European Cloud Service
Data Protection Certification

# Modularitätskonzept

**- Fassung 0.99 -**

Stand 13.01.2020

**Weitere AUDITOR-Dokumente:**

- Zertifizierungsgegenstand (Kurz- und Langfassung)
- Kriterienkatalog (https://doi.org/10.5445/IR/1000105506)
- Schutzklassenkonzept
- DIN SPEC 27557

Online verfügbar: www.auditor-cert.de

**Empfohlene Zitation:**

Sunyaev, A., Roßnagel, A., Teigeler, H., Lins, S. & Maier, N. (2019). AUDITOR-Modularitätskonzept – Fassung 0.99. Karlsruhe, Germany.

Beitrag zum Forschungsprojekt „European Cloud Service Data Protection Certification (AUDITOR)“, das aufgrund eines Beschlusses des Deutschen Bundestages vom Bundesministerium für Wirtschaft und Energie gefördert wird (FKZ 01MT17003A).

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

## Autoren

Ali Sunyaev[a], Alexander Roßnagel[b], Heiner Teigeler[a], Sebastian Lins[a], Natalie Maier[b]

[a] Forschungsgruppe Critical Information Infrastructures am Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) des Karlsruher Instituts für Technologie

[b] Projektgruppe verfassungsverträglichen Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel

Karlsruher Institut für Technologie

CRITICAL INFORMATION INFRASTRUCTURES RESEARCHGROUP

UNIKASSEL VERSITÄT

provet

# Inhaltsverzeichnis

# Abkürzungsverzeichnis

| | |
|---|---|
| Abs. | Absatz |
| Art. | Artikel |
| DSGVO | EU-Datenschutz-Grundverordnung |
| DSK | Datenschutzkonferenz |
| EDPB | European Data Protection Board |
| IaaS | Infrastructure as a Service |
| PaaS | Platform as a Service |
| SaaS | Software as a Service |

**Hinweis zur geschlechtsneutralen Formulierung:**

Alle personenbezogenen Bezeichnungen in diesem Dokument sind geschlechtsneutral zu verstehen. Zum Zweck der besseren Lesbarkeit wird daher auf die geschlechtsspezifische Schreibweise verzichtet, sodass die grammatikalisch maskuline Form kontextbezogen jeweils als Neutrum zu lesen ist (z.B. ist bei der Bezeichnung *Datenschutzbeauftragter* die Funktionsbezeichnung als Neutrum zu lesen und meint nicht einen ausschließlich maskulinen Personenbezug).

# A. Das AUDITOR-Modularisierungskonzept

## 1. Einleitung

Ein zentrales Element des AUDITOR-Zertifizierungsverfahrens bildet das AUDITOR-Modularisierungskonzept, das die horizontale und vertikale Modularisierung von Datenverarbeitungsvorgängen beschreibt. Durch das AUDITOR-Modularisierungskonzept wird die Flexibilität bei der Zertifizierung erhöht. So ist es beispielsweise möglich, dass ein Cloud-Dienst vollumfänglich oder lediglich ein einzelner Datenverarbeitungsvorgang des Cloud-Dienstes zertifiziert wird. Darüber hinaus dient das Modularitätskonzept als Grundlage für die Anerkennung von gleichwertigen Zertifizierungen im Rahmen einer AUDITOR-Zertifizierung oder auch für die Berücksichtigung anderer Zertifizierungen, die nicht durch eine akkreditierte Zertifizierungsstelle ausgestellt wurden.

## 2. Zertifizierungsgegenstand AUDITOR

Den Zertifizierungsgegenstand des AUDITOR-Verfahrens bilden Verarbeitungsvorgänge von personenbezogenen Daten im Kontext von Cloud-Diensten. Eine Datenverarbeitung ist nach Art. 4 Nr. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche 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.

