unabhängigkeit und Unparteilichkeit der Mitglieder des Prüfungsteams. Grundsätzlich können wichtige Gründe die Anpassung des Auditteams auch nach Angebotserstellung erfordern. Die Unparteilichkeit von gegebenenfalls neuen Teammitgliedern ist vor Aufnahme der Tätigkeit nach dem zuvor beschriebenen Verfahren durch die Zertifizierungsstelle sicherzustellen. Der Cloud-Anbieter muss über diese Entscheidung informiert werden.

Weiterhin sind folgende Hinweise bei der Zusammenstellung des Auditteams zu beachten:

- **Externes Personal**: Bei der Auswahl von externem Personal gelten grundsätzlich die gleichen Anforderungen wie bei der Auswahl von internem Personal.
- **Qualifikation und spezielle Fachkenntnisse**: Es dürfen ausschließlich Auditoren eingesetzt werden, die sich vorab bei der Zertifizierungsstelle beworben hatten, bei denen Qualifikation und Erfahrung ausreichend sind und die von der Zertifizierungsstelle anerkannt worden sind. In Fällen, wo spezielles technisches Wissen bezüglich Prozessabläufen, Informationssicherheit oder rechtlichen Anforderungen notwendig ist, können zusätzlich Fachexperten in das Auditteam aufgenommen werden. Wird insbesondere nach der Stage 1 Dokumentenprüfung festgestellt, dass spezielle Fachkompetenzen notwendig sind, erfolgt eine Erweiterung des Auditteams.
- **Dolmetscher und Übersetzer**: Beim Einsatz von Dolmetschern oder Übersetzern ist darauf zu achten, dass diese keinen unangemessenen Einfluss auf das Audit ausüben. Dies kann beispielsweise durch den Einsatz von vereidigten Übersetzern erfolgen.
- **Beobachter und Betreuer**: Der Auditor kann von einem Betreuer begleitet werden, der zur Unterstützung des Audits und des Auditteams dient. Einer möglichen Teilnahme von Beobachtern (außer DAkkS-Auditoren sowie Beobachtern der Datenschutz-Aufsichtsbehörde bei Witness-Audits) am Audit muss vor Durchführung von Zertifizierungsstelle und Kunde zugestimmt werden.
- **Auditoren in Ausbildung**: Auditoren in Ausbildung / Auditassistenten dürfen als Teilnehmer in das Auditteam aufgenommen werden, sofern der Kunde dem nicht widerspricht.

Die Entlohnung des internen und externen Zertifizierungspersonals ist unabhängig vom Erfolg des Zertifizierungsaudits.

2.5.3 Erstellung des Angebots inkl. Zertifizierungsvereinbarung

Nach erfolgter positiver Bewertung des Antrags erfolgt die Erstellung des Angebots inkl. der Zertifizierungsvereinbarung sowie die Übermittlung an den Kunden. Das Angebot stellt die schriftliche Vereinbarung (Vertrag) zwischen dem Kunden und der Zertifizierungsstelle dar und basiert auf dem Zertifizierungsantrag. Das Angebot berücksichtigt die nachfolgenden Dokumente:

- Vorgaben gemäß "GDPR CC Abschnitt 6, Anhang A: Festlegung der Ermittlungszeit”
  DIN EN ISO/IEC 27006, Annex B Audit Time"[1]

[1] Die Ermittlung der Aufwände für Zertifizierungen nach DIN EN ISO/IEC 20000-1 erfolgt ebenfalls nach den Vorgaben der DIN EN ISO/IEC 27006 Annex B.

- Ausgefülltes Kalkulationsschema GDPR CC gem. Abschnitt 2.5.1
- GDPR CC Angebotsmuster der PwC Certification Services GmbH in der aktuellen Fassung (siehe Anhang A Nr. 3, “FBL Angebotsmuster”)
- Zertifizierungsantrag des Kunden
- Gebührentabelle der PwC Certification Services GmbH in der aktuellen Fassung
- Allgemeine Auftragsbedingungen der PwC Certification Services GmbH und der PwC Cyber Security Services GmbH, Stand: März 2021
- Zertifizierungsprogramm GDPR CC

Das Angebot enthält alle relevanten Informationen zur Zertifizierung. Eine kundenspezifische Anpassung muss in der Zielstellung, bei der Beschreibung des Anwendungsbereichs (Zertifizierungsgegenstand), der Stellungnahme der Erfüllung der Zertifizierungskriterien, der Nichtanwendbarkeit von Zertifizierungskriterien, der Anerkennung von bereits bestehenden Zertifizierungen – wenn anwendbar, und in der Zusammenstellung des Auditteams sowie in der Aufwands- und Kostenkalkulation vorgenommen werden.

Die Zertifizierungsvereinbarung berücksichtigt u. a. die folgend genannten Anforderungen:

- Die Zertifizierungsvereinbarung beschreibt den Zertifizierungszyklus, inklusive der durchzuführenden Audittätigkeiten, die erforderlich sind, um nachzuweisen, dass das Zertifizierungsgegenstand des Kunden die für die Zertifizierung nach den ausgewählten Normen oder sonstigen normativen Dokumenten geltenden Anforderungen erfüllt. Dabei werden anzuerkennende Zertifikate als auch für den Zertifizierungsgegenstand nicht anwendbare Zertifizierungskriterien berücksichtigt.
- In der Regel wird eine GDPR CC-Zertifizierung für drei Jahre angeboten. Das Auditprogramm beinhaltet für die Zertifizierung ein zweistufiges Audit (Stage 1- und Stage 2-Prüfung) sowie Überwachungsaudits im ersten und zweiten Jahr nach der Zertifizierungsentscheidung (Erstzertifizierung). Für Re-Zertifizierungsaudits, Änderungszertifizierungen, oder Erweiterungen der Zertifizierung ist jeweils eine separate Zertifizierungsvereinbarung zu erstellen.
- Die Datenverarbeitungsvorgänge bedürfen während der Gültigkeitsdauer der Zertifizierung der Überwachung in Form von mindestens jährlich durchzuführenden Überwachungsaudits. Das jährlich durchzuführende Überwachungsaudit ist frühestens nach Ablauf des sechsten und spätestens bis zum Ablauf des zwölften Monats ab Zertifizierungserteilung oder der entsprechenden Zeitpunkte der Folgejahr durchführen. Erfolgt das Überwachungsaudit nicht in der festgelegten Frist, ergreift die Zertifizierungsstelle Maßnahmen gem. § 5.6.4 GDPR CC.

Die PwC Cert sowie Teile derselben juristischen Person und jegliche Einheit unter der Organisationskontrolle der Zertifizierungsstelle dürfen keine Beratungsleistungen zum Datenschutz in Cloud-basierten personenbezogenen Datenverarbeitungsvorgängen anbieten oder bereitstellen. Dies beinhaltet auch die Durchführung von internen Audits.

Die PwC Cert darf nicht die Zertifizierung eines Cloud-basierten personenbezogenen Datenverarbeitungsvorgangs (Zertifizierungsgegenstandes) einer anderen Zertifizierungsstelle anbieten und durchführen.

In keiner Weise (mündlich oder schriftlich (beispielsweise im Angebot) darf angegeben oder stillschweigend angedeutet werden, dass eine Zertifizierung unkomplizierter, leichter, schneller oder preiswerter ist/wäre, wenn eine bestimmte Beratungsorganisation zum Einsatz käme.

Im Falle von Änderungen an der Zertifizierungsvereinbarung nach Beginn der Zertifizierungstätigkeiten wird die Vertragsprüfung erneut durchgeführt. Jegliche Änderungen werden involvierten Parteien, d. h. der PwC Cert, ggf. ausgegliederten Auditoren und dem Cloud-Anbieter bekannt gemacht.

Der Vereinbarung zwischen Cloud-Anbieter und Zertifizierungsstelle muss ein schriftlicher Vertrag zugrunde liegen, der auf dem Zertifizierungsantrag basiert.

2.5.4 Versand des Angebots an den Cloud-Anbieter

Nach Unterzeichnung des verbindlichen Angebots wird dieses dem Antragsteller übermittelt. Spätestens nach drei Arbeitstagen ist der Angebotseingang dem Antragsteller zu ermitteln. Änderungsanforderungen des Antragstellers können nur berücksichtigt werden, wenn dadurch keine Vorgaben der Zertifizierungsstelle verletzt werden.

2.6 Angebotsannahme

Die folgenden Abschnitte stellen den Prozess zur Angebotsannahme durch den Cloud-Anbieter dar. Der Prozess beinhaltet die Angebotsannahme durch den Cloud-Anbieter und die Auftragsanlage.

2.6.1 Entscheidung über Angebotsannahme

Der Cloud-Anbieter entscheidet nach Erhalt des Angebots über die Annahme oder Ablehnung des Angebots. Bei positiver Entscheidung (Annahme) unterschreibt er das Angebot und erteilt der Zertifizierungsstelle den Auftrag zur Zertifizierung. Die Gegenzeichnung des schriftlichen Angebots durch den Antragsteller ist gleichfalls die Auftragsbestätigung. Hierzu wird das für den Antragsteller spezifisch angepasste Muster der Zertifizierungsvereinbarung (siehe “FBL Angebotsmuster”, Absatz Erteilung des Auftrags) verwendet.

2.6.2 Auftragsanlage und Planung

Nach der Auftragsannahme durch den Cloud-Anbieter erfolgt die Auftragsanlage und Auditplanung .

3 Zertifizierungsaudit

3.1 Auditgrundsätze

Für alle von der Zertifizierungsstelle durchgeführten GDPR CC-Audits gelten die folgenden vertrauensbildenden Auditgrundsätze:

- **Vermittlung von Vertrauen**
  Der Wert der Zertifizierung ist der Grad an öffentlichem Vertrauen, der durch einen unparteiischen und kompetenten Nachweis einer dritten Stelle vermittelt wird. Die Zertifizierung ermöglicht es Cloud-Anbietern gegenüber dem Markt nachzuweisen, dass ihre Datenverarbeitungsvorgänge festgelegte Zertifizierungskriterien erfüllen, deren Erfüllung durch eine unparteiische dritte Stelle bestätigt wurde.
- **Unparteilichkeit**
  Für die Zertifizierungsstelle und ihr Personal ist es erforderlich, unparteiisch zu sein und als unparteiisch empfunden zu werden. Die Zertifizierungsstelle darf keinen kommerziellen, finanziellen oder sonstigen Druck zulassen, der die Unparteilichkeit gefährdet. Die Zertifizierungsstelle stellt sicher, dass keine Interessenskonflikte zwischen der Zertifizierungsstelle, den (externen) Auditoren und der geprüften Organisation bestehen. Insbesondere für ausgegliederte Auditoren wird sichergestellt, dass eine Gefährdung der Unparteilichkeit durch Vertragsbeziehungen zwischen zu zertifizierenden Cloud-Anbieter und den ausgegliederten Auditoren ausgeschlossen werden kann. Alle relevanten Teilprozesse sind im Hinblick auf dieses Ziel geprüft.
- **Kompetenz**
  Die Zertifizierungsstelle stellt durch einen geeigneten Auswahl- und Überwachungsprozess sowie das Managementsystem der Zertifizierungsstelle sicher, dass die für die Zertifizierung notwendigen Ressourcen über die notwendigen Kompetenzen und Fachkenntnisse verfügen. Dies schließt interne wie externe Auditoren gleichermaßen ein.
- **Nicht-diskriminierende Bedingungen**
  Die Zertifizierungsstelle muss sicherstellen, dass grundsätzliche Regelungen und Verfahren im Rahmen derer die Zertifizierungsstelle tätig ist, sowie ihre Verwaltung, nicht-diskriminierend sind. Weiterhin stellt die Zertifizierungsstelle sicher, dass Tätigkeiten durch (ausgegliederte) Auditoren nicht-diskriminierend durchgeführt werden.
- **Vertraulichkeit und Offenheit**
  Alle die vom Antragsteller für die Zertifizierung zur Verfügung gestellten Informationen werden, soweit nicht explizit aufgeführt, vertraulich behandelt. Die Zertifizierungsstelle stellt sicher, dass insbesondere Personen, einschließlich Ausschussmitgliedern, Personal aus externen Stellen oder Personen, die im Auftrag der Zertifizierungsstelle tätig sind, die Tätigkeiten vertraulich durchführen und alle erhaltenen Informationen vertraulich behandeln. Offenheit ist ein Grundsatz für den Zugang zu oder die Offenlegung von entsprechenden Informationen. Es liegt in der Verantwortlichkeit der Zertifizierungsstelle für den öffentlichen Zugang und die Offenlegung sachgemäßer und rechtzeitiger Informationen über ihre Auswahl-, Ermittlungs- und Zertifizierungsprozesse sowie über den Zertifizierungsstatus eines jeglichen Datenverarbeitungsvorgangs Sorge zu tragen.
- **Verantwortung**
  Die Gesamtverantwortung für den Zertifizierungsprozess liegt bei der Leitung der Zertifizierungsstelle. Das schließt die Einholung von ausreichend objektiven Nachweisen als Basis für die Zertifizierungsentscheidung mit ein. Basierend auf der Bewertung der Nachweise, trifft die Zertifizierungsstelle die Zertifizierungsentscheidung, die Zertifizierung zu erteilen, wenn keine Nichtkonformitäten festgestellt wurden. Werden Nichtkonformitäten festgestellt bzw. die Konformität nicht ausreichend nachgewiesen, wird die Zertifizierung nicht erteilt.

- **Offenheit für Beschwerden**
  Die Zertifizierungsstelle verfügt über ein Verfahren, mit dem Beschwerden (insbesondere von Cloud-Anbietern oder interessierten Parteien) bezüglich des Zertifizierungsprozesses oder Einsprüchen bezüglich der Zertifizierungsentscheidungen aufgenommen und konstruktiv bearbeitet werden.

3.2 Beteiligte und Rollenbeschreibungen

Beteiligt sind alle Mitarbeiter der Zertifizierungsstelle, die Zertifizierungen planen und durchführen sowie Ergebnisse bewerten und Zertifizierungsentscheidungen treffen.

3.3 Beratungsverbot

Beratungsleistungen zu einer zertifizierten oder zu zertifizierenden Dienstleistung, insbesondere die Mitwirkung bei internen Audits des Kunden sowohl vor als auch während der Prüfung, sind ausgeschlossen. Insbesondere darf das Personal der Zertifizierungsstelle innerhalb von 24 Monaten nicht zur Bewertung von Datenverarbeitungsvorgängen oder zur Zertifizierungsentscheidung bezüglich Datenverarbeitungsvorgängen eingesetzt werden, für die es Beratungsleistungen bereitgestellt hat (vgl. GDPR CC § 3.1.2 (6)).

Um sicherzustellen, dass es keinen Interessenkonflikt gibt, darf das Personal einschließlich derjenigen Personen, die in leitender Position tätig sind und die für einen Cloud-Anbieter Beratungen geleistet haben oder durch einen Cloud-Anbieter angestellt sind, nicht durch die Zertifizierungsstelle eingesetzt werden, um die Lösung einer Beschwerde oder eines Einspruchs des betreffenden Cloud-Anbieters zu bewerten oder zu genehmigen, wenn sie innerhalb der letzten zwei Jahre in Beratungen oder in ein Arbeitsverhältnis gegenüber dem Cloud-Anbieter eingebunden waren (vgl. GDPR CC § 4.3.2 (12)).

3.4 Überblick über den Zertifizierungsprozess

Die Auditzeit-Kalkulation und die Zusammenstellung des Auditteams für das GDPR CC-Audit erfolgen durch die Zertifizierungsstelle bereits im Rahmen der Angebotserstellung (siehe Abschnitt 2.5.1). Vor Beginn der Stage 1-Dokumentenprüfung erstellt das Auditteam den Auditplan (inkl. detaillierter Zeitplanung, bereitzustellender Unterlagen, Darstellung der Ermittlungsmethoden und Angaben zum Auditteam).

Der Auditplan wird dem Cloud-Anbieter vor der Stage 1-Dokumentenprüfung durch die Zertifizierungsstelle zugesendet. In dem Begleitschreiben wird dem Cloud-Anbieter eine angemessene Frist zur Übermittlung aller Informationen gesetzt. Die Zertifizierungsstelle verpflichtet den Cloud-Anbieter, alle Informationen fristgemäß entsprechend der im Zertifizierungsplan festgelegten Meilensteine, Fristen oder anderweitiger Zeitpunkte zur Verfügung zu stellen.

Die Erstzertifizierung beinhaltet fünf Schritte, die in ihrer Abfolge in der nachstehenden Grafik dargestellt sind. Die einzelnen Schritte sind im folgenden Prüfschema beschrieben.

Abbildung 2 Prozess der Zertifizierung

Hinweis: Die Überwachungsaudits als Bestandteil des Zertifizierungszyklus für Zertifizierungen mit einer Gültigkeitsdauer von maximal 3 Jahren werden in Abschnitt 0 dargestellt.

3.5 Durchführung der Stage 1-Dokumentenprüfung

Die Stage 1-Dokumentenprüfung erfolgt im Rahmen des Erstzertifizierung durch die von der Zertifizierungsstelle beauftragten Auditoren.

Das Angebot (inkl. Zertifizierungsvereinbarung) und die anliegenden Dokumente (z. B. Zeitplanung, Übersicht der vom Cloud-Anbieter bereitzustellenden Unterlagen für die Stage 1-Dokumentenprüfung) bilden die Grundlage für die Durchführung der Stage 1-Dokumentenprüfung. Im Rahmen der Stage 1-Dokumentenprüfung erfolgt in einem ersten Schritt durch den Auditteamleiter eine Validierung dieser Unterlagen. Im Fall von erforderlichen Anpassungen obliegt es dem Auditteamleiter z. B. weitere Informationen bei dem Cloud-Anbieter anzufordern bzw. diesen über Anpassungen im Zeitablauf zu informieren. Durch den Auditteamleiter wird sichergestellt, dass der Cloud-Anbieter mit angemessener Vorlaufzeit über die Tätigkeiten im Rahmen der Stage 1-Dokumentenprüfung informiert wird.

Ziel der Stage 1-Dokumentenprüfung ist die Bewertung der von dem Cloud-Anbieter erhaltenen Informationen und beinhaltet die folgend aufgezeigten Prozessschritte.

Im Rahmen der Stage 1-Dokumentenprüfung müssen durch den Cloud-Anbieter insbesondere Dokumente zur Verfügung gestellt werden, welche die Cloud-Services, die Datenverarbeitungsvorgänge des Cloud-Anbieters sowie den Zertifizierungsgegenstand angemessen beschreiben. Ein Besuch der Standorte durch den Auditteamleiter bzw. die Auditoren ist in dieser Phase der Prüfung nicht vorgesehen.

3.5.1 Anforderung von erforderlichen Informationen

Die angeforderten Dokumente im Rahmen der Stage 1-Dokumentenprüfung, sollten die folgenden Informationen beinhalten:

- Informationen über den Cloud-Anbieter und den Datenverarbeitungsvorgang
- Detaillierte Informationen zum Zertifizierungsgegenstand sowie dem Geltungsbereich der angestrebten Zertifizierung (inkl. der vom Cloud-Anbieter genannten nicht anwendbaren Zertifizierungskriterien sowie die Erläuterung)
- Beschreibung der Organisation und der Standorte
- Relevante Verfahrensanweisungen
- Überblick über die einschlägigen rechtlichen und behördlichen Vorschriften (einschl. Genehmigungen) und die Vereinbarungen mit den Behörden
- Relevante interne und externe Audit- und Reviewprogramme und daraus resultierende Managementberichte

3.5.2 Bereitstellung von prüfungsrelevanten Informationen

Die Verantwortung für Bereitstellung von prüfungsrelevanten Unterlagen gemäß Anforderung obliegt dem Cloud-Anbieter. Dies umfasst die Wahl der Übertragung von Daten. Bei Bedarf stellt die Zertifizierungsstelle dem Cloud-Anbieter im Rahmen des Audits web-basierte PwC Services mit sicherer Authentifizierung für den Dokumentenaustausch zur Verfügung.

