Informationsblatt

Informationsblatt Auditierung und Zertifizierung GDPR CC

Dokumentenart:	Sonstige Dokumente
Autor:	Leiter der Zertifizierungsstelle-DL
Editor:	Niels Isenbort
QS:	Leiter der Zertifizierungsstelle-DL
Version:	1.0
Status:	Freigegeben
Verschwiegenheit:	ÖFFENTLICH

ÖFFENTLICH
Informationen, die ohne Einschränkungen bekannt gemacht werden können

pwc

Inhaltsverzeichnis

Dokumentenhistorie

Version	Datum	Änderung	Autor
0.1	01.10.2021	Dokument neu erstellt	Niels Isenbort
0.2	14.12.2022	Änderungen und Review	Sören Scholz
1.0	28.12.2022	Freigabe	Sören Scholz

1 Einleitung

1.1 Zielsetzung und Anwendung

Das vorliegende Dokument beschreibt die Anforderungen und den Ablauf für Audits und Zertifizierungen nach dem GDPR CC-Konformitätsbewertungsprogramm (im Folgenden auch GDPR CC genannt) sowie den darin referenzierten Dokumenten in ihren jeweils aktuellen Fassungen, die für die Erteilung eines GDPR CC-Zertifikats erfüllt beziehungsweise eingehalten werden müssen. Es berücksichtigt dabei auch die Anforderungen an Zertifizierungsstellen gemäß DIN EN ISO/IEC 17065.

1.2 Adressat

Der Adressat Dokuments sind potentielle Kunden (Cloud-Anbieter) mit dem Ziel, ihre personenbezogenen Datenverarbeitungsvorgänge (Cloud-Services) nach dem GDPR CC-Konformitätsbewertungsprogramm und dem GDPR CC-Kriterienkatalog zertifizieren zu lassen. Ihnen soll die Vorgehensweise des Audit- und Zertifizierungsprozesses erläutert werden.

1.3 Begrifflichkeiten

Die in diesem Dokument verwendeten Begrifflichkeiten, die im Kontext dieses Ablaufschemas eine besondere Bedeutung haben, sind im Folgenden näher erläutert.

Geltungsbereich der Zertifizierung

Der Geltungsbereich bzw. Anwendungsbereich der Zertifizierung (im Folgenden auch „Scope“ genannt), inkl. einer genauen Abgrenzung der Datenverarbeitungsvorgänge als Zertifizierungsgegenstand, definiert, für welchen Teil der zu zertifizierenden Organisation die Konformitätsaussage Anwendung findet.

Zertifizierungsstelle

Eine Zertifizierungsstelle ist autorisiert, eine Organisation auf die Einhaltung von Normen zu prüfen, für die sie akkreditiert ist. Man spricht auch von Konformitätsbewertungsstelle. Sie kann im Namen der ISO Zertifikate ausfertigen. Die Zertifizierungsstelle-Dienstleistung ist hier die zuständige Stelle innerhalb der PwC Certification Services GmbH.

Zertifikat

Das Zertifikat ist das offizielle Dokument, das als Konformitätsnachweis für eine erfolgreiche Prüfung dient.

Audit

Systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen und zu deren objektiver Auswertung, um zu ermitteln, inwieweit die Zertifizierungskriterien erfüllt sind.

Antragsteller

Eine Organisation (Cloud-Anbieter), die den Antrag auf Konformitätsbewertung gestellt hat.

Auditnachweis

Aufzeichnungen, Tatsachenfeststellungen oder andere Informationen, die für die Auditkriterien relevant und verifizierbar sind. Die Erhebung der Auditnachweise obliegt dem Auditteamleiter. Dazu zählen u.a. die anzuwendenden Ermittlungsmethoden, die Auswahl von quantitativen und qualitativen Nachweisen, sowie die Festlegung von Stichprobenumfängen.

Auditteam

Ein Auditteam besteht aus einem oder mehreren Auditoren, die ein Audit durchführen.

Auditor

Person mit der gegenüber der Zertifizierungsstelle nachgewiesenen Qualifikation, ein Zertifizierungsaudit durchzuführen.

Auditteamleiter

Der Auditteamleiter ist Auditor und fachlicher Leiter des Auditteams. Er ist für den Auditprozess weisungsbefugt gegenüber den sonstigen Auditoren im Auditteam.

