European Cloud Service
Data Protection Certification

AUDITOR-Zertifizierungsgegenstand

Kurzfassung

- Entwurfsfassung 0.4 -

Stand 16.3.2019

Weitere AUDITOR-Dokumente:

- Zertifizierungsgegenstand (Langfassung)
- Kriterienkatalog (https://doi.org/10.5445/IR/1000092273)
- Modularitätskonzept
- Schutzklassenkonzept
- DIN SPEC 27557

Online verfügbar: www.auditor-cert.de

Empfohlene Zitation:

Roßnagel, A., Sunyaev, A., Lins, S., Maier, N., & Teigeler, H. (2019). AUDITOR-Zertifizierungsgegenstand: Kurzfassung – Entwurfsfassung 0.4. Online verfügbar: www.auditor-cert.de

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

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

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

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

UNIKASSEL VERSITÄT

provet

Karlsruher Institut für Technologie

CRITICAL INFORMATION INFRASTRUCTURES RESEARCHGROUP

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
DSGVO	EU-Datenschutz-Grundverordnung (Geltung ab 25.5.18)
ggf.	gegebenenfalls
i.V.m.	in Verbindung mit
lit.	litera
s.u.	siehe unten
z.B.	zum Beispiel

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).

Hinweis zur Angabe von Quellen

Im Rahmen dieser Kurzfassung wird auf die Angabe von Quellen verzichtet. Für detaillierte Quellenangaben sei auf die Langfassung des Dokumentes verwiesen.

Der Zertifizierungsgegenstand des AUDITOR-Verfahrens

Das AUDITOR-Verfahren ist ein Prüfstandard für die Datenschutz-Zertifizierung von Cloud-Diensten gemäß den Anforderungen der EU-Datenschutz-Grundverordnung (DSGVO).

1. Datenverarbeitungsvorgänge als Zertifizierungsgegenstand

Zertifizierungsgegenstand des AUDITOR-Verfahrens sind Verarbeitungsvorgänge von personenbezogenen Daten, die in Produkten oder Diensten oder mit Hilfe von (auch mehreren) Produkten oder Diensten erbracht werden. Im AUDITOR-Verfahren werden die Datenverarbeitungsvorgänge betrachtet, die der Cloud-Anbieter als Auftragsverarbeiter im Rahmen der Auftragsverarbeitung gemäß Art. 28 DSGVO durchführt. Weiterhin werden Datenverarbeitungsvorgänge betrachtet, die der Cloud-Anbieter als Verantwortlicher vornimmt, um den Vertrag mit dem Cloud-Nutzer über die Bereitstellung des Cloud-Dienstes schließen und durchführen sowie um rechtliche Pflichten erfüllen zu können (s.u.).

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 personenbezogene Daten zu einem bestimmten Zweck verarbeiten und deren Datenschutzmaßnahmen in Datenschutzkonzepten erfasst und zu Datenschutzmanagementsystemen zusammengefasst sind. Der gesamte Datenverarbeitungsvorgang muss den Anforderungen der Datenschutz-Grundverordnung entsprechen.

Datenverarbeitungsvorgänge müssen eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen, innerhalb der die spezifischen Datenschutzrisiken des jeweiligen Cloud-Dienstes vollständig erfasst werden können. Dies bedeutet, dass auch Schnittstellen der zu zertifizierenden Datenverarbeitungsvorgänge zu anderen Datenverarbeitungsvorgängen des Dienstes betrachtet werden müssen, um Datenflüsse zu identifizieren, aus denen datenschutzrechtliche Risiken erwachsen können. Setzen die zu zertifizierenden Datenverarbeitungsvorgänge eines Cloud-Dienstes auf nicht-anbietereigene Plattformen oder Infrastrukturen auf oder setzt der Auftragsverarbeiter sonstige Subauftragsverarbeiter ein, so kann sich das Zertifikat nur auf diejenigen Datenverarbeitungsvorgänge beziehen, die im Verantwortungsbereich des jeweiligen Auftragsverarbeiters stehen. Der Auftragsverarbeiter muss sich jedoch davon überzeugen, dass auch diese fremden von ihm genutzten Plattformen, Infrastrukturen und Subauftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten und darf nur solche einsetzen, um seinen Dienst zu erbringen (s.u.).

