European Cloud Service
Data Protection Certification

AUDITOR-Kriterienkatalog

- Entwurfsfassung 0.9 -

Stand 15.03.2019

Weitere AUDITOR-Dokumente:

- Zertifizierungsgegenstand: Kurzfassung
- Zertifizierungsgegenstand
- 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-Kriterienkatalog – Entwurfsfassung 0.9. Karlsruhe, Germany: KIT. DOI: 10.5445/IR/1000092273

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) im Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) des Karlsruher Instituts für Technologie

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
Art.	Artikel
Alt.	Alternative
BDSG	Bundesdatenschutzgesetz neue Fassung (Geltung ab 25.05.18)
DSB	Datenschutzbeauftragter
DSGVO	EU-Datenschutz-Grundverordnung (Geltung ab 25.05.18)
EG	Erwägungsgrund
EWR	Europäischer Wirtschaftsraum
i.S.v.	Im Sinne von
i.V.m.	In Verbindung mit
lit.	litera (Buchstabe)
Nr.	Nummer
SDM	Standard-Datenschutzmodell v.1.1 vom 26.04.2018
TCDP	Trusted Cloud Datenschutz-Profil
TOM	technische und organisatorische Maßnahmen
Ziff.	Ziffer

Hinweis zur geschlechtsneutralen Formulierung:

Alle personenbezogenen Bezeichnungen im AUDITOR-Kriterienkatalog 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. Gegenstand und Ziele des AUDITOR-Kriterienkatalogs

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

1. Adressaten und Funktionen des AUDITOR-Kriterienkatalogs

Durch die AUDITOR-Datenschutz-Zertifizierung können Anbieter von Cloud-Diensten des privaten Sektors die Vereinbarkeit ihrer Datenverarbeitungsvorgänge mit datenschutzrechtlichen Anforderungen nachweisen. 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.

Zertifizierungsgegenstand AUDITOR

Den Zertifizierungsgegenstand des AUDITOR-Verfahrens sind 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. 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 zu können sowie um rechtliche Pflichten zu erfüllen.

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 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 *„Zertifizierungsgegenstand“* zu entnehmen.

Cloud-Anbieter als Adressat

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- 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 diesen 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.

   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.

Cloud-Nutzer als Nutznießer

Cloud-Nutzer im Sinne dieses Katalogs ist jede natürliche oder juristische Person, die als Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO Verarbeitungen personenbezogener Daten durchführt und allein oder gemeinsam mit anderen über Zwecke und Mittel dieser Verarbeitungen entscheidet und sich entschließt, diese Verarbeitungen an einen Cloud-Anbieter auszulagern.

Aufgrund der Zertifizierung der Datenverarbeitungsvorgänge eines Cloud-Dienstes kann der Cloud-Nutzer darauf vertrauen, dass der von ihm verwendete Cloud-Dienst datenschutzkonform ist. Der Anwendungsbereich der Datenschutz-Zertifizierung nach AUDITOR ist die Verarbeitung personenbezogener Daten im Auftrag (Auftragsverarbeitung) nach Art. 28 DSGVO durch einen Cloud-Anbieter. Hier muss sich der Cloud-Nutzer des Dienstes als Auftraggeber gemäß Art. 28 Abs. 1 DSGVO davon überzeugen, dass auf Seiten des Cloud-Anbieters hinreichende Garantien bestehen, die bestätigen, dass geeignete technische und organisatorische Maßnahmen (TOM) so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der Datenschutz-Grundverordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Der Nachweis hinreichender Garantien wird erleichtert, wenn der Cloud-Anbieter als Auftragnehmer ein Zertifikat vorweist, das die Erfüllung der gesetzlichen Anforderungen bestätigt. Ein Zertifikat kann gemäß Art. 28 Abs. 5 DSGVO als Faktor herangezogen werden, um hinreichende Garantien nachzuweisen. Für die Nutzung von Cloud-Diensten, die im Regelfall als standardisierte Dienste für eine Vielzahl von Nutzern erbracht werden, ist die Datenschutz-Zertifizierung besonders wichtig, da sie eine effiziente Möglichkeit zur Erfüllung der gesetzlichen Überprüfungspflicht darstellt.

Personenbezogene Daten als das zu schützende Gut

Als *personenbezogenen Daten* werden, der gesetzlichen Definition des Art. 4 Abs. 1 DSGVO entsprechend, alle Daten verstanden, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Im Cloud-Kontext können dies beispielsweise Anwendungsdaten des Cloud-Nutzers sein, soweit sie dem jeweiligen Datenverarbeiter die Identifizierung oder Identifizierbarkeit einer natürlichen Person ermöglichen. Die Cloud-Nutzer und Cloud-Anbieter müssen gemäß Art. 28 Abs. 3 Satz 1 DSGVO in einer rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festlegen, welche Arten personenbezogener Daten im Rahmen der Auftragsverarbeitung weisungsgebunden durch den Auftragsverarbeiter verarbeitet werden sollen.

Verantwortungsverteilung zwischen Cloud-Anbieter und Cloud-Nutzer

Da sich der Anwendungsbereich der Datenschutz-Zertifizierung nach AUDITOR auf die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO erstreckt, adressiert der AUDITOR-Kriterienkatalog schwerpunktmäßig die datenschutzrechtlichen Anforderungen an den Cloud-Anbieter in seiner Funktion als Auftragsverarbeiter. Datenverarbeitungsvorgänge, bei denen der Cloud-Anbieter nicht lediglich weisungsgebunden agiert, sondern als Verantwortlicher über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet, werden im Rahmen der AUDITOR-Zertifizierung nur betrachtet, soweit es um Datenverarbeitungsvorgänge geht, die erforderlich sind, um den Vertrag mit dem Cloud-Nutzer über die Bereitstellung des Cloud-Dienstes schließen und durchführen sowie um rechtliche Pflichten wie handels- und steuerrechtliche Aufzeichnungs- und Aufbewahrungspflichten erfüllen zu können.

Dass es beim Cloud Computing regelmäßig zu einem Nebeneinander der Verantwortlichkeiten zwischen dem Cloud-Anbieter und dem Cloud-Nutzer kommt, ist nicht ungewöhnlich. Allgemeine Leitlinien zur Verantwortungsabgrenzung sind nur schwer zu bilden, da die Verantwortungsverteilung maßgeblich von den Service-Modellen und den konkreten Ausgestaltungen sowie den individuellen Auftragsverarbeitungsvereinbarungen mit den jeweiligen Cloud-Nutzern abhängt. Daher liegt es an dem Cloud-Nutzer und dem Cloud-Anbieter Regelungen zur Verantwortungsverteilung zu treffen.

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 der Cloud.

Verantwortungsverteilung zwischen Cloud-Anbieter und Subauftragsverarbeiter

Der Cloud-Anbieter hat die Möglichkeit, den Cloud-Dienst nicht vollständig selbst zu erbringen, sondern sich für die Leistungserbringung weiterer Subauftragsverarbeiter zu bedienen, soweit der Cloud-Nutzer damit einverstanden ist. In diesem Fall können einzelne Abschnitte oder Teile des Datenverarbeitungsvorgangs an weitere Auftragsverarbeiter delegiert oder ausgelagert werden, sodass eine Leistungskette entsteht. Die Auslagerung der Datenverarbeitung an weitere Subauftragsverarbeiter darf jedoch nicht dazu führen, dass die Vorgaben der Datenschutz-Grundverordnung in der Leistungskette missachtet werden. Vielmehr muss der Cloud-Anbieter als Hauptauftragsverarbeiter dafür Sorge tragen, dass auf allen Stufen die einschlägigen Vorschriften der Datenschutz-Grundverordnung von allen Subauftragsverarbeitern eingehalten werden. Für die Auftragsdurchführung gegenüber dem Cloud-Nutzer bleibt der Cloud-Anbieter durchgängig verantwortlich. Setzen die zu zertifizierenden Verarbeitungsvorgänge 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 sonstigen Subauftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten und darf nur solche einsetzen, um seinen Dienst zu erbringen. 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. Kapitel V dieses Kriterienkatalogs regelt insbesondere die Subauftragsverarbeitung.

2. Fortentwicklung von TCDP gemäß der Datenschutz-Grundverordnung

Die Zertifizierung nach dem alten Bundesdatenschutzgesetz wurde im Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ durch das im September 2016 finalisierte Trusted Cloud Datenschutz-Profil (TCDP) untersucht. Da bei der Entwicklung der Zertifizierungskriterien nach TCDP noch nicht alle einschlägigen internationalen Normen, neu entwickelten relevanten Kriterienwerke – z. B. Cloud Computing Compliance Controls Catalogue (C5) – und insbesondere die Anforderungen der Datenschutz-Grundverordnung berücksichtigt werden konnten, muss mit dem Geltungsbeginn der Datenschutz-Grundverordnung ab dem 25.05.2018 das TCDP-Kriterienwerk an die neuen Regelungen angepasst werden. Dies geschieht mit dem AUDITOR-Kriterienkatalog. Dieser zielt insbesondere auf einheitliche Kriterien für eine unionsweite Zertifizierung.

Der AUDITOR-Kriterienkatalog fokussiert alle relevanten Vorschriften für die Datenschutz-Zertifizierung von Cloud-Diensten in der Datenschutz-Grundverordnung und konkretisiert diese zu prüffähigen Kriterien.

B. Aufbau und Nutzung des AUDITOR-Kriterienkatalogs

1. Elemente des Kriterienkatalogs

Der AUDITOR-Kriterienkatalog enthält „Kriterien“, „Erläuterungen“, „Umsetzungshinweise“ und „Nachweise“. Die *„Kriterien“* bezeichnen die normativen Voraussetzungen, die zu erfüllen sind, um ein Zertifikat auf der Grundlage des AUDITOR-Kriterienkatalogs zu erhalten. Sie stellen somit die Anforderungen dar, die eine akkreditierte Zertifizierungsstelle im Rahmen des Zertifizierungsverfahrens überprüft. Die *„Erläuterungen“* sollen das Verständnis der Kriterien und ihre Herleitung aus der Datenschutz-Grundverordnung erleichtern.

Für jedes Kriterium werden „Umsetzungshinweise“ als exemplarische Leitlinien und Hilfestellungen für das Verständnis und die Umsetzung der Kriterien gegeben, die jedoch keinen verpflichtenden Charakter haben. Zudem finden sich zu jedem Kriterium „Nachweise“. Die *„Nachweise“* liefern die Antwort auf die Frage, wie das Vorliegen der Kriterien im konkreten Zertifizierungsverfahren erwiesen werden kann. Sie stellen analog zu den Umsetzungshinweisen exemplarische Leitlinien und informative Hilfestellungen dar, die Cloud-Anbieter, Zertifizierungsstellen, Prüfer und weitere Interessierte bei der Beurteilung der Einhaltung von Kriterien unterstützen sollen. Es besteht keine Verpflichtung, die Nachweise gemäß diesem Dokument zu erbringen. Das akkreditierte AUDITOR-Konformitätsbewertungsprogramm legt fest, wie jedes Kriterium im Rahmen der Zertifizierung zu überprüfen ist.

Der Kriterienkatalog unterscheidet zwischen Kriterien, Erläuterungen, Umsetzungshinweisen und Nachweisen für die Auftragsverarbeitung von Anwendungsdaten (Kapitel C) und für die Verarbeitung von Bestands- und Nutzungsdaten, für die ein Cloud-Anbieter verantwortlich ist (Kapitel D).

2. Schutzklassen

Anforderungen an TOM des Cloud-Dienstes werden nach Schutzklassen differenziert. Dabei orientiert sich der AUDITOR-Kriterienkatalog an dem TCDP-Schutzklassenkonzept, berücksichtigt aber auch die Schutzbedarfsabstufungen nach dem Standard-Datenschutzmodell (SDM) der deutschen Datenschutzaufsichtsbehörden.

2.1 Das Schutzklassenkonzept

Das Schutzklassenklassenkonzept orientiert sich am Risiko der Datenverarbeitung für die Grundrechte und Grundfreiheiten natürlicher Personen. Daneben hat nach Art. 24, 25 und 32 DSGVO die Auswahl von TOM den Stand der Technik und die Implementierungskosten zu berücksichtigen. In Anlehnung an die EG 75, 76, 85, 90, 91, 94, 95 und 96 DSGVO hat der Verantwortliche jeweils die Risiken einer Verarbeitung personenbezogener Daten für die Rechte und Freiheiten natürlicher Personen vorab zu identifizieren. In einem weiteren Schritt ist abzuschätzen, ob die Verarbeitung zu einem materiellen oder immateriellen Schaden führen könnte, insbesondere wenn sie zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, einer unbefugten Aufhebung der Pseudonymität oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren.

Der Verantwortliche hat gemäß EG 76 Satz 1 DSGVO die Eintrittswahrscheinlichkeit und Schwere des Schadens für die Rechte und Freiheiten der betroffenen Person in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung zu bestimmen. Dieses Risiko soll er gemäß dem jeweiligen Verwendungskontext der verarbeiteten personenbezogenen Daten anhand eines objektiven Maßstabs beurteilen. Dabei hat er nach EG 76 Satz 2 DSGVO festzustellen, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt. Diese Risikoabstufungen werden mit dem AUDITOR-Schutzklassenkonzept umgesetzt.

Der Cloud-Anbieter muss umgekehrt durch seine Dienstbeschreibung zu erkennen geben, für welche Art und Kategorien von Daten und für welche Schutzklassen der angebotene Dienst geeignet ist. Dabei muss jeder geprüfte Datenverarbeitungsvorgang in diesem Cloud-Dienst diese Schutzklasse erfüllen. Schutzklassen werden daher nicht jedem einzelnen Datenverarbeitungsvorgang im jeweiligen Cloud-Dienst zugewiesen, sondern dem Cloud-Dienst als solchem.

Ziel des Schutzklassenkonzepts ist es, den individuellen Maßstab der Datenschutz-Grundverordnung – die Anforderungen an die TOM richten sich nach dem Schutzbedarf der jeweiligen Datenverarbeitung – durch Zuordnung in Schutzklassen zu vereinfachen. Die Schutzklassen haben dabei eine doppelte Funktion: Sie beschreiben zum einen den Schutzbedarf der Datenverarbeitungsvorgänge, zum anderen die Anforderungen an die TOM. Um die unterschiedlichen Funktionen deutlich zu machen, unterscheidet das Schutzklassenkonzept einerseits Schutzbedarfsklassen und andererseits Schutzanforderungsklassen.

Die *Schutzbedarfsklassen* definieren den Schutzbedarf für Datenverarbeitungsvorgänge anhand genereller Merkmale. Dieser ergibt sich aus der Art der Daten, dem Umfang, den Umständen und den Zwecken der konkreten Datenverarbeitung.

