European Cloud Service
Data Protection Certification

AUDITOR-Zertifizierungsgegenstand

Kurzfassung

- Fassung 1.00 -

Stand 05.06.2024

Weitere AUDITOR-Dokumente:

- Zertifizierungsgegenstand Langfassung
- Kriterienkatalog
- Konformitätsbewertungsprogramm
- Modularitätskonzept
- Schutzklassenkonzept

Online verfügbar: www.auditor-cert.de

Empfohlene Zitation:
Roßnagel, A., Sunyaev, A., Lins, S., Maier-Reinhardt, N., Müller, J., & Teigeler, H. (2024). AUDITOR-Zertifizierungsgegenstand, Kurzfassung – Fassung 1.00. 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 Klimaschutz gefördert wird (FKZ 01MT17003).

Gefördert durch:

aufgrund eines Beschlusses
des Deutschen Bundestages

Autoren

Alexander Roßnagel[a], Ali Sunyaev[b], Sebastian Lins[b], Natalie Maier-Reinhardt[a], Johannes Müller[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

A. 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

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. So umfasst der Zertifizierungsgegenstand beispielsweise Support- oder Wartungstätigkeiten, wenn personenbezogene Daten verarbeitet werden. 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.

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). Dagegen werden die datenschutzrechtlichen Anforderungen an den Auftraggeber (Cloud-Nutzer) nicht adressiert.

2.1. Die Verantwortlichkeit des Cloud-Anbieters für Datenverarbeitungsvorgänge

Cloud-Anbieter im Sinne dieses Katalogs ist jedes privatwirtschaftliche Unternehmen, das einen Cloud-Dienst am Markt anbietet und sich nach dem AUDITOR-Kriterienkatalog als Auftragsverarbeiter gemäß Art. 4 Nr. 8 DSGVO 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[1]- als auch B2C[2]-Anbieter sein. Wichtig ist nur, dass sie hinsichtlich der Daten, die in der Cloud verarbeitet werden (**„Inhalts- oder Anwendungsdaten“**[3]), 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 diesen durchführen zu können. Wird der Cloud-Dienst im B2C-Bereich angeboten, stellt der Cloud-Nutzer häufig auch die betroffene Person dar, deren Daten erforderlich sind, um den Cloud-Dienst bereitzustellen, sodass der Cloud-Anbieter seine datenschutzrechtlichen Pflichten (z.B. Informationspflichten) gegenüber dem Cloud-Nutzer erfüllen muss.

   Im B2B-Bereich ist zu beachten, dass Daten juristischer Personen wie z.B. Namen oder Adressen gemäß EG 14 vom Anwendungsbereich der Datenschutz-Grundverordnung ausgenommen sind. Dies gilt jedoch nicht, wenn die Daten der juristischen Person eine enge personelle oder wirtschaftliche Verbindung zu einer natürlichen Person aufweisen wie dies z.B. bei einer Ein-Mann-GmbH der Fall ist. Dann liegen ebenfalls personenbezogene Daten vor und die Datenschutz-Grundverordnung ist anwendbar.

   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

[1] Business to Business (B2B) bedeutet, dass der Kunde entweder eine juristische oder eine natürliche Person ist, die personenbezogene Daten im Rahmen ihrer Geschäftstätigkeit verarbeitet. Ein „Unternehmen“ ist jede natürliche oder juristische Person, die bei Verträgen zu Zwecken handelt, die ihrer gewerblichen oder beruflichen Tätigkeit zugerechnet werden können.

[2] Business to Consumer (B2C) bedeutet, dass der Kunde eine natürliche und private Person ist und daher keine personenbezogenen Daten im Rahmen seiner Geschäftstätigkeit verarbeitet. Siehe auch „Cloud-Nutzer als Nutznießer“ im Kriterienkatalog in Bezug auf den Cloud-Nutzer als natürliche Person, die unter die „Haushaltsausnahme“ fällt. Ein „Verbraucher“ ist jede natürliche Person, die bei Verträgen zu Zwecken handelt, die nicht ihrer gewerblichen oder beruflichen Tätigkeit zugerechnet werden können. Es ist jedoch zu beachten, dass ein Verbraucher nicht automatisch unter die sogenannte „Haushaltsausnahme“ gemäß Art. 2 Abs. 2 lit.c DSGVO fällt. Diese Ausnahme ist der Nichtanwendbarkeit in Bezug auf die Verarbeitung personenbezogener Daten durch eine natürliche Person im Rahmen einer rein persönlichen oder häuslichen Tätigkeit vorbehalten. Die Datenverarbeitung eines Verbrauchers kann also entweder unter diese Ausnahmeregelung fallen oder nicht, was zur Folge hat, dass seine Datenverarbeitung entweder privilegiert ist oder nicht. Im letzteren Fall ist der Verbraucher als für die Verarbeitung Verantwortlicher zu behandeln.