Fachexperte

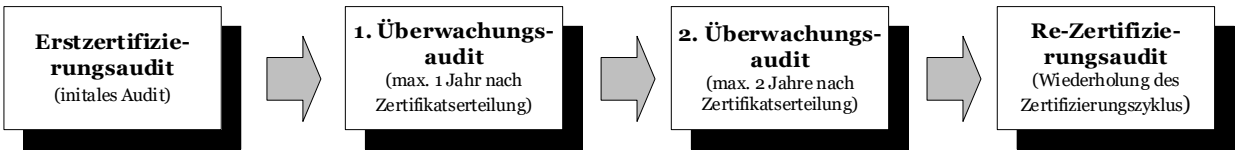
Zum Auditteam können auch Fachexperten gehören, die entweder spezielle Branchenkenntnisse oder sehr gute technische oder rechtliche Fachkenntnisse besitzen.

2 Der Beginn der Zertifizierung

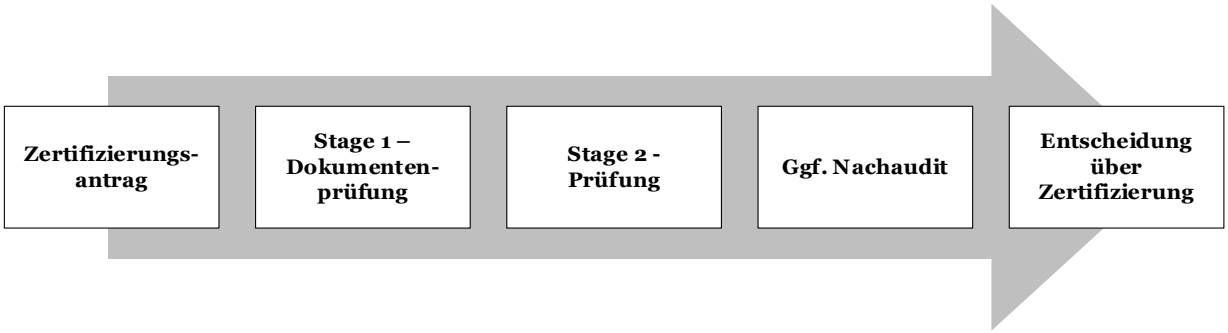
Dieses Kapitel beschreibt die Anforderungen und Schritte, die vor Aufnahme der Prüfungstätigkeiten erfüllt sein müssen.

2.1 Zertifizierungsprozess

Das vorliegende Ablaufschema hat Lenkungsfunktion für den Zertifizierungsprozess. Erteilung, Überwachung und Verlängerung des Zertifikats sind die unterschiedlichen „Lebensphasen“, die während der Laufzeit einer Zertifizierung zur Anwendung kommen.



Die Erstzertifizierung beinhaltet fünf Schritte, die ihrer Abfolge nach in der nachstehenden Grafik dargestellt sind. Die einzelnen Schritte sind im vorliegenden Ablaufschema beschrieben.



Die Schritte und -methoden in den Überwachungsaudits sowie im Re-Zertifizierungsaudit weichen nicht erheblich denen des Erstzertifizierungsaudits ab.

2.2 Auditgrundsätze

Für Audits von Zertifizierungsstellen gelten die folgenden vertrauensbildenden Maßnahmen:

Vermittlung von Vertrauen

Übergeordnetes Ziel der Zertifizierung ist es, allen Beteiligten das Vertrauen zu vermitteln, dass Datenverarbeitungsvorgänge in Cloud-Diensten fest gelegte Zertifizierungskriterien erfüllen. Der Wert der Zertifizierung ist der Grad an öffentlichem Vertrauen, der durch einen unparteiischen und kompetenten Nachweis einer dritten Stelle vermittelt wird. Die Zertifizierung soll es Cloud-Anbietern ermöglichen, gegenüber dem Markt nachzuweisen, dass ihren Datenverarbeitungsvorgängen die Erfüllung festgelegter Zertifizierungskriterien durch eine unparteiische dritte Stelle bestätigt wurde.

Unparteilichkeit

Um Vertrauen in ihre Tätigkeiten und Ergebnisse zu schaffen, ist es für die Zertifizierungsstellen und ihr Personal erforderlich, unparteiisch zu sein und als unparteiisch empfunden zu werden. Die Zertifizierungsstelle stellt sicher, dass keine Interessenkonflikte zwischen der Zertifizierungsstelle, den Auditoren und dem Kunden bestehen. Alle relevanten Teilprozesse sind im Hinblick auf dieses Ziel überprüft.