Den Zertifizierungsgegenstand bilden Datenverarbeitungsvorgänge, die in Produkten oder Diensten oder mit Hilfe von (auch mehreren) Produkten und Diensten erbracht werden. Schwerpunktmäßig werden im AUDITOR-Verfahren die Datenverarbeitungsvorgänge betrachtet, die der Cloud-Anbieter als Auftragsverarbeiter im Rahmen der Auftragsverarbeitung gemäß Art. 28 DSGVO durchführt. Es werden aber auch Datenverarbeitungsvorgänge betrachtet, die der Cloud-Anbieter als Verantwortlicher vornimmt, um den Vertrag mit dem Cloud-Nutzer über die Bereitstellung des Cloud-Dienstes schließen und diesen durchführen zu können und damit er rechtliche Pflichten erfüllen kann.

Bei der Bestimmung des Zertifizierungsgegenstands sind drei Komponenten wichtig, die Cloud-Anbieter als Adressaten des AUDITOR-Zertifizierungsverfahrens beachten müssen: 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. Somit besteht ein Datenverarbeitungsvorgang in der Regel sowohl aus technischen und automatisierten als auch aus nicht-technischen organisatorischen Komponenten, die zu Datenschutzkonzepten und -managementsystemen zusammengefasst sind. Der gesamte Datenverarbeitungsvorgang 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. Weiterführende Informationen zum Zertifizierungsgegenstand von AUDITOR sind dem Begleitdokument *„AUDITOR-Zertifizierungsgegenstand“* zu entnehmen, das eine detaillierte Herleitung des Gegenstands aus juristischer und technischer Sicht enthält.

# B. Horizontal und vertikal modulare Zertifizierung

Die modulare Zertifizierung spiegelt den Umstand wider, dass Datenverarbeitungsvorgänge häufig modular aufgebaut sind. So kann ein Cloud-Anbieter, der mehrere Cloud-Dienste anbietet, die Zertifizierung dieser anhand der Zusammenhänge untereinander kombinieren bzw. vereinfachen. Die Modularisierung beschreibt einen Vorgang, bei dem ein Cloud-Dienst und die entsprechenden Datenverarbeitungsvorgänge in einzelne Module aufgeteilt werden. So ist es möglich, dass ein Cloud-Dienst vollumfänglich zertifiziert wird, indem alle relevanten Datenverarbeitungsvorgänge gemeinsam zertifiziert werden. Dabei entspricht der Cloud-Dienst dann einem Modul. Darüber hinaus ist es auch möglich, lediglich einen einzelnen Datenverarbeitungsvorgang des Cloud-Dienstes zu zertifizieren. Dabei ist der Datenverarbeitungsvorgang dann als einzelnes Modul zu verstehen. Bereits zertifizierte Module können dann in zukünftigen Zertifizierungsverfahren anerkannt oder berücksichtigt werden (siehe Kapitel C), sodass der Aufwand und die Kosten für zukünftige Zertifizierungen verringert werden. Trotz der Modularisierung muss sichergestellt sein, dass die modularen Datenverarbeitungsvorgänge eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen und keine kritischen Verarbeitungsvorgänge ausgeklammert werden.

Die Modularisierung der Zertifizierung kann sowohl auf horizontaler als auch auf vertikaler Ebene erfolgen. In Abbildung 1 wird diese Unterscheidung vereinfacht dargestellt und in den nachfolgenden Unterkapiteln an den dort abgebildeten Beispielen erläutert. In der Abbildung bilden die drei grundlegenden Servicemodelle des Cloud-Computings, also Software as a Service (SaaS), Platform as a Service (PaaS) und Infrastructure as a Service (IaaS), die sogenannten Dienst-Ebenen (*‚Cloud-Stack'*).