Datenverarbeitung bezeichnet jeden Vorgang, der in einem Zusammenhang mit personenbezogenen Daten steht. Oftmals durchlaufen personenbezogene Daten beim Cloud Computing die nachfolgenden Vorgänge, ohne dass die Auflistung jedoch vollständig ist oder jeder Vorgang in einem zu zertifizierenden Datenverarbeitungsvorgang enthalten sein muss:

- Konzeptualisierung: Definition und Beschreibung von zu erhebenden und zu verarbeitenden personenbezogenen Daten.
- Erhebung / Erzeugung: Vorgänge zur Erhebung oder Erzeugung von relevanten Daten.
- Transfer und Weitergabe: Vorgänge, die dazu führen, dass die Daten ihren Speicher oder Verarbeitungsort erreichen, oder an Dritte weitergegeben werden.
- Speicherung: Vorgänge zur sicheren Speicherung der Daten.
- Zugriff / Verwendung: Lesender Zugriff auf Daten zur weiteren Verwendung und Verarbeitung.
- Veränderung / Aktualisierung: Schreibender Zugriff auf Daten, um die gespeicherten Werte zu verändern.
- Transformation: Zweckgerichtete Veränderung der Daten, insbesondere zu ihrem Schutz.
- Administration: Manuelle und automatische Vorgänge zur Verwaltung von Daten.
- Rückgabe: (Vollständige) Rückgabe der Daten an den Cloud-Nutzer.
- Löschung / Vernichtung: Löschung der Daten und ggf. Vernichtung der Speichermedien.

2. Betrachtete Datenverarbeitungsvorgänge im AUDITOR-Kriterienkatalog

Der AUDITOR-Kriterienkatalog beschreibt die datenschutzrechtlichen Anforderungen an die Verarbeitung von personenbezogenen Daten auf der Seite des Auftragnehmers (Cloud-Anbieter) und richtet sich an die Anbieter von Cloud-Diensten des privaten Sektors, die die Vereinbarkeit ihrer Datenverarbeitungsvorgänge mit datenschutzrechtlichen Anforderungen nachweisen möchten. Die datenschutzrechtlichen Anforderungen an den Auftraggeber (Cloud-Nutzer) werden nicht adressiert.

2.1. Die Verantwortlichkeit des Cloud-Anbieters für Datenverarbeitungsvorgänge

Cloud-Anbieter im Sinne des AUDITOR-Kriterienkatalogs ist jedes privatwirtschaftliche Unternehmen, das einen Cloud-Dienst am Markt anbietet und sich nach dem Kriterienkatalog zertifizieren lassen möchte. Cloud-Anbieter sind die Antragsteller im AUDITOR-Zertifizierungsverfahren und werden durch den AUDITOR-Kriterienkatalog in zweierlei Hinsicht adressiert:

1) ***Als Auftragsverarbeiter* von Datenverarbeitungsvorgängen.** Die Cloud-Anbieter können sowohl B2B- als auch B2C-Anbieter sein. Wichtig ist nur, dass sie hinsichtlich der Daten, die in der Cloud verarbeitet werden (**„Inhalts- oder Anwendungsdaten“**), als Auftragsverarbeiter und nicht als Verantwortliche tätig sind und die Datenschutzkonformität ihrer Datenverarbeitungsvorgänge durch ein Zertifikat bestätigen lassen möchten. Gerade im B2B-Bereich werden die Inhalts- und Anwendungsdaten häufig personenbezogene Daten von Kunden, Mitarbeitern oder anderen betroffenen Personen sein, mit denen der Cloud-Nutzer in Vertragsbeziehungen steht. Jedoch können Inhalts- und Anwendungsdaten auch personenbezogene Daten des Cloud-Nutzers sein.

2) ***Als Verantwortlicher* von Datenverarbeitungsvorgängen.** Der Cloud-Anbieter wird auch als Verantwortlicher von Datenverarbeitungsvorgängen adressiert, die erforderlich sind, um den Vertrag mit dem Cloud-Nutzer über die Bereitstellung des Cloud-Dienstes schließen und durchführen zu können. Bei diesen Datenverarbeitungsvorgängen geht es um den Schutz der personenbezogenen Daten des Cloud-Nutzers und um dessen Persönlichkeitsrecht. Der Umgang mit personenbezogenen Daten von Dritten wie etwa Kunden oder Mitarbeitern des Cloud-Nutzers findet im Rahmen der zwischen dem Cloud-Nutzer und dem Cloud-Anbieter vereinbarten Auftragsverarbeitung statt und verpflichtet den Cloud-Anbieter lediglich in seiner Rolle als Auftragsverarbeiter. Schließt der Cloud-Nutzer einen Vertrag mit dem Cloud-Anbieter über die Bereitstellung und Nutzung des Cloud-Dienstes ab, wird der Cloud-Anbieter vor allem durch handels- und steuerrechtliche Aufzeichnungs- und Aufbewahrungspflichten zur Verarbeitung personenbezogener Daten verpflichtet, sodass die Datenverarbeitung zur Erfüllung rechtlicher Pflichten ebenfalls in den Anwendungsbereich der AUDITOR-Zertifizierung fällt.