Die *Schutzanforderungsklassen* definieren in allgemeiner Form die technischen und organisatorischen Anforderungen, die für Datenverarbeitungsdienste der betreffenden Klasse maßgeblich sind. Dabei wird für jede Schutzbedarfsklasse eine korrespondierende Schutzanforderungsklasse definiert.

Die Unterscheidung von Schutzbedarfs- und Schutzanforderungsklasse korrespondiert mit den Rollen und Verantwortungen von Cloud-Nutzer und Cloud-Anbieter in der Auftragsverarbeitung. Der Cloud-Anbieter beansprucht im Rahmen des Zertifizierungsverfahrens für jeden Dienst auf Grundlage der Prüfung und anhand der konkreten TOM eine bestimmte Schutzanforderungsklasse. Dies wird durch die Zertifizierungsstelle überprüft. Im Zertifikat wird die Eignung des Cloud-Dienstes für eine konkrete Schutzanforderungsklasse zum Ausdruck gebracht. Der Cloud-Nutzer als Verantwortlicher und Auftraggeber hat hingegen die Aufgabe, den Schutzbedarf seiner Datenverarbeitung zu bestimmen, indem er eine Schutzbedarfsklasse auswählt. Lagert er seine Datenverarbeitungsvorgänge an einen Cloud-Dienst aus, muss er einen Cloud-Dienst auszuwählen, der mindestens die entsprechende Schutzanforderungsklasse erfüllt.

Hinsichtlich der Datenverarbeitung, für die der Cloud-Anbieter verantwortlich ist und die erforderlich ist, um den Auftrag mit dem Cloud-Nutzer über die Nutzung des Cloud-Dienstes durchzuführen, legt der Anbieter sowohl den Schutzbedarf als auch die Schutzanforderungen an die Datenverarbeitung fest, da beides in seiner Verantwortung liegt.

2.2 Die Schutzklassen des AUDITOR-Kriterienkatalogs

Der AUDITOR-Kriterienkatalog beruht auf der Unterscheidung von drei Schutzklassen (1, 2, 3), für die jeweils Schutzbedarf (Schutzbedarfsklassen) und Schutzanforderungen (Schutzanforderungsklassen) beschrieben werden.

Neben den drei Schutzklassen gibt es Datenverarbeitungsvorgänge, die keine Aussagen über persönliche oder sachliche Verhältnisse natürlicher Personen enthalten, erzeugen, unterstützen oder solche ermöglichen und daher keinen datenschutzrechtlichen Schutzbedarf aufweisen. Sie liegen unterhalb von Schutzklasse 1, weshalb sie in dem Schutzklassenkonzept nicht betrachtet werden.

Auch Datenverarbeitungsvorgänge mit extrem hohem Schutzbedarf (oberhalb von Schutzbedarfsklasse 3) werden in dem Schutzklassenkonzept und der AUDITOR-Zertifizierung nicht berücksichtigt. Ein extrem hoher Schutzbedarf liegt vor, wenn die Datenverarbeitungsvorgänge aufgrund der verwendeten Daten oder der konkreten Verarbeitung dieser Daten eine erhebliche Aussagekraft über die Persönlichkeit oder Lebensumstände der betroffenen Person haben, unterstützen oder zu einer solchen führen können oder sonst für die Verhältnisse der betroffenen Person von erheblicher Bedeutung sind und die unbefugte Verarbeitung dieser Daten zu einer konkreten Gefahr für eine wesentliche Beeinträchtigung von Leben, Gesundheit oder Freiheit der betroffenen Person führen würde.

Nicht abschließende Beispiele für Daten mit extrem hohem Schutzbedarf:

- Daten von V-Leuten des Verfassungsschutzes;
- Daten über Personen, die mögliche Opfer von strafbaren Handlungen sein können;
- Adressen von Zeugen in bestimmten Strafverfahren.

Auch Datenverarbeitungsvorgänge mit individuell stark divergierenden Umständen werden in dem Schutzklassenkonzept und der AUDITOR-Zertifizierung nicht betrachtet, weil sie der Generalisierung, die mit dem Schutzklassenkonzept einhergeht, nicht zugänglich sind.

a) Die Ermittlung der Schutzbedarfsklasse

Die Festlegung des Schutzbedarfs obliegt dem Cloud-Nutzer. Der Schutzbedarf wird in einem dreistufigen Verfahren ermittelt:

- Im 1. Schritt wird der abstrakte Schutzbedarf der zu verarbeitenden Daten nach der Datenart bestimmt.
- Im 2. Schritt ist zu prüfen, ob sich der Schutzbedarf aufgrund der konkreten Verwendung der Daten erhöht.
- Im 3. Schritt ist zu prüfen, ob der Schutzbedarf aufgrund konkreter Umstände sinkt.

Im Ergebnis wird der Schutzbedarf der konkreten Datenverarbeitung nach den Schutzbedarfsklassen kategorisiert. Die Schritte zwei und drei werden im AUDITOR-Katalog nicht weiter erläutert, weil sie vornehmlich den Cloud-Nutzer und nicht die Zertifizierung des Cloud-Anbieters als solche betreffen.

Zu beachten gilt jedoch, dass für die Datenverarbeitung zur Durchführung des Auftrags mit dem Cloud-Nutzer, der Cloud-Anbieter Verantwortlicher ist und daher auch den Schutzbedarf dieser Datenverarbeitung bestimmen muss.

Schutzbedarfsklassen nach Datenart (Abstrakter Schutzbedarf – Schritt 1)

Zunächst wird der abstrakte Schutzbedarf der zu verarbeitenden Daten nach der Datenart bestimmt. Diese bildet nur den Ausgangspunkt und dient nur der ersten Einordnung der Daten. Schließlich lässt sich die Schutzbedürftigkeit von Daten nicht abstrakt bestimmen, sondern hängt von ihrem jeweiligen Verwendungszusammenhang ab.

Datenarten mit normalem Schutzbedarf (Schutzbedarfsklasse 1)

Jede Verarbeitung personenbezogener Daten stellt einen Eingriff in die Grundrechte der betroffenen Person dar. Aus diesem Grund wird davon ausgegangen, dass jede Verarbeitung personenbezogener Daten mindestens einen normalen Schutzbedarf aufweist.

In Schutzbedarfsklasse 1 fallen alle Datenverarbeitungsvorgänge, die durch die einbezogenen Daten und die konkrete Verarbeitung dieser Daten Aussagen über die persönlichen oder sachlichen Verhältnisse der betroffenen Person enthalten, erzeugen, unterstützen oder ermöglichen. Die unbefugte Verwendung dieser Daten kann von der betroffenen Person leicht durch Aktivitäten verhindert oder abgestellt werden oder lässt keine besonderen Beeinträchtigungen erwarten.

Nicht abschließende Beispiele für Daten (ohne Verarbeitungskontext, soweit nicht Schutzbedarfsklasse 2 oder 3):

- Name;
- Geschlecht;
- Anschrift;
- Beruf;
- Geburtsjahr;
- Titel;
- Adressbuchangaben;
- Telefonverzeichnisse;
- Staatsangehörigkeit;
- Telefonnummer einer natürlichen Person.

Datenarten mit hohem Schutzbedarf (Schutzbedarfsklasse 2)

Datenverarbeitungsvorgänge, die aufgrund der verwendeten Daten oder der konkreten Verarbeitung dieser Daten eine Aussagekraft über die Persönlichkeit oder die Lebensumstände der betroffenen Person haben, unterstützen oder zu einer solchen führen können oder sonst für die Verhältnisse der betroffenen Person von Bedeutung sind. Die unbefugte Verarbeitung solcher Daten kann zu Beeinträchtigungen der betroffenen Person in ihrer gesellschaftlichen Stellung oder ihren wirtschaftlichen Verhältnissen führen („Ansehen“). Weiterhin ist bei Daten, die der Gesetzgeber als besonders schutzwürdig in Art. 9 Abs. 1 DSGVO ausgewiesen hat, von einem hohen Schutzbedarf auszugehen.

Nicht abschließende Beispiele für Daten ohne Verarbeitungskontext, soweit nicht Schutzbedarfsklasse 3):

- Name, Anschrift eines Vertragspartners;
- Geburtsdatum;
- Familienstand;
- verwandtschaftliche Beziehungen und Bekanntenkreis;
- Daten über Geschäfts- und Vertragsbeziehungen;
- Kontext zu einem Vertragspartner (z.B. Gegenstand einer vereinbarten Leistung);
- Verarbeitungen nicht veränderbarer Personendaten, die lebenslang als Anker für Profilbildungen dienen können wie genetische Daten i.S.v. Art. 4 Nr. 13 DSGVO oder biometrische Daten i.S.v. Art. 4 Nr. 14 DSGVO;
- Daten über die rassische und ethnische Herkunft;
- Daten über politische Meinungen;
- religiöse oder weltanschauliche Überzeugungen;
- Gewerkschaftsangehörigkeit;
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person;
- Verarbeitungen eindeutig identifizierender, hoch verknüpfbarer Daten wie Krankenversichertennummern oder Steuernummern;
- Daten, die mögliche Auswirkungen auf das Ansehen/die Reputation der betroffenen Person haben;
- Daten über den geschützten inneren Lebensbereich der betroffenen Person (z.B. Tagebücher);
- Gesundheitsdaten i.S.v. Art. 4 Nr. 15 DSGVO;
- Grad der Behinderung;
- Verarbeitung von Daten mit inhärenter Intransparenz für die betroffene Person (Schätzwerte beim Scoring, Anwendung von Algorithmen);
- Einkommen;
- Sozialleistungen;
- Steuern;
- Ordnungswidrigkeiten;
- Daten über Mietverhältnisse;
- Patientenverwaltungsdaten (mit Ausnahme von besonders sensiblen Diagnosedaten und dergleichen);
- Arbeitszeitzeitdaten;
- Mitgliederverzeichnisse;
- Melderegister;
- Zeugnisse und Prüfungsergebnisse;
- Versicherungsdaten;
- Personalverwaltungsdaten aus Beschäftigungsverhältnissen (mit Ausnahme von dienstlichen Beurteilungen und beruflicher Laufbahn);
- Verkehrsordnungswidrigkeiten;
- einfache Bewertungen eher geringer Bedeutung (z.B. Ja/Nein-Entscheidung bei Einstufung im Mobilfunkvertrag etc.);
- Zugangsdaten zu einem Dienst;
- Kommunikationsinhalte einer Person (z.B. E-Mail-Inhaltsdaten, Brief, Telefonat);
- (genauer) Aufenthaltsort einer Person;
- Finanzdaten einer Person (z.B. Kontostand, Kreditkartennummer, einzelne Zahlung);
- Kreditauskünfte;
- Verkehrsdaten der Telekommunikation.

Hinweis: Kommunikationsinhalte, insbesondere Schrift- oder Sprachaufzeichnungen jeder Art, können sehr unterschiedlichen Schutzbedarf, von niedrig bis sehr hoch aufweisen. Die Festlegung des Schutzbedarfs erfordert eine objektive Bewertung, in der das Ausmaß des Risikos der Datenverarbeitung beurteilt wird. Sofern der Cloud-Nutzer keine Kenntnis vom subjektiven Schutzbedarf der Kommunizierenden hat (Beispiel: allgemeiner Kollaborations-Service mit Datenablage, Videokonferenz und Mailfunktion) oder seine Dienste für besonders schutzbedürftige Kommunikationen anbietet (Beispiel: Konferenzservice für Rechtsanwälte und Mandanten, hier: Schutzklasse 3) darf er von Schutzbedarfsklasse 2 ausgehen.

Datenarten mit sehr hohem Schutzbedarf (Schutzbedarfsklasse 3)

Datenverarbeitungsvorgänge, die aufgrund der verwendeten Daten oder der konkreten Verarbeitung dieser Daten eine erhebliche Aussagekraft über die Persönlichkeit oder die Lebensumstände einer betroffenen Person haben, unterstützen oder zu einer solchen führen können oder sonst für die Verhältnisse der betroffenen Person von erheblicher Bedeutung sind. Die unbefugte Verarbeitung solcher Daten kann zu erheblichen Nachteilen für die betroffene Person hinsichtlich ihrer gesellschaftlichen Stellung und ihren wirtschaftlichen Verhältnissen führen („Existenz“).

Hinweis: Als Datenarten in diesem Sinne werden auch Datenmehrheiten, insbesondere verkettete Daten (z.B. Persönlichkeitsprofile) angesehen, aus denen sich ein neuer Informationsgehalt ergibt.

Nicht abschließende Beispiele für Daten mit sehr hohem Schutzbedarf:

- Daten, die einem Berufs-, Geschäfts-, Fernmelde-, oder Mandantengeheimnis unterliegen (z.B. Patientendaten, Mandantendaten);
- Daten, deren Kenntnis eine erhebliche konkrete Schädigung der betroffenen Person oder Dritter ermöglicht (z.B. Persönliche Identifikationsnummer, Transaktionsnummer im Online-Banking);
- Schulden;
- besonders sensitive Sozialdaten;
- Pfändungen;
- Personalverwaltungsdaten wie dienstliche Beurteilungen, berufliche Laufbahn und dergleichen, soweit nicht Schutzbedarfsklasse 2;
- Daten über Vorstrafen und strafprozessuale Verhältnisse (z.B. Ermittlungsverfahren) einer Person und entsprechende Verdachtsmomente; Straffälligkeit;
- besonders sensitive Gesundheitsdaten i.S.v. Art. 4 Nr. 15 DSGVO wie z.B. zu Krankheiten, deren Bekanntwerden der betroffenen Person in besonderem Maße unangenehm sind oder zu einer gesellschaftlichen Stigmatisierung der betroffenen Person führen können;
- Persönlichkeitsprofile, z.B. Bewegungsprofil, Beziehungsprofil, Interessenprofil, Kaufverhaltensprofil, mit erheblicher Aussagekraft über die Persönlichkeit der betroffenen Person.

b) Schutzanforderungsklassen

Die Schutzanforderungsklassen dienen dazu, die TOM festzulegen, die dazu geeignet sind, die Rechte und Freiheiten der betroffenen Personen in Bezug auf die jeweiligen in der Schutzbedarfsklasse festgestellten Risiken des Dienstes angemessen zu schützen.

Schutzanforderungsklasse 1

Der Cloud-Anbieter hat risikoangemessene TOM zu ergreifen, um die Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit von personenbezogenen Daten sicherzustellen (siehe auch Gewährleistungsziele aus dem SDM). Für den Bereich der Informationssicherheit bedeutet dies, dass die Daten, insbesondere gegen Vernichtung, Verlust, Veränderung, unbefugten Zugang und unbefugte Offenlegung, zu schützen sind sowie die Belastbarkeit des Cloud-Dienstes zu gewährleisten ist.