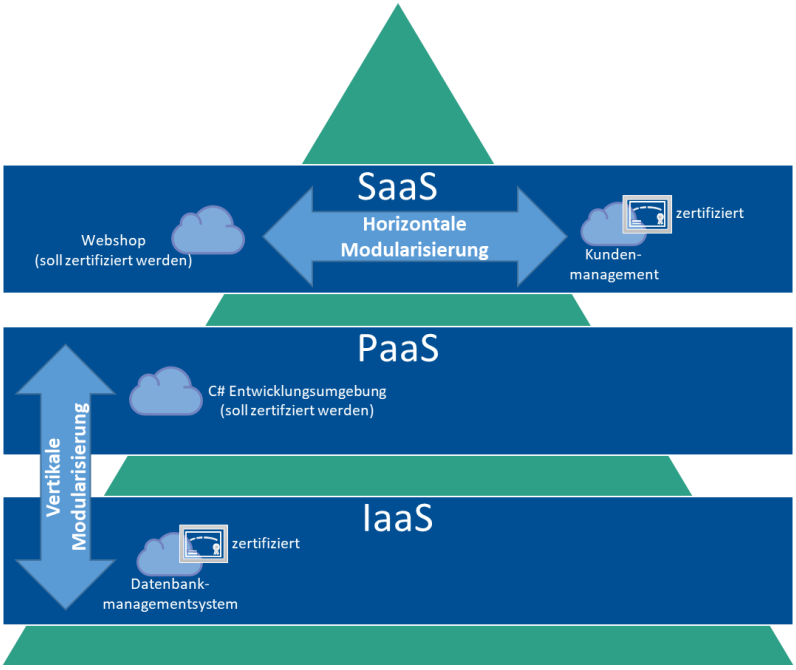


Abbildung 1. Horizontale und vertikale Modularisierung Beispiele

## 1. Horizontale Modularisierung von Datenverarbeitungsvorgängen

Die horizontale Modularisierung beschreibt die Aufteilung von Datenverarbeitungsvorgängen oder Cloud-Diensten innerhalb einer Dienst-Schicht des Cloud-Stacks. Wenn beispielsweise das Modul Kundenmanagement (d.h. alle dort relevanten Datenverarbeitungsvorgänge) bereits im Rahmen einer Zertifizierung geprüft und zertifiziert wurden, kann dieses Modul für andere angebundene Cloud-Dienste genutzt werden. So kann bei einer Zertifizierung eines cloud-basierten Webshops (als eigenständiges Modul) das bestehende Zertifikat des Kundenmanagements anerkannt oder berücksichtigt werden. Der Cloud-Anbieter profitiert von der horizontalen Modularisierung, wenn die von ihm angebotenen Cloud-Dienste auf einer Ebene (wie bspw. auf der SaaS-Ebene) Überschneidungen haben oder identische Datenverarbeitungsvorgänge nutzen.

## 2. Vertikale Modularisierung von Datenverarbeitungsvorgängen

Eine modulare Struktur lässt sich auch hinsichtlich der Zusammensetzung über die verschiedenen Ebenen des Cloud-Stacks hinweg feststellen. Die vertikale Modularisierung beschreibt die Aufteilung von Datenverarbeitungsvorgängen oder Cloud-Diensten übergreifend von verschiedenen Dienst-Schichten des Cloud-Stacks. Die vertikale Modularisierung bedeutet, dass bereits zertifizierte Datenverarbeitungsvorgänge anerkannt oder berücksichtigt werden können, wenn ein zu zertifizierender Cloud-Dienst auf anderer Ebene diese nutzt. Dies ist ähnlich wie bei der horizontalen Modularisierung nur möglich, wenn zwei Cloud-Dienste miteinander agieren oder verbunden sind. Der Cloud-Anbieter profitiert davon, dass die von ihm angebotenen Cloud-Dienste oftmals Datenverarbeitungsvorgänge in unteren Ebenen des Cloud-Stacks nutzen, beispielsweise identische Systeme, Hardware oder Gebäude. Wie in der Abbildung 1 dargestellt, kann diese vertikale Modularisierung beispielsweise zwischen den Ebenen PaaS und IaaS erfolgen. Wurde das Modul Datenbankmanagementsystem des IaaS bereits zertifiziert, so kann dies bei einer Zertifizierung eines anderen PaaS-Cloud-Dienstes anerkannt werden. In dem oben illustrierten Beispiel würde der zu zertifizierende Cloud-Dienst, eine C# Entwicklungsumgebung, das bereits zertifizierte Datenbankmanagementsystem nutzen und somit von dem bereits vorhandenen Zertifikat profitieren.