Neben der initialen Bereitstellung von Dokumenten kann es aus der Sicht der Zertifizierungsstelle im Verlauf des Zertifizierungsverfahrens notwendig sein, weitere notwendige Informationen und/oder Dokumentationen anzufordern, die durch den Cloud-Anbieter bereitzustellen sind.

Ist die Bereitstellung von vertraulichen oder sensiblen Informationen durch den Cloud-Anbieter für die angemessene Prüfung des Datenverarbeitungsvorgangs aus Sicht der Zertifizierungsstelle notwendig, wird eine individuell geeignete Zugangsvereinbarung geschlossen, damit der Antragssteller die Informationen bereitstellen kann. Die Zertifizierungsstelle besitzt das Recht, das Zertifizierungsverfahren auszusetzen oder abzubrechen, sofern der Cloud-Anbieter der Pflicht zur Beibringung der Informationen und/oder Dokumentationen nicht nachkommt.

3.5.3 Durchführen der Stage 1-Dokumentenprüfung

Die Zertifizierungsstelle nimmt eine Bewertung der vom Cloud-Anbieter erhaltenen Informationen vor.

Der GDPR CC-Kriterienkatalog sowie das GDPR CC-Konformitätsbewertungsprogramm bilden die Grundlage für die Dokumentenprüfung.

Die Ziele der Beurteilung in der Stage 1-Dokumentenprüfung sind:

- Den Vorbereitungsstand sowie das Verständnis des Kunden bezüglich der GDPR CC-Anforderungen zu bewerten:
  - Es soll sichergestellt werden, dass die Informationen über den Cloud-Anbieter und den Datenverarbeitungsvorgang für die Durchführung des Zertifizierungsprozesses ausreichend sind. Dieses beinhaltet folgende notwendige Informationen:
    - Standort(e) des Kunden,
    - Prozesse und eingesetzte Arbeitsmittel,
    - festgelegte Lenkungsebenen (insbesondere bei Kunden mit mehreren Standorten)
  - Es soll sichergestellt werden, dass die Zertifizierungsstelle ein ausreichendes Verständnis über den Datenverarbeitungsvorgang erlangen konnte. Die Ergebnisse der Stage 1-Dokumentenprüfung bilden die Basis für die Festlegung von Schwerpunkten für die Planung der Stage 2-Prüfung.
  - Es soll sichergestellt werden, dass alle relevanten Ansprechpartner des Cloud-Anbieters auf die Stage 2-Prüfung vorbereitet und die erforderlichen standortspezifischen Bedingungen gegeben sind.
  - Verständnis und abschließende Validierung des Geltungsbereichs der angestrebten Zertifizierung (Bestätigung des Zertifizierungsgegenstandes).
- Beurteilung, ob die internen Audits und Managementbewertungen geplant und durchgeführt werden und keine bekannten Schwachstellen oder identifizierte Risiken der Stage 2-Prüfung entgegenstehen. Grundlage für die Beurteilung bilden alle Einzelheiten zu intern erkannten Verstößen gegen Prozesse, Abläufe, und Anweisungen, zusammen mit Angaben zu den entsprechenden Korrektur- und Vorbeugungsmaßnahmen.
- Die Klärung aller bekannten Differenzen im Verständnis zwischen der Zertifizierungsstelle und dem Cloud-Anbieter.
- Sicherstellung, dass die Mittel zur Durchführung der Zertifizierung inkl. aller Auswahl- und Ermittlungstätigkeiten verfügbar sind.
- Sicherstellung, dass die Zertifizierungsstelle über die technische und juristische Kompetenz und die Fähigkeit verfügt, die geforderten Zertifizierungstätigkeiten für den individuellen Zertifizierungsgegenstand des Cloud-Anbieters durchzuführen.

Das Ergebnis der Dokumentenprüfung wird in einem Stage 1-Prüfungsbericht dokumentiert. Der Bericht des Auditteamleiters umfasst eine Liste mit Mängeln im Zusammenhang mit dem Audit der Stage 1 sowie eine Empfehlung, ob die Zertifizierungsprüfung in der Stage 2-Prüfung fortgesetzt werden kann.

3.5.4 Bewertung und Entscheidung zur Weiterführung des Audits der Stage 2

Der Bericht zur Stage 1-Dokumentenprüfung sowie die Empfehlung des Auditteamleiters zur Weiterführung der Prüfung wird der Zertifizierungsstelle zur Bewertung vorgelegt. Der Stage 1-Prüfungsbericht beinhaltet neben den Schlussfolgerungen des Auditteamleiters im Hinblick auf das Erreichen der Ziele der Stage 1-Prüfung auch die Einschätzung der Bereitschaft für die Stage 2-Prüfung, einschließlich der Hinweise zu identifizierten Schwachstellen, die während Stage 2 als Nichtkonformität eingestuft werden könnten. Weiterhin beinhaltet der Stage 1-Prüfungsbericht eine Stellungnahme für die Zertifizierungsstelle, ob die Ergebnisse von Stage 1-Prüfung zu einer Verschiebung oder zu einem Abbruch von Stage 2 führen können.

Die Zertifizierungsstelle entscheidet auf Grundlage der dokumentierten Bewertung des vorliegenden Berichts, ob die Prüfung weitergeführt wird oder, ob Gründe gegen eine Weiterführung sprechen. Der Bericht zur Entscheidung über die Weiterführung der Prüfung in Stage 2 wird dem Cloud-Anbieter übergeben.

Sollte die Zertifizierungsstelle feststellen, dass Erfahrung mit dem Zertifizierungsgegenstand oder dem Cloud-Dienst-Typ fehlen, werden sowohl technische als auch rechtliche Kompetenz in angemessenem Umfang für die Zertifizierungstätigkeiten des Einzelauftrages dargelegt.

Der Cloud-Anbieter hat die Möglichkeit, die gegebenenfalls aufgeführten Mängel gemäß Stage 1-Prüfungsbericht bis zum Beginn der Stage 2-Prüfung nachzubessern. Bei der Ermittlung des Abstands zwischen Stage 1-Dokumentenprüfung und Stage 2-Prüfung müssen die Erfordernisse des Kunden Berücksichtigung finden, um Lösungen zu Schwachstellen, die während Stage 1 identifiziert wurden, zu finden.

Auf Grundlage der von dem Cloud-Anbieter bereitgestellten Informationen erfolgt die Vorbereitung der Prüfung der jeweiligen Zertifizierungskriterien mit den ausgewählten Ermittlungsmethoden in der Stage 2-Prüfung. Einhergehend wird die Planung der Ressourcen für Stage 2 bewertet und bei Bedarf angepasst. Mögliche Auswirkungen auf den Auditplan werden mit dem Cloud-Anbieter abgestimmt. In diesem Zusammenhang macht die Zertifizierungsstelle den Cloud-Anbieter auf die weiteren Arten von Informationen und Aufzeichnungen aufmerksam, die für eine detaillierte Ermittlung gemäß Konformitätsbewertungsprogramm § 5.2 GDPR CC in der Stage 2-Prüfung erforderlich sein können.

3.6 Durchführen der Stage 2-Prüfung

Das Ziel der Ermittlungstätigkeiten der Stage 2-Prüfung ist insbesondere die Beurteilung der Konformität der Datenverarbeitungsvorgänge des Cloud-Anbieters mit den Anforderungen der EU-Datenschutzgrundverordnung (DS-GVO). Die Ermittlung umfasst abhängig vom Zertifizierungskriterium eine Prüfung mittels der folgenden Ermittlungsmethoden: Dokumentenprüfung, Inspektion, Prüfung, Audit, und/oder Entwicklungs- und Designprüfungen. Die Stage 2-Prüfung beinhaltet die nachfolgend beschriebenen Prozessschritte.

3.6.1 Planen der Ermittlung (Anpassung der Planung)

Zu Beginn der Stage 2-Prüfung wird die vorliegende Planung (Ressourcen-, Zeit- und Ermittlungsmethoden) durch den Auditteamleiter validiert und bei Bedarf angepasst. Insbesondere die Erkenntnisse aus der Stage 1-Dokumentenprüfung werden hierbei berücksichtigt. Der vor der Durchführung der Ermittlung angepasste Auditplan, welcher mindestens Angaben zum zeitlichen Ablauf, den Ressourcen zur Durchführung jeder Ermittlungsaufgabe sowie der anzuwenden Ermittlungsmethoden umfasst, ist dem Cloud-Anbieter mindestens eine Woche vor Beginn der Stage 2-Prüfung auszuhändigen.

Grundsätzlich kann eine Anpassung der festgelegten Ermittlungszeit erforderlich werden, insofern bspw. im Rahmen der Stage 1-Dokumentenprüfung oder der Ermittlung besondere Feststellungen gemacht wurden (wenn z. B. Prüfungen weiterer Standorte, andere Komplexität des Datenverarbeitungsvorgangs als ursprünglich geplant) oder Nachprüfungen (Feststellung von Nichtkonformitäten) erforderlich sind. Bei Anpassungen des Ermittlungszeitaufwandes ist das definierte Verfahren (siehe Abschnitt 2.5.1) anzuwenden.

3.6.2 Eröffnungsgespräch (Kickoff)

Eine offizielle Eröffnungsbesprechung muss gemeinsam mit dem Management des Kunden und gegebenenfalls mit den Personen, welche die Verantwortung für die zu auditierenden Funktionen oder Prozesse tragen, zu Beginn der Stage 2-Prüfung durchgeführt werden. Der Zweck der Eröffnungsbesprechung, die üblicherweise vom Auditteamleiter durchgeführt wird, besteht darin, kurz zu erläutern, auf welche Art und Weise die Audittätigkeiten durchgeführt werden. Der Detailgrad muss der Vertrautheit des Kunden mit dem Auditprozess angemessen sein und das Folgende berücksichtigen:

- Vorstellung der Teilnehmer einschließlich einer Kurzdarstellung ihrer Rollen.
- Bestätigung des Auditplans (inkl. zeitliche Planung und Erhebungsmethoden).
- Bestätigung des Zertifizierungsgegenstands und Geltungsbereichs der Zertifizierung.
- Bestätigung des Status von Ergebnissen der Stage 1-Dokumentenprüfung (bzw. aus dem vorangegangenen Audit), falls zutreffend.
- Bestätigung sonstiger relevanter Vereinbarungen mit dem Kunden, wie z. B. Datum und Uhrzeit der Abschlussbesprechung, der Zwischenbesprechungen zwischen dem Auditteam und dem Management des Kunden.
- Bestätigung der offiziellen Kommunikationskanäle zwischen Auditteam und Kunde.
- Bestätigung, dass die vom Auditteam benötigten Ressourcen und Einrichtungen zur Verfügung stehen.
- Bestätigung von Angelegenheiten, die sich auf Vertraulichkeit beziehen.
- Bestätigung der für das Auditteam zutreffenden Arbeitsschutz-, Notfall- und Sicherheitsverfahren.
- Bestätigung der Verfügbarkeit, Rollen und Identitäten von etwaigen Betreuern und Beobachtern.
- Informationen zu der Berichterstattung sowie den Bedingungen, die zum vorzeitigen Abbruch des Audits führen können.
- Bestätigung, dass der Auditteamleiter und das Auditteam in Vertretung der Zertifizierungsstelle die Verantwortung für das Audit tragen und die Leitungsfunktion für die Ausführung des Auditplans einschließlich der Audittätigkeiten und des Auditpfades innehaben müssen.
- Kurzdarstellung der Wahl von Stichproben bei der Erhebung.
- Bestätigung der für das Audit zu gebrauchender Sprache.
- Bestätigung, dass der Kunde während des Audits über dessen Fortschritt und alle auftretenden Probleme auf dem Laufenden gehalten wird.
- Möglichkeit für den Kunden, Fragen zu stellen.

3.6.3 Durchführen der Ermittlung

Die Ermittlung erfolgt in den Räumlichkeiten des Cloud-Anbieters (Detailermittlung) sowie außerhalb der Standorte des Cloud-Anbieters (z. B. Planung, Dokumentenprüfung, Kommunikation mit dem Personal des Cloud-Anbieters, Verfassen des Ermittlungsberichts). Wenn Remote-Techniken wie Web-Meetings, Telefonkonferenzen oder die elektronische Fernprüfung der Datenverarbeitungsvorgänge (bspw. Penetrationstests oder Schwachstellenanalysen) eingesetzt werden, sind diese Aktivitäten im Ermittlungsplan (als Teil der Detailermittlung) aufzuführen. Remote-Techniken dürfen jedoch nur in begründeten Ausnahmen mehr als 30 % der geplanten Ermittlungszeit vor Ort ausmachen.

Der GDPR CC-Kriterienkatalog bildet die Grundlage für die Ermittlung in der Stage 2-Prüfung (vgl. Template „FBL Prüfcheckliste GDPR CC“). Er enthält „die Zertifizierungskriterien“, „Erläuterungen“, „Umsetzungshinweise“ und „Nachweise“. Die „Zertifizierungskriterien“ bezeichnen die normativen Voraussetzungen, die zu erfüllen sind, um ein Zertifikat auf der Grundlage des GDPR CC-Kriterienkatalogs zu erhalten. Sie stellen somit die Anforderungen dar, die in der Stage 2-Prüfung abgedeckt werden. Die „Erläuterungen“ sollen das Verständnis der Kriterien und ihre Herleitung aus der Datenschutz-Grundverordnung erleichtern.

3.6.4 Ermittlungsobjekte

Die Ermittlung erfolgt auf Grundlage der im Auftrag klar abgegrenzten Beschreibung des Zertifizierungsgegenstands (siehe Abschnitt 2.3.4). Gegenstand der Ermittlung ist auch das Zusammenwirken der Datenverarbeitungsvorgänge oder deren Bestandteile mit anderen Bestandteilen, Datenverarbeitungsvorgängen oder Diensten (inkl. der Betrachtung möglicher Schnittstellen zu Sub-Auftragsverarbeitern), wobei sich ein Cloud-Dienst aus einem oder mehreren Datenverarbeitungsvorgängen zusammensetzen kann.

Einem Datenverarbeitungsvorgang können wiederum die folgenden Ermittlungsobjekte zugeordnet werden:

- Vereinbarungen: Bei rechtsverbindlichen Vereinbarungen als Ermittlungsobjekt werden die Eigenschaften und Inhalte von Verträgen oder Vereinbarungen mit Cloud-Nutzern oder Subauftragsverarbeitern bewertet.
- Prozesse: Ein Prozess oder eine entsprechende und realitätsnahe Prozessdokumentation kann geprüft werden, um die Konformität mit den Zertifizierungskriterien zu bestätigen.
- Anbietereigenschaften: Eine Prüfung von Anbietereigenschaften umfasst die Begutachtung von Eigenschaften und Ausprägungen des Cloud-Anbieters, bspw. die zugrundeliegende Organisationsstruktur.
- Diensteigenschaften: Zu den Diensteigenschaften gehören insbesondere Cloud-Dienst-Features und -Funktionen, die für den Cloud-Nutzer unmittelbar sichtbar sind und geprüft werden müssen.
- Infrastrukturkomponenten: Eine Überprüfung kann Infrastrukturkomponenten umfassen, also physische Objekte, wie bspw. Hardware-Komponenten oder die Rechenzentrumsinfrastruktur.
- Softwarekomponenten: Die Prüfung von Softwarekomponenten umfasst virtuelle Objekte, bspw. Quellcode sowie die Zusammenstellung und Interaktionen der einzelnen Komponenten der Datenverarbeitungsvorgänge.
- die Entwicklungsumgebung: Die Prüfung der Entwicklungsumgebung umfasst eingesetzte Entwicklungsmethoden, sichere und vom Produktivsystem getrennte Test- und Entwicklungsumgebung, und Abnahmetests.
- Mitarbeiter des Cloud-Anbieters: Die Prüfung von Mitarbeitern kann notwendig sein, um bspw. deren fachliche oder persönliche Eignung sicherzustellen.
- (Datenschutz-)Managementsystem: Die Prüfung des (Datenschutz-)Managementsystems ist notwendig, um zu erkennen, ob der Cloud-Anbieter für das Management der relevanten Aspekte seiner Tätigkeiten, Produkte und Dienstleistungen ein System umgesetzt hat, das im Einklang mit der Politik der Organisation und den Zertifizierungskriterien steht.

3.6.5 Ermittlungsmethoden

Im Rahmen von Prüfungen nach GDPR CC umfasst die Ermittlung, abhängig vom Zertifizierungskriterium, eine Prüfung der vom Cloud-Anbieter zur Verfügung gestellten Dokumentationen, Inspektionen, Prüfungen, Audits, und/oder Entwicklungs- und Designprüfungen.

Die anzuwendenden Ermittlungsmethoden sind im Begleitdokument „GDPR CC-Ermittlungsmethoden“ für jedes Zertifizierungskriterium spezifiziert und werden entsprechend durch die Auditoren angewandt. Dabei können die Ermittlungsmethoden bei Bedarf kombiniert werden, um (zusätzliche) fundierte Informationen über das Ermittlungsobjekt zu erheben. Zudem kann die Ermittlung stichprobenartig erfolgen (vgl. Abschnitt 3.6.7).

Bei der Bereitstellung von Informationen und Daten durch den Cloud-Anbieter für die Ermittlung stellt die Zertifizierungsstelle die Integrität der Informationen und Daten durch konkrete Verifikation oder sonstige Kontrollen sicher.

Die Ausführung von einzelnen Ermittlungstätigkeiten wird protokolliert. Die Aufzeichnungen beinhalten das Datum und die Identität der Personen, die für die jeweiligen Ermittlungstätigkeiten verantwortlich sind. Beobachtungen, Daten und Berechnungen werden zu dem Zeitpunkt, zu dem sie gemacht werden, aufgezeichnet und der speziellen Ermittlungstätigkeit zugeordnet. Änderungen an den Aufzeichnungen zu früheren Versionen oder zu ursprünglichen Beobachtungen können durch die Versionierung der Dokumentation zurückverfolgt werden.

Dokumentenprüfung

Mit der Dokumentprüfung prüft der Auditor die Einhaltung der Zertifizierungskriterien anhand der Angaben in der Dokumentation des Cloud-Anbieters. Ein Cloud-Anbieter legt entsprechende Dokumente, (technische) Logs, Testate oder andere Dokumentationen vor. Insbesondere findet hierbei eine Rechtsanalyse statt (bspw. der rechtsverbindlichen Vereinbarungen), um sicherzugehen, dass die geltenden rechtlichen Kriterien erfüllt werden.

Zudem können im Rahmen einer Dokumentenprüfung auch Personenzertifikate (im Sinne der DIN EN ISO/IEC 17024) zum Kompetenznachweis für das Personal bzw. einer natürlichen Person (bspw. Des Datenschutzbeauftragten) und zur Gewährleistung eines angemessenen Datenschutzniveaus geprüft werden. Eine Dokumentprüfung wird stets mit geeigneten Ermittlungsmethoden ergänzt, um sicherzustellen, dass die dokumentierten Anweisungen, Verfahren, Regeln etc. auch fortlaufend vom Cloud-Anbieter umgesetzt werden.

Inspektion

Im Rahmen einer Inspektion (im Sinne der DIN EN ISO/IEC 17020) wird die Konformität eines Produktes oder Prozesses mit spezifischen Anforderungen (hier DS-GVO und den Zertifizierungskriterien) untersucht. Inspektionsparameter schließen Fragen zur Quantität, Qualität, Sicherheit, Zweckmäßigkeit sowie fortdauernden Einhaltung der Sicherheit von in Betrieb befindlichen Anlagen oder Systemen ein.