Die TOM müssen geeignet sein, um im Regelfall solche Vorgänge aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert. Jeder Eingriff muss nachträglich festgestellt werden können.

Schutzanforderungsklasse 2

Ein hoher Schutzbedarf führt dazu, dass zusätzliche oder wirksamere risikoangemessene TOM ergriffen werden müssen, um die Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit von personenbezogenen Daten sicherzustellen (siehe auch Gewährleistungsziele aus dem SDM). Für die Informationssicherheit bedeutet dies, dass die Daten, insbesondere gegen Vernichtung, Verlust, Veränderung, unbefugten Zugang und unbefugte Offenlegung, zu schützen sind sowie die Belastbarkeit des Cloud-Dienstes zu gewährleisten ist. Gleichzeitig müssen die für Schutzanforderungsklasse 1 geeigneten Maßnahmen erfüllt und ihre Ausführung an den Schutzbedarf angepasst werden.

Dies kann erreicht werden, indem die Wirkung einer Maßnahme erhöht wird, soweit diese einen Ansatzpunkt für eine solche Skalierung bietet. Ein Beispiel hierfür ist die Erhöhung der Länge eingesetzter kryptografischer Schlüssel oder der Einsatz von Hardware-Token oder einer Zwei-Faktor-Authentifizierung. Weiterhin kann eine Anpassung dadurch erfolgen, dass mit größerer Zuverlässigkeit eine spezifikationsgerechte Ausführung der Maßnahme sichergestellt wird. Dazu müssen mögliche Störeinflüsse bestimmt und die Robustheit der Maßnahmen durch zusätzliche Vorkehrungen – oft organisatorischer Natur – erhöht werden.

Die ergriffenen Maßnahmen müssen geeignet sein, um im Regelfall solche Vorgänge aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder seiner Mitarbeiter, oder fahrlässiger Handlungen Dritter auszuschließen. Die Maßnahmen müssen auch geeignet sein, Schädigungen durch fahrlässige Handlungen Befugter im Regelfall zu verhindern. Gegen vorsätzliche Eingriffe ist ein Schutz vorzusehen, der zu erwartende Eingriffe hinreichend sicher ausschließt. Dazu gehört insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die Eingriffe im Regelfall (nachträglich) festgestellt werden können.

Schutzanforderungsklasse 3

Der Cloud-Anbieter muss über die TOM der Schutzanforderungsklassen 1 und 2 hinaus risikoangemessene TOM ergreifen, um die Daten, insbesondere gegen Vernichtung, Verlust, Veränderung, unbefugten Zugang und unbefugte Offenlegung, zu schützen.

Die Maßnahmen müssen geeignet sein, um solche Vorgänge aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, oder fahrlässiger oder vorsätzlicher Handlungen hinreichend sicher auszuschließen. Dazu gehört insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Verfahren zur Erkennung von Missbräuchen. Jeder Eingriff muss nachträglich festgestellt werden können.

3. Nichtanwendbarkeit von Kriterien

Im Rahmen des Zertifizierungsverfahrens stellt der Cloud-Anbieter der Zertifizierungsstelle ausreichend Informationen zur Beurteilung, Abgrenzung und abschließenden Festlegung des Zertifizierungsgegenstands zur Verfügung. Dies schließt insbesondere die Dokumentation von Verantwortlichkeiten und – insofern anwendbar – die Einbindung von Subauftragsverarbeitern in die zu zertifizierenden Datenverarbeitungsvorgänge ein. Bei der Festlegung des Zertifizierungsgegenstands oder im Rahmen des Prüfprozesses kann die Zertifizierungsstelle feststellen, dass einzelne Kriterien für den betrachteten Datenverarbeitungsvorgang nicht anwendbar sind. Das akkreditierte AUDITOR-Konformitätsbewertungsprogramm regelt die Voraussetzungen und das Verfahren zur Feststellung und Beurteilung der Nichtanwendbarkeit von Kriterien. So ist unter anderem gefordert, dass nichtanwendbare Kriterien im Zertifikat kenntlich gemacht werden.

Nichtanwendbar sind Kriterien insbesondere dann, wenn der Cloud-Anbieter diese nicht erfüllen kann, weil sie außerhalb seines Verantwortungsbereichs liegen. So wird der Cloud-Anbieter beispielsweise nach Kriterium Nr. 6.1 zur Unterstützung des Cloud-Nutzers bei der Auskunftserteilung verpflichtet. Das Kriterium ist jedoch auf die Datenverarbeitungsvorgänge des Cloud-Anbieters nicht anwendbar und der Cloud-Anbieter somit von der Auskunftserteilung entbunden, wenn der Verantwortungsbereich für die betreffenden Daten beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt. Das gleiche gilt, wenn nicht der Cloud-Anbieter, sondern Subauftragsverarbeiter für den Zugang zu Datenverarbeitungssystemen nach Nr. 2.3 verantwortlich sind. In diesem Fall ist Kriterium Nr. 2.3 auf den Cloud-Anbieter nicht anwendbar. Der Cloud-Anbieter muss sich jedoch davon überzeugen, dass die Subauftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten (siehe Nr. 10.4) und somit ihrerseits das Kriterium Nr. 2.3 erfüllen.

Weiterhin sind Kriterien beispielsweise nicht anwendbar, wenn der Cloud-Anbieter die in den Kriterien adressierten Handlungen nicht vornimmt. Setzt der Cloud-Anbieter beispielsweise keine Subauftragsverarbeiter ein oder findet keine Datenverarbeitung außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums statt, sind die Kriterien aus Kapitel V und VI nicht anwendbar.

C. Kriterien und Umsetzungsempfehlungen für die Auftragsverarbeitung

Kapitel I: Rechtsverbindliche Vereinbarung zur Auftragsverarbeitung

Erläuterung

Der Cloud-Anbieter muss sicherstellen, dass die Leistungen gegenüber dem Cloud-Nutzer aufgrund einer rechtsverbindlichen Vereinbarung[1] erbracht werden, die die gesetzlichen Anforderungen der Datenschutz-Grundverordnung an die Auftragsverarbeitung erfüllt. Die gesetzlichen Anforderungen an diese Vereinbarung werden durch die nachfolgenden Kriterien der Nummern 1.1 bis 1.8 konkretisiert.

Nr. 1 – Wirksame und eindeutige Vereinbarung zwischen Cloud-Anbieter und Cloud-Nutzer (Art. 28 Abs. 3 DSGVO)

Nr. 1.1 – Dienstleistung aufgrund einer rechtsverbindlichen Vereinbarung und Form der Vereinbarung (Art. 28 Abs. 3 Satz 1 und Abs. 9 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch geeignete technische oder organisatorische Vorkehrungen sicher, dass der Dienst erst nach dem Abschluss einer rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung mit dem Cloud-Nutzer erbracht wird.

(2) Diese Vereinbarung muss die Kriterien dieses Kapitels (Nr. 1.1 bis 1.8) erfüllen.

(3) Die rechtsverbindliche Vereinbarung ist schriftlich oder in einem elektronischen Format[2] abzufassen.

Erläuterung

Die rechtsverbindliche Vereinbarung zur Datenverarbeitung im Auftrag ist wesentlich, da mit dieser die Rolle des Cloud-Anbieters als Auftragsverarbeiter i.S.v. Art. 4 Nr. 8 DSGVO gegenüber der Rolle des Cloud-Nutzers als Verantwortlichem ausdrücklich klargestellt wird. Oft liegt dieser Vereinbarung eine weitere Vereinbarung über die Leistungserbringung zugrunde; beide Vereinbarungen sind zu unterscheiden.

Umsetzungshinweis

Der Cloud-Anbieter trifft technische oder organisatorische Vorkehrungen, die einen automatischen Vereinbarungsschluss vor der eigentlichen Dienstnutzung sicherstellen. Hierzu kann dem potentiellen Cloud-Nutzer während der Registrierung eine entsprechende Vereinbarung angezeigt werden, die dieser vor der Dienstnutzung bestätigen muss.

Bei standardisierten Massengeschäften werden in der Regel, auch unter Unternehmern, vorformulierte Vertragsklauseln (Allgemeine Geschäftsbedingungen - AGB) eingesetzt, die wirksam im Sinne des jeweiligen AGB-Rechts zu sein haben.

Nachweis

Der Cloud-Anbieter kann im Rahmen der Zertifizierung alle oder eine repräsentative Stichprobe von rechtsverbindlichen Vereinbarungen vorlegen, die er mit den Cloud-Nutzern schließt. Außerdem kann

---

[1] Art. 28 Abs. 3 Satz 1 DSGVO schreibt die Auftragsverarbeitung auf Grundlage eines Auftragsverarbeitungsvertrags vor. Alternativ zum Vertrag kann auch ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht der Mitgliedstaaten im Sinne des Art. 28 Abs. 3 Satz 1 DSGVO als Rechtsgrundlage für die Auftragsverarbeitung dienen.

[2] Für das elektronische Format reicht die Textform i.S.v. § 126b BGB aus.

er anhand einer geeigneten Dokumentation nachweisen, dass technische oder organisatorische Vorkehrungen getroffen wurden, die eine Dienstnutzung erst nach Abschluss der Vereinbarung sicherstellen.

Nr. 1.2 – Gegenstand und Dauer der Verarbeitung (Art. 28 Abs. 3 Satz 1 DSGVO)

Kriterium

(1) Der Gegenstand und die Dauer des Auftrags sind in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung so konkret wie möglich festzulegen.

(2) Die Vereinbarung muss die Dauer des Auftrages durch einen Start- und Endpunkt oder den Verweis auf eine unbestimmte Nutzungszeit festlegen.

(3) Die Voraussetzungen einer Kündigung sind in die Vereinbarung aufzunehmen.

Umsetzungshinweis

Für beide Parteien sollte anhand dieser Eingrenzung des Auftragsgegenstands klar hervorgehen, welche Verarbeitungsvorgänge oder Verarbeitungskategorien durch den Cloud-Anbieter für den Cloud-Nutzer durchgeführt werden. Insbesondere sollte in transparenter Form dargelegt werden, welche Einflussmöglichkeiten dem Cloud-Anbieter bei der Wahl der Verarbeitungsmittel zur Ausführung von Verarbeitungsvorgängen, in denen personenbezogene Daten verarbeitet werden, zukommen. Regelungen zum Gegenstand des Auftrags sollten auch die abgegrenzten Verantwortungsbereiche zwischen Cloud-Nutzer und Cloud-Anbieter abbilden.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen Entwurf einer rechtsverbindlichen Vereinbarung mit diesen Angaben vorhält und ein Verfahren implementiert hat, wonach die Vereinbarung mit diesen Festlegungen geschlossen wird.

Nr. 1.3 – Art, Umfang und Zwecke der Datenverarbeitung (Art. 28 Abs. 3 Satz 1 DSGVO)

Kriterium

In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung werden der Umfang, die Art und der Zweck der vorgesehenen Verarbeitung von Daten im Auftrag, die Art der verarbeiteten Daten sowie die Kategorien betroffener Personen festgelegt.

Umsetzungshinweis

Diese Einzelangaben müssen zwar nicht jeden konkreten Einzelfall abdecken, sollten jedoch so präzise sein, dass die im Rahmen der Auftragsverarbeitung zulässigen Datenverarbeitungsvorgänge im Einzelnen aus Sicht des Cloud-Nutzers nachvollzogen werden können.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen Entwurf einer rechtsverbindlichen Vereinbarung mit diesen Angaben vorhält und ein Verfahren implementiert hat, wonach die Vereinbarung mit diesen Festlegungen geschlossen wird.

Nr. 1.4 – Festlegung von Weisungsbefugnissen (Art. 28 Abs. 3 Satz 2 lit. a DSGVO)

Kriterium

(1) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung sieht vor, dass die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation – verarbeitet werden.

(2) Wird im Rahmen standardisierter Massengeschäfte keine individuelle rechtsverbindliche Vereinbarung geschlossen, hat der Cloud-Anbieter in seiner Dienstbeschreibung die durch ihn technisch ausführbaren Dienstleistungen auf eine aus der Cloud-Nutzer-Perspektive nachvollziehbare Weise so präzise wie möglich zu benennen, um diesem eine Auswahl nach Art. 28 Abs. 1 DSGVO zu ermöglichen.

Erläuterung

Die Weisungsgebundenheit wird in der Datenschutz-Grundverordnung an mehreren Stellen genannt (Art. 28 Abs. 3 Satz 2 lit. a, 28 Abs. 3 Satz 3; indirekt in Art. 28 Abs. 10 und 29 und 32 Abs. 4 DSGVO).

Überschreitet der Cloud-Anbieter die Maßgaben des Cloud-Nutzers nach dessen Weisungen, so liegt ein Verstoß gegen Art. 28 Abs. 10 und 29 DSGVO vor, und der Cloud-Anbieter hat mit haftungsrechtlichen Konsequenzen zu rechnen.

Umsetzungshinweis

Es sollte aus der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung hervorgehen, wer zur Erteilung von Weisungen befugt ist und wer auf Seiten des Cloud-Anbieters mit der Entgegennahme der Weisungen betraut ist. Die zu Weisungen befugten Abteilungs- und Funktionsebenen können in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung benannt und ihre Authentifizierungsmittel festgelegt werden.

Im der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung oder in vorformulierten Klauseln des Cloud-Anbieters sind die technisch ausführbaren Dienstleistungen und Weisungsbefugnisse des Cloud-Nutzers aufzuführen. Die rechtsverbindliche Vereinbarung sollte die Möglichkeiten darstellen, die dem Cloud-Nutzer zur Ausübung seiner Weisungsbefugnis eingeräumt werden. Diese können insbesondere auch in automatisierten Verfahren bestehen. Anhand einer (im Massengeschäft einseitig vorgegebenen) Dienstbeschreibung des Cloud-Anbieters sollen die potentiellen Cloud-Nutzer eine Auskunft für ihre Auswahl nach Art. 28 Abs. 1 DSGVO erhalten. In diesem Fall weist der Cloud-Nutzer durch die Auswahl des Cloud-Dienstes den Cloud-Anbieter an, die beschriebene, standardisierte Dienstleistung auszuführen.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er entsprechende Regelungen zur Weisungserteilung in rechtsverbindlichen Vereinbarungen offenlegt und vorhandene Dokumentationen von Einzelanweisungen vorzeigt.

Nr. 1.5 – Ort der Datenverarbeitung (indirekt Art. 28 Abs. 3 Satz 2 lit. a DSGVO)

Kriterium

(1) In der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung wird festgelegt, ob sich der Ort der Datenverarbeitung innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums oder in einem Drittland befindet.

(2) Wird die Datenverarbeitung in einem Drittland durchgeführt, ist dieses konkret in der rechtsverbindlichen Vereinbarung zu benennen.