   Obwohl der Cloud-Anbieter grundsätzlich frei darin ist, den Zweck einer Verarbeitung und die hierfür passende Rechtsgrundlage aus Art. 6 Abs. 1 UAbs. 1 lit. a bis f DSGVO zu wählen und Art. 5 Abs. 1 lit. b i.V.m. Art. 6 Abs. 4 DSGVO auch keine strikte Zweckbindung, sondern nur eine Zweckvereinbarkeit kennt, werden im Rahmen der AUDITOR-Zertifizierung nur Datenverarbeitungen des Cloud-Anbieters in seiner Rolle als Verantwortlicher betrachtet, die in einem inneren Zusammenhang zum Vertrag zwischen dem Cloud-Anbieter und dem Cloud-Nutzer über die Bereitstellung und Nutzung des Cloud-Dienstes und die Durchführung der Auftragsverarbeitung stehen. Im Rahmen der AUDITOR-Zertifizierung werden daher nur Datenverarbeitungsvorgänge betrachtet, die der Cloud-Anbieter durchführt, um den Cloud-Dienst gegenüber dem Cloud-Nutzer zu erbringen, um diesem die Nutzung zu ermöglichen und um den Dienst abzurechnen.

   Um den Vertrag mit dem Cloud-Nutzer über die Nutzung des Cloud-Dienstes abzuschließen und durchzuführen, entscheidet der Cloud-Anbieter, welche personenbezogenen Daten er erhebt und verarbeitet. In der Regel werden hier Daten wie Namen, Adressen, Zahlungsdaten wie beispielsweise Bankverbindungen, Rufnummern, Benutzernamen und Passwörter fürs Einloggen in den Cloud-Dienst verarbeitet. Diese können unter dem Begriff **„Bestandsdaten“** zusammengefasst werden.

   Um dem Cloud-Nutzer die Inanspruchnahme des Cloud-Dienstes zu ermöglichen und diese abzurechnen, muss der Cloud-Anbieter weitere personenbezogene Daten wie beispielsweise

Ein- und Auslogdaten zu Nutzkonten, IP-Adressen, die genutzten Dienstmodule und den Umfang der Nutzung verarbeiten. Diese Daten können unter dem Begriff **„Nutzungsdaten“** zusammengefasst werden.

2.2. Zertifizierungsreichweite

Beim Cloud Computing kommt es regelmäßig zu einem Nebeneinander der Verantwortlichkeiten. Einerseits zwischen dem Cloud-Anbieter und dem Cloud-Nutzer und andererseits zwischen dem Cloud-Anbieter und weiteren eingesetzten Auftragnehmern (Subauftragsverarbeiter), sodass sich die Frage nach der Zertifizierungsreichweite stellt.

Verantwortlichkeit zwischen Cloud-Anbieter und Cloud-Nutzer

Allgemeine Leitlinien zur Verantwortungsabgrenzung zwischen Cloud-Anbieter und Cloud-Nutzer sind nur schwer zu bilden, da die Verantwortungsverteilung maßgeblich von den Service-Modellen und den konkreten Ausgestaltungen sowie den individuellen Auftragsverarbeitungsvereinbarungen mit den Cloud-Nutzern abhängt. Daher liegt es an dem Cloud-Nutzer und dem Cloud-Anbieter, Regelungen zur Verantwortungsverteilung zu treffen. Beispielsweise ist in der Regel der Cloud-Nutzer verantwortlich für Datensicherungen oder -archivierungen. Daher wird in den meisten Auftragsverarbeitungsvereinbarungen zwischen IaaS-Anbietern und Cloud-Nutzern eine entsprechende Regelung der Verantwortlichkeiten enthalten sein.

Die Regelungen müssen die Intentionen und Zwecksetzungen der Parteien abbilden. Im Verhältnis zwischen Cloud-Nutzer und Cloud-Anbieter ist der Cloud-Anbieter immer dann Auftragnehmer, wenn er mit den zu verarbeitenden Daten keine eigenen Zwecke verfolgt, auch wenn er die Entscheidungen über die Mittel der Datenverarbeitung trifft. Er ist nur dann Verantwortlicher, wenn er mit den Daten eigene Zwecke verfolgt. Er bleibt jedoch Auftragsverarbeiter, wenn der Cloud-Nutzer den Zweck der Verarbeitung klar definiert, dem Cloud-Anbieter jedoch die Entscheidungsbefugnis über die Wahl der technischen und organisatorischen Mittel überlässt, solange diese Mittel angemessen sind, um den Verarbeitungszweck zu erreichen und er den Cloud-Nutzer über diese informiert.