In Bezug auf die GDPR CC-Datenschutzzertifizierung wird mittels einer (rechtlichen) Inspektion insbesondere die Einhaltung von geeigneten technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 lit. a) bis d) DS-GVO geprüft. Die Inspektion kann alle Phasen im Rahmen der Lebensdauer der Ermittlungsobjekte betreffen, einschließlich der Entwicklungsphase. Bei der Inspektion können bspw. Datenverarbeitungsvorgänge im Rahmen einer Dienstnutzung durchgeführt werden, um die Funktionsweise und die Ergebnisse der Vorgänge beurteilen zu können. Ein Auditor vergleicht hierbei die zu erwartenden Ergebnisse gemäß der vorliegenden Dokumentation mit den tatsächlichen Ergebnissen, welche durch eine Dienstnutzung erbracht werden. Er erhält somit keinen Einblick in die internen Verarbeitungsschritte der Verarbeitungsvorgänge (‚Black-Box-Test‘). Daneben kann ein Vorgang oder eine Vorgangsreihe auch angestoßen und die tatsächliche Ausführung überwacht (‚Monitoring‘) oder Logs der Vorgangsausführung geprüft werden (‚White-Box-Test‘).

Prüfung

Eine Prüfung (im Sinne der DIN EN ISO/IEC 17025) umfasst Tests oder Messungen zur Untersuchung des Datenverarbeitungsvorgangs bzw. des Ermittlungsobjektes und zur Feststellung ihrer Übereinstimmung mit den Zertifizierungskriterien. So kann eine Assetprüfung durchgeführt werden, indem bei der Prüfung ein Asset (z. B. Hardware oder Softwarecode und ggf. die dazugehörige Dokumentation) untersucht wird.

Die Prüfung kann in Begleitung oder unter Anweisung eines Mitarbeiters des Cloud-Anbieters oder eigenständig durch den Auditor durchgeführt werden.

Der Cloud-Anbieter wird vorab über die Prüfung informiert und stellt den Auditor bspw. Notwendige Zugänge (bspw. Test-Accounts) oder (technische) Logs über die Ausführung des Vorgangs zur Durchführung der Prüfung bereit. Insofern notwendig, wählt der Auditor geeignete Testdaten. Hierzu zählen zufällig erzeugte Werte, die eine realistische und funktionskonforme Prüfung des Vorgangs ermöglichen. Ein Auditor kann zur Prüfung und Überwachung des Vorgangs (‚Monitoring') geeignete (ggf. extern bereitgestellte) Testierungs- und Auditierungsprodukte und -dienstleistungen nutzen. Die eingesetzten Produkte und Dienstleistungen zur Prüfung werden im Ermittlungsbericht dokumentiert.

Bei invasiven Ermittlungsverfahren oder Verfahren, die zu einer Beeinträchtigung von Datenverarbeitungsvorgängen des Cloud-Dienstes führen könnten, ist eine Abstimmung mit dem Cloud-Anbieter notwendig. Der Cloud-Anbieter ist verpflichtet, den Auditor bei der Durchführung zu unterstützen.

In Bezug auf die GDPR CC-Zertifizierung wird mittels einer (rechtlichen) Prüfung insbesondere die Einhaltung von geeigneten technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 lit. A) bis d) DS-GVO geprüft. Bspw. Kann mittels Sicherheitstests die korrekte und starke Verschlüsselung von Daten festgestellt werden. Bei der Durchführung von Sicherheitstests sei weiterführend auf die DIN EN ISO/IEC 15408 und DIN EN ISO/IEC 18045 hingewiesen.

Audit

Ein Audit (im Sinne der DIN EN ISO/IEC 17021-1) wird zum Zweck der Zertifizierung des (Datenschutz-) Managementsystems des Cloud-Anbieters durchgeführt, um zu erkennen, dass der Cloud-Anbieter für das Management der relevanten Aspekte seiner Tätigkeiten, Produkte und Dienstleistungen ein System verwendet, das im Einklang mit der Politik der Organisation sowie den Zertifizierungskriterien steht. Audits können vor Ort, aus der Ferne oder in einer Kombination aus beidem durchgeführt werden. Der Einsatz dieser Methoden sollte angemessen ausgewogen sein, unter anderem auf Grundlage der Berücksichtigung der damit verbundenen Risiken und Chancen.

Im Rahmen des Audits können insbesondere Befragungen, Beobachtungen und Prüfungen durchgeführt werden, um Informationen über Wissen und Fertigkeiten zu ermitteln sowie festzustellen, ob Prozesse und das Managementsystem beim Cloud-Anbieter gelebt werden. Die Befragung von Mitarbeitern des Cloud-Anbieters oder anderen Personen, die mit der Erbringung der Datenverarbeitungsvorgänge befasst sind, kann zur Sachverhaltsermittlung einzelner Aspekte und zur Überprüfung der Richtigkeit der Dokumentation eingesetzt werden. Sie soll insbesondere zur Überprüfung bei vom Auditor als kritisch erkannten Aspekten eingesetzt werden. Befragungen können schriftlich oder persönlich durchgeführt werden. Sie sollen jedenfalls hinsichtlich zentraler Aspekte als mündliche Befragung durchgeführt werden. Soweit eine persönliche Befragung unverhältnismäßig wäre, kann sie in Form von Videokonferenzen durchgeführt werden. Eine Person bei der Erfüllung einer Aufgabe zu beobachten, kann durch die damit dargelegte Anwendung von Wissen und Fertigkeiten zur Erzielung eines gewünschten Ergebnisses direkte Nachweise für die Kompetenz liefern. Schriftliche, mündliche und praktische Prüfungen können gute und gut dokumentierte Nachweise für vorhandenes Wissen und — je nach angewendeter Methodik — auch für Fertigkeiten liefern.

Eine Vor-Ort-Prüfung umfasst die Inaugenscheinnahme der Verfahren und technischen Einrichtungen in den Räumlichkeiten des Cloud-Anbieters. In Bezug auf die GDPR CC-Zertifizierung sollen insbesondere (rechtliche) Audits durchgeführt werden, um eine korrekte Einrichtung, Aufrechterhaltung und Pflege eines Datenschutz-Managementsystems (im Sinne von Art. 24 und 25, 32, 33, 34 sowie 37 bis 39 DS-GVO) zu prüfen. Die Sicherstellung eines Datenschutz-Managementsystems sollte der fortwährenden Sicherstellung des Datenschutzniveaus des zertifizierten Cloud-Dienstes dienen. Für weiterführende Literatur zur Durchführung von Audits sei insbesondere auf die DIN EN ISO/IEC 17021-1:2015 Tz. 9.4 und DIN EN ISO 19011 verwiesen. Für die Durchführung von Audits aus der Ferne sei auf IAF MD 4 verwiesen.

Entwicklungs- und Designprüfung

Eine Entwicklungsprüfung umfasst die Prüfung von Entwicklungsmethoden und -verfahren sowie bei Bedarf eine Prüfung der Testsysteme und -umgebungen, welche bei der Entwicklung von Hard- und Software zur Erbringung der Datenverarbeitungsvorgänge eingesetzt werden. Bei der Designprüfung können unter anderem die gewählte Architektur, Datenbankdiagramme, Datenflussdiagramme, Designentscheidungen aber auch die Konfiguration des Cloud-Dienstes zur Erbringung des Datenverarbeitungsvorgangs geprüft werden. Eine Entwicklungs- und Designprüfung sollte auch eine Rechtsanalyse umfassen, um sicherzugehen das die geltenden rechtlichen Kriterien erfüllt werden. So kann eine rechtliche Entwicklungs- und Designprüfung insbesondere im Rahmen der Prüfung zur Erfüllung des Art. 25 DS-GVO oder zur Überprüfung der Datenschutz-Folgenabschätzung erforderlich sein.

3.6.6 Stichprobenartige Prüfung der Zertifizierungskriterien bei anerkannten Zertifikaten

Soweit die Zertifizierungsstelle Zertifikate für Bestandteile von Datenverarbeitungsvorgängen anerkennt, erfolgt eine Validierung der bereits erfolgten Anerkennung von bestehenden Zertifizierungen durch eine stichprobenartige Prüfung der Einhaltung der GDPR CC-Zertifizierungskriterien.

Ergeben sich im Rahmen der Prüfung Unregelmäßigkeiten in Hinblick auf anerkannte Zertifizierungen (bspw. Vermutung von Abweichungen), so ist die Ermittlung im Rahmen des laufenden Zertifizierungsverfahrens zu erweitern und ggf. vollumfänglich auf die Zertifizierungskriterien, die durch das anerkannte Zertifikat abgedeckt werden, auszudehnen (siehe GDPR CC § 5.1.7).

3.6.7 Wahl von Stichproben bei der Ermittlung

Im Rahmen der Ermittlung kann eine Erhebung als Stichprobe erfolgen, wenn es weder praktikabel noch kostengünstig ist (z. B., wenn Aufzeichnungen zu zahlreich oder geographisch zu weit gestreut sind), alle verfügbaren Informationen während einer Ermittlung zu prüfen.

Die Stichprobenentnahme umfasst folgende Schritte (siehe DIN EN ISO 19011:2018 Tz. A.6.1):

a) Festlegen der Ziele der Stichprobenentnahme;
b) Auswahl des Ausmaßes sowie der Zusammensetzung der Grundgesamtheit, aus der die Stichprobe zu entnehmen ist;
c) Auswahl einer Methode zur Stichprobenauswahl;
d) Bestimmen der Größe der zu entnehmenden Stichprobe;
e) Durchführen der Stichprobenauswahl;
f) Zusammenstellen, Beurteilen, Berichten und Dokumentieren der Ergebnisse.

Die Auswahl einer geeigneten Stichprobe sollte sich sowohl auf das Probenentnahmeverfahren als auch auf die Art der geforderten Daten stützen, z. B., um ein bestimmtes Verhaltensmuster abzuleiten oder Schlüsse über eine Grundgesamtheit zu ziehen (siehe DIN EN ISO 19011:2018 Tz. A.6.1).

Die Stichprobe ist mindestens so umfassend zu wählen, dass die Untersuchung der ausgewählten Proben einen Rückschluss auf die Erfüllung der Zertifizierungskriterien zulässt. Die folgenden Maßgaben sind für die Stichprobenauswahl durch die Auditoren heranzuziehen, um sicherzustellen, dass eine genommene Probe die Grundgesamtheit repräsentiert.

a) In der Regel wird eine Stichprobengröße von 3 % als repräsentativ angesehen.
b) Bei einer sehr großen Grundgesamtheit (bspw. bei der Prüfung von rechtsverbindlichen Vereinbarungen) kann in begründeten Ausnahmen die folgende Formel verwendet werden:

a. $y = \lceil(\sqrt{x}2{,}5)\rceil$.

c) Der Umfang der Stichprobe muss die 2,5-Wurzel der Grundgesamtheit sein, gerundet auf die höhere ganze Zahl, wobei y = die Anzahl an Objekten ist, die in die Stichprobe aufzunehmen sind und x = die Gesamtanzahl an Objekten.

Beispiel:

In der folgenden Tabelle ist beispielhaft angegeben, wie groß die Stichprobe bei der gegebenen Grundgesamtheit gewählt werden muss. (z. B. sollen bei 1000 geschlossenen rechtsverbindlichen Vereinbarungen 16 Vereinbarungen in die Stichprobe aufgenommen und geprüft werden).

#	Grundgesamtheit (x = die Gesamtanzahl an Objekten)	Stichprobenumfang (y = Stichprobenumfang)
1	1	1
2	10	3
3	50	5
4	100	6
5	500	12
6	1000	16
7	1000000	251

Praxishinweis: Die 2,5-Wurzel der Grundgesamtheit berechnet sich in Excel mit der Formel

=POWER(GRUNDGESAMTHEIT;1/2,5)

Bei der Stichprobenauswahl sollten durch die Auditoren sowohl technische als auch organisatorische Ermittlungsobjekte einbezogen werden, insofern diese von den Zertifizierungskriterien betroffen sein könnten.

Bei der Stichprobenentnahme sollte die Qualität der verfügbaren Daten berücksichtigt werden, da Probenentnahmen aus unzureichenden und ungenauen Daten kein brauchbares Ergebnis liefern (siehe DIN EN ISO 19011:2018 Tz. A.6.1).

Es können entweder die entscheidungsbasierte Stichprobenentnahme oder die statistische Stichprobenentnahme angewandt werden.

Entscheidungsbasierte Stichprobenentnahme (siehe DIN EN ISO 19011:2018 Tz. A.6.2):

Entscheidungsbasierte Stichprobenentnahme stützt sich bei der Festlegung von Proben auf Kompetenz und Erfahrungen der Auditoren. Bei der entscheidungsbasierten Stichprobenentnahme sollte Folgendes durch den Auditor berücksichtigt werden:

a) frühere Ermittlungserfahrungen bei vergleichbaren Zertifizierungsverfahren und Zertifizierungsgegenständen;
b) Anforderungen und Komplexität der Zertifizierungskriterien für die eine Probe genommen werden soll;
c) Komplexität des Ermittlungsobjektes und vorliegende Wechselwirkungen (bspw. mit anderen Vorgängen);
d) Grad der Veränderung und Vielfältigkeit des Ermittlungsobjektes in Bezug auf die Technik, den menschlichen Faktor oder das Datenschutz-Managementsystem;

e) mögliche Risiken, die das Ermittlungsobjekt betreffen oder dem Zertifizierungskriterium inne sind;
f) Ergebnisse aus Überwachungstätigkeiten oder vorangegangenen Ermittlungen.

Statistische Stichprobenentnahme (siehe DIN EN ISO 19011:2018 Tz. A.6.2):

Statistische Verfahren zur Stichprobenentnahme verwenden ein Auswahlverfahren, das auf Wahrscheinlichkeitstheorie beruht. Stichprobenprüfungen anhand der Anzahl fehlerhafter Einheiten (Attributprüfungen) werden verwendet, wenn es nur zwei mögliche Ergebnisse bei jeder Stichprobe gibt (z. B. richtig/falsch oder bestanden/nicht bestanden). Stichprobenprüfungen anhand quantitativer Merkmale (Variablenprüfungen) werden verwendet, wenn die Ergebnisse der Stichproben in einem kontinuierlichen Bereich auftreten. Der Plan zur Stichprobenentnahme sollte berücksichtigen, ob die Ergebnisse, die geprüft werden, wahrscheinlich attributbasiert oder variablenbasiert sind. Bspw. könnte bei der Beurteilung der Konformität abgeschlossener Vereinbarungen mit den Zertifizierungskriterien ein attributbasierter Ansatz verwendet werden. Bei der Prüfung der Anzahl der Sicherheitsverstöße würde ein variablenbasierter Ansatz wahrscheinlich besser geeignet sein. Elemente, die einen Einfluss auf die Stichprobenentnahme haben können und daher beachtet werden müssen, sind:

a) Kontext, Größe, Art und Komplexität des Ermittlungsobjektes sowie mögliche Wechselwirkungen.
b) Anforderungen und Komplexität der Zertifizierungskriterien für die eine Stichprobe gezogen werden soll.
c) Die Häufigkeit der Stichprobenentnahme.
d) Der Zeitpunkt der Stichprobenentnahme.
e) Das gewählte Vertrauensniveau, in der Regel sollte das Probenentnahmerisiko nicht größer als 5% sein. Ein Probenentnahmerisiko von 5 % bedeutet, dass der Auditor bereit ist, das Risiko zu akzeptieren, dass 5 von 100 der geprüften Proben nicht die tatsächlichen Werte widerspiegeln, die sich ergeben würden, wenn die Grundgesamtheit geprüft worden wäre.
f) Das Auftreten von unerwünschten und/oder unerwarteten Ereignissen.

Aufzeichnungen der Daten zur Probenentnahme, die Teil der durchzuführenden Ermittlung sind, sind durch die Auditoren nachzuhalten und müssen als Teil der Prüfungsdokumentation, wo zutreffend, Folgendes enthalten:

a) Einen Verweis auf das angewandte Verfahren zur Stichprobenauswahl und etwaige Auswahlkriterien, die für die Beurteilung verwendet wurden (z. B. was eine annehmbare Stichprobe ist).
b) Das Datum der Stichprobe.
c) Eine Begründung für Probennahme.
d) Das Ermittlungsobjekt für das eine Stichprobe genommen wird.
e) Beschreibung der Grundgesamtheit sowie der zugrunde liegende Zeitraum.
f) Daten zur Identifizierung und Beschreibung der Probe (z. B. Größe, Nummer, Menge, Bezeichnung).
g) Eine Benennung des Personals, welches die Stichprobe zieht.
h) Informationen zur verwendeten Software oder Hardware zur Probennahme (insofern eingesetzt).
i) Ggf. die verwendeten statistischen Parameter.
j) Das Ergebnis der Stichprobe.

3.6.8 Ermittlung bei mehreren Standorten

In Situationen, in denen der Cloud-Anbieter einen Datenverarbeitungsvorgang an mehreren Standorten durchführt, sind solche Standorte in den Ermittlungsplan einzubeziehen (siehe IAF MD 5:2015 Tz. 9.1).

Die durchgeführten Ermittlungsverfahren bei mehreren Standorten sollten jeweils vollständig dokumentiert und im Hinblick auf ihre Wirksamkeit beurteilt werden (darunter Prinzipien und Vorgehensweisen bei der Ermittlung) (siehe IAF MD 5:2015 Tz 9.4).

Standorte müssen in die Ermittlung vollständig einbezogen werden, wenn an diesen Schlüsseltätigkeiten des Cloud-Anbieters ausgeübt werden. Somit muss mindestens die Zentrale (festgelegt durch den Cloud-Anbieter, nicht notwendigerweise der Hauptsitz) zwingend geprüft werden. Insbesondere wenn die Standorte sehr ähnliche Prozesse/Tätigkeiten ausführen (siehe IAF MD 1:2018 Tz. 4.6, 6.1.1.1) muss für die Stichprobenauswahl eine repräsentative Berücksichtigung der Haupt- und Nebenstandorte sichergestellt werden (siehe IAF MD 1:2018 Tz. 6.1.2.1).

Bei der Festlegung der Stichprobengröße sind folgende Maßgaben heranzuziehen (siehe IAF MD 1:2018 Tz. 6.1.3):

a) Das in dem Abschnitt “Wahl von Stichproben bei der Ermittlung” definierte Verfahren zur Bestimmung der Größe der Stichprobe ist bei der Ermittlung von mehreren Standorten verbindlich anzuwenden.
b) Jedes durchgeführte Stichprobenverfahren ist nachvollziehbar zu dokumentieren. Dieses umfasst neben der Beschreibung des Stichprobenverfahrens insbesondere die Anlage von ermittelten Grundgesamtheiten sowie für die Stichprobenauswahl genutzte Templates (Sample Generator Template).
c) Die Mindestanzahl an Standorten, die pro Ermittlung zu begehen sind, ist für die Erstprüfung und die Überwachungsprüfung festgelegt und anzuwenden:
    a) Erstprüfung: Der Umfang der Stichprobe muss die Quadratwurzel der Anzahl der Nebenstandorte sein: ($y = \sqrt{x}$), gerundet auf die höhere ganze Zahl, wobei y = die Anzahl an Nebenstandorten ist, die in die Stichprobe aufzunehmen sind und x = die Gesamtanzahl an Nebenstandorten.
    b) Überwachungsprüfung: Der Umfang der jährlichen Stichprobe muss die Quadratwurzel der Anzahl der Standorte sein, multipliziert mit dem Faktor von 0,6 als Koeffizient ($y = 0{,}6*\sqrt{x}$), aufgerundet auf die nächste ganze Zahl.

a. Die Zentrale musswährend jeder Erstzertifizierung und mindestens einmal jährlich als Teil der Überwachung geprüft werden.
b. Mindestens 25 % der Stichproben sind nach dem Zufallsprinzip auszuwählen (siehe IAF MD 1:2018 Tz. 6.1.2.2). Der Rest ist so auszuwählen, dass die Unterschiede der Standorte, die über den Gültigkeitszeitraum der Zertifizierung ausgewählt werden, so groß wie möglich sind (siehe IAF MD 1:2018 Tz. 6.1.2.3). Zudem muss über den Gültigkeitszeitraum der Zertifizierung jeder Standort mindestens einmal geprüft werden.
c. Der Umfang oder die Häufigkeit der Stichprobe wird erhöht, wenn die Risikoanalyse der Zertifizierungsstelle für den Datenverarbeitungsvorgang oder den Nebenstandorten besondere Umstände erkennen lässt (bspw. Veränderungen des Standorts, Ergebnisse interner Audits des Cloud-Anbieters, Veränderung von Risiken).
d. Bei Änderung der Struktur des Cloud-Anbieters (bspw. Aufnahme eines neuen Standorts) ist das Stichprobenverfahren durch die Auditoren anzupassen. Dazu gehört die Erwägung, ob der/die neue(n) Standort(e) zu prüfen ist/sind oder nicht.