Kompetenz

Um Zertifizierungen erbringen zu können, die Vertrauen erzeugen, ist Kompetenz des Personals, unterstützt durch das Managementsystem der Zertifizierungsstelle, erforderlich. Die Zertifizierungsstelle stellt durch einen geeigneten Auswahl- und Überwachungsprozess sowie das Managementsystem der Zertifizierungsstelle sicher, dass Auditoren über die notwendigen Kompetenzen und Fachkenntnisse verfügen. Dies schließt interne wie externe Auditoren gleichermaßen ein.

Vertraulichkeit und Offenheit

Das Gleichgewicht zwischen den Zertifizierungsanforderungen, die sich auf die Vertraulichkeit und die Offenheit beziehen, hat einen Einfluss auf das Vertrauen der interessierten Parteien sowie deren Wahrnehmung über den Wert der durchgeführten Zertifizierung. Alle vom Kunden 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.

Nicht-diskriminierende Bedingungen

Die Zertifizierungsstelle stellt sicher, 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.

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. Werden Tätigkeiten von ausgegliederten Auditoren durchgeführt, ist die Zertifizierungsstelle dafür verantwortlich, dass alle Zertifizierungsanforderungen von den ausgegliederten Auditoren erfüllt und eingehalten werden. Basierend auf der Bewertung der Nachweise, trifft die Zertifizierungsstelle die Zertifizierungsentscheidung, die Zertifizierung zu erteilen, wenn keine Nicht-Konformitäten festgestellt wurden. Werden Nicht-Konformitäten festgestellt bzw. die Konformität nicht ausreichend nachgewiesen, wird die Zertifizierung nicht erteilt.

Offenheit für Beschwerden

Die Zertifizierungsstelle ist offen für Beschwerden von Cloud-Anbietern oder anderen interessierten Parteien. Die Zertifizierungsstelle verfügt über ein Verfahren, mit dem Beschwerden bezüglich des Zertifizierungsprozesses oder Einsprüchen bezüglich der Zertifizierungsentscheidungen aufgenommen und konstruktiv bearbeitet werden.

2.3 Zertifizierungsantrag

Die Zertifizierungsstelle stellt ein Antragsformular zur Verfügung, das vom Interessenten auszufüllen ist. Die Zertifizierungsstelle kann die Annahme eines Zertifizierungsantrags verweigern, sofern Anhaltspunkte für Interessenskonflikte bestehen. Alle Regelungen zur Vermeidung von Interessenskonflikten der PwC Certification Services GmbH finden Anwendung. Ein angenommener Antrag ist Voraussetzung für die Einleitung der Auditaktivitäten.

2.4 Scope der Zertifizierung (Festlegung des Zertifizierungsgegenstandes)

Der Scope der Zertifizierung und damit der Zertifizierungsgegenstand wird bei der Beantragung der Zertifizierung durch den Cloud-Anbieter festgelegt. Zertifizierungsgegenstand 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. Bei der Festlegung des Scopes ist darauf zu achten, dass auf (1.) personenbezogene Daten, (2.) technische Systeme (Infrastruktur, Hardware und Software, die genutzt werden, um personenbezogene Daten zu verarbeiten) und (3.) Prozesse und Verfahren,

die mit Verarbeitungsvorgängen in Verbindung stehen, Bezug genommen wird. Durch die Zertifizierungsstelle wird geprüft, ob sich der zu prüfende Bereich ausreichend scharf von anderen Bereichen, wie z. B. einzelnen Geschäftseinheiten, Standorten und eingesetzten technischen Systemen des zu zertifizierenden Unternehmens klar abgrenzen lässt. Darüber hinaus muss eine klare Verantwortungsabgrenzung zwischen Cloud-Anbieter und Cloud-Nutzer bzw. Subauftragsverarbeitern sichergestellt werden. 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. Der Scope der Zertifizierung bildet die Grundlage für die Risikobeurteilung und Risikobehandlungsoptionen.

Die Zertifizierungsstelle hat das Recht, den Zertifizierungsgegenstand abzulehnen beziehungsweise Nachbesserung zu fordern.

2.5 Rechtliche Voraussetzungen

Der Vereinbarung zwischen Cloud-Anbieter und Zertifizierungsstelle muss ein schriftlicher Vertrag zugrunde liegen, der auf dem Zertifizierungsantrag basiert. Der Vertrag muss den gesamten Geltungsbereich des dem Zertifikat zugrundeliegenden Anwendungsbereichs umfassen.