[3] Inhaltsdaten tragen die Informationen über eine betroffene Person in sich, wohingegen Anwendungsdaten Informationen über eine betroffene Person sind, die aus der Verwendung einer Softwareanwendung abgeleitet werden, z. B. wären Inhaltsdaten in einem Dokument die Bedeutung in Worten, während Anwendungsdaten aus dem Softwareprogramm stammen würden, das verwendet wird, um den Inhalt des Dokuments zu lesen.

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. Gerade im B2B-Bereich können neben den Daten des Cloud-Nutzers auch Daten anderer betroffener Personen wie beispielsweise von Mitarbeitern des Cloud-Nutzers erforderlich sein, um den Vertrag über die Nutzung des Cloud-Dienstes mit dem Cloud-Nutzer schließen und durchführen zu können. So werden z.B. Namen und Kontaktdaten von Mitarbeitern des Cloud-Nutzers verarbeitet, die dem Cloud-Anbieter als Ansprechpartner dienen sollen. Da der Cloud-Anbieter den Vertrag über die Cloud-Nutzung nicht mit dem Mitarbeiter schließt, kann Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO nicht die Verarbeitung der Mitarbeiterdaten legitimieren. Stattdessen kann sich der Cloud-Anbieter auf Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO und seine berechtigten Interessen an der Datenverarbeitung stützen, solange wie die Daten zur Begründung und Erfüllung des Vertrags mit dem Cloud-Nutzer erforderlich sind.

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“**[4] zusammengefasst werden. Auch die Verarbeitung von Telemetrie- und Diagnosedaten fällt unter diesen Begriff, sofern die Daten für die Durchführung des Vertrags mit dem Cloud-Nutzer erforderlich sind.

Da die Datenschutz-Grundverordnung die Unterscheidung in Bestands- und Nutzungsdaten nicht kennt, werden diese Daten im Rahmen dieses Kriterienkatalogs als **personenbezogene Daten** bezeichnet, die ihm Rahmen der Durchführung des Auftrags über die Erbringung des Cloud-Dienstes anfallen.

Datenverarbeitungsvorgänge, die der Cloud-Anbieter **als für die Verarbeitung Verantwortlicher** vornimmt, um den Vertrag mit dem Cloud-Nutzer über die Bereitstellung des Cloud-Dienstes schließen und diesen durchführen zu können, sind z.B.:

- um den Vertrag schließen zu können: solche Daten, die der Anbieter entweder benötigt, um eine technische Schnittstelle bereitzustellen oder um zu entscheiden, ob seine derzeitigen Schnittstellen zur technischen Basis des Cloud-Nutzers für die Nutzung des Dienstes passen. Zu den Daten, die verarbeitet werden können, gehören beispielsweise technische Daten für die Erbringung des Dienstes, wie der verwendete Browser und Gerätetyp, die Version des Betriebssystems, eindeutige Gerätekennungen und Informationen über das Mobilfunknetzwerk. Dazu zählen etwa der Name, eine Telefonnummer, eine Adresse, eine E-Mail-Adresse, um ein Angebot übersenden zu können.

- solche zur Durchführung: Daten, die sich aus der Verarbeitung der in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung vereinbarten Daten ergeben, um den Dienst im Hinblick

[4] "Nutzungsdaten" sind zusätzliche personenbezogene Daten wie z.B. Login-/Logout-Daten für Nutzerkonten, IP-Adressen, die genutzten Servicemodule und der Umfang der Nutzung, die sich aus der Nutzung des Dienstes ergeben.

auf das konzeptionelle Ziel des Dienstes zu erhalten, sowie Nutzungsdaten[5], um entsprechend die Dienstnutzung abrechnen zu können. Zu den Daten, die verarbeitet werden können, gehören beispielsweise Zahlungsinformationen (z. B. Bankverbindung), Benutzernamen und Passwörter für die Anmeldung beim Cloud-Dienst oder nutzerspezifische Qualitätsindikatoren (z. B. für die Überwachung oder die Erbringung von Dienstleistungen). Dazu zählen etwa der Name, eine Telefonnummer, eine Adresse, eine E-Mail-Adresse, um eine Rechnung übersenden zu können.

- solche zur Erfüllung rechtlicher Verpflichtungen: Daten, die erforderlich sind, um Anomalien in Bezug auf kritische Infrastrukturen zu erkennen (z. B. An- und Abmeldedaten für Benutzerkonten und IP-Adressen, Standortdaten, etc.)

Im Gegensatz dazu stellen die folgenden Beispiele keine Datenverarbeitungsvorgänge dar, die von einem Cloud-Anbieter als für die Verarbeitung Verantwortlichem durchgeführt werden, um einen Vertrag mit einem Cloud-Nutzer zu schließen oder zu erfüllen:

- Datenverarbeitungsvorgänge für Marktforschung und -analyse (z. B. Erhebung und Analyse von Daten, um Erkenntnisse über Markttrends, Kundenpräferenzen und -verhalten zu gewinnen),
- Datenverarbeitungsvorgänge für Marketingzwecke (z. B. Erhebung und Verarbeitung von Daten zur Information über verwandte Produkte),
- Datenverarbeitungsvorgänge zur (betrieblichen) Geschäftsoptimierung, die nicht mit dem Cloud-Dienst zusammenhängen (z. B. Nutzung von Daten zur Optimierung interner Prozesse und Verfahren, um Kosten zu sparen).