Beispiel:

1 Hauptniederlassung (Zentrale):

- Begehung bei jedem Ermittlungszyklus (Erstprüfung und Überwachungsprüfung)

4 nationale Zweigstellen:

- Stichprobe = 2: mindestens 1 nach dem Zufallsprinzip

27 regionale Geschäftsstellen:

- Stichprobe = 6: mindestens 2 nach dem Zufallsprinzip

Einschränkungen der Stichprobenverfahren zur Ermittlung bei mehreren Standorten sind zulässig, wenn das beschriebene Stichprobenverfahren im Ermessen des Auditors nicht angemessen ist, um ausreichend Vertrauen zu schaffen (siehe IAF MD 1:2018 Tz. 6.1.1.4, 6.1.2.4, IAF MD 5:2015 Tz. 9.2, 10.3). Gründe für Einschränkungen müssen durch die Auditoren dokumentiert werden und können im Hinblick auf folgende Faktoren begründet werden:

a) Die Risiken für einen Datenverarbeitungsvorgang für einen Standort.
b) Gesamtzahl des Personals am Standort.
c) Signifikante Unterschiede in der Größe der Standorte.
d) Komplexität der Tätigkeiten am Standort.
e) Abweichungen im Geschäftszweck der Standorte.
f) Abweichungen in Arbeitsverfahren oder den durchgeführten Aktivitäten.
g) Komplexität der Informationssysteme an den verschiedenen Standorten.
h) Mögliche Wechselwirkungen mit kritischen Informationssystemen.
i) Vorhandensein von mehreren/eigenen Datenschutzmanagementsystemen pro Standort.
j) Variationen des Designs und der Funktionsweise der Steuerungen.
k) Aufzeichnungen zu Beschwerden und anderen relevanten Aspekten zu Korrektur- und vorbeugenden Maßnahmen.
l) Vorfälle im Bereich der Daten- und Informationssicherheit an den einzelnen Standorten.
m) Ergebnisse interner Audits an den Standorten und Managementbewertungen oder frühere Zertifizierungsaudits;
n) Abweichende gesetzliche Anforderungen.
o) Unterschiede in Kultur oder Sprache.
p) Geografische Standortverteilung.
q) Handelt es sich um permanente oder temporäre Standorte.

Wird durch die Auditoren festgestellt, dass kein stichprobenbasiertes Verfahren angewendet werden kann, so ist eine einzelne Prüfung der Standorte erforderlich (siehe IAF MD 1:2018 Tz. 1, 4.6, 6.2):

- Das Ermittlungsprogramm muss eine Erstprüfung für alle Standorte umfassen.
- Bei Überwachungsprüfungen sind 30 % aller Standorte, gerundet auf die nächste ganze Zahl, jährlich zu prüfen.
- Jede Prüfung muss die Zentrale umfassen.
- Die für die zweite Überwachungsprüfung ausgewählten Standorte unterscheiden sich in der Regel von denjenigen Standorten, die für die erste Überwachungsprüfung ausgewählt wurden.

Üblicherweise würden an Nebenstandorten Vor-Ort-Prüfungen durchgeführt werden. Jedoch sollten die folgenden Verfahren als mögliche Alternativen berücksichtigt werden, um einige Vor-Ort-Prüfungen zu ersetzen (siehe IAF MD 5:2015 Tz. 9.3):

- Persönliche Interviews oder Treffen mit dem Cloud-Anbieter.
- Überprüfung von Tätigkeiten an Nebenstandorten anhand von Dokumenten.

- Fernabfrage von elektronischen Standorten, die Aufzeichnungen oder anderweitige Informationen beinhalten, die in Bezug auf den Datenverarbeitungsvorgang und den/die Nebenstandort(e) begutachtungsrelevant sind.
- Nutzung von Video- und Telefonkonferenzen sowie anderen Technologien, die eine wirksame Ermittlung aus der Ferne ermöglichen.

3.6.9 Während des Audits

Während des Audits müssen die Auditfeststellungen, die Konformitäten zusammenfassend und Nichtkonformitäten detailliert beschreiben, festgestellt, eingeordnet und aufgezeichnet werden, um auf Grundlage von Informationen eine Zertifizierungsentscheidung treffen oder die Zertifizierung aufrechterhalten zu können.

Verbesserungsmöglichkeiten dürfen ermittelt und aufgezeichnet werden, sofern dies nicht nach den Anforderungen des Zertifizierungsprogramms verboten ist. Jedoch dürfen Auditfeststellungen, die Nichtkonformitäten sind, nicht als Verbesserungsmöglichkeiten aufgezeichnet werden.

Nichtkonformitäten müssen bezüglich einer bestimmten Anforderung aufgezeichnet werden und müssen eine klare Angabe der Nichtkonformität enthalten, welche die objektiven Nachweise für die Nichtkonformität im Einzelnen beschreiben. Nichtkonformitäten müssen mit dem Kunden erörtert werden, um sicherzustellen, dass die dafür gefundenen Nachweise korrekt sind und diese Nichtkonformitäten verstanden werden. Allerdings muss sich der Auditor zurückhalten, Ursachen von Nichtkonformitäten oder deren Lösungen vorzuschlagen.

Der Auditteamleiter muss versuchen, alle eventuellen Meinungsverschiedenheiten zwischen Auditteam und Kunden in Bezug auf Auditnachweise oder Auditfeststellungen aufzulösen, wobei ungelöst bleibende Punkte aufgezeichnet werden müssen.

Außerdem werden zwischen den Mitgliedern des Auditteams sowie dem Kunden in regelmäßigen zeitlichen Abständen Informationen über den Fortschritt und Stand des Audits ausgetauscht. Der Kunde und das Auditteam werden über nichterreichbare Auditziele und Risiken informiert. Gegenmaßnahmen und Änderungsbedarf werden gemeinsam mit dem Kunden erörtert und in Form von Veränderung des Auditplans, Änderungen an den Zielen, am Auditumfang oder durch Abbruch des Audits erfolgen. Der Auditteamleiter erstattet über den Verlauf, die Ergebnisse und Änderungen Bericht.

3.6.10 Abschlussbesprechung

Vor der Abschlussbesprechung muss das Auditteam:

- die Auditfeststellungen und alle sonstigen im Verlauf des Audits gesammelten geeigneten Informationen gegenüber den Auditzielen bewerten;
- gemeinsam die Auditschlussfolgerungen unter Berücksichtigung von Ungewissheiten bezüglich des Auditprozesses ziehen;
- alle erforderlichen Auditfolgemaßnahmen ermitteln;
- die Eignung des Auditprogramms bestätigen oder alle erforderlichen Veränderungen ermitteln (z. B. Auditumfang, Auditdauer, den für das Audit gewählten Zeitraum, die Überwachungshäufigkeit, Kompetenzen).

Eine offizielle Abschlussbesprechung muss gemeinsam mit dem Management des Kunden und gegebenenfalls mit den Personen, welche die Verantwortung für die zu auditierenden Funktionen oder Prozesse tragen, durchgeführt werden. Die Anwesenheit bei dieser Abschlussbesprechung muss dokumentiert werden. Der Zweck der Abschlussbesprechung, die üblicherweise vom Auditteamleiter

durchgeführt wird, besteht darin, die aus dem Audit gezogenen Schlussfolgerungen einschließlich der Empfehlung hinsichtlich der Zertifizierung vorzustellen. Alle Nichtkonformitäten müssen so dargestellt werden, dass sie verstanden werden, und es muss ein Zeitrahmen für deren Beantwortung vereinbart werden.

Die Abschlussbesprechung muss darüber hinaus die nachstehenden Punkte umfassen, wobei der Grad der Detailliertheit der Vertrautheit des Kunden mit dem Auditprozess angemessen sein muss:

- Hinweis an den Kunden, dass die erhaltenen Auditnachweise auf einer Stichprobe an Informationen basieren und daher ein gewisses Unsicherheitselement beinhalten.
- Methode und Zeitraum der Berichterstattung einschließlich Einstufung der Auditfeststellungen.
- Prozess der Zertifizierungsstelle für die Behandlung von Nichtkonformitäten einschließlich aller Konsequenzen, die den Status der Zertifizierung des Kunden betreffen.
- Zeitrahmen, innerhalb dessen der Kunde eine Ursachenanalyse und einen Plan für Korrekturen und Korrekturmaßnahmen in Bezug auf die im Verlauf des Audits ermittelten Nichtkonformitäten vorlegen muss – in der Regel 2 Monate.
- nach dem Audit erfolgende Tätigkeiten der Zertifizierungsstelle.
- Informationen zu den Prozessen für die Behandlung von Beschwerden und Einsprüchen.

Der Kunde muss die Möglichkeit erhalten, Fragen zu stellen. Alle Meinungsverschiedenheiten zwischen dem Auditteam und dem Kunden in Bezug auf die Auditfeststellungen oder die aus dem Audit gezogenen Schlüsse müssen erörtert und wenn möglich ausgeräumt werden. Alle nicht gelösten Meinungsverschiedenheiten müssen aufgezeichnet und an die Zertifizierungsstelle weitergeleitet werden.

3.6.11 Erstellung Ermittlungsbericht durch Auditteamleiter

Der Auditteamleiter erstellt auf der Grundlage der Ermittlung einen Ermittlungsbericht, indem die Ermittlungsergebnisse genau, klar, eindeutig und objektiv dargelegt werden (siehe DIN EN ISO/IEC 17065:2013 Tz. 7.4.9, DSK Tz. 7.4).

Im Allgemeinen muss der Ermittlungsbericht die zwei geprüften Ebenen beim Cloud-Anbieter widerspiegeln. Zum einen das Datenschutz-Managementsystem des Cloud-Anbieters als Organisation und zum anderen die Erfüllung der Zertifizierungskriterien in Bezug auf den/die zu zertifizierenden Datenverarbeitungsvorgang/-gänge. Der Ermittlungsbericht enthält mindestens folgende Angaben:

- Eindeutige Kennzeichnung, so dass alle Teile des Ermittlungsberichts als Teil eines vollständigen Berichts erkannt werden sowie eine eindeutige Kennzeichnung des Endes.
- Das Ausstellungsdatum des Berichts.
- Angaben zu den Auditoren zur Durchführung des Ermittlungsverfahrens, darunter den Namen und die Unternehmensanschrift.
- Angaben zum Cloud-Anbieter, darunter den Namen und die Anschrift.
- Eine detaillierte Beschreibung des Zertifizierungsgegenstandes, mit Angabe aller relevanten Datenverarbeitungsvorgänge, sodass eine abgeschlossene Verfahrensstruktur gewährleistet wird (siehe § 5.1.4).
- Eine Darstellung des zeitlichen Ablaufs, darunter mindestens das Start- und Enddatum der Ermittlung.
- Eine Darstellung des Umfangs der Ermittlung mit Angabe der Standorte und Räumlichkeiten, an bzw. in denen die Ermittlung erfolgt ist, einschließlich wenn sie in den Räumlichkeiten des Cloud-Anbieters oder an anderen Orten als den permanenten Räumlichkeiten der Auditoren oder Zertifizierungsstelle oder in zugehörigen zeitweiligen oder mobilen Räumlichkeiten durchgeführt werden.

- Die Maßnahmen, welche die Auditoren zur Ermittlung angewendet hat, insbesondere Angaben zu Ermittlungsmethoden nach § 5.2.4 und –sofern für das Verständnis erforderlich– eine Begründung für deren Einsatz.
- Eine Aufstellung der geprüften Objekte (siehe § 5.2.3)
- Angaben zur Verwendung technischer Prüfsoftware und -hardware (z. B. verwendete Programme zur Durchführung von technischen Ermittlungen).
- Die Angabe der durch die Zertifizierungsstelle anerkannten Zertifikate sowie die Ergebnisse über die stichprobenartige Überprüfung.
- Eine Aussage über die Prüfung des Zusammenwirkens der Datenverarbeitungsvorgänge.
- Ggf. Angaben über spezielle Ermittlungsbedingungen, wie etwa Umgebungsbedingungen.
- Bei Bedarf, welche Ermittlungsungenauigkeiten auftreten können, oder welche Gefahren für Ermittlungsgenauigkeit, -wiederholbarkeit und -reproduzierbarkeit bestehen (siehe DIN ISO/IEC 17007:2021 Tz. 5.4.1).
- Eine Beschreibung der Umsetzung des Datenschutz-Managementsystem eine Beschreibung der Umsetzung der einzelnen Zertifizierungskriterien. Hierbei ist der Detailgrad der Beschreibung mindestens so umfassend zu wählen, dass alle notwendigen Informationen enthalten sind, um eine eindeutige Bewertung der Konformität zu einzelnen Zertifizierungskriterien zweifelsfrei und ohne Unsicherheiten durchführen zu können.
- Wenn erforderlich, eine Aussage zur Konformität mit den einzelnen Zertifizierungskriterien. Die Auditoren müssen bezüglich der Aussage zur Konformität so berichten, dass deutlich wird, für welche Ergebnisse die Aussage zur Konformität gilt, welche Zertifizierungskriterien von einem Ermittlungsobjekt erfüllt oder nicht erfüllt werden, und welche Entscheidungsregel angewendet wurde. Meinungen und Interpretationen von Aussagen aus Ermittlungen sind von Aussagen zur Konformität erkennbar abzugrenzen.
- Die Erklärung eines Auditors, dass er die Zertifizierungsanforderungen dieses Konformitätsbewertungsprogramms bezüglich Unabhängigkeit und Unparteilichkeit erfüllt hat und keine Befangenheit vorliegt.

Der Bericht sollte folgende ergänzenden Aussagen enthalten:

- Anmerkungen zu den Nichtkonformitäten und, wo zutreffend, zu Korrekturen und Korrekturmaßnahmen, die vom Kunden ergriffen wurden.
- Behebungstermine für geringfügige Abweichungen.
- Bestätigung der an die Zertifizierungsstelle bei Antragstellung gelieferten Informationen und
- Empfehlung, ob die Zertifizierung gewährt werden soll oder nicht, zusammen mit Bedingungen bzw. Beobachtungen.

Der Auditteamleiter muss für alle im Bericht bereitgestellten Informationen die Verantwortung tragen, es sei denn, die Informationen werden vom Cloud-Anbieter oder einer dritten Partei bereitgestellt. Daten, die von einem Cloud-Anbieter oder einer dritten Partei bereitgestellt werden, müssen eindeutig gekennzeichnet werden. Zusätzlich muss der Bericht eine Aussage enthalten, wenn die Informationen vom Cloud-Anbieter oder einer dritten Partei bereitgestellt wurden und sich auf die Validität der Ermittlungsergebnisse auswirken können.

Anmerkung: Der Ermittlungsbericht ist im Akkreditierungsverfahren und jederzeit auf Wunsch der Datenschutz-Aufsichtsbehörde vollumfänglich zugänglich zu machen (siehe EDPB, Annex 1 Tz. 7.4).

3.6.12 Verteilung des Ermittlungsberichts

Der Auditteamleiter stellt den unterschriebenen Ermittlungsbericht elektronisch oder als Papierversion der Zertifizierungsstelle und dem Cloud-Anbieter zur Verfügung. Der Auftraggeber erhält an den Leistungsergebnissen ein einfaches, unbefristetes, nicht übertragbares, nicht unterlizenzierbares Nutzungsrecht, soweit nicht im Einzelfall eine abweichende Regelung vertraglich vereinbart wurde.

Der Cloud-Anbieter darf den Ermittlungsbericht Dritten grundsätzlich nur im vollen Wortlaut und unter Angabe des Ausstellungsdatums zur Verfügung stellen und hat solchen Dritten entsprechende Nutzungsbeschränkungen aufzuerlegen. Die Zertifizierungsstelle behält sich das Recht zur Veröffentlichung und zur öffentlichen Wiedergabe im Sinne von § 15 Abs. 2 UrhG vor. Entsprechende Textpassagen sind in dem Bericht durch den Auditteamleiter aufzunehmen.

3.7 Bewertung

Das Ziel der Bewertung ist die Feststellung der Konformität von Datenverarbeitungsvorgängen des Cloud-Anbieters mit den Anforderungen der EU-Datenschutzgrundverordnung (DS-GVO) durch die Zertifizierungsstelle. Die Bewertung umfasst die Identifizierung von Nichtkonformitäten (inkl. Erstellung des Abweichungsberichts, die Nachbesserung sowie die Bewertung der Nachbesserung durch die Zertifizierungsstelle und die Vorbereitung des Prüfungsberichts im Entwurf als Grundlage für die anschließende Entscheidung über die Zertifizierung.

3.7.1 Bewertung der Ermittlung durch die Zertifizierungsstelle

Nach Abschluss der Ermittlung und Fertigstellung des Ermittlungsberichts informiert der Auditteamleiter die Zertifizierungsstelle über die Fertigstellung des Ermittlungsberichts.

Die Bewertung wird durch die Zertifizierungsstelle vorgenommen und berücksichtigt den Ermittlungsbericht sowie die Dokumentation bzgl. der Erfüllung der Zertifizierungskriterien des Zertifizierungsgegenstandes nach GDPR CC-Kriterienkatalogs mit Bezug auf die festgelegte Schutzklasse. Dabei ist sowohl eine Bewertung hinsichtlich der Erfüllung der einzelnen Zertifizierungskriterien des GDPR CC-Kriterienkatalogs als auch hinsichtlich der Erfüllung der gesamten Zertifizierungskriterien des GDPR CC-Kriterienkatalogs, jeweils bezogen auf eine bestimmte Schutzklasse, erforderlich.

Der dabei angewandte Bewertungsmaßstab für Zertifizierungskriterien sowie Maßnahmen im Fall von festgestellten Nichtkonformitäten sind in den folgenden Abschnitten beschrieben.

In dem Prozess der Bewertung wird durch die Zertifizierungsstelle sichergestellt, dass der Bewerter sowie der Entscheider nicht an den Ermittlungstätigkeiten beteiligt waren. Diese Funktionstrennung beugt möglichen Interessenkonflikten vor und sichert die Unparteilichkeit (siehe DIN EN ISO/IEC 17065:2013 Tz. 7.5.1, DSK Tz. 7.5).

Die Zertifizierungsstelle kann zusätzliche Auskünfte und Nachweise vom Cloud-Anbieter erheben, soweit dies für die Bewertung erforderlich ist.