2.6 Auswahl der Auditoren

Die Auswahl der Auditoren, die mit dem Zertifizierungsaudit beauftragt werden, obliegt der Zertifizierungsstelle. Eine Auswahl durch den Antragsteller ist ausgeschlossen. Die Qualifikation der Auditoren ist über entsprechende Fachkundenachweise sichergestellt. Die Prüfungsplanung erfolgt im Auftrag der Zertifizierungsstelle zwischen dem Auditteamleiter und dem Cloud-Anbieter.

2.7 Leistungsabgrenzung

Beratungsleistungen im Datenschutz sowie die Mitwirkung bei internen Audits des Cloud-Anbieters sowohl vor als auch während der Prüfung sind ausgeschlossen. Dieser Ausschluss beschränkt sich auf Beratungstätigkeiten, die innerhalb von zwei Jahren vor dem Zertifizierungsantrag oder einem Überwachungsaudit stattgefunden haben. Die Umsetzung der während der Prüfung als notwendig identifizierten Maßnahmen ist ebenfalls nicht Bestandteil der Leistung. Die Umsetzung wird auch außerhalb der Zertifizierungstätigkeit von der PwC Certification Services GmbH nicht als Leistung angeboten.

3 Der Zertifizierungsprozess

Für eine Auditierung nach den ISO-Normen existieren drei unterschiedlichen Audittypen:

- **Erstzertifizierung**
  Das initiale Audit, das zur ersten Vergabe des Zertifikats führt. Das Zertifikat hat eine Gültigkeit von drei Jahren ab Ausstellungsdatum.
- **Überwachungsaudit**
  Während der Gültigkeitsdauer des Zertifikats muss in jährlichen Abständen ein Überwachungsaudit stattfinden. Dies stellt sicher, dass die Zertifizierungskriterien dauerhaft erfüllt sind. Darüber hinaus können anlassbezogene Überwachungen bei Auffälligkeiten erfolgen, die eine Nichtkonformität der Zertifizierungskriterien befürchten lassen.
- **Re-Zertifizierungsaudit**
  Bis zum Ablauf der Zertifikatsgültigkeit muss eine Re-Zertifizierung erfolgen. Ansonsten ist der Zertifizierungszyklus unterbrochen.

Die drei Arten sind im Folgenden näher beschrieben.

3.1 Erstzertifizierungsaudit

Die vom Antragsteller vorgelegten Referenzdokumente werden gesichtet und gemäß den Anforderungen bewertet. Alle Bewertungen der Referenzdokumente werden in den Auditbericht übernommen. Die durchgeführten Prüfungen müssen angemessen und reproduzierbar sein. Die Prüfungsergebnisse und Bewertungen müssen im Auditbericht verständlich und nachvollziehbar dokumentiert werden. Das Erstzertifizierungsaudit umfasst zwei Stufen, die zeitlich wie logisch aufeinander aufbauen.

3.1.1 Stage 1-Dokumentenprüfung

Die Stage 1-Dokumentenprüfung fokussiert auf die generelle Bereitschaft des Cloud-Anbieters (Antragsteller) und stellt sicher, dass die Informationen über den Cloud-Anbieter und den Datenverarbeitungsvorgang für die Durchführung des Zertifizierungsprozesses in der Stage 2-Prüfung durchführbar ist. Hierzu werden in der Stage 1-Dokumentenprüfung folgende Informationen angefordert:

- 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.

Im Rahmen der Stage 1-Dokumentenprüfung erfolgt eine Beurteilung:

- ob die Informationen über den Cloud-Anbieter und den Datenverarbeitungsvorgang für die Durchführung des Zertifizierungsprozesses ausreichend sind. Dieses beinhaltet folgende notwendige Informationen:
  - Standort(e) des Cloud-Anbieters,
  - Prozesse und eingesetzte Arbeitsmittel,
  - festgelegte Lenkungsebenen (insbesondere bei Cloud-Anbietern mit mehreren Standorten)
- ob ein ausreichendes Verständnis über den Datenverarbeitungsvorgang anhand der übermittelten Dokumente durch die Zertifizierungsstelle erlangt werden konnte.
- ob der Cloud-Anbieter ausreichende Ressourcen für die Stage 2-Prüfung bereitstellt.
- ob alle relevanten Ansprechpartner des Cloud-Anbieters auf die Stage 2-Prüfung vorbereitet und die erforderlichen standortspezifischen Bedingungen gegeben sind.