(3) In der rechtsverbindlichen Vereinbarung wird festgelegt, dass in den Fällen, in denen sich während ihres Geltungszeitraums der Ort der Verarbeitung aus Gründen ändert, die im Verantwortungsbereich des Cloud-Anbieters liegen oder für beide Parteien unvorhersehbar sind, der Cloud-Anbieter diese Änderung dem Cloud-Nutzer unverzüglich mitteilt.

(4) Bei jeder wesentlichen Abweichung von der Festlegung des Ortes der Datenverarbeitung wird dem Cloud-Nutzer in der rechtsverbindlichen Vereinbarung ein sofortiges Kündigungsrecht eingeräumt.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen Entwurf einer rechtsverbindlichen Vereinbarung vorhält, in dem er sich verpflichtet, den Cloud-Nutzer unverzüglich über Änderungen des Ortes der Datenverarbeitung zu informieren.

Nr. 1.6 – Verpflichtung zur Vertraulichkeit (Art. 28 Abs. 3 Satz 2 lit. b DSGVO)

Kriterium

Der Cloud-Anbieter verpflichtet sich in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung, dass die zur Verarbeitung von personenbezogenen Daten befugten Personen vor Aufnahme der datenverarbeitenden Tätigkeit zur Vertraulichkeit verpflichtet werden, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen.

Erläuterung

Die Verpflichtung zur Vertraulichkeit und die Belehrung zur Verschwiegenheit fördern das Gewährleistungsziel der Vertraulichkeit (SDM 6.2.3).

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen Entwurf einer rechtsverbindlichen Vereinbarung vorhält, in dem er sich verpflichtet, Mitarbeiter, die zur Verarbeitung von personenbezogenen Daten befugt sind, vor Aufnahme der datenverarbeitenden Tätigkeit zur Vertraulichkeit zu verpflichten, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen.

Nr. 1.7 – Technisch-organisatorische Maßnahmen, Unterbeauftragung und Unterstützung (Art. 28 Abs. 3 Satz 2 lit. c bis f i.V.m. Kap. III und Art. 32 – 36 DSGVO)

Kriterium

(1) Die Schutzklasse und die für sie zu treffenden TOM werden in einer rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt.

(2) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung enthält die Angabe, ob der Cloud-Anbieter oder der Cloud-Nutzer eine Pseudonymisierung, Anonymisierung oder Verschlüsselung (Nr. 2.7, Nr. 2.8 und Nr. 2.9) der zu verarbeitenden personenbezogenen Daten vornimmt und ob diese auch gegenüber den Mitarbeitern des Cloud-Anbieters wirksam sind. Die maximale Anzahl an Personen aus den Mitarbeitern des Cloud Anbieters und seiner Subauftragsverarbeiter sind anzugeben, für die die Pseudonymisierung oder Verschlüsselung nicht wirksam sind.

(3) Der Cloud-Anbieter legt in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung fest, auf welchem Niveau und wie rasch (innerhalb welchen Zeitraums) er nach einem physischen oder technischen Zwischenfall die Daten des Cloud-Nutzers und den Cloud-Dienst wiederherstellen und dem Cloud-Nutzer Zugang zum Cloud-Dienst und zu den Daten gewährleisten kann (Nr. 2.11).

(4) In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung wird bestimmt, wie der Cloud-Anbieter die Bedingungen gemäß Art. 28 Abs. 2 und 4 DSGVO für die Inanspruchnahme der Dienste weiterer Auftragsverarbeiter einhält.

(5) Die Verfahren zur Unterstützung des Cloud-Nutzers bei der Erfüllung der Betroffenenrechte gemäß Nr. 6, bei der Durchführung einer Datenschutz-Folgenabschätzung gemäß Nr. 7 und zur Erfüllung der Meldepflicht bei Datenschutzverletzungen nach Nr. 8.2 werden in der rechtgültigen Vereinbarung über die Auftragsverarbeitung festgelegt.

Umsetzungshinweis

Angaben zur Umsetzung der Kriterien unter Nr. 2 können an Gewährleistungszielen ausgerichtet werden, während die konkreten Maßnahmen der Zielerreichung dem Cloud-Anbieter überlassen werden können. Für den Cloud-Nutzer ist es wichtig zu wissen, welcher Schutzanforderungsklasse der Cloud-Dienst entspricht.

Die Vorgaben des Art. 28 Abs. 3 Satz 2 lit. d DSGVO sollten in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung präzisiert werden, so dass ihre Einhaltung für den Cloud-Nutzer leicht überprüfbar ist.

Da dem Cloud-Nutzer bei Änderungen in der Unterbeauftragung ein Einspruchsrecht zusteht (Nr. 10.3), sollten in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung die Voraussetzungen und Folgen eines Einspruchs geregelt werden, beispielsweise ob der Cloud-Nutzer bei Einspruch die Vereinbarung aufkündigen darf.

Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung soll die Unterstützungspflichten des Cloud-Anbieters unter Berücksichtigung der Ausgestaltung des konkreten Cloud-Dienstes und der dem Cloud-Anbieter zumutbaren und geeigneten TOM konkretisieren. Dies soll Unsicherheiten hinsichtlich der sich aus der Vereinbarung ergebenden Rechte und Pflichten vermeiden.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen Entwurf einer rechtsverbindlichen Vereinbarung mit diesen Angaben vorhält und ein Verfahren implementiert hat, wonach die Vereinbarung mit diesen Festlegungen geschlossen wird.

Nr. 1.8 – Rückgabe von Datenträgern und Löschung von Daten (Art. 28 Abs. 3 Satz 2 lit. g DSGVO)

Kriterium

> Die Pflichten des Cloud-Anbieters zur Rückgabe von Datenträgern, Rückführung von Daten und Löschung von Daten nach Ende der Auftragsverarbeitung sind in einer rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festzulegen.

Erläuterung

Ist der Cloud-Anbieter auch nach Ende der Auftragsverarbeitung aufgrund gesetzlicher Pflichten zur Speicherung oder Aufbewahrung von Daten verpflichtet, sind diese nicht zu löschen. Dies ist entsprechend in der rechtsverbindlichen Vereinbarung zu vermerken.

Umsetzungshinweis

Der Nachweis der Rückgabe von Datenträgern und der Löschung von Daten kann auch durch Verweis auf entsprechende Grundsätze des Cloud-Anbieters erfolgen. Der Cloud-Nutzer kann zwischen den Abwicklungsmodalitäten wählen. Die Pflichten des Cloud-Anbieters entfallen, wenn er eine Pflicht zur Speicherung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten hat.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen Entwurf einer rechtsverbindlichen Vereinbarung mit diesen Festlegungen vorhält und ein Verfahren implementiert hat, wonach die Vereinbarung mit diesen Festlegungen geschlossen wird.

Kapitel II: Rechte und Pflichten des Cloud-Anbieters

Nr. 2 – Gewährleistung der Datensicherheit durch geeignete TOM nach dem Stand der Technik

Nr. 2.1 – Datensicherheitskonzept (Art. 24, 25, 28, 32, 35 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

(1) Der Cloud-Anbieter führt eine Risikoanalyse in Bezug auf die Datensicherheit durch und verfügt über ein Datensicherheitskonzept entsprechend seiner Schutzklasse, das den spezifischen Risiken seiner Datenverarbeitungsvorgänge angemessen ist.

(2) Im Datensicherheitskonzept stellt der Cloud-Anbieter dar, welche Datensicherheitsmaßnahmen er ergriffen hat, um die bestehenden Risiken abzustellen oder einzudämmen. Der Cloud-Anbieter schildert auch die Abwägungen, die er vorgenommen hat, um zu diesen Maßnahmen zu gelangen.

(3) Das Datensicherheitskonzept ist schriftlich zu dokumentieren.

(4) Das Datensicherheitskonzept ist in regelmäßigen Abständen auf Aktualität und Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren.

(5) Das Datensicherheitskonzeptkonzept beschreibt, welche Datenverarbeitungsvorgänge in der Verantwortung des Cloud-Anbieters liegen und für welche Datenverarbeitungsvorgänge eingebundene Subauftragsverarbeiter verantwortlich sind.

(6) Das Datensicherheitskonzept beschreibt, welche Datenverarbeitungsvorgänge in der Verantwortung des Cloud-Anbieters liegen und welche der Verantwortung des Cloud-Nutzers unterliegen.

(7) Soweit das Datensicherheitskonzept Sicherheitsmaßnahmen des Cloud-Nutzers verlangt, sind diese dem Cloud-Nutzer in Schriftform oder in einem elektronischen Format mitzuteilen.

Erläuterung

Der Cloud-Anbieter hat risikoangemessene TOM festzulegen, um Risiken einer Verletzung der Rechte und Freiheiten von natürlichen Personen zu verhindern. Insbesondere hat er Risiken gegen unbeabsichtigte und unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugten Zugang zu personenbezogenen Daten auszuschließen oder zu minimieren. Bei der Festlegung der konkreten Maßnahmen berücksichtigt er nicht nur die Modalitäten der Verarbeitung und die Eintrittswahrscheinlichkeit und Schwere des Schadens, sondern auch den Stand der Technik sowie die Implementierungskosten der Maßnahmen. Die dabei getroffenen Abwägungen müssen aus dem Datensicherheitskonzept ersichtlich sein. Der Cloud-Anbieter legt für seinen angebotenen Dienst die Schutzanforderungsklasse fest. Der Cloud-Nutzer wählt einen Cloud-Dienst aus, der eine zu seiner Schutzbedarfsklasse passende Schutzanforderungsklasse bietet.

Umsetzungshinweis

Das Datensicherheitskonzept soll die sich aus den spezifischen Umständen des Cloud-Dienstes, seiner Datenverarbeitungsvorgänge und Räumlichkeiten ergebenden Risiken abdecken und zu jedem Risiko eine oder gegebenenfalls mehrere Schutzmaßnahmen beinhalten sowie Ressourcen, Verantwortlichkeiten und Priorisierungen für den Umgang mit Informationssicherheitsrisiken spezifizieren. Alle identifizierten Restrisiken des Cloud-Dienstes, die nicht vollständig behandelt werden können, sollten von der Geschäftsleitung des Cloud-Anbieters zur Kenntnis genommen werden. Der Risikobewertungsansatz und die Risikobewertungsmethodik des Cloud-Anbieters sollten dokumentiert werden.

Bei der Analyse von Risiken können folgende Merkmale analysiert und evaluiert werden:

1) Evaluierung der Auswirkungen auf die Organisation, Technik oder Dienstbereitstellung aufgrund eines Sicherheitsausfalls und Berücksichtigung der Konsequenzen des Verlusts von Vertraulichkeit, Integrität oder Verfügbarkeit;

2) Evaluierung der realistischen Wahrscheinlichkeit eines solchen Sicherheitsausfalls unter Berücksichtigung aller denkbaren Bedrohungen und Sicherheitslücken;

3) Abschätzung des möglichen Schadensausmaßes für die Grundrechte und Freiheiten der betroffenen Personen;

4) Prüfung, ob alle möglichen Optionen für die Behandlung der Risiken identifiziert und evaluiert sind;

5) Bewertung, ob das verbleibende Risiko akzeptierbar oder eine Gegenmaßnahme erforderlich ist.

Das Datensicherheitskonzept sollte unter Berücksichtigung neu auftretender Sicherheitsherausforderungen kontinuierlich aktualisiert und verbessert werden. Dabei sollten Risikobewertungen, das mögliche Schadensausmaß und die identifizierten akzeptablen Risiken regelmäßig unter Berücksichtigung des Wandels der Organisation, Technologie, Geschäftsziele und -prozesse, erkannten Bedrohungen, der Auswirkung der implementierten Kontrollen und externen Ereignisse überprüft werden.

Nachweis

Das Datensicherheitskonzept und seine Angemessenheit kann der Cloud-Anbieter dadurch nachweisen, dass er dieses vorlegt.

Nr. 2.2 – Sicherheitsbereich und Zutrittskontrolle (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter stellt durch risikoangemessene TOM sicher, dass Räume und Anlagen gegen Schädigung durch Naturereignisse[3] gesichert werden und Unbefugten der Zutritt zu Räumen und Datenverarbeitungsanlagen verwehrt wird, um unbefugte Kenntnisnahmen personenbezogener Daten und Einwirkungsmöglichkeiten auf die Datenverarbeitungsanlagen auszuschließen.

(2) Die Maßnahmen sind geeignet, um im Regelfall den Zutritt Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert.

Schutzklasse 2

(3) Die Kriterien von Schutzklasse 1 sind erfüllt.

(4) Die Maßnahmen sind geeignet, Schädigungen durch fahrlässige Handlungen Befugter im Regelfall auszuschließen. Weiterhin ist sichergestellt, dass unbefugter Zutritt durch fahrlässige und vorsätzliche Handlungen hinreichend sicher ausgeschlossen ist. Dies schließt Schutz gegen Zutrittsversuche durch Täuschung oder Gewalt ein. Es besteht ein hinreichender Schutz gegen bekannte Angriffsszenarien.

(5) Jeder unbefugte Zutritt und Zutrittsversuch ist nachträglich feststellbar.

Schutzklasse 3

(6) Die Kriterien von Schutzklasse 1 und Schutzklasse 2 sind erfüllt.

(7) Jeder autorisierte Zutritt wird protokolliert.

Erläuterung

Dieses Kriterium konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und 5 Abs. 1 lit. f DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Integrität, Vertraulichkeit

[3] Naturereignisse stellen ungewöhnliche, in der Natur ablaufende Vorgänge dar, die vom Menschen nicht beeinflusst werden können und zeitlich begrenzt sind. Beispiele sind Blitze, Hochwasser, Trockenheit.

und Verfügbarkeit (SDM 6.2.1 – 6.2.3) von personenbezogenen Daten und Diensten auf Dauer zu gewährleisten. Soweit der Cloud-Anbieter für den Sicherheitsbereich und die Zutrittskontrolle zu Räumen und Datenverarbeitungsanlagen verantwortlich ist, benötigt er ein Berechtigungskonzept für den Zutritt zu Datenverarbeitungsanlagen. Die Zutrittskontrolle gewährleistet den Zutrittsschutz nicht nur im Normalbetrieb, sondern auch im Zusammenhang mit Naturereignissen.

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27001 Ziff. A11 und ISO/IEC 27018 Ziff. 11 sind anwendbar.

Um sicherzustellen, dass Unbefugte keinen Zutritt zu Räumen und Datenverarbeitungsanlagen erhalten, sollte der Zutritt ins Rechenzentrum über Videoüberwachungssysteme, Bewegungssensoren, Alarmsysteme und von geschultem Sicherheitspersonal permanent überwacht werden.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Datensicherheitskonzept die TOM zur Zutrittskontrolle darlegt.