Sobald der Cloud-Anbieter sich entschließt die Zertifizierung zu erlangen, wird er mit der Zertifizierungsstelle ausführliche Gespräche führen, um den Umfang der Zertifizierung und die konkreten Datenverarbeitungsvorgänge, die zertifiziert werden sollen, festzulegen. Das AUDITOR-Konformitätsbewertungsprogramm spezifiziert diese Prozesse und die Zertifizierungsstellen sind verpflichtet, die entsprechenden Prozesse zu befolgen und anzuwenden.[6] Beispiele für Datenverarbeitungsvorgänge, die ***nicht*** unter der AUDITOR-Zertifizierung zertifiziert werden können sind: a) Datenverarbeitungsvorgänge, die ausschließlich für die Verarbeitung als Verantwortlicher durchgeführt werden, um den Vertrag mit dem Cloud-Nutzer über die Erbringung des Cloud-Dienstes abzuschließen und zu erfüllen, OHNE dass die Datenverarbeitungsvorgänge in seiner Rolle als Auftragsverarbeiter zertifiziert werden; b) Datenverarbeitungsvorgänge, die der Durchführung rechtswidriger Tätigkeiten dienen; oder c) wenn die den Cloud-Anbieter betreffenden Rechtsvorschriften ihn daran hindern würden, die Grundsätze der DSGVO einzuhalten.

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

[5] "Nutzungsdaten" sind zusätzliche personenbezogene Daten wie z.B. Login-/Logout-Daten für Nutzerkonten, IP-Adressen, die genutzten Servicemodule und der Umfang der Nutzung, die sich aus der Nutzung des Dienstes ergeben.

[6] Unter anderem muss eine Zertifizierungsstelle die Durchführung einer bestimmten Zertifizierung ablehnen, wenn ihr (a) die Kompetenz oder Fähigkeit zur erforderlichen Durchführung der Zertifizierungsaktivitäten fehlt, (b) wenn ihr die Ressourcen fehlen, um alle Auswahl- und Ermittlungstätigkeiten durchzuführen, oder c) wenn ihre Unparteilichkeit gefährdet ist. Eine Zertifizierungsstelle kann ferner den Antrag eines Cloud-Anbieters auf Zertifizierung ablehnen, wenn der Cloud-Anbieter in illegale Aktivitäten verwickelt ist, der Cloud-Anbieter wiederholt gegen die AUDITOR-Zertifizierungskriterien verstoßen hat oder es Beweise für ähnliche Probleme in Bezug auf den Cloud-Anbieter gibt. Die Zertifizierungsstelle ist aufgefordert, Auswahlverfahren durchzuführen, die frei von Willkür bei der Bewertung sind, und ihre Entscheidungen transparent zu dokumentieren.

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 tatsächlichen Einflussmöglichkeiten zwischen den Parteien abbilden. Je größer die Einflussmöglichkeiten des Cloud-Anbieters auf die Datenverarbeitung sind, desto eher muss er als Verantwortlicher angesehen werden. Als Verantwortlicher ist gemäß Art. 4 Nr. 7 DSGVO stets derjenige anzusehen, der über die Zwecke und Mittel der Datenverarbeitung entscheidet. Der Cloud-Anbieter ist Auftragsverarbeiter, wenn er die Auftragsverarbeitung weisungsgemäß durchführt und mit den zu verarbeitenden Daten keine eigenen Zwecke verfolgt. Häufig verfügt der Cloud-Anbieter jedoch über gewisse Entscheidungsbefugnisse hinsichtlich der Wahl der technischen und organisatorischen Mittel. Solange diese Mittel angemessen sind, um den Verarbeitungszweck zu erreichen und er den Cloud-Nutzer über diese informiert und dieser damit einverstanden ist, bleibt der Cloud-Anbieter jedoch Auftragsverarbeiter.

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 sonstigen Subauftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten und darf nur solche für die Erbringung seines Dienstes einsetzen.

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 den Nachweis durchlaufener Zertifizierungsverfahren oder durch die Befolgung von anerkannten Verhaltensregeln (‚Code of Conduct‘) gemäß Art. 40 DSGVO erbringen.

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. Im Rahmen der Datenflussanalyse sollte insbesondere auch überprüft werden, ob im Hinblick auf die Verarbeitungsvorgänge des Zertifizierungsgegenstands eine Übermittlung personenbezogener Daten außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums oder an internationale Organisationen erfolgt.

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
DSGVO	EU-Datenschutz-Grundverordnung (Geltung ab 25.5.18)
ggf.	gegebenenfalls
i.V.m.	in Verbindung mit
lit.	litera = Buchstabe
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.