# C. Anerkennung und Berücksichtigung von bestehenden Zertifikaten

Besitzt ein Cloud-Anbieter bereits Zertifikate, so können diese wie folgt anerkannt oder berücksichtigt werden:

- **Fall 1: Anerkennung.** Es besteht die Möglichkeit Zertifikate anzuerkennen, die durch eine akkreditierte Zertifizierungsstelle vergeben wurden (s. DSK Tz. 7.4). Hierzu zählen insbesondere Datenschutzzertifizierungen nach Art. 42 DSGVO.
- **Fall 2: Berücksichtigung.** Ausgestellte Zertifikate von Zertifizierungsstellen, die nicht akkreditiert sind, können lediglich im Rahmen der Prüfung berücksichtigt werden. Eine Anerkennung ist ausgeschlossen.

Wenn der Cloud-Anbieter eine Berücksichtigung oder Anerkennung bestehender Zertifizierungen für Bestandteile seines Datenverarbeitungsvorgangs anstrebt, prüft die Zertifizierungsstelle unverzüglich, ob und inwieweit eine Berücksichtigung oder Anerkennung anhand der im Konformitätsbewertungsprogramm definierten Richtlinien erfolgen kann. Grundsätzlich ist stets die Gleichwertigkeit des Zertifikats zu prüfen (siehe C.3). Im Folgenden werden die Voraussetzungen und notwendigen Prüfungen für die zwei beschriebenen Fälle aufgeschlüsselt. In allen beschriebenen Fälle ändert sich die Gültigkeitsdauer der anerkannten oder berücksichtigten Zertifizierungen nicht.

### 1. Fall 1: Anerkennung von Zertifikaten von akkreditierten Zertifizierungsstellen

**Voraussetzungen**

- Das Zertifikat
  (1) bestätigt die erfolgreiche **Datenschutzzertifizierung nach Art. 42 DSGVO** oder
  (2) ein anderes, erfolgreich abgeschlossenes Zertifizierungsverfahren einer akkreditierten Zertifizierungsstelle.
- Die **Zertifizierungsstelle**, die gemäß der Prüfkriterien geprüft und das Zertifikat ausgestellt hat, muss
  (1) nach ISO/IEC 17065 i.V.m. den ergänzenden Anforderungen der DSK zur Akkreditierung nach Art. 43 Abs. 3 DSGVO akkreditiert sein, oder
  (2) basierend auf den Anforderungen des ausgestellten Zertifikats akkreditiert sein (bspw. ISO/IEC 17021, 17025, 17065).
- Die zu anerkennenden Kriterien müssen das im AUDITOR-Zertifizierungsverfahren angestrebte Schutzniveau erfüllen (insb. die Schutzklasse und die Wiederherstellbarkeitsklasse).
- Der zu zertifizierende Datenverarbeitungsvorgang muss Bestandteil des Geltungsbereichs der bestehenden Zertifizierung sein.
- Zertifizierungen müssen bei der Antragsstellung abgeschlossen sein.

**Beispiele**

(1) European Privacy Seal (EuroPriSe) (sobald genehmigt gemäß Art. 42 DSGVO)
(1) ePrivacyseal EU (sobald genehmigt gemäß Art. 42 DSGVO)
(2) ISO/IEC 27001
(2) ISO/IEC 9001