3.7.2 Nichtkonformitäten von Zertifizierungskriterien und Abweichungsbericht

Die Zertifizierungsstelle nimmt eine Bewertung der Konformität von Zertifizierungskriterien vor. Dafür muss die Konformität jeder einzelnen Nummer pro Zertifizierungskriterium bewertet werden. Hierbei ist der folgende Bewertungsmaßstab pro Nummer für ein Zertifizierungskriterium anzuwenden:

1. Erfüllung: Die Nummer des jeweiligen Zertifizierungskriteriums ist erfüllt.

2. Erfüllung mit Empfehlung: Abweichung, die in ihrer Geringfügigkeit die Einhaltung der Datenschutzanforderungen insgesamt nicht in Frage stellt (Verbesserungspotential).

   Beispiele:

   1. Das eingesetzte Verschlüsselungsverfahren ist gerade noch „Stand der Technik“, sollte aber zeitnah ausgetauscht werden.
   2. Da keine Passwortrichtlinie bzgl. der erneuten Verwendung von Passwörtern gesetzt ist, können Mitarbeiter ein ursprüngliches Passwort erneut verwenden.
   3. Das IT-Sicherheitshandbuch sollte gepflegt werden und einer standardisierten Methodik folgen.

3. Nichtkonformität: Wesentliche Abweichung, sodass erhebliche Zweifel bestehen, dass die Datenschutzanforderungen grundsätzlich eingehalten werden.

   Beispiele:

   1. Die benötigten Dokumentationen (z. B. Prozessdokumentation, Funktionsdokumentation oder Logs) können nicht vom Cloud-Anbieter vorgelegt werden oder die Durchführung von Datenverarbeitungsvorgängen zur Überprüfung der Einhaltung von Kriterien ist nicht möglich.
   2. Prozessdokumentationen liegt vor, diese wird jedoch beim Cloud-Dienst-Betrieb nicht fortlaufend durchgeführt (‚gelebt‘).
   3. Sicherheitstests haben schwerwiegende Mängel oder Schwachstellen in der eingesetzten Software des Cloud-Dienstes ergeben.
   4. Befragung oder Vor-Ort-Prüfung im Rahmen eines Audits hat die fehlende Umsetzung von Zertifizierungskriterien aufgedeckt.

Wird eine Nummer eines Kriteriums mit „Nichtkonformität“ bewertet, so gilt dieses Kriterium auch als nicht erfüllt. Nichtkonformitäten müssen vor Erteilung einer Zertifizierung behoben sein. Falls zum Zeitpunkt des Entscheidungsprozesses einer der Standorte eine Nichtkonformität aufweist, muss die Zertifizierung gegenüber der gesamten Multi-Standort-Organisation verweigert werden, bis zufriedenstellende Korrekturmaßnahmen umgesetzt wurden (siehe IAF MD 1:2018 Tz. 7.7.3, 7.7.4). Es ist nicht erlaubt, dass der Cloud-Anbieter einen „problematischen“ Standort während des Zertifizierungsprozesses ausschließt, um die Hindernisse, die durch die Existenz einer Nichtkonformität bei einem einzelnen Standort aufgetreten sind, zu überwinden.

Die Zertifizierungsstelle hat dem Cloud-Anbieter deutlich zu beschreiben, welche Mängel oder Abweichungen vorliegen, die eine Erfüllung der Zertifizierungskriterien verhindern (siehe DIN EN ISO/IEC 17065:2013 Tz. 7.4.6, EDPB, Annex 1 Tz. 7.4).

Die Beschreibung der Mängel erfolgt in dem Abweichungsbericht. Die finale Entscheidung über den Abweichungsbericht trifft die Zertifizierungsstelle (siehe Abschnitt 3.8).

Wenn Nichtkonformitäten an einzelnen Standorten identifiziert werden (z. B. auf Grundlage von eingesehenen Berichten der Internen Revision des Cloud-Anbieters oder durch Ermittlung der Auditoren) muss beurteilt werden, ob die anderen Standorte ebenfalls betroffen sein können (siehe IAF MD 1:2018 Tz. 7.7.1). Aus diesem Grund muss die Zertifizierungsstelle von dem Cloud-Anbieter im Rahmen der Nachbesserung fordern, dass der Cloud-Anbieter Nichtkonformitäten geprüft, um nachzuweisen, dass weitere Standorte nicht von dem bekannten Defizit betroffen sind. Entsprechende Anforderungen sind in den Abweichungsbericht aufzunehmen.

Wurde bei der Bewertung festgestellt, dass eine oder mehrere Zertifizierungskriterien nicht erfüllt sind, prüft die Zertifizierungsstelle, ob eine Nachbesserung in angemessener Frist vom Cloud-Anbieter erfolgreich durchgeführt werden kann (siehe DIN EN ISO/IEC 17065:2013 Tz. 7.4.7).

Der Abweichungsbericht und die festgelegte Frist zur Bearbeitung durch den Cloud-Anbieter werden durch die Zertifizierungsstelle an den Cloud-Anbieter versendet. Mit dem Abweichungsbericht fordert die Zertifizierungsstelle vom Cloud-Anbieter, die Ursachen zu analysieren und die spezifischen, durchgeführten oder geplanten Korrekturen und Korrekturmaßnahmen zu beschreiben, um die erkannten Nichtkonformitäten in dem festgelegten Zeitraum (Frist) zu beseitigen.

Die im Rahmen der Beurteilung festgestellten Nichtkonformitäten sowie die Festlegung der Frist für die Bearbeitung und die Berichterstattung (inkl. Kommunikation mit dem Cloud-Anbieter) werden dokumentiert. Dieses umfasst insbesondere die folgenden Bestandteile:

- Abweichungsbericht
- Vergütung für die Beurteilung der Nachbesserung als Anlage zum Abweichungsbericht (erfolgt nach Aufwand entsprechend der Gebührentabelle der Zertifizierungsstelle).
- Beurteilung und Festsetzung zur Frist für die Bearbeitung durch den Cloud-Anbieter
- Dokumentation der Kommunikation (E-Mails etc.) mit dem Cloud-Anbieter

3.7.3 Korrekturmaßnahmen durch den Cloud-Anbieter

Der Cloud-Anbieter plant die erforderlichen Korrekturmaßnahmen und die Zeitlinie zur Bearbeitung auf Grundlage der von der Zertifizierungsstelle gesetzten Fristen und dem bereitgestellten Abweichungsbericht. Die Zertifizierungsstelle muss bei etwaigen Rückfragen zur Klärung von Unklarheiten beitragen, soweit die Unparteilichkeit dadurch nicht gefährdet wird. Die von der Zertifizierungsstelle gesetzte Frist für die Nachbesserung kann auf Antrag des Cloud-Anbieters und in Abstimmung mit der Zertifizierungsstelle verlängert werden.

Alle Rückfragen oder ergänzende Informationen, die von der Zertifizierungsstelle bereitgestellt werden, sowie Anpassungen der Frist sind nachzuhalten.

Im Rahmen der Nachbesserung muss der Cloud-Anbieter dafür Sorge tragen, dass alle Mängel und Abweichungen zur Erfüllung der Zertifizierungskriterien abgestellt werden.

Der Cloud-Anbieter stellt der Zertifizierungsstelle nach Abschluss der Nachbesserung alle notwendigen Dokumente zur Verfügung, um die erfolgreiche Nachbesserung belegen zu können.

3.7.4 Bewertung der Nachbesserung

Nach Erhalt der vorgelegten Korrekturmaßnahmen und entsprechender Nachweise vom Cloud-Anbieter bewertet die Zertifizierungsstelle, ob sie annehmbar sind (siehe DIN EN ISO/IEC 17065:2013 Tz. 7.4.7, 7.4.8). Die Zertifizierungsstelle (ggf. mit Unterstützung des Auditleiters) muss die Wirksamkeit aller durchgeführten Korrekturmaßnahmen verifizieren. Die Zertifizierungsstelle kann abhängig vom Umfang und der Schwere der erforderlichen Nachbesserung eine Nachprüfung mit angemessener Frist zur Durchführung ansetzen. Im Rahmen dieser Nachprüfung gelten die Zertifizierungsanforderungen der Ermittlung und es sind entsprechende Ermittlungstätigkeiten nach § 5.2.4 GDPR CC ggf. stichprobenartig anzuwenden.

Die erlangten Nachweise über die Behebung der Nichtkonformitäten werden dokumentiert. Die Dokumentation umfasst mindestens die folgenden Bereiche:

- Ablage der vom Cloud-Anbieter erhaltenen Dokumente (Korrekturen sowie Nachweise)
- Bewertung der erhaltenen Nachweise

- Ergebnis der Bewertung
- Kommunikation mit dem Cloud-Anbieter

Der Cloud-Anbieter muss von der Zertifizierungsstelle über das Ergebnis der Überprüfung und Verifizierung informiert werden.

Wenn Nichtkonformitäten an einzelnen Standorten identifiziert werden (z. B. auf Grundlage von eingesehenen Berichten der Internen Revision des Cloud-Anbieters oder durch Ermittlung der Auditoren) muss bewertet werden, ob die anderen Standorte ebenfalls betroffen sein können (siehe IAF MD 1:2018 Tz. 7.7.1). Aus diesem Grund muss die Zertifizierungsstelle von dem Cloud-Anbieter im Rahmen der Nachbesserung fordern, dass der Cloud-Anbieter Nichtkonformitäten geprüft, um nachzuweisen, dass weitere Standorte nicht von dem bekannten Defizit betroffen sind. Je nach Ergebnis der Nachbesserung ergeben sich zusätzliche Anforderungen an die Nachbesserung des Cloud-Anbieters:

- Falls festgestellt wird, dass weitere Standorte betroffen sind, so müssen Korrekturmaßnahmen durchgeführt und geprüft werden, und zwar sowohl in der Zentrale als auch an den einzelnen betroffenen Nebenstandorten (siehe IAF MD 1:2018 Tz. 7.7.1).
- Falls festgestellt wird, dass keine weiteren Standorte betroffen sind, muss der Cloud-Anbieter in der Lage sein, gegenüber der Zertifizierungsstelle nachzuweisen, dass eine Einschränkung der Folgemaßnahmen gerechtfertigt ist (siehe IAF MD 1:2018 Tz. 7.7.1).

Wurde bei der Bewertung der Korrekturen oder der Nachprüfung festgestellt, dass eine oder mehrere Zertifizierungskriterien weiterhin nicht erfüllt sind, prüft die Zertifizierungsstelle, ob eine weitere Nachbesserung in angemessener Frist vom Cloud-Anbieter erfolgreich durchgeführt werden kann und angemessen erscheint. Die Ergebnisse der Beurteilung werden dem Cloud-Anbieter in diesem Fall nach dem bereits beschriebenen Verfahren (siehe Abschnitt 3.7.2) übermittelt. Auch diese Frist kann auf Antrag des Cloud-Anbieters verlängert werden.

Im Rahmen der Überwachung wird von der Zertifizierungsstelle geprüft, ob den Empfehlungen entsprochen wurde. Wenn nicht, prüft die Zertifizierungsstelle, ob die bisherige Empfehlung aufgrund geänderter Rahmenbedingungen zur Nichtkonformität geworden ist (vgl. auch Abschnitt 0).

Der Cloud-Anbieter wird von der Zertifizierungsstelle über das Ergebnis der Prüfung informiert (siehe Abschnitt 3.8).
Hierbei können die folgenden Szenarien unterschieden werden:

a) Kann durch den Cloud-Anbieter nachgewiesen werden, dass die Korrekturmaßnahmen zur vollständigen Erfüllung der Zertifizierungskriterien angemessen umgesetzt wurden, informiert der Bewerter den Cloud-Anbieter (formlos). Im weiteren Prozessverlauf erhält der Cloud-Anbieter die formale Entscheidung zur Zertifizierung durch den Entscheider.
b) Wurde im Rahmen der Nachprüfung festgestellt, dass eine oder mehrere Zertifizierungskriterien weiterhin nicht erfüllt sind, erfolgt die Information des Cloud-Anbieters nach dem bereits beschriebenen Verfahren (siehe Abschnitt 3.7.2). Eine erneute Nachbesserung ist jedoch nur umsetzbar, wenn die Zertifizierungsstelle zu dem Schluss kommt, dass eine weitere Nachbesserung vom Cloud-Anbieter in angemessener Frist erfolgreich durchgeführt werden kann.
c) Wurde während der Beurteilung der Nachbesserung durch den Bewerter festgestellt, dass ein oder mehrere Zertifizierungskriterien nicht erfüllt sind und nach Einschätzung der Zertifizierungsstelle auch nicht in angemessener Zeit behoben werden können, informiert der Bewerter den Cloud-Anbieter (formlos). Im weiteren Prozessverlauf erhält der Cloud-Anbieter die formale Entscheidung zur Zertifizierung durch den Entscheider.

3.7.5 Bewertungsergebnis

Die Bewertung mündet in einer Empfehlung für die Entscheidung über die Zertifizierung. Die Zertifizierungsstelle erstellt bei positivem Bewertungsergebnis ein Zertifikat und ein Kurzgutachten als Anhang zum Zertifikat zur Veröffentlichung auf der Webseite der Zertifizierungsstelle.

3.8 Entscheidung über die Zertifizierung

Die Entscheidung über die Zertifizierung erfolgt durch die Zertifizierungsstelle und berücksichtigt mögliche Einsprüche des Cloud-Anbieters oder der Datenschutz-Aufsichtsbehörde. Der Prozess gliedert sich in die folgenden Schritte.

3.8.1 Entscheidung der Zertifizierungsstelle

Die Zertifizierungsstelle entscheidet auf Grundlage der Bewertung des Ermittlungsberichts sowie der Detailinformationen über die Erteilung der Zertifizierung und die Verleihung der Konformitätszeichen.

Der Zeitraum zwischen dem Abschluss der letzten Ermittlung und der Zertifizierungsentscheidung darf nur in berechtigten Ausnahmefällen die Dauer von 3 Monaten überschreiten (siehe DSK Tz. 7.3).

Die Dokumentation der Entscheidung der Zertifizierungsstelle umfasst die folgenden Bereiche:

- Dokumentation der durchgeführten Qualitätssicherungsmaßnahmen.
- Darstellung der beteiligten Rollen (Auditoren, Beurteiler, Entscheider, Unterstützer) sowie die Einhaltung der definierten Funktionstrennung (Trennung Auditoren – Entscheider)
- Ablage des Prüfungsberichts
- Die Zertifizierungsstelle legt detailliert dar, wie ihre Unabhängigkeit und Verantwortlichkeit im Hinblick auf die Zertifizierungsentscheidung sichergestellt wurde (siehe DSK Tz. 7.6, EDPB, Annex 1 Tz. 7.6). Zu diesem Zweck wird auf die Bestätigung der persönlichen Unabhängigkeit der beteiligten Personen sowie die Unabhängigkeitsprüfung der Zertifizierungsstelle verwiesen.
- Das von der Zertifizierungsstelle unterschriebene öffentliche Kurzgutachten.

Die Zertifizierungsstelle muss den Cloud-Anbieter über eine Entscheidung, die Zertifizierung nicht zu gewähren, informieren (siehe DIN EN ISO/IEC 17065:2013 Tz. 7.6.6). In diesem Fall wird die Entscheidung der Zertifizierungsstelle unter Nennung der Gründe die Zertifizierung nicht zu gewähren, an den Cloud-Anbieter versendet (siehe auch Abschnitt 3.7.2).

Wenn der Cloud-Anbieter Interesse an der Fortsetzung des Zertifizierungsprozesses äußert, kann die Zertifizierungsstelle die Auswahl- und Ermittlungsprozesse wieder aufnehmen.

3.8.2 Einspruch durch den Cloud-Anbieter

Der Cloud-Anbieter kann gegen eine Entscheidung Einspruch bei der Zertifizierungsstelle einlegen. Der Einspruch ist zu begründen. Ein Einspruch ist ein Verlangen des Cloud-Anbieters gegenüber einer Zertifizierungsstelle, ihre Entscheidung bezüglich des Zertifizierungsgegenstands zu überprüfen (siehe DIN EN ISO/IEC 17000:2020 Tz. 8.6). Der Einspruch ist in Textform innerhalb einer Frist von 4 Wochen nach Zugang der Zertifizierungsentscheidung einzureichen.

Die Zertifizierungsstelle prüft, ob der Einspruch begründet ist. Soweit sich der Einspruch gegen die Auswahl- oder Ermittlungstätigkeiten oder die Feststellungen der Auditoren richtet, informiert die Zertifizierungsstelle die Auditoren über den Einspruch und holt eine Stellungnahme der Auditoren ein.

Soweit der Einspruch gerechtfertigt ist, ändert die Zertifizierungsstelle die Zertifizierungsentscheidung. Soweit die Zertifizierungsstelle dem Einspruch nicht abhilft, ist dies zu begründen. Die Entscheidung über den Einspruch einschließlich Begründung ist dem Cloud-Anbieter in Textform mitzuteilen.

3.8.3 Erstellung öffentliches Kurzgutachten

Die Zertifizierungsstelle erstellt (ggf. mit Unterstützung des Auditteamleiters) ein öffentliches Kurzgutachten bzgl. des jeweiligen Zertifizierungsergebnisses, aus dem sich folgende Punkte ableiten lassen (siehe DSK Tz. 7.8):

- Namen der Zertifizierungsstelle,
- den Namen und den geografischen Ort des Kunden,
- die Daten zur Erteilung, Erweiterung, Änderung oder Erneuerung der Zertifizierung,
- der genaue Zertifizierungsgegenstand (inklusive Versions- oder Funktionsstand),
- das Evaluationsverfahren (inklusive der der Zertifizierung zugrunde liegenden Kriterien (ggf. mit Versionsangabe) und einer Angabe über Kriterien, die nicht anwendbar waren),
- das Evaluationsergebnis,
- das Ablaufdatum oder das Fälligkeitsdatum zur Re-Zertifizierung und
- das Zertifizierungszeichen der Zertifizierungsstelle

Das Kurzgutachten muss die Nutzung des Zertifizierungsgegenstands im Einsatzgebiet und im Anwendungsfall in transparenter und nachvollziehbarer Weise dokumentieren, so dass auch der (End-) Kunde bzw. eine betroffene Person in angemessener Zeit nachvollziehen kann, was unter Nutzung des Zertifizierungsgegenstands im datenschutzrechtlichen Sinn gewährleistet ist.

3.8.4 Mitteilung an die zuständige Datenschutz-Aufsichtsbehörde

Die Zertifizierungsstelle unterrichtet die zuständige Datenschutz-Aufsichtsbehörde über die Zertifizierung schriftlich mindestens eine Woche vor Erteilung der Zertifizierung (siehe DSK Tz. 7.6, EDPB Annex 1 Tz. 7.8).

Diese Unterrichtung muss:

- den Namen der Zertifizierungsstelle,
- die Beschreibung des Zertifizierungsgegenstands und
- das öffentliche Kurzgutachten enthalten.

Die Mitteilung inklusive der geforderten Angaben wird durch die Zertifizierungsstelle an die jeweils zuständige Datenschutz-Aufsichtsbehörde gesendet.

3.9 Erteilung der Zertifizierung

Die Zertifizierung ist durch die Zertifizierungsstelle im beantragten Umfang zu erteilen, wenn die Datenverarbeitungsvorgänge die Zertifizierungskriterien des GDPR CC-Kriterienkatalogs erfüllen und die Zertifizierungsstelle die zuständige Datenschutz-Aufsichtsbehörde über die Gründe für die Erteilung der Zertifizierung informiert hat.

Der Prozessablauf zur Erteilung der Zertifizierung umfasst die nachfolgenden Schritte.

3.9.1 Vorbereitung der Zertifizierungsdokumentation

Die Zertifizierungsstelle ist verpflichtet, vor der Erteilung der Zertifizierung (mindestens eine Woche nach Information der zuständigen Datenschutz-Aufsichtsbehörde) sicherzustellen, dass durch die Datenschutz-Aufsichtsbehörde kein Einspruch gegen die Zertifizierung eingelegt wurde.