- ob alle notwendigen Informationen über den Geltungsbereich der angestrebten Zertifizierung vorliegen.
- welche Schwerpunkte für die Stage 2-Prüfung festgelegt werden.
- ob interne Audits und Managementbewertungen belegen, dass der Grad der Umsetzung des Managementsystems entsprechend ausreichend ist, um mit der Stage 2 – Prüfung zu beginnen.

Als Ergebnis der Stage 1-Dokumentenprüfung erhält der Cloud-Anbieter (Antragsteller) eine Bewertung, welche Schwachstellen während der Stage 2-Dokumentenprüfung als Nichtkonformität eingestuft werden könnten.

Zwischen der Stage 1-Dokumentenprüfung und Stage 2-Prüfung muss ausreichend zeitlicher Abstand bestehen, damit dem Cloud-Anbieter die Möglichkeit gegeben wird, angemessene Lösungen für die identifizierten Schwachstellen zu finden. Hierbei darf es jedoch nicht dazu kommen, dass die Stage 1-Dokumentenprüfung als Vorbereitung und Hilfestellung für die Erlangung des Zertifikats in der Stage 2-Prüfung genutzt wird. Prüfungsfeststellungen aus der Stage 1-Dokumentenprüfung müssen entsprechend im abschließenden Prüfungsbericht enthalten sein.

Die Zertifizierungsstelle bewertet und entscheidet auf Basis der Empfehlung des Auditteamleiters, ob mit der Stage 2-Prüfung fortgefahren werden kann, oder ob das Audit abgebrochen wird.

3.1.2 Stage 2-Prüfung

Mit den dokumentierten Ergebnissen der Stage 1-Dokumentenprüfung sowie der Entscheidung zur Weiterführung beginnt die Stage 2-Prüfung.

Die Stage 2-Prüfung beinhaltet ein Audit vor Ort und umfasst alle relevanten Standorte der zu zertifizierenden Organisation. Vor Beginn dieses Audits wird dem Antragsteller ein Auditplan zur Verfügung gestellt. Dieser Schritt umfasst immer auch eine Eröffnungs- und eine Abschlussbesprechung. Bei kritischen Ereignissen, die eine Auditierung vor Ort nicht erlauben, kann die Auditierung mit Mitteln der Informations- und Kommunikationstechnik auch über eine räumliche Distanz hinweg durchgeführt werden. Es die Vorgaben des IAF MD 4 (IAF Mandatory document for the use of information and communication technology (ICT) for auditing / assessment purposes).

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

Die Ermittlung erfolgt auf Grundlage der im Auftrag klar abgegrenzten Beschreibung des Zertifizierungsgegenstands, der – inklusive aller technischen und organisatorischen Vorgänge – den anwendbaren Zertifizierungskriterien entsprechen muss. Dabei setzt sich ein Cloud-Dienst aus einem oder mehreren Datenverarbeitungsvorgängen zusammen. Einem Datenverarbeitungsvorgang können wiederum Ermittlungsobjekte zugeordnet werden. Zur Feststellung der Konformität können die folgenden Ermittlungsobjekte begutachtet 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.

Die Bewertung und Entscheidung über die Erteilung der GDPR CC-Zertifizierung erfolgt durch die Zertifizierungsstelle. Die Zertifizierungsstelle hat die zuständige Datenschutz-Aufsichtsbehörde über die Zertifizierung schriftlich und mindestens eine Woche vor Erteilung der Zertifizierung zu informieren. Mögliche Einsprüche der Datenschutz-Aufsichtsbehörde oder des Cloud-Anbieters werden bei der Erteilung der Zertifizierung berücksichtigt.

3.1.3 Nachbesserungen und Nachforderungen

Nachbesserungen

Sowohl in der Stage 1-Dokumentenprüfung sowie in der Stage 2-Prüfung können sich Abweichungen ergeben. Diese müssen sachgerecht behoben werden. Dabei gibt es verschiedene Stufen der Behandlung von Abweichungen, je nach Schwere:

- **Nichtkonformität**
  Wesentliche Abweichung, sodass erhebliche Zweifel bestehen, dass die Datenschutzanforderungen grundsätzlich eingehalten werden. Beispiele können sein:
  - 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.
  - Prozessdokumentationen liegt vor, diese wird jedoch beim Cloud-Dienst-Betrieb nicht fortlaufend durchgeführt (‚gelebt').
  - Sicherheitstests haben schwerwiegende Mängel oder Schwachstellen in der eingesetzten Software des Cloud-Dienstes ergeben.
  - Befragung oder Vor-Ort-Prüfung im Rahmen eines Audits hat die fehlende Umsetzung von Zertifizierungskriterien aufgedeckt.
- **Erfüllung mit Empfehlung**
  Abweichung, die in ihrer Geringfügigkeit die Einhaltung der Datenschutzanforderungen insgesamt nicht in Frage stellt (Verbesserungspotential). Beispiele können sein:
  - Das eingesetzte Verschlüsselungsverfahren ist gerade noch „Stand der Technik", sollte aber zeitnah ausgetauscht werden.
  - Da keine Passwortrichtlinie bzgl. der erneuten Verwendung von Passwörtern gesetzt ist, können Mitarbeiter ein ursprüngliches Passwort erneut verwenden.
  - Das IT-Sicherheitshandbuch sollte gepflegt werden und einer standardisierten Methodik folgen.

Nichtkonformitäten müssen vor der Erteilung Zertifizierung behoben sein. Wurde durch die Zertifizierungsstelle festgestellt, dass mindestens ein Zertifizierungskriterium nicht erfüllt ist, prüft die Zertifizierungsstelle, ob eine Nachbesserung in angemessener Frist vom Cloud-Anbieter durchgeführt werden kann. Die Zertifizierungsstelle beschreibt dem Cloud-Anbieter deutlich, welche Mängel oder Abweichungen vorliegen, die einer Erfüllung der Zertifizierungskriterien entgegenstehen. Die Zertifizierungsstelle fordert von dem Cloud-Anbieter, die Ursachen zu analysieren und die spezifischen, durchgeführten oder geplanten Korrekturen und Korrekturmaßnahmen zu beschreiben, um die erkannten Nichtkonformitäten in einem festgelegten Zeitraum zu beseitigen.

Der Cloud-Anbieter plant die erforderlichen Maßnahmen und die Zeitlinie zur Bearbeitung auf Grundlage der von der Zertifizierungsstelle gesetzten Fristen und dem bereitgestellten Mängelbericht. Er stellt der Zertifizierungsstelle nach Abschluss der Nachbesserung alle notwendigen Dokumente zur Verfügung, um die erfolgreiche Nachbesserung belegen zu können.

Die Zertifizierungsstelle kann abhängig von dem Umfang und der Schwere der erforderlichen Nachbesserung eine Nachprüfung mit angemessener Frist zur Durchführung ansetzen.

Nachforderungen

Im Einzelfall kann es zutreffen, dass die Zertifizierungsstelle Dokumente und Nachweise anfordert, deren Einsicht zur abschließenden Beurteilung über eine Zertifikatsvergabe notwendig sind die bis zu diesem Zeitpunkt der Zertifizierungsstelle nicht vorlagen. Die Nachforderungen und deren Erfüllung wird im dem Prüfungsbericht festgehalten. Die Nachforderungen sind in Art und Umfang nicht begrenzt.

3.1.4 Kriterien für die Zertifikatsvergabe

Nach Abschluss der Audittätigkeiten werden vom Auditteamleiter alle relevanten Informationen zur Prüfung bei der Zertifizierungsstelle eingereicht. Dies umfasst im Wesentlichen:

- die Bestätigung, dass die in Stage 1-Dokumentenprüfung geforderten Informationen vorliegen,
- den Auditbericht des Auditteamleiters für die Stage 2-Prüfung, inkl. der Darstellung der identifizierten Mängel und Feststellungen zur Nichtkonformität,
- durch den Kunden geplante oder eingeleitete oder abgeschlossene Korrekturmaßnahmen,
- eine Empfehlung, ob das Zertifikat gewährt werden soll sowie eventuell damit verbundene Bedingungen
- und Auflagen.

Bei Abweichungen verbunden mit einer positiven Empfehlung ist für jeden Einzelfall zu begründen, warum das Zertifikat trotz der festgestellten Mängel erteilt werden sollte.

3.2 Überwachungstätigkeiten

Nach Erteilung des Zertifikats, das eine Gültigkeit von längstens drei Jahren hat, müssen geeignete Maßnahmen seitens der Zertifizierungsstelle geplant werden, um die kontinuierliche Konformität des Zertifikatinhabers für alle für den maßgeblichen Bereich relevanten Tätigkeiten hinreichend sicherstellen zu können.