**Implikationen bei Anerkennung**

- Werden bestehende Zertifizierungen des Cloud-Anbieters anerkannt, so ist eine Prüfung der abgedeckten Kriterien im Rahmen der AUDITOR-Zertifizierung nicht erforderlich.
- Die Gültigkeitsdauer der AUDITOR-Zertifizierung auf das Ablaufdatum der kürzest laufenden und anerkannten Zertifizierung reduziert (s. DSK Tz. 7.4). Bei der Rezertifizierung der anerkannten Zertifizierung wird die Ablauffrist der AUDITOR-Zertifizierung auf die Laufzeit des anerkannten Zertifikats verlängert, jedoch maximal auf die Standardlaufzeit der AUDITOR-Zertifizierung von 3 Jahren oder bei weiteren berücksichtigten Fremdzertifikaten auf die kürzeste Laufzeit. Wird keine Rezertifizierung des anerkannten Zertifikats durchgeführt, muss mindestens der ursprünglich abgedeckte Bereich erneut geprüft werden, um die Gültigkeit der AUDITOR-Zertifizierung aufrecht zu erhalten.

**Aufgaben der Cloud-Anbieter**

- Zertifizierungsstelle darüber in Kenntnis setzen, dass die Anerkennung bestehender Zertifizierungen angestrebt wird (s. DSK Tz 7.4).
- Vorlage der verfügbaren Dokumente der Zertifizierung bei der Zertifizierungsstelle. Hierzu zählen u.a.:
    (1) Zertifizierungsurkunde oder ähnliche Bescheinigung,
    (2) Vollständiges Zertifizierungsgutachten (Ermittlungsbericht bzw. Auditreport). Insofern dies nicht möglich ist (bspw. keine Weitergabe der Dokumente aus rechtlichen oder vertraglichen Gründen möglich), muss der Cloud-Anbieter ausreichende Informationen bereitstellen, die eine Bewertung der Zertifizierung ermöglichen (s. DSK Tz 7.4, EDPB Annex 1 Tz 7.4). Hierzu zählt insbesondere eine eindeutige und ausführliche Beschreibung des Zertifizierungsumfangs,
    (3) Kriterienkatalog und
    (4) Beschreibung des Zertifizierungsgegenstands, inkl. Darstellung der Schnittstellen.

- Zertifizierungsstelle mit ausreichend Vorlaufzeit darüber in Kenntnis setzen, wenn ein anerkanntes Zertifikat die Gültigkeit planmäßig verliert (d.h. bei regulärem Ablauf des Gültigkeitszeitraums) oder außerplanmäßig verliert (d.h. vor dem von der Zertifizierungsstelle vermerkten Ende des regulären Gültigkeitszeitraum), und welche Maßnahmen der Cloud-Anbieter vornehmen will (bspw. Rezertifizierung). Strebt der Cloud-Anbieter keine Rezertifizierung des anerkannten Zertifikats an, muss mindestens der ursprünglich abgedeckte Bereich erneut geprüft werden, um die Gültigkeit der AUDITOR-Zertifizierung aufrecht zu erhalten.

**Aufgaben der Zertifizierungsstelle**

- Bestehende Zertifizierung kritisch bewerten und dokumentieren, in welchem Umfang diese bei der Ermittlung anerkannt werden kann. Notwendig für eine Bewertung der Anerkennung ist das Vorliegen eines vollständigen Zertifizierungsgutachtens (bspw. Auditreport) oder von Informationen, die eine Bewertung der Zertifizierungstätigkeit und -ergebnisse ermöglichen (s. DSK Tz. 7.4, EDPB Annex 1 Tz. 7.4). Eine Zertifizierungsurkunde oder ähnliche Bescheinigungen über eine Zertifizierung sind hierbei nicht ausreichend.
- Ergeben sich im Rahmen der AUDITOR-Zertifizierung Unregelmäßigkeiten in Hinblick auf anerkannte Zertifizierungen (bspw. Vermutung von Abweichungen), so ist die Ermittlung im Rahmen des laufenden Zertifizierungsverfahrens zu erweitern und ggf. auf den gesamten, bereits zertifizierten Gegenstand auszudehnen.
- Die Anerkennung, insbesondere hinsichtlich der Schutzklasse und der Wiederherstellbarkeitsklasse muss begründet und ausreichend dokumentiert werden. Insbesondere muss dokumentiert werden, wie und in welchem Umfang die Anerkennung stattfindet und welche Auswirkungen diese konkret auf den verbleibenden Ermittlungsumfang und die Ermittlungsmethoden hat (s. DSK Tz. 7.4).
- Die Befristung der anerkannten Zertifikate ist zu notieren und für die Entscheidung vorzuhalten. Werden bestehende Zertifizierungen des Cloud-Anbieters anerkannt, so wird die Gültigkeitsdauer der AUDITOR-Zertifizierung auf das Ablaufdatum der kürzest laufenden und anerkannten Zertifizierung reduziert (s. DSK Tz. 7.4). Die Zertifizierungsstelle notiert die Gültigkeitsdauer der anerkannten Zertifikate. Die fortlaufende Gültigkeit der anerkannten Zertifikate wird mindestens