Wird die Zertifizierungsstelle von der Datenschutz-Aufsichtsbehörde angewiesen keine Zertifizierung zu erteilen, sind die folgenden Maßnahmen durch die Zertifizierungsstelle umzusetzen:

- Der Cloud-Anbieter wird über die Entscheidung der Datenschutz-Aufsichtsbehörde keine Zertifizierung zu erteilen und über die Folgen draus informiert.
- Entsprechende Registereinträge werden angepasst bzw. aktualisiert (falls notwendig).
- Die Durchführung der umgesetzten Maßnahmen wird der Datenschutz-Aufsichtsbehörde bestätigt.

Die Zertifizierungsstelle vergibt für jede Zertifizierung eine eindeutige Zertifizierungsnummer. Sie setzt sich zusammen aus der eindeutigen Bezeichnung (Schlüssel) der Zertifizierungsstelle und einer fortlaufenden eindeutigen Nummer (Beispiel: PwC-GDPR-000). Die Zertifizierungsnummer wird durch die Zertifizierungsstelle vergeben und im Register der Zertifizierungen GDPR CC erfasst. Die Zertifizierungsnummer ist auf allen Konformitätszeichen zur Rückverfolgbarkeit anzugeben.

3.9.2 Ausstellung der Konformitätszeichen (Gütesiegel und Zertifikat)

Vor der Bereitstellung der Zertifizierungsdokumentation an den Cloud-Anbieter werden Gütesiegel und Zertifikat durch die Zertifizierungsstelle erstellt.

Das Gütesiegel muss die folgenden Angaben enthalten:

- das graphische Konformitätszeichen
- Kurztitel Datenverarbeitungsvorgang und Datenschutzrolle („als Auftragsverarbeiter gemäß Art. 4 Nr. 8 DS-GVO“)
- die Zertifizierungsnummer
- die Gültigkeitsdauer der Zertifizierung mit Angabe des Zeitraums (Ausstellung, Laufzeit bis)
- die Bezeichnung GDPR CC mit Schutzklasse 1, 2 oder 3
- die Angabe des Wiederherstellbarkeitsklasse 1, 2 oder 3.

Wird das Gütesiegel in elektronischen Medien (bspw. Webseite) angebracht, so ist dieses mit einem Link auf den Eintrag im Zertifizierungsregister der Zertifizierungsstelle zu versehen (siehe § 4.4.2), um die Rückverfolgbarkeit durch Cloud-Nutzer und interessierte Parteien zu ermöglichen. Mit Übergabe des Gütesiegels an den Cloud-Anbieter wird durch die Zertifizierungsstelle auf die entsprechende Nutzungsvereinbarung hingewiesen.

Das Zertifikat muss mindestens die folgenden Angaben enthalten:

- Den Cloud-Anbieter, ggf. als Kurzbezeichnung.
- Anschrift des Cloud-Anbieters, ggf. Nebenstandorte.
- Datenschutzrolle gemäß DS-GVO „als Auftragsverarbeiter gemäß Art. 4 Nr. 8 DS-GVO“.
- Geltungsbereich Regional: Deutschland, EU, Drittland.
- Den Zertifizierungsgegenstand, ggf. als Kurzbezeichnung.
- Die Zertifizierungsstelle und deren Anschrift.

- Die Zertifizierungsaussage, wonach die zertifizierten Datenverarbeitungsvorgänge die einschlägigen Vorgaben der DS-GVO und des BDSGs gemäß dem GDPR CC-Kriterienkatalog in der jeweiligen Fassung für eine konkrete Schutzklasse und eine konkrete Wiederherstellbarkeitsklasse sowie die zusätzlichen Anforderungen der Datenschutz-Aufsichtsbehörden erfüllt.
- Die Bezeichnung der maßgeblichen Fassung des GDPR CC-Konformitätsbewertungsprogramm und des -Kriterienkatalogs.
- Eine eindeutige Zertifizierungsnummer.
- Tag der Zertifizierungsentscheidung.
- Angabe letzter Tags der Prüfung vor Ort: <tt.mm.jjjj> /Berichtsnummer/Datum.
- Die Gültigkeitsdauer der Zertifizierung mit Angabe des Zeitraums, Datum der Ausstellung des Zertifikats: „Datum der Ausstellung <tt.mm.jjjj>“ und „Laufzeit bis <tt.mm.jjjj> max. 3 Jahre>“. Die Zertifizierung wird für eine Gültigkeitsdauer von drei Jahren erteilt. Die Frist beginnt mit dem im Konformitätszeichen ausgewiesenen Datum der Erteilung. Die Zertifizierungsstelle kann die erneute Zertifizierung bei rechtzeitiger Beantragung und abgeschlossenem Zertifizierungsverfahren auf das Datum unmittelbar nach Ablauf der Gültigkeitsdauer der vorangegangenen Zertifizierung ausstellen. Werden bestehende Zertifizierungen des Cloud-Anbieters anerkannt, so wird die Gültigkeitsdauer der GDPR CC-Zertifizierung auf das Ablaufdatum der als nächsten fälligen Re-Zertifizierung des anerkannten Zertifikates reduziert.
- Kurzangabe zur Überwachung, bspw. „innerhalb der Laufzeit des Zertifikats jährlich auf Konformität überwacht wird“; und „nächste geplante Überwachung bis spätestens <tt.mm.jjjj>“.
- Angabe zur Mitteilung der Entscheidung an die Datenschutz-Aufsichtsbehörde: „Die Gründe für die Erteilung des Zertifikats wurden der [Datenschutz-Aufsichtsbehörde NAME] gemäß Art. 43 Abs. 5 DS-GVO am TT.MM.JJJJ mitgeteilt.“
- Eine Anlage mit den Angaben nach (siehe Anlage 1 und Anlage 2); sowie die Hinweise auf diese Anlagen „[Datenverarbeitungsvorgang] gemäß Anlage 1“ und „unter Beachtung der Nutzungsausschlüsse gemäß Anlage 2“.
- Akkreditierungssymbol.
- Ggf. Logo der Zertifizierungsstelle.
- Unterschrift Leitung der Zertifizierungsstelle.

Die Anlage 1 und Anlage 2 zum Zertifikat müssen mindestens die folgenden Angaben enthalten:

Anlage 1:

- die eindeutige Bezeichnung des Cloud-Anbieters, inkl. Anschrift;
- die ausführliche Beschreibung des Zertifizierungsgegenstands;
- einen Verweis auf das öffentliche Kurzgutachten (siehe auch Abschnitt “Erstellung öffentliches Kurzgutachten”) über das Ergebnis der Zertifizierung gem. Tz. 7.6 und 7.8 der Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i. V. m. DIN EN ISO/IEC 17065 der Datenschutzkonferenz (DSK);
- ggf. die Bezeichnung der angewendeten Regelwerke der Zertifizierungsstelle;
- ggf. weitere Hinweise der Zertifizierungsstelle.

Anlage 2:

Auflistung aller Nutzungsausschlüsse (d. h. was unter Einsatz des Zertifizierungsgegenstands im Anwendungsgebiet nicht gewährleistet wird).

3.9.3 Bereitstellung der Zertifizierungsdokumentation an den Cloud-Anbieter

Nach der Entscheidung zur Erteilung einer Zertifizierung sowie dem Abschluss der Vorbereitungsarbeiten wird die Zertifizierungsdokumentation dem Cloud-Anbieter durch die Zertifizierungsstelle zur Verfügung gestellt. Die Zertifizierungsdokumentation umfasst:

- den Prüfungsbericht,
- das Kurzgutachten,
- das Gütesiegel,
- das Zertifikat und
- die “Richtlinie zur Zeichennutzung”.

Vor Versand der Zertifizierungsdokumentation wird durch die Zertifizierungsstelle sichergestellt, dass alle Prüfungshandlungen abgeschlossen wurden und die notwendigen Genehmigungen für den Versand der Zertifizierungsdokumentation vorliegen.

3.9.4 Veröffentlichung von Zertifizierungsentscheidungen

Die Zertifizierungsstelle führt ein Verzeichnis der zertifizierten Dienstleistungen inkl. der ausgelaufenen Zertifikate. Das Verzeichnis wird gemäß der Zertifizierungsentscheidung durch die Zertifizierungsstelle aktualisiert.

Das Verzeichnis enthält:

- Die Identifizierung der Dienstleistung,
- die normativen Dokumente, nach denen die Konformität zertifiziert wurde,
- eine Identifizierung des Kunden.

Mit der Übermittlung der Zertifizierungsdokumentation an den Cloud-Anbieter erfolgt die Veröffentlichung der Zertifizierungsentscheidung. Der entsprechende Eintrag der Datenverarbeitungsvorgänge in dem Verzeichnis von zertifizierten Datenverarbeitungsvorgängen durch die Zertifizierungsstelle wird aktualisiert. Darüber hinaus wird auch das Kurzgutachten zur Zertifizierung (gemäß der DIN EN ISO/IEC 17065:2013 Tz. 7.8) auf der Webseite der PwC Cert veröffentlicht. Mit dem Kurzgutachten wird der Zertifizierungsgegenstand (inkl. der Version oder des Funktionszustands), die zugrundeliegenden Kriterien und die angewendeten Ermittlungsmethoden sowie die Ergebnisse veröffentlicht.

Das öffentliche Verzeichnis und die Verlinkung auf die Kurzgutachten sind unter www.pwc-cert.com/auditor abrufbar.

4 Zertifikat- und Zeichennutzung

In diesem Abschnitt erfolgt die Festlegung von Verwendungsmöglichkeiten sowie von Verwendungsverboten von Zertifikaten und Zeichen, welche auf eine Zertifizierung durch die Zertifizierungsstelle hinweisen.

Im Rahmen der Zertifizierung nach GDPR CC sind das Zertifikat der PwC Cert sowie das AUDITOR Gütesiegel des Kompetenznetzwerks Trusted Cloud e.V. Zeichen im Sinne dieser Vorgaben.

4.1 Eigentümer des Zertifikats und des Zeichens

Die Zertifizierungsstelle ist Eigentümer der in diesem Dokument aufgeführten Zertifikate. Das Kompetenznetzwerk Trusted Cloud e.V. ist Eigentümer des AUDITOR-Gütesiegels. Die Verwendung des Gütesiegels im Rahmen GDPR CC-Zertifizierung bei der Ausstellung des Zertifikats erfolgt auf Basis der Nutzungsvereinbarung zwischen der PwC Certification Services GmbH und dem Kompetenznetzwerk Trusted Cloud e.V. als Programmeigner.

4.2 Zeichennutzer (Zertifikatinhaber)

Zeichennutzer sind die von der Zertifizierungsstelle-DL der PwC Cert zertifizierten Organisationen, welche durch die Nutzung von Zertifizierungszeichen ihre Konformität im überprüften Geltungsbereich präsentieren.

4.3 Rechte und Pflichten

Den von der Zertifizierungsstelle-DL zertifizierten Organisationen stehen verschiedene Möglichkeiten offen, auf ihre gültige Zertifizierung hinzuweisen. In den folgenden Abschnitten sind die Regeln zur Nutzung von Zertifikaten und Zeichen beschrieben.

4.3.1 Recht zur Zeichennutzung

Die zertifizierte Organisation erlangt mit Erhalt eines von der Zertifizierungsstelle-DL der PwC Cert ausgestellten und gültigen Zertifikates ein zeitlich befristetes und nicht übertragbares Nutzungsrecht für dieses Zertifikat. Das Zertifikat ist Eigentum der Zertifizierungsstelle.

Mit Erhalt des Zertifikats verbunden ist ein zeitlich befristetes und nicht übertragbares Nutzungsreicht für das dazugehörige Zeichen (AUDITOR-Gütesiegel).

4.3.2 Benutzung des Zeichens und des Zertifikats

Der Zertifikatinhaber stellt sicher, dass die Benutzung des Zertifikats und der Zeichen in der Werbung oder bei sonstigen Maßnahmen im Rahmen dieser Vorgaben erfolgt.

Zertifikat und Zeichen dürfen nur in Verbindung mit einer gültigen Zertifizierung und zum Nachweiseiner der erfolgreichen Zertifizierung sowie zu Werbezwecken genutzt werden. Das Zeichen (AUDITOR-Gütesiegel) muss folgende Angaben enthalten:

a) das graphische Konformitätszeichen;
b) Kurztitel Datenverarbeitungsvorgang und Rolle Datenschutzrolle („als Auftragsverarbeiter gemäß Art. Nr. 8 DS-GVO“);
c) die Zertifizierungsnummer (Beispiel: PwC-GDPR-000)

d) die Gültigkeitsdauer der Zertifizierung mit Angabe des Zeitraums (Ausstellung, Laufzeit bis);
e) die Bezeichnung AUDITOR mit Schutzklasse 1, 2 oder 3;
f) die Angabe des Wiederherstellbarkeitsklasse 1, 2 oder 3.

Eine reprofähige Vorlage des jeweiligen Zeichens wird auf Anfrage von PwC Cert zur Verfügung gestellt.

Wird das Zeichen in elektronischen Medien (bspw. Webseite) angebracht, so ist dieses mit einem direkten Link auf den Eintrag im Zertifizierungsregister der Zertifizierungsstelle-DL zu versehen, um die Rückverfolgbarkeit durch Cloud-Nutzer und Interessierte Parteien zu ermöglichen.

Folgende allgemeine Regeln sind bei der Nutzung des Zeichens zu beachten:

a) Die Werbung mit der Zertifizierung muss den Inhalt des ausgestellten Zertifikates korrekt wiedergeben.
b) Das Zeichennutzungsrecht ist beschränkt auf die im Zertifikat genannten Angaben (u. a. Cloud-Anbieter, Geltungsbereich, Zertifizierungsgegenstand (ggf. als Kurzbezeichnung),
c) Zertifizierungsstelle, Zertifizierungsaussage, Gültigkeitsdauer, konkrete Schutzklasse und Wiederherstellbarkeitsklasse …).
d) Das Zeichennutzungsrecht ist an die Gültigkeit des Zertifikats gebunden.
e) Bei Zeichennutzung muss der Verweis auf die Zertifizierungsstelle der PwC Certification Services GmbH sowie die eindeutige Zertifizierungsnummer kenntlich sein.
f) In Zweifelsfällen einer Zeichen- oder Zertifikatsnutzung ist PwC Cert verpflichtet, vor Genehmigung der Nutzung die DAkkS einzubeziehen.

4.3.3 Hinweis auf den Anwendungsbereich (Scope) der Zertifizierung

Bei der Nutzung des Zertifikats und Zeichens ist ein Hinweis auf den Anwendungsbereich der Zertifizierung anzugeben, um eine irreführende Darstellung des Geltungsbereiches zu verhindern. Alle Werbematerialien sind unverzüglich zu ändern, wenn das Zertifikat ausgesetzt bzw. gelöscht wurde oder der Geltungsbereich der Zertifizierung reduziert wurde (siehe auch Abschnitt 4.3.5).

4.3.4 Auswirkung des Missbrauchs des Zertifikats / Zeichens

Die Verletzung der Rechte der Zertifizierungsstelle der PwC Cert an den angegebenen Zeichen, ein Zertifikatsmissbrauch oder ein Zeichenmissbrauch können zur Aberkennung des Zertifikates und des Zeichennutzungsrechts führen.

Wird dem Zertifikatsinhaber ein Missbrauch von angegebenen Zeichen / des erteilten Zertifikates bekannt, so hat er die Zertifizierungsstelle der PwC Cert hierüber umgehend zu informieren.

Fälschungen oder Kopien von Zertifikaten, des Zertifizierungszeichens bzw. des Zeichenlayouts durch Dritte werden von der PwC Cert mit rechtlichen Mitteln verfolgt.

4.3.5 Verlust des Rechts auf Zeichenführung

Erlöschen
Die Erlaubnis zur Nutzung der Zertifizierungsurkunde und dem damit verbundenen Zeichennutzungsrecht erlöschen mit dem auf der Urkunde angegebenen Datum. Die Erlaubnis zur Nutzung der Zertifizierungsurkunde erlischt vor Ablauf der regulären Gültigkeit, wenn gegen die Zertifizierungsdokumente der geschlossenen Zertifizierungsvereinbarung verstoßen wird oder, wenn die Zertifizierungsstelle-DL der PwC Cert von der Datenschutzaufsichtsbehörde angewiesen wird, eine erteilte Zertifizierung gemäß Art. 58 Abs. 2 lit. h DS-GVO zu widerrufen.

Wenn die der Dienstleistung zugrunde gelegten Anforderungen, z. B. eine Norm, zurückgezogen oder geändert werden, entscheidet PwC Cert darüber, ob die Erlaubnis zur Nutzung der Zertifizierungsurkunde erlischt.

Die Zertifizierung und damit das Zeichennutzungsrecht erlischt darüber hinaus, wenn PwC Cert nicht mehr als Zertifizierungsstelle für Cloud-Anbieter als Auftragsverarbeiter gemäß GDPR CC akkreditiert ist (siehe hierzu Abschnitt 4.4)

Das Erlöschen der Zertifizierungsurkunde und des damit verbundenen Nutzungsrechts wird schriftlich mitgeteilt. Der Auftraggeber (Cloud-Anbieter) ist mit Erlöschen des Nutzungsrechts der Zertifizierungsurkunde zur Rücksendung der Urkunde an die PwC Cert verpflichtet. Das Zertifizierungsregister wird entsprechend angepasst und die Datenschutzaufsichtsbehörde in Kenntnis gesetzt. Die Verwendung von Werbematerialien und die Präsentation von Informationen im Internet, die mit der Zertifizierung werben, muss unverzüglich eingestellt werden.

Aussetzung
PwC Cert ist berechtigt, die Erlaubnis zur Nutzung der Zertifizierungsurkunde in begründeten Fällen für einen befristeten Zeitraum auszusetzen. Der Auftraggeber wird hierüber schriftlich informiert. Der Auftraggeber ist in diesem Zeitraum nicht berechtigt, das Zeichen und die zugehörige Zertifizierungsnummer zu verwenden (siehe Abschnitt 4.3.2).

Einschränkungen
Wird die Zertifizierung eingeschränkt, wird der Cloud-Anbieter hierüber und über die Folgen informiert. Die Einschränkung der Zertifizierung wird drei Wochen nach Zustellung der Entscheidung über die Einschränkung wirksam. Die Zertifizierungsstelle setzt alle erforderlichen Änderungen an formalen Zertifizierungsdokumenten um und aktualisiert öffentlich verfügbare Informationen. Hierzu zählen insbesondere die Änderung des Zeichens sowie die Änderung des Eintrags der Datenverarbeitungsvorgänge in dem Verzeichnis von zertifizierten Datenverarbeitungsvorgängen.

Die Verwendung von Werbematerialien und die Präsentation von Informationen im Internet, die mit der Zertifizierung werben, muss in Einklang mit der Einschränkung angepasst werden bzw. müssen weitere von der Zertifizierungsstelle definierte Maßnahmen durch den Cloud-Anbieter umsetzt werden. Der Cloud-Anbieter ist verpflichtet, seine Cloud-Nutzer über die Einschränkung zu informieren. Eine Information über die Einschränkung an die Aufsichtsbehörde erfolgt durch die Zertifizierungsstelle.

4.4 Besondere Regeln zum Akkreditierungssymbol der DAkkS

Die PwC Cert wurde von der DAkkS als Zertifizierungsstelle gemäß GDPR CC (DIN EN ISO/IEC 17065 i. V. m. den ergänzenden Anforderungen zur Akkreditierung nach Art. 43 Abs. 3 DS-GVO und GDPR CC) akkreditiert und durch den HBDI (Hessischer Beauftragter für Datenschutz und Informationsfreiheit) entsprechend befugt. Bestandteile der Akkreditierungsprüfung durch die DAkkS waren neben der Fachkunde unter anderem auch die Unabhängigkeit und Unparteilichkeit der Zertifizierungsstelle.