Nr. 2.3 – Zugangskontrolle
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter stellt sicher, dass Unbefugte keinen Zugang zu Datenverarbeitungssystemen erhalten und auf diese einwirken können. Dies gilt auch für Sicherungskopien, soweit diese personenbezogene Daten enthalten.

(2) Der Cloud-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zugang zu Datenverarbeitungssystemen in regelmäßigen Abständen auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

(3) Der Cloud-Anbieter überprüft den Zugang von Befugten über das Internet durch eine starke Authentifizierung, die mindestens zwei Elemente der Kategorie Wissen, Besitz oder Inhärenz verwendet. Die Elemente sind voneinander unabhängig, sodass die Überwindung eines Elements die Zuverlässigkeit des anderen nicht beeinflusst. Sie sind so konzipiert, dass die Vertraulichkeit der Authentifizierungsdaten gewährleistet ist. Der Zugang über das Internet erfolgt über einen verschlüsselten Kommunikationskanal.

(4) Die Maßnahmen zur Zugangskontrolle sind geeignet, um im Regelfall den Zugang zu Datenverarbeitungssystemen durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen. Gegen vorsätzliche Eingriffe besteht ein Mindestschutz, der diese erschwert.

Schutzklasse 2

(5) Die Kriterien von Schutzklasse 1 sind erfüllt.

(6) Gegen zu erwartenden vorsätzlichen unbefugten Zugang besteht ein Schutz, der zu erwartende Zugangsversuche hinreichend sicher ausschließt. Dazu gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, die einen unbefugten Zugang im Regelfall nachträglich feststellbar machen.

Schutzklasse 3

(7) Die Kriterien von Schutzklasse 1 und Schutzklasse 2 sind erfüllt.

(8) Der Cloud-Anbieter schließt den unbefugten Zugang zu Datenverarbeitungssystemen hinreichend sicher aus. Dies schließt regelmäßig Maßnahmen zur aktiven Erkennung von Angriffen ein. Jeder unbefugte Zugang und entsprechende Versuche sind nachträglich feststellbar.

Erläuterungen

Das Kriterium der Zugangskontrolle konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele der Integrität, Vertraulichkeit und Verfügbarkeit (SDM 6.2.1 – 6.2.3) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen. Soweit der Cloud-Anbieter für den Zugang zu Datenverarbeitungssystemen verantwortlich ist, benötigt er ein Berechtigungskonzept für den Zugang zu Datenverarbeitungssystemen.

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27001 Ziff. A12.1.4, A12.4.2 und ISO/IEC 27018 Ziff. 9 sind anwendbar.

Die Aufgaben und Rollen zur Wahrung der Informationssicherheit für Datenverarbeitungsvorgänge des Cloud-Anbieters sollten klar definiert und verständlich dokumentiert sein. Alle Anlagen des Cloud-Anbieters sollten korrekt gewartet werden, damit ihre fortgesetzte Verfügbarkeit und Integrität gewährleistet werden können.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Datensicherheitskonzept die TOM zur Zugangskontrolle darlegt.

Nr. 2.4 – Zugriffskontrolle (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter stellt durch TOM sicher, dass Berechtigte nur im Rahmen ihrer Berechtigungen Zugriff auf personenbezogene Daten nehmen können und unbefugte Einwirkungen auf personenbezogene Daten ausgeschlossen werden. Dies gilt auch für Datensicherungen, soweit sie personenbezogene Daten enthalten.

(2) Der Cloud-Anbieter kontrolliert alle Zugriffe auf personenbezogene Daten.

(3) Die Maßnahmen sind geeignet, um im Regelfall den Zugriff auf personenbezogene Daten durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen. Gegen vorsätzliche Eingriffe besteht ein Mindestschutz, der diese erschwert.

(4) Für Zugriffe von Befugten auf personenbezogene Daten über das Internet ist eine starke Authentifizierung erforderlich, die mindestens zwei Elemente der Kategorie Wissen, Besitz oder Inhärenz verwendet, die insofern voneinander unabhängig sind, als die Überwindung eines Elements die Zuverlässigkeit des anderen nicht in Frage stellt, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten gewährleistet ist.

(5) Der Cloud-Anbieter schützt administrative Zugriffe und Tätigkeiten auf kritischen Systemen durch einen starken Authentisierungsmechanismus und protokolliert diese. Die Fernadministration des Cloud-Dienstes durch Mitarbeiter des Cloud-Anbieters erfolgt über einen verschlüsselten Kommunikationskanal.

(6) Ist ein privilegierter Zugriff der Mitarbeiter des Cloud-Anbieters auf personenbezogene Daten auf Weisung im Cloud-Dienst vorgesehen, ist dieser eindeutig geregelt und dokumentiert. Die privilegierten Zugriffe weisen eine andere Nutzeridentität auf als die Zugriffe für die tägliche Arbeit.

Schutzklasse 2

(7) Die Kriterien von Schutzklasse 1 sind erfüllt.

(8) Zu erwartende vorsätzliche unbefugte Zugriffe sind hinreichend sicher ausgeschlossen. Dazu gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die ein unberechtigter Zugriff im Regelfall nachträglich festgestellt werden kann.

(9) Der Cloud-Anbieter stellt sicher, dass der Cloud-Nutzer verschiedene zweckbezogene Nutzerrollen für seine Mitarbeiter festlegt, um nicht zweckgemäße Zugriffe auf personenbezogene Daten logisch auszuschließen.

(10) Ist ein privilegierter Zugriff der Mitarbeiter des Cloud-Anbieters auf personenbezogene Daten auf Weisung vorgesehen, ist dieser eindeutig zu regeln und zu dokumentieren. Der privilegierte Zugriff darf nur in Rollen erfolgen, die von der Administration und vom Rechenzentrumsbetrieb unabhängig sind. Der Zugriff ist mit Zwei-Faktor-Authentifizierung abzusichern und die Anzahl der Mitarbeiter mit privilegiertem Zugriff ist so gering wie möglich zu halten.

Schutzklasse 3

(11) Die Kriterien von Schutzklasse 1 und Schutzklasse 2 sind erfüllt.

(12) Unbefugte Zugriffe auf Daten sind hinreichend sicher ausgeschlossen. Dies schließt regelmäßig Maßnahmen zur aktiven Erkennung von Angriffen ein. Jeder unbefugte Zugriff und entsprechende Versuche ist nachträglich feststellbar.

Erläuterungen

Das Kriterium der Zugriffskontrolle konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Integrität, Vertraulichkeit und Verfügbarkeit (SDM 6.2.1 – 6.2.3) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen. Dies setzt ein Berechtigungskonzept für den Zugriff auf personenbezogenen Daten voraus.

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27002 Ziff. 13.2 und ISO/IEC 27018 Ziff. 9.2, 9.2.1, 9.4.2 sind anwendbar.

Berechtigungskonzepte müssen sowohl für die Nutzer des Dienstes als auch für die Mitarbeiter des Cloud-Anbieters bestehen.

Ein geeigneter Managementprozess für die Zugriffskontrolle sollte etabliert werden, der die Erforderlichkeit der Berechtigungen in regelmäßigen Abständen auf Angemessenheit überprüft, die Vergabe, Aktualisierung, Kontrolle und den Entzug von Berechtigungen regelt, Zugriffspolitiken überwacht und aktualisiert sowie Passwortrichtlinien überprüft und die Einhaltung sicherstellt.

Es sollten angemessene Sicherheitsmaßnamen gegen sowohl interne auch gegen externe Angriffe implementiert werden, um einen unbefugten Zugriff zu verhindern. Hierzu zählen beispielsweise sämtliche Standardmaßnahmen für den Schutz des Cloud-Hosts, d. h. Host Firewalls, Network-Intrusion-Prevention-Systeme, Applikationsschutz, Antivirus, regelmäßige Integritätsüberprüfungen wichtiger Systemdateien und Host-based Intrusion-Detection-Systeme. Der Cloud-Dienst sollte ununterbrochen auf Angriffe und Sicherheitsvorfälle überwacht werden, um verdächtige Aktivitäten (z.B. Extraktion großer Datenmengen mehrerer Mandanten), Angriffe und Sicherheitsvorfälle rechtzeitig erkennen und angemessene und zeitnahe Reaktionen einleiten zu können.

Um vorsätzliche Eingriffe auf Datenverarbeitungsvorgänge durch Mitarbeiter zu erschweren, ist der Kreis der Berechtigten klein zu halten und sind Zugriffsberechtigungen restriktiv zu vergeben. Mitarbeiter sollten nur Zugriff auf die Daten und Datenverarbeitungsvorgänge haben, die sie für ihre Aufgabenerledigung benötigen. Eine weitere Maßnahme, um vorsätzliche Eingriffe durch Mitarbeiter zu erschweren, kann die Implementierung eines Vier-Augen-Prinzips sein, das bestimmte Aktionen an Datenverarbeitungsvorgängen nur zulässt, wenn mindestens ein weiterer Mitarbeiter der Aktion zugestimmt hat. Um Zugriffe durch befugte Mitarbeiter nachträglich nachverfolgen zu können, sind die Zugriffe zu protokollieren.

Sämtliche relevanten Sicherheitsereignisse einschließlich aller Sicherheitslücken oder -vorfälle sollten erfasst, protokolliert, revisionssicher archiviert und ausgewertet werden. Ein handlungsfähiges Team für Security-Incident-Handling und Trouble-Shooting sollte ununterbrochen erreichbar sein, damit Sicherheitsvorfälle gemeldet und zeitnah bearbeitet werden können.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Datensicherheitskonzept die TOM zur Zugriffskontrolle darlegt.

Nr. 2.5 – Übertragung von Daten und Transportverschlüsselung (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f und Abs. 2 DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter setzt bei Datenübertragungsvorgängen eine Transportverschlüsselung nach dem Stand der Technik oder gleichermaßen angemessene Maßnahmen ein oder fordert dies durch entsprechende Konfiguration von Schnittstellen. Die eingesetzte Transportverschlüsselung muss gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

(2) Die Maßnahmen sind geeignet, im Regelfall Angriffe Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen. Die Maßnahmen sind ferner geeignet, die fahrlässige Weitergabe von Daten an Unbefugte durch den Cloud-Anbieter und seine Mitarbeiter auszuschließen. Gegen vorsätzliche Eingriffe besteht ein Mindestschutz, der diese erschwert. Bei verschlüsselter Übertragung sind die Schlüssel sicher aufzubewahren.

(3) Der Cloud-Anbieter protokolliert automatisiert die Metadaten aller Datenübertragungsvorgänge, einschließlich der Empfänger, auch solche vom und an den Cloud-Nutzer oder an Subauftragsverarbeiter.

(4) Die Anforderungen dieses Kriteriums gelten auch für die Übertragung von Daten im eigenen Netzwerk des Cloud-Anbieters und seiner Subauftragsverarbeiter und zwischen diesen.

(5) Der Cloud-Anbieter schützt den Transport von Datenträgern mit TOM, sodass personenbezogene Daten beim Transport der Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Der Cloud-Anbieter dokumentiert die Transporte.

Schutzklasse 2

(6) Die Kriterien von Schutzklasse 1 sind erfüllt.

(7) Der Cloud-Anbieter schützt die Daten gegen vorsätzliches unbefugtes Lesen, Kopieren, Verändern oder Entfernen und schließt zu erwartende Versuche hinreichend sicher aus. Zu den Schutzmaßnahmen gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen im Regelfall (nachträglich) festgestellt werden kann.

Schutzklasse 3

(8) Die Kriterien von Schutzklasse 1 und Schutzklasse 2 sind erfüllt.

(9) Cloud-Anbieter schließt unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Daten hinreichend sicher aus. Er ergreift regelmäßig Maßnahmen zur aktiven Erkennung und Abwehr von Angriffen und stellt jedes unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten und auch jeden entsprechenden Versuch nachträglich fest. Bei verschlüsselter Übertragung stellt er durch TOM sicher, dass weder er noch seine Mitarbeiter Zugriff auf die Schlüssel haben.

Erläuterungen

Das Kriterium der Übertragungs- und Transportkontrolle konkretisiert die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Integrität, Vertraulichkeit und Verfügbarkeit (SDM 6.2.1 – 6.2.3) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen und personenbezogene Daten gegen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugten Zugang oder unbefugte Offenlegung während der elektronischen Übertragung, des Transports oder der Speicherung auf Datenträgern zu schützen.

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27018 Ziff. 10.1.1, A.10.6, A.10.9, ISO/IEC 27002 Ziff. 12.4, ISO/IEC 27040:2017-03 Ziff. 6.7.1 und ISO/IEC 27040:2017-03 Ziff. 7.7.1 sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Datensicherheitskonzept die TOM zur Übertragungskontrolle darlegt.

Nr. 2.6 – Nachvollziehbarkeit der Datenverarbeitung (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. c, e, f und Abs. 2 DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter protokolliert Eingaben, Veränderungen und Löschungen personenbezogener Daten, die bei der bestimmungsgemäßen Nutzung des Cloud-Dienstes durch den Cloud-Nutzer oder bei administrativen Maßnahmen des Cloud-Anbieters erfolgen, um eine nachträgliche Prüfbarkeit und Nachvollziehbarkeit der Datenverarbeitung sicherzustellen. Er beachtet bei Protokollierungen die Grundsätze der Erforderlichkeit, Zweckbindung und Datenminimierung. Er bewahrt die Protokolldaten sicher auf.

(2) Der Cloud-Anbieter gestaltet die Protokollierung so, dass die Nachvollziehbarkeit von Eingaben, Veränderungen und Löschungen im Regelfall auch bei technischen oder organisatorischen Fehlern, einschließlich Bedienfehlern des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässige Handlungen des Cloud-Nutzers oder Dritter gewahrt bleibt. Er sieht einen Mindestschutz gegen vorsätzliche Manipulationen an den Maßnahmen zur Nachvollziehbarkeit vor, der solche Manipulationen erschwert.

Schutzklasse 2

(3) Die Kriterien von Schutzklasse 1 sind erfüllt.

(4) Der Cloud-Anbieter sieht gegen zu erwartende vorsätzliche Manipulationen der Protokollierungsinstanzen und gegen vorsätzliche Zugriffe auf oder Manipulationen von Protokollierungsdateien (Logs) durch Unbefugte einen Schutz vor, der zu erwartende Manipulationsversuche hinreichend und sicher ausschließt. Zu diesen Schutzmaßnahmen gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die eine Manipulation im Regelfall (nachträglich) festgestellt werden kann.

Schutzklasse 3

(5) Die Kriterien von Schutzklasse 1 und Schutzklasse 2 sind erfüllt.

(6) Der Cloud-Anbieter schließt Manipulationen von Protokollierungsinstanzen und -dateien (Logs) hinreichend sicher aus. Er ergreift regelmäßig Maßnahmen zur aktiven Erkennung von Manipulationen und stellt jede Manipulation und möglichst auch jeden entsprechenden Versuch nachträglich fest.