im Rahmen der Überwachungsaudits von der Zertifizierungsstelle überprüft. Teilt der Cloud-Anbieter der Zertifizierungsstelle mit, dass eine Rezertifizierung der anerkannten Zertifizierung durchgeführt wurde, so wird die Ablauffrist der AUDITOR-Zertifizierung auf die Laufzeit des anerkannten Zertifikats verlängert, jedoch maximal auf die Standardlaufzeit der AUDITOR-Zertifizierung von 3 Jahren oder bei weiteren berücksichtigten Fremdzertifikaten auf die kürzeste Laufzeit. Wird keine Rezertifizierung durchgeführt, muss zur Aufrechterhaltung der AUDITOR-Zertifizierung mindestens der ursprünglich abgedeckte Bereich erneut von der Zertifizierungsstelle geprüft werden.

## 2. Fall 2: Berücksichtigung von Zertifikaten von Zertifizierungsstellen ohne Akkreditierung

**Voraussetzungen**

- Vorliegen eines vollständigen Zertifizierungsgutachtens (bspw. Auditreport). Falls dies aus rechtlichen Gründen nicht möglich ist, können Informationen bereitgestellt werden, die eine Bewertung der Zertifizierungstätigkeit und -ergebnisse ermöglichen (s. DSK Tz. 7.4, EDPB Annex 1 Tz. 7.4).
- Die Kriterien müssen das im AUDITOR-Zertifizierungsverfahren angestrebte Schutzniveau erfüllen (insb. die Schutzklasse und die Wiederherstellbarkeitsklasse).
- Der zu zertifizierende Datenverarbeitungsvorgang muss Bestandteil des Geltungsbereichs der bestehenden Zertifizierung sein.
- Zertifizierungen müssen bei der Antragsstellung abgeschlossen sein.

**Beispiele**

- Trusted Cloud Service (TÜV Trust IT)
- EuroCloud Star Audit (ECSA)
- BSI C5

**Implikationen bei Berücksichtigung**

- Werden bestehende Zertifizierungen eines Cloud-Anbieters berücksichtigt, so können diese im Rahmen des AUDITOR-Zertifizierungsverfahrens als Nachweis herangezogen werden.
- Die Einhaltung der berücksichtigten Zertifizierungskriterien muss dennoch durch die Zertifizierungsstelle durch geeignete Ermittlungsmethoden vollumfänglich überprüft werden.

**Aufgaben der Cloud-Anbieter**

- Zertifizierungsstelle darüber in Kenntnis setzen, dass die Berücksichtigung bestehender Zertifizierungen angestrebt wird (s. DSK Tz 7.4).
- Vorlage sämtlicher Dokumente der Zertifizierung bei der Zertifizierungsstelle. Hierzu zählen:
  (1) Zertifizierungsurkunde oder ähnliche Bescheinigung,
  (2) Vollständiges Zertifizierungsgutachten (Ermittlungsbericht bzw. Auditreport). Insofern dies nicht möglich ist (bspw. keine Weitergabe der Dokumente aus rechtlichen oder vertraglichen Gründen möglich), muss der Cloud-Anbieter ausreichende Informationen bereitstellen, die eine Bewertung der Zertifizierung ermöglichen (s. DSK Tz 7.4, EDPB Annex 1 Tz 7.4). Hierzu zählt insbesondere eine klare und ausführliche Beschreibung des Zertifizierungsumfangs,
  (3) Kriterienkatalog und
  (4) Beschreibung des Zertifizierungsgegenstands, Darstellung der Schnittstellen.