Die erteilte Zertifizierung / Zertifikat und das mit verbundene Zeichennutzungsrecht sind nur solange gültig, wie die PwC Cert von der DAkkS als Zertifizierungsstelle für Cloud-Anbieter als Auftragsverarbeiter gemäß GDPR CC akkreditiert ist.

Das Akkreditierungssymbol der DAkkS darf durch den Zertifikatinhaber jedoch nicht genutzt werden.

Eine Aussetzung (temporärer Entzug der Akkreditierung oder Zurückziehung der Akkreditierung, d. h. dauerhafter Widerruf der Akkreditierung) der PwC Cert für GDPR CC führt zur Ungültigkeit der erteilten Zertifizierung des Cloud-Anbieters. Die PwC Cert ist in diesem Fall dazu verpflichtet, Sie umgehend über die Aussetzung oder Zurückziehung der Akkreditierung zu informieren, auf die daraus resultierenden Konsequenzen hinzuweisen sowie die vergebenen Zertifizierungen zu widerrufen.

Im Weiteren ist die PwC Cert im Falle eines Erlöschens als Zertifizierungsstelle für GDPR CC und dem damit einhergehenden Widerruf der erteilten Zertifizierung des Cloud-Anbieters verpflichtet, einen Transfer der Zertifizierung des Cloud-Anbieters an eine aufnehmende Zertifizierungsstelle mit gültiger GDPR CC Akkreditierung innerhalb von sechs Monaten durchzuführen.

Ist ein Transfer der Zertifizierung aus oben genannten Gründen notwendig, so stellt die PwC Cert durch ein angemessenes Transferkonzept den zeitgemäßen und korrekten Transfer der Zertifizierung an eine aufnehmende Zertifizierungsstelle sicher. Das geltende Transferkonzept umfasst die Pflichten der PwC Cert gem. GDPR CC, Regelungen zur Begutachtung des Transfers durch die DAkkS und die Informationspflichten gegenüber der zuständigen Datenschutzaufsichtsbehörde sowie dem Programmeigner über den Transfer. Die Datenschutzaufsichtsbehörde ist auf ihr eigenes Verlangen hin in den Transfer einzubeziehen.

5 Überwachungsaudit

Die Datenverarbeitungsvorgänge bedürfen während der Gültigkeitsdauer der Zertifizierung der Überwachung in Form einer mindestens jährlich durchzuführenden Zwischenprüfung. Darüber hinaus können anlassbezogene Überwachungen bei Auffälligkeiten erfolgen, die eine Nichtkonformität der Zertifizierungskriterien befürchten lassen. Für die Zwischenprüfung gelten die GDPR CC-Anforderungen für durchzuführende Auswahl-, Ermittlungs-, Bewertungs-, und Entscheidungstätigkeiten entsprechend. Im Folgenden wird der Prozess der Überwachungstätigkeiten beschrieben:

Der Cloud-Anbieter ist verpflichtet, die Zertifizierungsstelle unverzüglich detailliert zu informieren, wenn ihm bekannt wird, dass die Voraussetzungen für die Erteilung der Zertifizierung nicht vorlagen oder nicht mehr vorliegen (bspw. Aussetzung oder Erlöschen anerkannter Zertifikate).

Wenn die Zertifizierungsstelle aufgrund der Überwachungstätigkeiten, von Mitteilungen des Cloud-Anbieters oder eines Dritten oder aufgrund sonstiger Umstände Grund zur Annahme hat, dass die Voraussetzungen für die Zertifizierungserteilung nicht vorlagen oder nicht mehr vorliegen (siehe auch GDPR CC § 5.3.2, § 5.3.3), ergreift sie unverzüglich die erforderlichen Maßnahmen, um das Vorliegen der Voraussetzungen festzustellen (siehe DIN EN ISO/IEC 17065:2013 Tz.7.11.1). Die Zertifizierungsstelle kann die folgenden Maßnahmen ergreifen:

- Die Zertifizierungsstelle kann insbesondere feststellen, dass eine Zwischenprüfung zur Aufrechterhaltung der Zertifizierung erforderlich ist (siehe Abschnitt 3.1 - 3.5).
- Die Zertifizierungsstelle kann dem Cloud-Anbieter eine Änderungszertifizierung empfehlen (siehe Abschnitt 4.2).
- Die Zertifizierungsstelle kann die Weiterführung der Zertifizierung unter Bedingungen, die von der Zertifizierungsstelle festgelegt werden (z. B. verstärkte Überwachung), erlauben insofern die Verletzung von Zertifizierungskriterien die Anforderungen der zertifizierten Schutzklasse nicht gefährdet und sofortige Abstellmaßnahmen durch den Cloud-Anbieter vorgenommen werden.

Die Zertifizierungsstelle hat dem Cloud-Anbieter deutlich zu beschreiben, unter welchen Aspekten Zweifel an der Einhaltung der Zertifizierungskriterien bestehen (siehe EDPB, Annex 1 Tz. 7.4).

Anmerkung: Die Zertifizierungsstelle notiert die Gültigkeit und Befristung der anerkannten Zertifikate. Die fortlaufende Gültigkeit der anerkannten Zertifikate wird mindestens im Rahmen der Überwachungsaudits von der Zertifizierungsstelle geprüft. Darüber hinaus verpflichtet die Zertifizierungsstelle den Cloud-Anbieter, diese mit ausreichend Vorlaufzeit darüber in Kenntnis zu setzen, wenn ein anerkanntes Zertifikat die Gültigkeit planmäßig verliert (d. h. bei regulärem Ablauf des Gültigkeitszeitraums) oder außer-planmäßig verliert (d. h. vor dem von der Zertifizierungsstelle vermerkten Ende des regulären Gültigkeitszeitraum), und welche Maßnahmen der Cloud-Anbieter vornehmen will (bspw. Re-Zertifizierung). Strebt der Cloud-Anbieter keine Re-Zertifizierung des anerkannten Zertifikats an, muss mindestens der ursprünglich abgedeckte Bereich erneut geprüft werden, um die Gültigkeit der GDPR CC-Zertifizierung aufrecht zu erhalten.

5.1 Durchführung von regelmäßigen und anlassbezogenen Überwachungstätigkeiten (Zwischenprüfung)

Die Datenverarbeitungsvorgänge bedürfen während der Gültigkeitsdauer der Zertifizierung der Überwachung in Form einer mindestens jährlich durchzuführenden Zwischenprüfung. Auf Grundlage der Zwischenprüfungsergebnisse hat die Zertifizierungsstelle festzustellen, ob die zertifizierten Datenverarbeitungsvorgänge die Zertifizierungskriterien nach der festgelegten Schutzklasse weiterhin

erfüllen. Die jährliche Zwischenprüfung ist frühestens nach Ablauf des sechsten und spätestens bis zum Ablauf des zwölften Monats ab Zertifizierungserteilung oder der entsprechenden Zeitpunkte der Folgejahre durchzuführen. Die Zertifizierungsstelle erinnert bzw. informiert den Cloud-Anbieter und bei Bedarf (ausgegliederte) Auditoren rechtzeitig an eine anstehende Zwischenprüfung bzw. über eine anlassbezogene Überwachung und weist insbesondere den Cloud-Anbieter auf die Folge des Unterbleibens der Zwischenprüfung hin. Der Cloud-Anbieter ist zur Mitwirkung an Überwachungstätigkeiten zu verpflichten.

Darüber hinaus können anlassbezogene Überwachungen bei Auffälligkeiten erfolgen, die eine Nichtkonformität der Zertifizierungskriterien z. B. bei vorliegenden Beschwerden befürchten lassen. Die Planung und Durchführung von anlassbezogenen Überwachungsaudits obliegt dem Verantwortungsbereich der Zertifizierungsstelle. Bei Auffälligkeiten (z. B. Beschwerden) wird der Umfang der durchzuführenden Tätigkeiten durch die Zertifizierungsstelle festgelegt. Die Auditoren führen die anlassbezogene Überwachung gemäß dem vereinbarten Zeitplan und in Absprache mit dem Cloud-Anbieter vor Ort durch. Stellt die Zertifizierungsstelle die Erforderlichkeit einer Zwischenprüfung fest, so müssen folgende Anforderungen erfüllt werden:

a) Die Zertifizierungsstelle setzt dem Cloud-Anbieter eine angemessene Frist zur Durchführung der Zwischenprüfung. Die Frist kann auf Antrag des Cloud-Anbieters verlängert werden.
b) Eine angeordnete Zwischenprüfung muss die Anforderungen der Ermittlung, Bewertung und Entscheidung im Rahmen dieser Verfahrensanweisung erfüllen (siehe DIN EN ISO/IEC 17065:2013 Tz. 7.11.2, Tz. 7.11.5). Dieses umfasst die folgenden Anforderungen:
    i) Werden Auswahl- und Ermittlungstätigkeiten für eine Zwischenprüfung notwendig, werden diese durch (ausgegliederte) Auditoren durchgeführt.
    ii) Notwendige Bewertungs- und Entscheidungstätigkeiten erfolgen auf Grundlage des Zwischenprüfungsberichts der Auditoren und müssen von der Zertifizierungsstelle durchgeführt werden.

Für die regelmäßige oder anlassbezogene Überwachung (bei Auffälligkeiten) folgt grundsätzlich dem in Abschnitt 3.5 und 3.6 beschriebenen Verfahren zur Ermittlung. Die folgenden Punkte ergänzen die Beschreibung des bestehenden Verfahrens für das Überwachungsaudit.

- Der Auditteamleiter führt die Zwischenprüfung gemäß dem vereinbarten Zeitplan und in Absprache mit dem Cloud-Anbieter vor Ort durch.
- Der Umfang der Zwischenprüfung ist so zu wählen, dass mindestens die seit der letzten Prüfung erfolgten Änderungen der Datenverarbeitungsvorgänge durch Ermittlungsmethoden (siehe Abschnitt 3.6.5 geprüft werden. Durch geeignete Stichproben (siehe Abschnitt 3.6.6 unter Anwendung der Ermittlungsmethoden ist festzustellen, ob die Datenverarbeitungsvorgänge insgesamt die Zertifizierungskriterien weiterhin erfüllen (siehe ISO/IEC 17000:2020 Tz. A.5.4).
- Im Rahmen der Überwachung prüft die Zertifizierungsstelle insbesondere, ob anerkannte Zertifikate weiterhin gültig sind und ob das Konformitätszeichen korrekt verwendet wurde. Bei der Re-Zertifizierung der anerkannten Zertifizierung wird die Ablauffrist der GDPR CC-Zertifizierung auf die Laufzeit des anerkannten Zertifikats verlängert, jedoch maximal auf die Standardlaufzeit der GDPR CC-Zertifizierung von 3 Jahren oder bei weiteren anerkannten Fremdzertifikaten auf die kürzeste Laufzeit.

Die Ergebnisse der Zwischenprüfung werden durch den Auditteamleiter in einem Zwischenprüfungsbericht (Ermittlungsbericht) zusammengefasst. Der Zwischenprüfungsbericht wird von dem Auditteamleiter inkl. einer Empfehlung (z. B. vor Ablauf des Zwischenprüfungszeitraums) an die Zertifizierungsstelle gesendet.

Das Verfahren und die notwendigen Einträge zur Überwachung in der Zertifizierungsvereinbarung mit dem Cloud-Anbieter sind im Akkreditierungsverfahren und auf Wunsch der Datenschutz-Aufsichtsbehörde jederzeit nachzuweisen.

5.2 Bewertung der Überwachungstätigkeiten

Die Bewertung der Überwachungstätigkeiten erfolgt durch die Zertifizierungsstelle. Der Prozess wird analog zu dem Verfahren gemäß Abschnitt 3.7 durchgeführt.

Wird durch die Zertifizierungsstelle im Rahmen der Bewertung einer der folgenden Sachverhalte festgestellt wird, dass:

- ein anerkanntes Zertifikat nicht mehr gültig ist und der Cloud-Anbieter die Zertifizierungsstelle auch nicht vorab informiert hat und gemeinsam entsprechende Maßnahmen durchgeführt wurden (bspw. Änderungszertifizierung); oder
- erfolgt die Zwischenprüfung nicht in der festgelegten Frist; oder
- eine Nichtkonformität mit Zertifizierungskriterien, entweder als Ergebnis der Überwachung oder anderweitig, nachgewiesen wird,

ergreift die Zertifizierungsstelle Maßnahmen (Einschränkung, Aussetzung oder Widerruf der Zertifizierung) gemäß GDPR CC § 5.6.4 (siehe Abschnitt 5.3). Die Ergebnisse der Bewertung dienen der Zertifizierungsstelle als Grundlage ihrer Zertifizierungsentscheidung.

5.3 Entscheidung der Zertifizierungsstelle

Der Prozess wird analog zu dem Verfahren gemäß Abschnitt 3.8 (ausgenommen Abschnitt 3.8.3) durchgeführt.

Die Zertifizierungsstelle erhält den bewerteten Zwischenprüfungsbericht und entscheidet auf der Grundlage der vorliegenden Informationen (Zwischenprüfungsbericht und Dokumentation) über die Aufrechterhaltung, Einschränkung, Aussetzung oder den Widerruf der Zertifizierung. Erfolgt Bewertung und Entscheidung nicht durch dieselbe Person, ist die Entscheidung basierend auf Grundlage der Bewertung entsprechend zu dokumentieren.

Werden im Rahmen der Bewertung Nichtkonformitäten festgestellt, entscheidet die Zertifizierungsstelle über die zur Einhaltung des GDPR CC-Kriterienkatalogs erforderlichen Maßnahmen. Hierzu gehören:

a) Die Zertifizierungsstelle kann die Zertifizierung einschränken (siehe Abschnitt 5.4.1).
b) Die Zertifizierungsstelle kann die Zertifizierung für einen festgelegten Zeitraum vorbehaltlich der Abstellmaßnahmen durch den Cloud-Anbieter aussetzen (siehe Abschnitt 5.4.2).
c) Die Zertifizierungsstelle kann die Zertifizierung widerrufen (siehe Abschnitt 5.4.3).

Die Entscheidung ist durch die Zertifizierungsstelle zu begründen und dem Cloud-Anbieter schriftlich zuzustellen. Auf Antrag des Cloud-Anbieters kann eine Änderungszertifizierung erfolgen (siehe Abschnitt 6.1).

5.4 Einschränkung, Aussetzung oder Widerruf der Zertifizierung

Wurden im Rahmen der Bewertung Nichtkonformitäten festgestellt, so entscheidet die Zertifizierungsstelle über die Einschränkung, Aussetzung oder den Widerruf der Zertifizierung. Eine Beschreibung der Maßnahmen ist in den folgenden Abschnitten dargestellt.

5.4.1 Einschränkung der Zertifizierung

Die Zertifizierung kann mit Einschränkungen erteilt oder anstelle eines Widerrufs bzw. einer Aussetzung der Gültigkeit eingeschränkt werden, wenn zwar die Zertifizierungskriterien für die beantragte Schutzklasse nicht erfüllt sind, aber die Zertifizierungskriterien einer geringeren Schutzklasse erfüllt sind.

In diesen Fällen kann die Zertifizierung für eine geringere Schutzklasse erteilt werden. Der Cloud-Anbieter kann jederzeit die Einschränkung der Zertifizierung beantragen. Dem Antrag ist zu entsprechen, soweit diesem keine schwerwiegenden Gründe entgegenstehen.

Mit der Einschränkung der Zertifizierung nimmt die Zertifizierungsstelle unverzüglich alle erforderlichen Änderungen an formalen Zertifizierungsdokumenten, öffentlichen Informationen, Genehmigungen zur Nutzung von Konformitätszeichen, usw. vor, um sicherzustellen, dass der eingeschränkte Geltungsbereich der Zertifizierung dem Cloud-Anbieter klar mitgeteilt wird und eindeutig in der Zertifizierungsdokumentation sowie in öffentlichen Informationen beschrieben ist (siehe DIN EN ISO/IEC 17065:2013 Tz. 7.11.3). Hierzu zählen insbesondere

- die Änderung des Konformitätszeichens sowie
- die Änderung des Eintrags der Datenverarbeitungsvorgänge in dem Verzeichnis von zertifizierten Datenverarbeitungsvorgängen.

5.4.2 Aussetzung der Zertifizierung

Eine Aussetzung bezeichnet ein vorübergehendes Außerkraftsetzen der Konformitätsaussage für den gesamten festgelegten Geltungsbereich der Bestätigung oder für Teile davon (siehe ISO/IEC 17000:2020 Tz. 8.2). Die Aussetzung wird sofort wirksam.

Der Cloud-Anbieter kann jederzeit die Aussetzung der Zertifizierung beantragen. Dem Antrag ist zu entsprechen, soweit diesem nicht schwerwiegende Gründe entgegenstehen.

Mit der Aussetzung der Zertifizierung nimmt die Zertifizierungsstelle unverzüglich alle erforderlichen Veränderungen an formellen Zertifizierungsdokumenten, öffentlichen Informationen, Genehmigungen zur Nutzung von Zeichen, usw. vor, um sicherzustellen, dass sie keinen Hinweis darauf geben, dass die Datenverarbeitungsvorgänge weiterhin zertifiziert sind (siehe DIN EN ISO/IEC 17065:2013 Tz. 7.11.3). Hierzu zählen insbesondere

- der Entzug des Konformitätszeichens sowie
- die Entfernung der Datenverarbeitungsvorgänge aus dem Verzeichnis von zertifizierten Datenverarbeitungsvorgängen.

Die Zertifizierungsstelle kann die Zertifizierung für die Dauer eines Feststellungsverfahrens aussetzen. Die Zertifizierungsstelle muss die ausgesetzte Zertifizierung wiederherstellen, wenn das Problem, das zur Aussetzung geführt hat, gelöst worden ist. Wenn die Zertifizierung nach Abschluss des Feststellungsverfahrens (z. B. anlassbezogene Überwachung) wieder in Kraft gesetzt wird, muss die Zertifizierungsstelle alle Änderungen an formalen Zertifizierungsdokumenten, öffentlichen Informationen, Genehmigungen zur Nutzung von Zeichen, usw. vornehmen, um sicherzustellen, dass alle entsprechenden Hinweise, dass die Datenverarbeitungsvorgänge weiterhin zertifiziert sind, vorhanden sind (siehe DIN EN ISO/IEC 17065:2013 Tz. 7.11.6). Hierzu zählen insbesondere

- die Bereitstellung des Konformitätszeichens sowie
- die Eintragung der Datenverarbeitungsvorgänge in dem Verzeichnis von zertifizierten Datenverarbeitungsvorgängen.

Die Inkraftsetzung der Zertifizierung nach einer Aussetzung wird sofort wirksam. Der Cloud-Anbieter darf dann auch die Werbung mit der Zertifizierung fortsetzen. Wurde die Zertifizierung bereits fünf Monate ausgesetzt, so wird dem Kunden eine Frist von vier Wochen gesetzt, um die (anlassbezogene) Zwischenprüfung zu gestatten beziehungsweise zu beauftragen. Erfolgt keine Beauftragung, wird durch die Zertifizierungsstelle eine Entscheidung über den Widerruf der Zertifizierung getroffen.

5.4.3 Widerruf der Zertifizierung

Der Widerruf bezeichnet das Zurückziehen der Zertifizierung (siehe ISO/IEC 17000:2004 Tz. 6.3).

Der Cloud-Anbieter kann jederzeit den Widerruf der Zertifizierung beantragen. Dem Antrag ist zu entsprechen, soweit diesem keine schwerwiegenden Gründe entgegenstehen.