Erläuterung

Das Kriterium der Nachvollziehbarkeit konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Integrität, Vertraulichkeit und Verfügbarkeit (SDM 6.2.1 – 6.2.3) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen und personenbezogene Daten gegen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugten Zugang oder unbefugte Offenlegung zu schützen. Hierzu muss nachträglich überprüft und festgestellt werden können, ob, wann und von wem und mit welchen inhaltlichen Auswirkungen personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, um gegebenenfalls Zugriffsrechte für die Zukunft anders zu gestalten. Zur sicheren Aufbewahrung der Protokolldaten gehört auch, dass die Auswertbarkeit der Protokolldaten sichergestellt ist.

Da im Rahmen von Protokollierungen regelmäßig personenbezogene Daten anfallen, unterliegt der Umgang mit Protokollierungsdaten ebenfalls datenschutzrechtlichen Anforderungen. Auf die Datenschutzgrundsätze aus Art. 5 DSGVO wird Bezug genommen. Auf das Gewährleistungsziel der Datenminimierung und der Zweckbindung aus Art. 5 Abs. 1 lit. c und b DSGVO ist besonderes Augenmerk zu legen.

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27018 Ziff. 12.4.1, 12.4.2 und ISO/IEC 27002 Ziff. 12.4 sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Datensicherheitskonzept dokumentiert, wie er durch Festlegung von Gegenstand und Umfang der Protokollierung, Aufbewahrung und Verwendung der Protokolldaten, Integritätsschutz und Löschung von Protokollen, die Datenschutzziele sicherstellt.

Nr. 2.7 – Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter ermöglicht es dem Cloud-Nutzer, Daten zu verarbeiten, die der Cloud-Nutzer pseudonymisiert überträgt.

Schutzklasse 2 und 3

(2) Der Cloud-Anbieter stellt sicher, dass die Daten pseudonymisiert verarbeitet werden. Entsprechend der rechtsverbindlichen Vereinbarung (Nr. 1.7) pseudonymisiert der Cloud-Nutzer die personenbezogenen Daten selbst oder der Cloud-Anbieter führt die Pseudonymisierung auf Weisung des Cloud-Nutzers durch.

(3) Wird die Pseudonymisierung vom Cloud-Anbieter durchgeführt, so stellt dieser sicher, dass die zusätzlichen Informationen zur Identifizierung der betroffenen Person gesondert aufbewahrt werden. Der Datensatz mit der Zuordnung des Kennzeichens zu einer Person muss so geschützt werden, dass zu erwartende Manipulationsversuche hinreichend und sicher ausgeschlossen werden.

(4) Erfordert die Art des Auftrags mit dem Cloud-Nutzer die De-Pseudonymisierung der Daten, stellt der Cloud-Anbieter sicher, dass die De-Pseudonymisierung nur auf dokumentierte Weisung des Cloud-Nutzers erfolgt.

(5) Der Cloud-Anbieter gewährleistet, dass er die technische Entwicklung im Bereich der Pseudonymisierungsverfahren laufend verfolgt und seine Verfahren den aktuellen technischen Empfehlungen (best practice) entsprechen.

Erläuterung

In Schutzklasse 1 muss der Cloud-Anbieter, sofern er personenbezogene Daten des Cloud-Nutzers verarbeitet, selbst keinen Pseudonymisierungsdienst anbieten, wohl aber pseudonyme Daten unter Wahrung der Pseudonymität verarbeiten.

Die Pseudonymisierung wird neben der Verschlüsselung in Art. 32 Abs. 1 lit. a DSGVO explizit als einzusetzende Sicherheitsmaßnahme benannt. Sie trägt dazu bei, das Gewährleistungsziel der Nichtverkettung (SDM 6.2.4) zu fördern. Da durch Pseudonymisierung Dritte selbst bei einem unbefugten Zugriff auf den Cloud-Dienst keine Kenntnis von den personenbezogenen Daten erlangen können oder der Personenbezug zumindest erheblich erschwert wird, mindert die Pseudonymisierung die Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen.

Umsetzungshinweis

Der Cloud-Nutzer hat zu prüfen, ob es bereichsspezifische oder generische technische Standards für die Pseudonymisierung gibt, die als verpflichtend vorgeschrieben sind oder empfohlen werden. Der Cloud-Anbieter sollte öffentlich bekannt geben, welche dieser technischen Standards sein Pseudonymisierungsverfahren erfüllt. Beispielsweise kann zur Pseudonymisierung in der medizinischen Informatik DIN EN ISO 25237 herangezogen werden.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Datensicherheitskonzept dokumentiert, wie er selbst Pseudonymisierungen durchführt, Identifizierungsdaten sicher aufbewahrt und pseudonymisierte Daten verarbeitet.

Nr. 2.8 – Anonymisierung (Art. 5 Abs. 1 lit. c DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter ermöglicht es dem Cloud-Nutzer, anonyme Daten zu verarbeiten.

Schutzklasse 2 und 3

(2) Soweit mit dem Cloud-Nutzer vereinbart (Nr. 1.7), stellt der Cloud-Anbieter sicher, dass die Daten anonymisiert verarbeitet werden. Entsprechend der rechtsverbindlichen Vereinbarung anonymisiert der Cloud-Nutzer die personenbezogenen Daten selbst oder der Cloud-Anbieter auf Weisung.

(3) Wird die Anonymisierung vom Cloud-Anbieter durchgeführt, so gewährleistet er, dass er die technische Entwicklung im Bereich der Anonymisierungsverfahren laufend verfolgt und seine Verfahren den aktuellen technischen Empfehlungen (best practice) entsprechen. Die Anonymisierung muss nach dem Stand der Technik eine Re-Identifizierung der betroffenen Person ausschließen.

Erläuterung

In Schutzklasse 1 muss der Cloud-Anbieter, sofern er personenbezogene Daten des Cloud-Nutzers verarbeitet, selbst keinen Anonymisierungsdienst anbieten, wohl aber anonyme Daten unter Wahrung der Anonymität verarbeiten.

Die Anonymisierung ist neben dem Verzicht der Datenerhebung die wirksamste Maßnahme zur Datenvermeidung und Datenminimierung. Sie trägt dazu bei, das Gewährleistungsziel der Datenminimierung (SDM 7.1) zu fördern.

Umsetzungshinweis

Der Cloud-Nutzer sollte prüfen, ob es bereichsspezifische technische Standards für die Anonymisierung gibt, die als verpflichtend vorgeschrieben sind oder empfohlen werden. Der Cloud-Anbieter sollte öffentlich bekannt geben, welche dieser technischen Standards sein Anonymisierungsverfahren erfüllt.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Datensicherheitskonzept dokumentiert, wie er selbst Anonymisierungen durchführt und anonymisierte Daten verarbeitet.

Nr. 2.9 – Verschlüsselung gespeicherter Daten (Art. 32 Abs. 1 lit. a DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter ermöglicht dem Cloud-Nutzer die Speicherung von verschlüsselten Daten.

Schutzklasse 2

(2) Sofern der Cloud-Anbieter personenbezogene Daten des Cloud-Nutzers speichert, bietet er Verschlüsselungsverfahren an, um dem Cloud-Nutzer die Speicherung von verschlüsselten Daten zu ermöglichen oder auf dessen Weisung hin, die Daten selbst zu verschlüsseln.

(3) Der Cloud-Anbieter verfolgt laufend die technische Entwicklung im Bereich der Verschlüsselung. Die von ihm getroffenen Maßnahmen entsprechen den aktuellen technischen Empfehlungen (best practice).

(4) Der Cloud-Anbieter prüft fortdauernd die Eignung seiner Verschlüsselungsverfahren und aktualisiert diese bei Bedarf.

(5) Der Cloud-Anbieter überprüft die angemessene Implementierung seiner Verschlüsselungsverfahren durch geeignete Tests und dokumentiert diese.

Schutzklasse 3

(6) Auf Weisung des Cloud-Nutzers unterstützt der Cloud-Anbieter diesen bei der Verschlüsslung und Entschlüsselung der Daten. Die Unterstützung erfolgt in Form von Dokumentationen und Hilfsmaßnahmen zur Durchführung von Verschlüsselung, ohne dass der Cloud-Anbieter den Schlüssel kennen kann.

(7) Der Cloud-Anbieter verfolgt die technische Entwicklung im Bereich der Verschlüsselung und hält seine unterstützenden Maßnahmen in Form von Dokumentationen und Hilfsmaßnahmen zur Durchführung von Verschlüsselung auf dem Stand der aktuellen technischen Empfehlungen (best practice).

Erläuterung

In Schutzklasse 1 muss der Cloud-Anbieter, sofern er personenbezogene Daten des Cloud-Nutzers speichert, kein Verfahren zur Verschlüsselung anbieten, wohl aber verschlüsselte Daten unter Wahrung der Verschlüsselung speichern.

In Schutzklasse 3 verschlüsselt der Cloud-Nutzer die Daten selbst. Daher liegt es auch in seiner Verantwortung, die Schlüssel sicher aufzubewahren.

Die Verschlüsselung wird neben der Pseudonymisierung in Art. 32 Abs. 1 lit. a DSGVO explizit als eine einzusetzende Sicherheitsmaßnahme benannt. Zweck der Verschlüsselung ist es, die Gewährleistungsziele der Vertraulichkeit und Integrität (SDM 6.2.2 und 6.2.2) sicherzustellen. Die Schwelle, ab der zu verschlüsseln ist, ist niedrig, sodass personenbezogene Daten bereits bei niedrigem Risiko verschlüsselt werden sollten, soweit dies möglich ist.

Umsetzungshinweis

Der Stand der Technik ergibt sich aus aktuellen technischen Normen für kryptographische Verfahren und deren Anwendung. Die Umsetzungshinweise aus ISO/IEC 27018 Ziff. 10 und ISO/IEC 27002, Z. 10 sind anwendbar.

Soweit der Cloud-Anbieter Daten verschlüsselt, sollte die Schlüsselerzeugung in einer sicheren Umgebung und unter Einsatz geeigneter Schlüsselgeneratoren erfolgen. Kryptografische Schlüssel sollten möglichst nur einem Einsatzzweck dienen und generell nie in klarer Form, sondern grundsätzlich verschlüsselt im System gespeichert werden. Die Speicherung muss stets redundant gesichert und wiederherstellbar sein, um einen Verlust eines Schlüssels auszuschließen. Schlüsselwechsel müssen regelmäßig durchgeführt werden. Der Zugang zum Schlüsselverwaltungssystem sollte eine separate Authentisierung erfordern. Cloud-Administratoren dürfen keinen Zugriff auf Nutzerschlüssel haben.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Datensicherheitskonzept dokumentiert, dass die angebotenen und angewandten Verschlüsselungsverfahren den aktuellen technischen Anforderungen entsprechen. Er legt Prozessdokumentationen vor, wie er die technische Entwicklung im Bereich der Verschlüsselung verfolgt und die Geeignetheit des Verfahrens fortdauernd prüft und es gegebenenfalls aktualisiert. Er weist in seinem Datensicherheitskonzept nach, dass er bei Diensten der Schutzklasse 2 die Verschlüsselungstechniken durch geeignete technische Tests geprüft hat.

Nr. 2.10 – Getrennte Verarbeitung (Art. 5 Abs. 1 lit. b i.V.m. Art. 24, 25, 32 Abs. 1 lit. b und Abs. 2 DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter verarbeitet die Daten des Cloud-Nutzers logisch oder physisch getrennt von den Datenbeständen anderer Cloud-Nutzer und von anderen Datenbeständen des Cloud-Anbieters und ermöglicht dem Cloud-Nutzer, die Datenverarbeitung nach verschiedenen Verarbeitungszwecken zu trennen (sichere Mandantentrennung).

(2) Die Datentrennung muss im Regelfall auch bei technischen oder organisatorischen Fehlern, einschließlich Bedienfehlern, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter gewahrt sein. Der Cloud-Anbieter realisiert einen Mindestschutz, der vorsätzliche Verstöße gegen das Trennungsgebot verhindert.

Schutzklasse 2

(3) Die Kriterien von Schutzklasse 1 sind erfüllt.

(4) Der Cloud-Anbieter bietet gegen zu erwartende vorsätzliche Verstöße einen Schutz, der diese hinreichend sicher ausschließt. Dazu gehören im Rahmen der Datenspeicherung die Verschlüsselung mit individuellen Schlüsseln und die Verwendung getrennter Betriebsumgebungen für verschiedene Verarbeitungen oder der Einsatz gleichwertiger Verfahren. Der Cloud-Anbieter kann vorsätzliche Verstöße gegen das Trennungsgebot im Regelfall (nachträglich) feststellen, z.B. durch Protokollierung der Zugriffe.

Schutzklasse 3

(5) Die Kriterien von Schutzklasse 1 und Schutzklasse 2 sind erfüllt.

(6) Der Cloud-Anbieter schließt eine Verletzung der Datentrennung hinreichend sicher aus. Dazu gehören im Rahmen der Datenspeicherung die Verschlüsselung mit getrennten Schlüsseln und die Verwendung getrennter Betriebsumgebungen für verschiedene Verarbeitungen oder der Einsatz gleichwertiger Verfahren. Er betreibt ein Verfahren zur Erkennung von vorsätzlichen Verstößen gegen die getrennte Verarbeitung.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Verfügbarkeit, Integrität, Vertraulichkeit und Nichtverkettung (SDM 6.2.1 – 6.2.4) und zielt damit auch auf die Sicherstellung des Zweckbindungsgrundsatzes aus Art. 5 Abs. 1 lit. b DSGVO. Eine sichere Mandantentrennung schützt die Daten vor unbefugtem Zugang, Veränderungen und Vernichtung und verhindert eine unerwünschte Verkettung der Daten.

Hinsichtlich der Trennung der Datenverarbeitung nach verschiedenen Verarbeitungszwecken ist zu beachten, dass der Cloud-Anbieter lediglich die technische Möglichkeit der getrennten Verarbeitung bieten muss, während die Umsetzung der getrennten Datenverarbeitung nach Verarbeitungszwecken dem Cloud-Nutzer obliegt.

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27002 Ziff. 12.1.4, 13.1.3 sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Datensicherheitskonzept dokumentiert, welche TOM er ergriffen hat, um die Daten unterschiedlicher Nutzer voneinander zu trennen und die Daten eines Nutzers nach den Verarbeitungszwecken trennen zu können.