Die Datenverarbeitungsvorgänge bedürfen während der Gültigkeitsdauer der Zertifizierung der Überwachung in Form eines mindestens jährlich durchzuführenden Überwachungsaudits. Es ist frühestens nach Ablauf des sechsten und spätestens bis zum Ablauf des zwölften Monats ab Zertifizierungserteilung oder der entsprechenden Zeitpunkte der Folgejahre durchzuführen.

Neben jährlichen Überwachungsaudits werden die folgenden Tätigkeiten durchgeführt:

- Befragung des Zertifikatinhabers bezüglich wesentlicher Aspekte der Zertifizierung,
- Bewertung der erhaltenen Informationen,
- Befragung zur Verwendung der Zertifizierungsnachweise durch den Zertifikatinhaber und Bewertung des Umgangs mit zertifizierungsbezogenen Werbemaßnahmen sowie
- Sichtung von unterjährig vom Zertifikatinhaber bereitgestellten Dokumenten und Aufzeichnungen.

Darüber hinaus können anlassbezogene Überwachungen bei Auffälligkeiten erfolgen, die eine Nichtkonformität der Zertifizierungskriterien z. B. bei vorliegenden Beschwerden befürchten lassen. Sollten anlassbezogene Überwachungstätigkeiten notwendig sein, wird die Zertifizierungsstelle den Cloud-Anbieter kontaktieren.

Der Cloud-Anbieter ist verpflichtet, die Zertifizierungsstelle unverzüglich und mit ausreichender Vorlaufzeit detailliert zu informieren, wenn ihm bekannt wird, dass die Voraussetzungen für die Erteilung der Zertifizierung nicht vorlagen oder nicht mehr vorliegen (z. B. planmäßige oder außerplanmäßige Erlöschung von im Rahmen der GDPR CC-Zertifizierung anerkannter Zertifikate).

3.2.1 Überwachungsaudit

Für die regelmäßige oder anlassbezogene Überwachung (bei Auffälligkeiten) folgt grundsätzlich analog zu dem beschriebenen Verfahren zur Ermittlung der Konformität mittels Stage 1-Dokumentenprüfung und Stage 2 – Prüfung. 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 Überwachungsprüfung wird so gewählt, dass mindestens die seit der letzten Prüfung erfolgten Änderungen der Datenverarbeitungsvorgänge durch Ermittlungsmethoden geprüft werden.

Durch geeignete Stichproben unter Anwendung der Ermittlungsmethoden wird festgestellt, ob die Datenverarbeitungsvorgänge insgesamt die Zertifizierungskriterien weiterhin erfüllen.

- Im Rahmen der Überwachung prüft die Zertifizierungsstelle insbesondere, ob anerkannte Zertifikate weiterhin gültig sind.
    - Bei der Re-Zertifizierung der anerkannten Zertifizierung wird die Ablauffrist der Zertifizierung auf die Laufzeit des anerkannten Zertifikats verlängert, jedoch maximal auf die Standardlaufzeit der Zertifizierung von 3 Jahren oder bei weiteren anerkannten Fremdzertifikaten auf die kürzeste Laufzeit.
    - Strebt der Cloud-Anbieter im Fall eines erloschenen Zertifikats keine Re-Zertifizierung des anerkannten Zertifikats an, muss mindestens der ursprünglich abgedeckte Bereich erneut geprüft werden, um die Gültigkeit der Zertifizierung aufrecht zu erhalten.

Im Rahmen der Überwachungsprüfung wird nicht notwendigerweise eine vollständige Prüfung aller Zertifizierungskriterien durchgeführt. Es werden jedoch mindestens die folgenden Aspekte beurteilt:

- geplante und durchgeführte Maßnahmen bei festgestellter Nichtkonformität in Teilbereichen,
- Änderungen des Managementsystems, speziell des Scopes,
- vom Kunden durchgeführte interne Audits,
- Maßnahmen im Rahmen eines kontinuierlichen Verbesserungsprozesses sowie Wirksamkeit des Managementsystems sowie,
- Änderungsmanagement.

Die Ergebnisse des Überwachungsaudits werden durch den Auditteamleiter in einem Bericht zusammengefasst. Die Zertifizierungsstelle bewertet und entscheidet basierend auf dem Bericht hinsichtlich der Aufrechterhaltung, oder im Falle der Feststellung von Nichtkonformitäten hinsichtlich der Einschränkung, Aussetzung oder dem Widerruf der Zertifizierung.