Die Zertifizierung ist zu widerrufen, wenn:

a) die Zertifizierungsstelle feststellt, dass die Voraussetzungen für die Erteilung der Zertifizierung nicht vorlagen oder nicht mehr vorliegen.
b) die für den Cloud-Anbieter zuständige Datenschutz-Aufsichtsbehörde feststellt, dass die Voraussetzungen für die Zertifizierung nicht vorliegen oder nicht mehr vorliegen (siehe EDPB, Annex 1 Tz. 7.11). Der Widerruf erfolgt durch die Zertifizierungsstelle auf Anweisung der zuständigen Datenschutz-Aufsichtsbehörde (Art. 58 Abs. 2 lit. h DS-GVO)
c) wenn eine Zwischenprüfung nicht oder nicht innerhalb der festgelegten Frist durchgeführt wird.
d) wenn die Akkreditierung der Zertifizierungsstelle ausgesetzt oder widerrufen wird (siehe § 4.1.1).
e) wenn der Programminhaber von GDPR CC feststellt, dass der GDPR CC-Kriterienkatalog die gesetzlichen Vorgaben der Datenschutz-Grundverordnung und des BDSG oder die an deren Stelle tretenden gesetzlichen Bestimmungen nicht oder nicht mehr erfüllt. Dies gilt nicht, wenn der Cloud-Anbieter unverzüglich eine Änderungszertifizierung nach einer neuen Version der GDPR CC-Kriterienkatalogs beantragt und diese unverzüglich durchgeführt wird.

Mit dem Widerruf der Zertifizierung nimmt die Zertifizierungsstelle unverzüglich alle erforderlichen Veränderungen an formellen Zertifizierungsdokumenten, öffentlichen Informationen, Genehmigungen zur Nutzung von Zeichen, usw. vor, um sicherzustellen, dass sie keinen Hinweis darauf geben, dass der Datenverarbeitungsvorgang weiterhin zertifiziert ist (siehe DIN EN ISO/IEC 17065:2013 Tz. 7.11.3). Hierzu zählen insbesondere

- der Entzug des Konformitätszeichens sowie
- die Entfernung des Datenverarbeitungsvorgangs aus dem Verzeichnis von zertifizierten Datenverarbeitungsvorgängen.

Der Widerruf wird drei Wochen nach Zustellung der Entscheidung über den Widerruf wirksam.

5.5 Information der Aufsichtsbehörde und des Cloud-Anbieters

Nach Abschluss des Überwachungsaudits wird der unterschriebene Prüfungsbericht und das Ergebnis der Überwachung an den Cloud-Anbieter versendet (siehe Abschnitt 5.3).

Wenn bei einem negativen Überwachungsergebnis durch die Zertifizierungsstelle entschieden wurde, die Zertifizierung einzuschränken, auszusetzen oder zu widerrufen, ist die Aufsichtsbehörde über die Einschränkung, Aussetzung oder den Widerruf zu informieren (siehe EDPB, Annex 1 Tz. 7.11).

Die Zertifizierungsstelle stellt sicher, dass der Cloud-Anbieter die Werbung mit der Zertifizierung in Einklang mit einer Einschränkung ändert bzw. einer Aussetzung oder einem Widerruf einstellt. Der Kunde ist zu sensibilisieren, dass Werbung mit der ursprünglichen Zertifizierung nicht mehr gestattet ist. Der Cloud-Anbieter wird durch die Zertifizierungsstelle informiert, dass die Einschränkung bzw. Unterlassung der Werbung mit der ursprünglichen Zertifizierung von der Zertifizierungsstelle überwacht wird. Dazu kann die Website des Kunden geprüft werden, um unlauteren Wettbewerb festzustellen.

Die Zertifizierungsstelle fordert den Cloud-Anbieter auf, seine Cloud-Nutzer über die Einschränkung, die Aussetzung oder den Widerruf zu informieren.

6 Änderung und Erweiterung der Zertifizierung

Die Zertifizierungsstelle hat Prozesse zur Bearbeitung von Änderungen und Erweiterungen von Zertifizierungen definiert, die im Folgenden beschrieben werden.

6.1 Änderungszertifizierung

Die Zertifizierungsstelle hat einen Prozess implementiert, über den sichergestellt wird, dass alle Änderungen, die sich auf die Zertifizierung auswirken können, berücksichtigt werden und entscheidet über die geeigneten Maßnahmen.

In der folgenden Beschreibung sind Änderungen, die sich auf die Zertifizierung aufgrund von Änderungen im Programm, Veränderungen an Datenverarbeitungsvorgängen des Kunden und Veränderungen an rechtlichen Rahmenbedingungen ergeben können, dargestellt.

6.1.1 Änderungen am Programm

Die Zertifizierungsstelle wird vom Programmeigner darüber informiert, wenn dieser z. B. aufgrund von Änderungen an den rechtlichen Rahmenbedingungen Änderungen an den festgelegten Zertifizierungskriterien, Zertifizierungsanforderungen und dem Zertifizierungsprogramm durchführt.

Die Zertifizierungsstelle hat einen Prozess zur Entgegennahme und Behandlung von entsprechenden Meldungen durch den Programmeigner etabliert, sodass:

- Maßnahmen eingeleitet werden können, um Änderungen an den Zertifizierungsanforderungen zeitnah umzusetzen;
- bei Änderungen an Zertifizierungskriterien, die Einfluss auf die Konformitätsbewertungsaussage haben könnten, den Sachverhalt für jeden zertifizierten Datenverarbeitungsvorgang zu ermitteln und geeignete Maßnahmen zu er-greifen.

Bei Mitteilung der Änderungen am Zertifizierungsprogramm wird dem Cloud-Anbieter eine angemessene Frist zur Umsetzung der Änderungen auferlegt. Die Frist kann auf Antrag des Cloud-Anbieters verlängert werden. Die Umsetzung der Änderungen durch die Cloud-Anbieter werden durch die Zertifizierungsstelle geprüft.

6.1.2 Veränderungen an Datenverarbeitungsvorgängen des Kunden

Der Cloud-Anbieter ist verpflichtet, die Zertifizierungsstelle während der gesamten Gültigkeitsdauer der Zertifizierung unverzüglich über Veränderungen zu informieren, die die Erfüllung der Zertifizierungskriterien beeinträchtigen können.
Beispiele für Veränderungen, die die Erfüllung der Zertifizierungskriterien beeinträchtigen können, sind:

- Veränderung bei dem rechtlichen, wirtschaftlichen oder organisatorischen Status oder die bei der Eigentümerschaft und Änderungen der tatsächlichen oder rechtlichen Verhältnisse;
- Veränderung bei Organisation und Management (z. B. Änderungen von Schlüsselpositionen, Entscheidungsprozessen oder technischem Personal);
- Wesentliche Änderungen an Software oder Hardware, welche zur Erbringung der Datenverarbeitungsvorgänge erforderlich sind;
- Wesentliche Änderungen hinsichtlich der Verarbeitung personenbezogener Daten;

- Änderungen der für den Zertifizierungsgegenstand einschlägigen Rechtsnormen sowie des Stands der Technik;
- Änderungen an Rechenzentren (bspw. Standortwechsel);
- Änderungen bei der Einbindung von Subauftragsverarbeitern mit Relevanz für den Datenverarbeitungsvorgang.

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 (siehe DSK Tz. 4.1.2.2).

6.1.3 Veränderungen an rechtlichen Rahmenbedingungen

Die Zertifizierungsstelle hat einen Prozess implementiert, um sicherzustellen, dass Änderungen der rechtlichen Rahmenbedingungen, die die internen Abläufe der Zertifizierungsstelle bzw. die Zertifizierung betreffen, fortlaufend und zeitnah erkannt werden sowie mit geeigneten Maßnahmen adressiert werden.

Beispiele für Veränderungen sind (siehe DSK Tz. 7.10, EDPB, Annex 1 Tz. 7.10):

- Gesetzesnovellierungen,
- Erlass delegierter Rechtsakte der Europäischen Kommission,
- Entscheidungen des Europäischen Datenschutzausschusses,
- Gerichtsentscheidungen und
- Fortentwicklungen des Stands der Technik (soweit relevant für die künftige Zertifizierung und Überwachung).

Die Zertifizierungsstelle hat einen Prozess zur um Überwachung von rechtlichen Rahmenbedingungen, inklusive:

- der Ableitung von Maßnahmen, die die Zertifizierungsstelle betreffen und die Ableitung der von geeigneten Maßnahmen sowie die Kommunikation mit dem Cloud-Anbieter bezüglich der ihn bzw. die Zertifizierung betreffenden rechtlichen Rahmenbedingungen und
- der Information des Programmeigners, falls die Änderungen einen Einfluss auf die Zertifizierungsanforderungen oder Zertifizierungskriterien haben, oder von großer Bedeutung sind,

implementiert. Im Rahmen des Prozesses wird sichergestellt, dass durch die Zertifizierungsstelle geeignete Maßnahmen definiert und kommuniziert werden. Die Zertifizierungsstelle hat darüber hinaus sicherzustellen, dass in vergleichbaren Fällen vergleichbare Maßnahmen ergriffen werden.

Die Zertifizierungsstelle ist bei Hinweisen auf die zuvor dargestellten Änderungen (Programm, Kunde oder Rahmenbedingungen), die Einfluss auf die Konformitätsbewertungsaussage haben könnten, verpflichtet, den Sachverhalt zu ermitteln und geeignete Maßnahmen zu ergreifen. Die Zertifizierungsstelle hat einen Prozess implementiert, der sicherstellt, dass durch die Zertifizierungsstelle geeignete Maßnahmen definiert werden und alle beteiligten Parteien (inklusive der Auditteams) über die Umsetzung dieser Maßnahmen sowie die Zeitplanung für die Umsetzung der Maßnahmen informiert werden.

Geeignete Maßnahmen sind beispielsweise:

a. Die Zertifizierungsstelle stellt fest, dass eine **Zwischenprüfung zur Aufrechterhaltung der Zertifizierung erforderlich** ist und prüft die Umsetzung der Änderungen. Die Zertifizierungsstelle beschreibt dem Cloud-Anbieter deutlich, unter welchen Aspekten Zweifel an

der Einhaltung der Zertifizierungsvoraussetzungen bestehen. Die Zertifizierungsstelle setzt dem Cloud-Anbieter eine angemessene Frist zur Durchführung der Zwischenprüfung. Diese Frist kann auf Antrag des Kunden verlängert werden. Eine erforderliche Zwischenprüfung erfolgt nach dem in Abschnitt 0 (anlassbezogene Zwischenprüfung) beschriebenen Verfahren.

b. Die Zertifizierungsstelle empfiehlt dem Cloud-Anbieter eine **Änderungszertifizierung.**
c. bei Feststellung einer Nichtkonformität von Zertifizierungskriterien die Durchführung der unter § 5.6.4 beschriebenen Maßnahmen gemäß den dort festgelegten Anforderungen ergreifen.
d. Die Zertifizierungsstelle setzt die Zertifizierung für die Dauer der Änderungszertifizierung aus. Weitere Anforderungen an die **Aussetzung der Zertifizierung** sind in Abschnitt 5.4.2 beschrieben.

Für die Änderungszertifizierung gelten die GDPR CC-Anforderungen für durchzuführende Auswahl-, Ermittlungs-, Bewertungs-, und Entscheidungstätigkeiten entsprechend. Im Folgenden wird der Prozess der Änderungszertifizierung beschrieben:

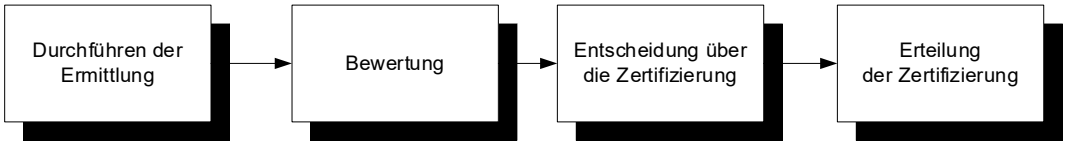

Abbildung 3 Prozess der Änderungszertifizierung

Durchführen der Ermittlung

Die Ermittlung folgt grundsätzlich dem in Abschnitt 3.5 und 3.6 beschriebenen Verfahren. Die folgenden Punkte ergänzen die Beschreibung des bestehenden Verfahrens für die Änderungszertifizierung.

- Der Auditteamleiter erhält Informationen zu relevanten Änderungen und die festgelegten Maßnahmen von der Zertifizierungsstelle und führt die Prüfung gemäß dem vereinbarten Zeitplan und in Absprache mit dem Cloud-Anbieter vor Ort durch.
- Der Umfang der Ermittlung ist so zu wählen, dass mindestens die Änderungen (beispielsweise Zertifizierungskriterien oder Änderungen der Datenverarbeitungsvorgänge) durch Ermittlungsmethoden (siehe Abschnitt 3.6.5) geprüft werden. Durch geeignete Stichproben (siehe Abschnitt 3.6.7) unter Anwendung der Ermittlungsmethoden ist festzustellen, ob die Datenverarbeitungsvorgänge insgesamt die Zertifizierungskriterien weiterhin erfüllen.

Die Ergebnisse der Ermittlung werden durch den Auditteamleiter in dem Ermittlungsbericht inkl. einer Empfehlung an die Zertifizierungsstelle zur Bewertung und Entscheidung gesendet.

Bewertung

Die Bewertung der Überwachungstätigkeiten erfolgt durch die Zertifizierungsstelle. Der Prozess wird analog zu dem Verfahren gemäß Abschnitt 3.7 durchgeführt.

Wird durch die Zertifizierungsstelle festgestellt wird, dass eine Nichtkonformität mit Zertifizierungskriterien nachgewiesen wird, ergreift die Zertifizierungsstelle Maßnahmen (Einschränkung, Aussetzung oder Widerruf der Zertifizierung, siehe Abschnitt 5.3). Die Ergebnisse der Bewertung dienen der Zertifizierungsstelle als Grundlage für ihre Zertifizierungsentscheidung.

Entscheidung der Zertifizierungsstelle

Der Prozess wird analog zu dem Verfahren gemäß Abschnitt 3.8 durchgeführt.

Die Zertifizierungsstelle trifft die Zertifizierungsentscheidung auf der Grundlage der vorliegenden Informationen (Zwischenprüfungsbericht und Dokumentation).

Erteilung der Zertifizierung

Der Prozess umfasst die Anpassung der Konformitätszeichen, der Zertifizierungsdokumentation sowie das die Veröffentlichung der Zertifizierungsentscheidung und wird analog zu dem Verfahren gemäß Abschnitt 3.9 durchgeführt.

6.2 Erweiterung der Zertifizierung

Der Cloud-Anbieter kann jederzeit die Erweiterung der Zertifizierung bei der Zertifizierungsstelle beantragen. Die Erweiterung bezeichnet z. B. die Erhöhung der Schutzklasse.

Die Zertifizierungsstelle bewertet die Ergebnisse der Änderungszertifizierung und entscheidet über die Vergabe einer Zertifizierung mit höherer Schutzklasse. Die Anforderungen für Ermittlungs-, Bewertungs-, und Entscheidungstätigkeiten sind auch bei der Änderungsprüfung für eine Erweiterung anzuwenden.

Der Cloud-Anbieter muss im Rahmen einer Änderungszertifizierung nachweisen, dass er die Anforderungen der höheren Schutzklasse erfüllt. Das Verfahren zur Änderungszertifizierung wird im Abschnitt 6.1 beschrieben.

7 Re-Zertifizierung

Die Planung der Re-Zertifizierung erfolgt äquivalent zum Zertifizierungsaudit. Die Fristen von Zertifizierungsstelle gesetzten Fristen sind durch den Cloud-Anbieter zwingend einzuhalten. Die Re-Zertifizierungsprüfung muss vor Ablauf der Zertifizierung abgeschlossen werden.

Grundsätzlich muss die Re-Zertifizierung noch während der Laufzeit des aktuellen Zertifikates abgeschlossen sein. Dies gilt auch für die Übernahme von akkreditierten Zertifizierungen anderer Zertifizierungsgesellschaften. Um dies zu ermöglichen, sollte das Re-Zertifizierungsaudit möglichst 45 Tage vor Ablauf des Zertifikates abgeschlossen werden, muss jedoch spätestens 36 Monate nach dem Zertifizierungsaudit abgeschlossen sein. Aus diesem Grund ist bei der Planung zu berücksichtigen, dass die Fristen für die Bearbeitung von möglicherweise identifizierten Abweichungen angepasst werden müssen. Der Termin für den Abschluss des Vor-Ort-Audits sollte mindestens 3 Wochen vor Ablauf des Zertifikates geplant werden, damit die Maßnahmen noch bewertet werden können und die Zertifizierungsstelle das Verfahren abschließend beurteilen kann.

Wenn die Re-Zertifizierungstätigkeiten vor Ablauf der bestehenden Zertifizierung erfolgreich abgeschlossen werden, dann kann das Ablaufdatum der neuen Zertifizierung auf dem Ablaufdatum der bestehenden Zertifizierung beruhen. Das Ausgabedatum des neuen Zertifikats muss dem Tag der Re-Zertifizierungsentscheidung oder einem späteren entsprechen.

Sollten Probleme mit der oben genannten Terminierung bestehen oder ist zu befürchten, dass die Re-Zertifizierung nicht vor Ablauf des Zertifikates abgeschlossen werden kann, sollte der Auditteamleiter die Zertifizierungsstelle informieren. Formal ist der Kunde nach Ablauf des alten Zertifikates nicht mehr zertifiziert und darf somit nicht mehr mit der Zertifizierung werben. Die DAkkS akzeptiert in schriftlich begründeten Ausnahmefällen, dass eine Re-Zertifizierung noch in einer Frist von 6 Monaten nach Ablauf des Zertifikates durchgeführt wird. Dies bedeutet aber, dass das Audit spätestens 3 Monate nach Ablauf des Zertifikates durchgeführt wird, damit der Kunde noch Zeit für die Bearbeitung von Abweichungen hat. Nach Abschluss des Verfahrens erhält der Kunde ein Zertifikat, das sich an der der ursprünglichen Laufzeit des vorherigen Zertifikates orientiert. Das bedeutet, dass das neue Zertifikat weniger als 3 Jahre Gültigkeit hat. Alle weiteren Audits sind auf Basis des Audittermins der Erstzertifizierung zu planen.

Sollte das Verfahren nicht innerhalb der 6 Monate abgeschlossen sein, ist eine Erstzertifizierung durchzuführen. Jegliche Arbeitsergebnisse aus der vergangenen Zertifizierung sind nicht zu berücksichtigen.

Wenn die Zertifizierungsstelle vor Ablauf des Zertifizierungsdatums das Re-Zertifizierungsaudit nicht abgeschlossen hat oder außerstande ist, die Umsetzung von Korrekturen und Korrekturmaßnahmen für eine beliebige wesentliche Nichtkonformität zu verifizieren, dann darf keine Empfehlung für die Re-Zertifizierung ausgesprochen werden und die Gültigkeit der Zertifizierung darf nicht verlängert werden. Der Kunde muss informiert und die Konsequenzen erläutert werden.

Unter der Voraussetzung, dass die ausstehenden Re-Zertifizierungstätigkeiten abgeschlossen worden sind, kann die Zertifizierungsstelle innerhalb von 6 Monaten nach Ablauf der Zertifizierung die Zertifizierung wiederherstellen; andernfalls ist mindestens die Stage 2-Prüfung durchzuführen. Das Gültigkeitsdatum des Zertifikats muss dem Tag der Re-Zertifizierungsentscheidung oder einem späteren entsprechen und das Ablaufdatum muss auf dem vorangegangenen Zertifizierungszyklus basieren.

Die Zertifizierungsstelle entscheidet auf Grundlage der Ergebnisse des Re-Zertifizierungsaudits über die Erneuerung der Zertifizierung. Dem Kunden werden die daraus resultierenden Zertifizierungsdokumente erneut zugestellt.