Nr. 2.11– Wiederherstellbarkeit nach physischem oder technischem Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch risikoangemessene TOM sicher, dass nach einem physischen oder technischen Zwischenfall der Cloud-Dienst und die Daten so rasch wiederhergestellt werden und verfügbar sind, wie es in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung vereinbart ist. Hierbei wird zwischen den Wiederherstellbarkeitsklassen 1, 2 und 3 unterschieden:

Wiederherstellbarkeitsklasse 1

Der Cloud-Anbieter sichert seinen Dienst gegen zu erwartende, naheliegende Ereignisse so zuverlässig ab, dass diese Risiken bei normalem Verlauf nicht zu einem Ausfall des Cloud-Dienstes oder einem endgültigen Datenverlust führen. Ereignisse sind zu erwartend und naheliegend, wenn sie nicht vorkommen sollen, nach der Lebenserfahrung aber trotz hinreichender Vorsicht nicht ausgeschlossen werden können, wie etwa Unfälle im Straßenverkehr oder der technische Defekt von Hardware.

Wiederherstellbarkeitsklasse 2

Der Cloud-Anbieter sichert seinen Dienst gegen seltene Ereignisse so zuverlässig ab, dass diese Risiken bei normalem Verlauf der Datenverarbeitung nicht zu einem Ausfall des Cloud-Dienstes oder einem endgültigen Datenverlust führen. Ereignisse sind selten, wenn sie nicht vorkommen sollen und nach der Lebenserfahrung bei hinreichender Vorsicht wenig wahrscheinlich, aber gleichwohl in einigen Fällen zu beobachten sind, wie etwa „Jahrhunderthochwasser“ oder gezielte, umfangreiche Angriffe auf den Cloud-Dienst oder ein plötzlich erhöhtes Zugriffsvolumen.

Widerherstellbarkeitsklasse 3

Der Cloud-Anbieter gewährleistet für seinen Dienst einen hohen Schutz zu, der außergewöhnliche, aber nicht als theoretisch auszuschließende Ereignisse so zuverlässig absichert, dass diese Risiken bei normalem Verlauf der Datenverarbeitung nicht zu einem Ausfall des Cloud-Dienstes oder einem endgültigen Datenverlust führen. Ereignisse sind außergewöhnlich, aber nicht als theoretisch auszuschließen, wenn sie nicht vorkommen sollen und nach der Lebenserfahrung nicht auftreten, aber gleichwohl in extrem seltenen Einzelfällen zu beobachten sind, wie etwa „Black Swan“-Ereignisse oder ein unkontrollierbarer Blitzeinschlag ins Rechenzentrum.

(2) Der Cloud-Anbieter stellt dem Cloud-Nutzer sein Konzept der geeigneten TOM auf Anfrage zur Verfügung.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Verfügbarkeit (SDM 6.2.1). Gemäß Art. 32 Abs. 1 lit. c DSGVO muss die Wiederherstellung „rasch“ erfolgen. Was als „rasch“ gilt, hängt auch von der Schwere des Zwischenfalls und der Bedeutung der Systeme und Daten ab. Der Cloud-Nutzer muss wählen können, welcher Wiederherstellungszeitraum ihm ausreicht. Z.B. sind an die Wiederherstellbarkeit des Dienstes und der Daten im Krankenhaus strengere Anforderungen zu stellen als an die im Datenarchiv.

Da die Verfügbarkeit von Diensten und personenbezogenen Daten nicht notwendigerweise mit ihrer Schutzbedürftigkeit nach dem Schutzklassenkonzept zusammenfallen muss, sondern auf der Seite des Cloud-Nutzers auch das Erfordernis bestehen kann, dass personenbezogene Daten der Schutzklasse 1 nach einem physischen oder technischen Zwischenfall sehr schnell wiederhergestellt sein müssen, wird bei diesem Kriterium nicht nach den Schutzklassen unterschieden. Stattdessen wird die Möglichkeit der Wiederherstellung in den Wiederherstellbarkeitsklassen 1, 2 und 3 ausgedrückt. Für eine Differenzierung spricht auch, dass es bei der Wiederherstellung nach einem physischen oder technischen Zwischenfall nicht wie bei den anderen Kriterien der Nummer 2 um den Normalbetrieb geht, sondern um physische oder technische Störfälle.

Als Ereignisse gelten Naturereignisse, Störungen der Infrastruktur sowie Betriebsstörungen, Bedienungsfehler oder vorsätzliche Eingriffe.

Umsetzungshinweis

Zur Wiederherstellung von Daten und Systemen sollte ein Cloud-Anbieter ein wirksames Datensicherungskonzept erstellen, in dem er Systeme zu Datensicherungen, ein Notfallmanagement, Pläne zur Wiederherstellung und zur Schadensbegrenzung sowie einen Plan zur regelmäßigen Überprüfung und Aktualisierung der vorgesehenen Maßnahmen vorsieht.

Es sollten regelmäßig Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß einem Datensicherungskonzept angefertigt werden. Hierin sollten auch Aufbewahrungs- und Schutzanforderungen festgelegt werden. Für die Aufstellung eines Datensicherungskonzepts sind die Umsetzungshinweise aus ISO/IEC 27018 Ziff. 12.3.1, A.10.3 anwendbar.

Die Datensicherungsstrategien und -maßnahmen des Datensicherungskonzepts sollten für Cloud-Nutzer transparent definiert werden, sodass alle Informationen nachvollziehbar sind, einschließlich Umfang, Speicherintervallen, Speicherzeitpunkten und Speicherdauern.

Neben der Erstellung von Sicherheitskopien sollte der Cloud-Anbieter ein Notfallmanagement mit entsprechenden Notfallplänen etablieren. Dabei gilt es unter anderem, mögliche Unterbrechungen zu identifizieren und zu bewerten, sodass Pläne zur Wiederherstellung und Schadensbegrenzung entwickelt und im Notfall eingesetzt werden können. Die entwickelten Notfallpläne sind fortlaufend zu aktualisieren und auf ihre Wirksamkeit zu testen, um bei einem Eintritt einer Unterbrechung eine möglichst schnelle Reaktion sicherzustellen.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Datensicherheitskonzept dokumentiert, welche Wiederherstellbarkeitszeiten sein Dienst bietet, mit welchen Ereignissen er sich auseinandergesetzt hat, die zu einem physischen, organisatorischen oder technischen Zwischenfall führen können, und welche konkreten Maßnahmen zur Wiederherstellbarkeit der Daten nach einem Zwischenfall er ergriffen hat.

Nr. 3 – Sicherstellung der Weisungsbefolgung (Art. 28 Abs. 3 Satz 2 lit. a; 29 DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter führt die Datenverarbeitung im Auftrag ausschließlich auf dokumentierte Weisung des Cloud-Nutzers aus.

(2) Der Cloud-Anbieter gewährleistet, dass die Verarbeitung der Daten des Cloud-Nutzers nur nach Maßgabe der Weisungen des Cloud-Nutzers erfolgt. Er schließt im Regelfall Abweichungen von den Weisungen aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter aus. Gegen vorsätzliche Manipulationen von Weisungen ist ein Mindestschutz vorzusehen, der diese erschwert.

(3) Im Rahmen von standardisierten Massengeschäften gewährleistet der Cloud-Anbieter die Einhaltung einer konkreten und nachvollziehbaren Dienstbeschreibung zu den von ihm technisch ausführbaren Dienstleistungen, sodass der Cloud-Nutzer den Cloud-Anbieter durch seine Auswahl für eine Auftragsverarbeitung anweisen kann. Zudem ermöglicht er dem Cloud-Nutzer, Weisungen mittels Softwarebefehlen zu erteilen, die automatisiert ausgeführt und dokumentiert werden.

Schutzklasse 2

(4) Die Kriterien von Schutzklasse 1 sind erfüllt.

(5) Der Cloud-Anbieter schließt ein Abweichen von den Weisungen durch zu erwartende vorsätzliche Eingriffe hinreichend sicher aus und stellt Eingriffe im Regelfall (nachträglich) fest.

Schutzklasse 3

(6) Die Kriterien von Schutzklasse 1 und Schutzklasse 2 sind erfüllt.

(7) Der Cloud-Anbieter schließt Abweichungen von den Weisungen des Cloud-Nutzers hinreichend sicher aus, und protokolliert fortlaufend und umfassend Administratorenzugriffe.

Umsetzungshinweis

Der Cloud-Anbieter unterweist alle Mitarbeiter, deren Tätigkeiten im Zusammenhang mit der Verarbeitung von personenbezogenen Daten stehen, in die vertraglich dokumentierten Weisungen (Art. 29 DSGVO) und stellt auch in einer etwaigen Datenverarbeitungskette die Weisungsbefolgung sicher. Der Cloud-Anbieter hat regelmäßig zu kontrollieren, ob die Weisungen des Cloud-Nutzers eingehalten werden.

In der Praxis werden Weisungen des Cloud-Nutzers insbesondere mittels Softwarebefehlen automatisiert ausgeführt (z.B. durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeileneingabe), weshalb diese Nutzerinteraktionen auch automatisiert protokolliert oder dokumentiert werden sollten.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Datensicherheitskonzept dokumentiert, wie er Weisungen des Cloud-Nutzers empfängt, umsetzt und dokumentiert. Bei Massengeschäften erbringt der Cloud-Anbieter den Nachweis über seine konkrete Dienstbeschreibung zu seinen technisch ausführbaren Dienstleistungen und den Nachweis zur Ausführbarkeit von Weisungen durch Softwarebefehle in Form einer technischen Dokumentation oder durch Dienstnutzung.

Nr. 4 – Hinweispflicht des Cloud-Anbieters

Nr. 4.1 – Weisungen entgegen datenschutzrechtlicher Vorschriften (Art. 28 Abs. 3 Satz 3 i.V.m Art. 29 DSGVO)

Kriterium

Der Cloud-Anbieter informiert den Cloud-Nutzer unverzüglich, wenn er der Ansicht ist, dass eine Weisung des Cloud-Nutzers gegen datenschutzrechtliche Vorschriften verstößt.

Erläuterung

Die Verantwortung für die Konformität einer Weisung mit dem geltenden Datenschutzrecht liegt beim Cloud-Nutzer. Dennoch darf der Cloud-Anbieter eine Weisung, deren Rechtmäßigkeit er bezweifelt, nicht unbesehen ausführen. Vielmehr muss er den Cloud-Nutzer warnen, wenn er Zweifel an der Vereinbarkeit einer Weisung mit dem geltenden Datenschutzrecht hat, und die Entscheidung des Cloud-Nutzers abwarten.

Umsetzungshinweis

Bei der Aufnahme von Weisungen in die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung und bei jeder nach deren Abschluss ergangenen Weisung sollte der Cloud-Anbieter seinen Datenschutzbeauftragten konsultieren, wenn sich die Datenschutzwidrigkeit der Weisung einem datenschutzrechtlich geschulten Mitarbeiter des Cloud-Dienstes aufdrängt. Der Cloud-Anbieter hat keine Pflicht, eine Weisung ohne Anlass zu überprüfen.

Bei Massengeschäften, in denen der Cloud-Nutzer durch die Auswahl des Cloud-Dienstes aufgrund einer Dienstbeschreibung des Cloud-Anbieters die Weisung erteilt, hat der Cloud-Anbieter TOM zu treffen, durch die er den Cloud-Nutzer darauf hinweist, wenn dieser seinen Dienst datenschutzwidrig entgegen der Dienstbeschreibung nutzt (z.B. die vom Cloud-Anbieter zur Verfügung gestellten Datensicherungsmaßnahmen wie Verschlüsselung und Pseudonymisierung nicht nutzt).

Die Umsetzungshinweise aus ISO/IEC 27018 Ziff. 16.1.1 sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er dokumentiert, wie er Weisungen prüft, Zweifel an deren datenschutzrechtlicher Zulässigkeit erkennt und den Cloud-Nutzer vor Ausführung der Weisung darauf hinweist.

Nr. 4.2 – Änderungen des Datenverarbeitungsortes (indirekt Art. 28 Abs. 3 Satz 2 lit. a DSGVO)

Kriterium

Der Cloud-Anbieter informiert den Cloud-Nutzer unverzüglich in allen Fällen, in denen sich während des Geltungszeitraums der Vereinbarung der Ort der Datenerarbeitung gegenüber dem in der Vereinbarung festgelegten (Nr. 1.5) aus Gründen ändert, die im Verantwortungsbereich des Cloud-Anbieters liegen oder für beide Parteien unvorhersehbar sind.

Umsetzungshinweis

Bei Massengeschäften sollte ein Kommunikationsprozess, möglichst unterstützt durch ein automatisiertes Informationssystem innerhalb des Cloud-Dienstes, beispielsweise auf der Website des Cloud-Anbieters, eingerichtet werden, wodurch der Cloud-Nutzer bei Ortsänderungen die Möglichkeit der Kenntnisnahme vom Ort der Datenverarbeitung erhält.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er Maßnahmen und Zuständigkeiten dokumentiert, die er implementiert hat, um den Cloud-Nutzer bei Änderungen des Datenverarbeitungsortes zu informieren.

Nr. 5 – Sicherstellung der Vertraulichkeit beim Personal (Art. 28 Abs. 3 Satz 2 lit. b DSGVO)

Kriterium

(1) Der Cloud-Anbieter richtet ein organisatorisches Verfahren ein, um sicherzustellen, dass die zur Verarbeitung von personenbezogenen Daten befugten Personen vor Aufnahme der datenverarbeitenden Tätigkeit zur Vertraulichkeit gemäß der Vereinbarung zur Auftragsverarbeitung (Nr. 1.6) verpflichtet werden, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Das organisatorische Verfahren umfasst auch die Dokumentation der Verpflichtungserklärungen sowie ihre Anpassungen, wenn sich Zugriffs- und Verarbeitungsbefugnisse ändern.

Erläuterung

Die Verpflichtung zur Vertraulichkeit und die Belehrung zur Verschwiegenheit fördern das Gewährleistungsziel der Vertraulichkeit (SDM 6.2.3) (s. auch Nr. 1.6).

Umsetzungshinweis

Den Mitarbeitern des Cloud-Anbieters sollte der Cloud-Anbieter eine Ausfertigung des Verpflichtungstextes mitsamt den Hinweisen auf mögliche Folgen von Verschwiegenheitspflichtverletzungen aushändigen. Er sollte die Belehrung in angemessenen Abständen wiederholen, etwa im Zusammenhang mit Schulungen oder insbesondere bei Änderung der Zugriffs- und Verarbeitungskompetenz des jeweiligen Mitarbeiters. Außerdem sollte der Cloud-Anbieter die betroffenen Personen zu Fragen des Datenschutzes und der Datensicherheit in Bezug auf ihre Tätigkeit regelmäßig sensibilisieren.

In der Dokumentation des Verfahrens sollte er Festlegungen treffen, wer für die Vornahme der Belehrung und Verpflichtung verantwortlich ist, wer sie wann und in welcher Weise durchführt, welche Personen zu welchem Zeitpunkt verpflichtet und belehrt werden müssen und welcher Nachweis über die Verpflichtung und Belehrung wo und wie lange aufbewahrt wird.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er Belehrungen und Verpflichtungen sowie die zugehörigen Verfahren und Zuständigkeiten dokumentiert.