Die Zwischenprüfung ist mit der Entscheidung der Zertifizierungsstelle abgeschlossen.

3.3 Re-Zertifizierung

Mit Ablauf des dritten Jahres nach Erteilung des Zertifikats verliert dieses seine Gültigkeit. Eine Verlängerung im Sinne von zusätzlichen Überwachungsaudits ist nicht möglich. Stattdessen existiert die Möglichkeit, ein Re-Zertifizierungsaudit durchzuführen. Ein Re-Zertifizierungsaudit muss geplant und durchgeführt werden, um die anhaltende Erfüllung aller Anforderungen der Zertifizierunggrundlagen zu beurteilen. Zweck des Re-Zertifizierungsaudits ist es, die kontinuierliche Konformität und Wirksamkeit des Zertifizierungsgegenstandes hinsichtlich der Einhaltung der Zertifizierungskriterien zu bestätigen.

Um einen nahtlosen Übergang zwischen den beiden Zertifikaten zu erreichen, muss eine Beantragung zur Re-Zertifizierung rechtzeitig erfolgen. Eine Re-Zertifizierung umfasst die initiale Ermittlung der Konformität mittels Stage 1-Dokumentenprüfung und Stage 2-Prüfung sowie zwei darauffolgende Überwachungsaudits über die Standardlaufzeit der Zertifizierung von 3 Jahren. Die Re-Zertifizierungsprüfung muss vor Ablauf der vorangegangenen Zertifizierung abgeschlossen werden, um eine lückenlose Zertifizierung zu erreichen und sollte mindestens 6 Monate vor Ablauf des dreijährigen Zertifizierungszyklus besprochen bzw. vereinbart werden.

Wenn während eines Re-Zertifizierungsaudits Fälle von Nichtkonformitäten oder mangelnde Nachweise für die Konformität identifiziert werden, muss die Zertifizierungsstelle Fristen für umzusetzende Korrekturen und Korrekturmaßnahmen noch vor Ablauf der noch gültigen Zertifizierung bestimmen.

Die Entscheidung über die Re-Zertifizierung liegt bei der Zertifizierungsstelle. Hierzu werden neben den Ergebnissen des Re-Zertifizierungsaudits auch die Ergebnisse von internen Audits sowie aus der Bewertung des Managementsystems über den Zeitraum der Zertifizierung sowie die ggf. von den Nutzern der Zertifizierung erhaltenen Beschwerden berücksichtigt.

3.4 Einschränkung, Aussetzung, und Widerruf von Zertifizierungen

Wurden im Rahmen der Bewertung Nichtkonformitäten festgestellt, so entscheidet die Zertifizierungsstelle über die Einschränkung, Aussetzung oder den Widerruf der Zertifizierung.

Eine Aussetzung, Zurückziehung oder Einschränkung der Zertifizierung kann darüber hinaus erfolgen, wenn Cloud-Anbieter die Aussetzung, Zurückziehung oder Einschränkung der Zertifizierung beantragt.

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.

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. Werbung mit der ursprünglichen Zertifizierung ist nicht mehr gestattet.

Aussetzung der Zertifizierung

Eine Aussetzung bezeichnet ein vorübergehendes Außerkraftsetzen der Konformitätsaussage für den gesamten festgelegten Geltungsbereich der Bestätigung oder für Teile davon (s. ISO/IEC 17000:2004 Tz. 6.2). Die Aussetzung wird sofort wirksam.

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. Werbung mit der ursprünglichen Zertifizierung ist nicht mehr gestattet.

Widerruf der Zertifizierung

Der Widerruf bezeichnet das Zurückziehen der Zertifizierung. Der Widerruf wird drei Wochen nach Zustellung der Entscheidung über den Widerruf wirksam.

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. 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.
e) wenn der Programminhaber 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. Werbung mit der ursprünglichen Zertifizierung ist nicht mehr gestattet.

3.5 Besondere Pflichten des Zertifikatsinhabers

Der Zertifikatsinhaber ist verpflichtet, die hier bekanntgemachten Termine eigenständig einzuhalten und die Zertifizierungsstelle bei wesentlichen Änderungen des Zertifizierungsgegenstandes bzw. der darin zertifizierten cloudbasierten personenbezogenen Datenverarbeitungsvorgänge, die Auswirkung auf die Zertifizierung haben können, unverzüglich zu informieren.