**Aufgaben der Zertifizierungsstelle**

- Bestehende Zertifizierung kritisch bewerten und dokumentieren, in welchem Umfang diese bei der Ermittlung berücksichtigt werden kann. Notwendig für eine Bewertung der Berücksichtigung ist das Vorliegen eines vollständigen Zertifizierungsgutachtens (bspw. Auditreport) oder von Informationen, die eine Bewertung der Zertifizierungstätigkeit und -ergebnisse ermöglichen (s. DSK Tz. 7.4, EDPB Annex 1 Tz. 7.4). Eine Zertifizierungsurkunde oder ähnliche Bescheinigungen über eine Zertifizierung sind hierbei nicht ausreichend.
- Die Einhaltung der Zertifizierungskriterien muss durch die Zertifizierungsstelle dennoch durch geeignete Ermittlungsmethoden vollumfänglich überprüft werden. Die bestehende Zertifizie-

rung, die im Rahmen der Berücksichtigung herangezogen wird, ersetzt keine Prüfung. Die Zertifizierungsstelle kann bei der Überprüfung der Zertifizierungskriterien daher die vorliegenden Dokumente der Zertifizierung lediglich als weitere Dokumentation heranziehen.

## 3. Gleichwertigkeit bestehender Zertifikate

Voraussetzung einer Anerkennung oder Berücksichtigung von Zertifikaten anderer Zertifizierungsstellen ist, dass die Prüfung durch die Zertifizierungsstelle, auf deren Zertifikat verwiesen wird, einer eigenen Prüfung gleichwertig ist.

Es muss sowohl die materielle als auch die verfahrensmäßige Gleichwertigkeit der Ergebnisse von Konformitätsbewertungen sichergestellt werden, um ein gleiches Niveau des Vertrauens in die Konformität sicherzustellen (s. DSK Tz. 7.4, ISO/IEC 17000:2004 Tz. 7.4). Eine materielle Gleichwertigkeit liegt dann vor, wenn das bestehende Zertifikat auf Zertifizierungskriterien beruht, die denen des AUDITOR-Kriterienkatalogs im Hinblick auf das Schutzniveau gleichwertig sind oder diese übertreffen. Die Zertifizierungsstelle stellt insbesondere fest, mit welcher Schutzklasse und welcher Wiederherstellbarkeitsklasse das Zertifikat anerkannt oder berücksichtigt wird. Eine verfahrensmäßige Gleichwertigkeit liegt dann 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 Datenschutzzertifizierungen nach Art. 43 DSGVO.

Bei einer Kombination von Zertifikaten unterschiedlicher Zertifizierungsstellen ergeben sich Fragen hinsichtlich der Verantwortlichkeit und Haftung, die weiterer Erörterung bedürfen. Dies ändert aber nichts daran, dass der Verweis auf Zertifikate anderer Zertifizierungsstellen möglich ist, soweit die dort erfolgte Prüfung einer eigenen Prüfung der Zertifizierungsstelle gleichwertig ist und den Anforderungen gemäß Art. 43 Abs. 3 DSGVO und den Anforderungen der DSK entsprechen. Wesentliche Grundlage eines Systems modularer Zertifizierung ist damit, dass hinsichtlich der Prüfanforderungen und der Gleichwertigkeit von Prüfungen Transparenz und Rechtssicherheit bestehen.

# D. Referenzen

| | |
|---|---|
| DSK | Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO in Verbindung mit DIN EN ISO/IEC 17065. Version 1.0 (28.08.2018) |
| EDPB Annex 1 | EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) - Annex 1. Stand 04.12.2018 |