Als Faustformel kann festgehalten werden, dass der Cloud-Nutzer regelmäßig für diejenigen personenbezogenen Daten als Verantwortlicher anzusehen ist, die er oder ihm zurechenbare Personen in die Cloud übertragen. Dies betrifft die Inhalts- und Anwendungsdaten des Cloud-Nutzers. Der Cloud-Anbieter wird für diejenigen Datenverarbeitungsvorgänge verantwortlich sein, die er vornimmt, um den Cloud-Dienst zu erbringen und um dessen Nutzung und Abrechnung zu ermöglichen. In der Regel betrifft dies Bestands- und Nutzungsdaten.

Verantwortlichkeit zwischen Cloud-Anbieter und Subauftragsverarbeitern

Häufig setzen Cloud-Anbieter Subauftragsverarbeiter ein, um ihren Cloud-Dienst zu erbringen. Setzen die zu zertifizierenden Datenverarbeitungsvorgänge eines Cloud-Dienstes auf nicht-anbietereigene Plattformen oder Infrastrukturen auf oder setzt der Auftragsverarbeiter sonstige Subauftragsverarbeiter ein, so kann sich das Zertifikat nur auf diejenigen Datenverarbeitungsvorgänge beziehen, die im Verantwortungsbereich des jeweiligen Auftragsverarbeiters liegen. Der Auftragsverarbeiter muss sich jedoch als Hauptauftragsverarbeiter davon überzeugen, dass auch diese fremden von ihm genutzten Plattformen, Infrastrukturen und Subauftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten und darf nur solche für die Erbringung seines Dienstes einsetzen. Der Cloud-Anbieter muss dafür Sorge tragen, dass von allen Subauftragsverarbeitern die einschlägigen Vorschriften der Datenschutz-Grundverordnung eingehalten werden. Ein Cloud-Anbieter darf daher nur solche Subauftragsverarbeiter auswählen, die gemäß Art. 28 Abs. 1 DSGVO ebenfalls *„geeignete Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet“.* Subauftragsverarbeiter können die geforderten geeigneten Garantien ihrerseits beispielsweise durch ein datenschutzspezifisches Zertifikat oder durch die Befolgung von anerkannten Verhaltensregeln (‚Code of Conduct‘) gemäß Art. 40 DSGVO erbringen.

Ist ein Cloud-Anbieter selbst Teil eines Cloud-Dienstes, der aus mehreren Datenverarbeitungsvorgängen besteht, wird er im Allgemeinen auch nur seinen klar abgegrenzten Datenverarbeitungsvorgang, für den er verantwortlich ist, zertifizieren lassen. Wichtig dabei ist, dass eine solche „Domänenzertifizierung“ eine Anerkennung im Rahmen von übergeordneten Zertifizierungsverfahren ermöglicht.

3. Vorgehen zur Bestimmung des Zertifizierungsgegenstands

Zur Festlegung des Zertifizierungsgegenstands kann folgendermaßen vorgegangen werden: Zunächst sollte eine vollständige Datenflussanalyse der Anwendung mit allen an der Verarbeitung personenbezogener Daten beteiligten Akteuren wie beispielsweise auch der Subauftragsverarbeiter erstellt und sodann bestimmt werden, welche Datenverarbeitungsschritte dem erweiterten Verantwortungsbereich des Cloud-Anbieters zuzuordnen sind. Hierbei ist auch eindeutig darzulegen, wie die Zugriffsmöglichkeiten der Cloud-Nutzer und des Cloud-Anbieters selbst in den jeweiligen Datenvorgängen ausgestaltet sind. Diese internen Datenverarbeitungsschritte und -schnittstellen sind vollständig zu erfassen.

Auch Schnittstellen zu anderen Datenverarbeitungsvorgängen oder Diensten müssen bedacht und beschrieben werden. Selbst in dem Fall, in dem beispielsweise nur einzelne Verarbeitungsvorgänge eines Dienstes zertifiziert werden sollen, ein Dienst aber aus mehreren Verarbeitungsvorgängen besteht, können Verarbeitungsvorgänge nur dann aus dem Zertifizierungsgegenstand herausgenommen werden, wenn sie keine direkten Verbindungen mit den zu zertifizierenden Verarbeitungsvorgängen haben. Auch in diesem Fall sind jedoch die Verbindungen der jeweiligen Verarbeitungsvorgänge zu beschreiben, um sie klar zu unterscheiden und eventuelle Datenflüsse zwischen diesen zu identifizieren.