Nr. 6 – Unterstützung des Cloud-Nutzers bei der Wahrung der Betroffenenrechte

Erläuterung

Für die Erfüllung der Rechte der betroffenen Personen ist der Cloud-Nutzer als Verantwortlicher zuständig. Soweit ihm dies aber nicht selbst möglich ist, muss ihn der Cloud-Anbieter als Auftragsverarbeiter unterstützen. Für diesen Fall muss er eine Kontaktstelle für den Cloud-Nutzer vorhalten, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann.

Nr. 6.1 – Auskunftserteilung (Art. 28 Abs. 3 lit. e i.V.m. Art. 15 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass der Cloud-Nutzer die Möglichkeit hat, betroffenen Personen Auskunft über die Datenverarbeitung zu erteilen und ihnen eine Kopie der personenbezogenen Daten zur Verfügung zu stellen oder dies durch den Cloud-Anbieter vornehmen zu lassen.

(2) Der Cloud-Anbieter dokumentiert Weisungen zur Umsetzung der Betroffenenrechte.

(3) Der Cloud-Anbieter ist von der Auskunftserteilung in jenen Fällen entbunden, in denen der Verantwortungsbereich beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt.

Erläuterung

Der Cloud-Nutzer ist nach Art. 15 DSGVO verpflichtet, der betroffenen Person auf Antrag Auskunft über eine Datenverarbeitung und ihre Umstände zu erteilen. Der Cloud-Anbieter hat den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM 6.2.5 und 6.2.6).

Umsetzungshinweis

Soweit dem Cloud-Nutzer eine Umsetzung der Betroffenenrechte nicht selbst möglich ist, sollte eine organisatorische Kontaktstelle für den Cloud-Nutzer vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er dokumentiert, welche Maßnahmen er ergriffen hat, um dem Cloud-Nutzer die Auskunftserteilung gegenüber einer betroffenen Person zu ermöglichen oder die Auskunft durch den Cloud-Anbieter erteilen zu lassen. Auch können anhand einer Prozessdokumentation die tatsächlich durchgeführten Auskunftserteilungen nachgewiesen werden.

Nr. 6.2 – Berichtigung und Vervollständigung (Art. 28 Abs. 3 lit. e i.V.m. Art. 16 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch geeignete Maßnahmen sicher, dass der Cloud-Nutzer die Möglichkeit hat, die Berichtigung und Vervollständigung personenbezogener Daten selbst vorzunehmen oder durch den Cloud-Anbieter vornehmen zu lassen.

(2) Der Cloud-Anbieter dokumentiert Weisungen zur Umsetzung der Betroffenenrechte.

(3) Der Cloud-Anbieter ist von der Berichtigung und Vervollständigung in jenen Fällen entbunden, in denen der Verantwortungsbereich beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt.

Erläuterung

Der Cloud-Nutzer ist nach Art. 16 DSGVO verpflichtet, auf Antrag unrichtige personenbezogene Daten zu berichtigen und unvollständige personenbezogene Daten zu vervollständigen. Der Cloud-Anbieter ist verpflichtet, den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Die Berichtigung gemäß Art. 16 DSGVO fördert das Gewährleistungsziel der Intervenierbarkeit (SDM 6.2.6).

Umsetzungshinweis

Soweit dem Cloud-Nutzer eine Umsetzung der Betroffenenrechte nicht selbst möglich ist, sollte eine organisatorische Kontaktstelle für den Cloud-Nutzer vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Maßnahmen er ergriffen hat, um dem Cloud-Nutzer die Berichtigung und Vervollständigung von Daten zu ermöglichen oder diese durch den Cloud-Anbieter vornehmen zu lassen. Auch können anhand einer Prozessdokumentation die tatsächlich durchgeführten Berichtigungen und Vervollständigungen nachgewiesen werden.

Nr. 6.3 – Löschung (Art. 28 Abs. 3 lit. e i.V.m. Art. 17 Abs. 1 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass der Cloud-Nutzer die Möglichkeit hat, die Löschung personenbezogener Daten selbst vorzunehmen oder durch den Cloud-Anbieter vornehmen zu lassen.

(2) Der Cloud-Anbieter dokumentiert Weisungen zur Umsetzung der Betroffenenrechte.

(3) Der Cloud-Anbieter ist von der Löschung in jenen Fällen entbunden, in denen der Verantwortungsbereich beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt.

Erläuterung

Der Cloud-Nutzer ist nach Art. 17 Abs. 1 DSGVO verpflichtet, personenbezogene Daten zu löschen. Der Cloud-Anbieter ist verpflichtet, den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert die Gewährleistungsziele der Intervenierbarkeit und Nichtverkettung (SDM 6.2.4 und 6.2.6).

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27040:2017-03 Ziff. 6.8.1 zur Datenlöschung sind anwendbar.

Die Erstellung eines Löschkonzepts, z.B. nach DIN 66398-2016, wird empfohlen. Dieses kann die Festlegung von Löschverfahren beinhalten, mit denen es dem Cloud-Nutzer ermöglicht wird, seinen Löschungspflichten nachzukommen. Dies sollte auch Backup- und Ausfallsicherungssysteme, einschließlich aller Vorgängerversionen der Daten, temporäre Dateien, Metadaten und Dateifragmente umfassen. Die Maßnahmen aus DIN 66398 zur Erstellung eines Löschkonzepts sowie DIN 66993 zur Vernichtung von Datenträgern können hinzugezogen werden.

Alle Datenträger des Cloud-Anbieters sollten durch den Einsatz eines formalen Managementverfahrens sicher und geschützt entsorgt werden, wenn sie nicht mehr benötigt werden.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Maßnahmen er ergriffen hat, um dem Cloud-Nutzer die Löschung von Daten zu ermöglichen oder diese durch den

Cloud-Anbieter vornehmen zu lassen. Auch können anhand einer Prozessdokumentation die tatsächlich durchgeführten Löschungen nachgewiesen werden.

Nr. 6.4 – Einschränkung der Verarbeitung (Art. 28 Abs. 3 lit. e i.V.m. Art. 18 Abs. 1 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass der Cloud-Nutzer die Möglichkeit hat, die Verarbeitung personenbezogener Daten selbst einzuschränken oder die Einschränkung durch den Cloud-Anbieter vornehmen zu lassen.

(2) Der Cloud-Anbieter dokumentiert Weisungen zur Umsetzung der Betroffenenrechte.

(3) Der Cloud-Anbieter ist von der Einschränkung der Verarbeitung in jenen Fällen entbunden, in denen der Verantwortungsbereich beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt.

Erläuterung

Der Cloud-Nutzer ist nach Art. 18 Abs. 1 DSGVO verpflichtet, die Verarbeitung personenbezogener Daten unter bestimmten Voraussetzungen einzuschränken. Der Cloud-Anbieter ist verpflichtet, den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM 6.2.6).

Umsetzungshinweis

Soweit dem Cloud-Nutzer eine Umsetzung der Betroffenenrechte nicht selbst möglich ist, sollte eine organisatorische Kontaktstelle für den Cloud-Nutzer vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Maßnahmen er ergriffen hat, um dem Cloud-Nutzer die Einschränkung der Verarbeitung von Daten zu ermöglichen oder dies durch den Cloud-Anbieter vornehmen zu lassen.

Nr. 6.5 – Mitteilungspflicht bei Berichtung, Löschung oder Einschränkung der Verarbeitung (Art. 28 Abs. 3 lit. e i.V.m. Art. 19 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass der Cloud-Nutzer die Möglichkeit hat, Empfängern, denen er personenbezogene Daten offengelegt hat, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitzuteilen oder die Mitteilung durch den Cloud-Anbieter vornehmen zu lassen, sowie die betroffene Person auf Verlangen über die Empfänger zu unterrichten.

(2) Der Cloud-Anbieter dokumentiert Weisungen zur Umsetzung der Betroffenenrechte.

(3) Der Cloud-Anbieter ist von der Mitteilungspflicht in jenen Fällen entbunden, in denen der Verantwortungsbereich beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt.

Erläuterung

Der Cloud-Nutzer ist nach Art. 19 DSGVO verpflichtet, Empfängern, denen er personenbezogene Daten offengelegt hat, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitzuteilen und die betroffene Person auf Verlangen über die Empfänger zu unterrichten. Soweit der Cloud-Anbieter an der Offenlegung beteiligt war, ist er verpflichtet, den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM 6.2.5 und 6.2.6).

Umsetzungshinweis

Soweit dem Cloud-Nutzer eine Umsetzung der Betroffenenrechte nicht selbst möglich ist, sollte eine organisatorische Kontaktstelle für den Cloud-Nutzer vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Maßnahmen er ergriffen hat, um es dem Cloud-Nutzer zu ermöglichen, Empfängern, denen er personenbezogene Daten offengelegt hat, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitzuteilen und die betroffene Person auf Verlangen über die Empfänger zu unterrichten oder dies durch den Cloud-Anbieter vornehmen zu lassen.

Nr. 6.6 – Datenübertragung
(Art. 28 Abs. 3 lit. e i.V.m. Art. 20 Abs. 1 und 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass der Cloud-Nutzer die Möglichkeit hat, die von einer betroffenen Person bereitgestellten personenbezogenen Daten dieser Person oder einem anderen Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln oder durch den Cloud-Anbieter übermitteln zu lassen.

(2) Der Cloud-Anbieter dokumentiert Weisungen zur Umsetzung der Betroffenenrechte.

(3) Der Cloud-Anbieter ist von der Datenübertragung in jenen Fällen entbunden, in denen der Verantwortungsbereich beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt.

Erläuterung

Der Cloud-Nutzer ist nach Art. 20 Abs. 1 und 2 DSGVO verpflichtet, auf Wunsch der betroffenen Person ihr oder einem anderen Verantwortlichen ihre bereitgestellten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln. Der Cloud-Anbieter sollte die ihm möglichen gängigen Formate in der rechtsverbindlichen Vereinbarung auflisten, um diesbezügliche Klarheit herzustellen.

Der Cloud-Anbieter ist verpflichtet, den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM 6.2.6).

Umsetzungshinweis

Der Cloud-Anbieter sollte geeignete technische Funktionen innerhalb seines angebotenen Dienstes bereitstellen, die es ermöglichen, Daten in ein strukturiertes, gängiges und maschinenlesbares Format zu übertragen. Hierzu gehören z.B. Exportfunktionen in XML- oder JSON-Formate.

Soweit dem Cloud-Nutzer eine Umsetzung der Betroffenenrechte nicht selbst möglich ist, sollte eine organisatorische Kontaktstelle für den Cloud-Nutzer vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Maßnahmen er implementiert hat, um es dem Cloud-Nutzer zu ermöglichen, der betroffenen Person oder einem anderen Verantwortlichen die von dieser betroffenen Person bereitgestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln oder durch den Cloud-Anbieter übermitteln zu lassen.

Nr. 6.7 – Widerspruch
(Art. 28 Abs. 3 lit. e i.V.m. Art. 21 Abs. 1 und Art. 32 Abs. 1 lit. b DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass er dem Cloud-Nutzer alle Daten zur Verfügung stellt, die erforderlich sind, damit dieser beurteilen kann, ob das Widerspruchsrecht der betroffenen Person wirksam ausgeübt worden ist.

(2) Ist der Widerspruch gegen die Datenverarbeitung wirksam, stellt der Cloud-Anbieter im Rahmen seiner Möglichkeiten sicher, dass die Daten nicht mehr verarbeitet werden können.

(3) Der Cloud-Anbieter dokumentiert Weisungen zur Umsetzung der Betroffenenrechte.

(4) Ausgenommen sind die Fälle, in denen der Verantwortungsbereich beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt.

Erläuterung

Der betroffenen Person steht entsprechend Art. 21 DSGVO das Recht zu, Widerspruch gegen eine Verarbeitung ihrer Daten einzulegen. Hat die betroffene Person das Widerspruchsrecht wirksam ausgeübt, ist der Cloud-Nutzer verpflichtet, die Verarbeitung der betroffenen personenbezogenen Daten für die Zukunft zu unterlassen. Der Cloud-Anbieter ist verpflichtet, den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM 6.2.6).

Umsetzungshinweis

Der Cloud-Anbieter sollte über ein Konzept verfügen, aus dem hervorgeht, durch welche Maßnahmen er sicherstellt, dass er dem Cloud-Nutzer alle erforderlichen Daten zur Verfügung stellen und die künftige Verarbeitung der Daten unterbinden kann.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Maßnahmen er implementiert hat, um dem Cloud-Nutzer die erforderlichen Daten zur Verfügung zu stellen.

Nr. 7 – Unterstützung bei der Datenschutz-Folgenabschätzung
(Art. 28 Abs. 3 lit. f i.V.m. Art. 35 und 36 DSGVO)

Kriterium

(1) Der Cloud-Anbieter unterstützt den Cloud-Nutzer bei der Durchführung seiner Datenschutz-Folgenabschätzung.

(2) Ist dem Cloud-Anbieter durch eine vorher beim Cloud-Nutzer durchgeführte Datenschutz-Folgenabschätzung das hohe Risiko der Verarbeitung bekannt, hat der Cloud-Anbieter risikoangemessene Vorkehrungen bereitzuhalten.

(3) Der Cloud-Anbieter stellt dem Cloud-Nutzer alle Informationen zur Verfügung, die in seinen Verantwortungsbereich fallen und die der Cloud-Nutzer für seine Datenschutz-Folgenabschätzung benötigt.

(4) Der Cloud-Anbieter unterstützt den Cloud-Nutzer bei der Bewältigung der Risiken der durch den Cloud-Nutzer geplanten Abhilfemaßnahmen, die z.B. Sicherheitsvorkehrungen und sonstige Verfahren enthalten und der Sicherstellung des Schutzes von personenbezogenen Daten dienen.

Erläuterung

Soweit der Cloud-Nutzer zu einer Datenschutz-Folgenabschätzung verpflichtet ist, hat ihn der Cloud-Anbieter durch Informationen, Analysen und Schutzmaßnahmen zu unterstützen.

Umsetzungshinweis

Die Unterstützungspflichten bei der Datenschutz-Folgenabschätzung sollten am Einflussbereich des Cloud-Anbieters ausgerichtet werden, etwa im Bereich der TOM zur Gewährleistung der Datensicherheit. Zur Einschätzung, ob ein oder welches Risiko bei den jeweiligen Datenverarbeitungsvorgängen des Cloud-Dienstes gegeben ist, können Datenflussmodelle und -analysen erstellt werden, wenn diese nicht bereits aus der Dienstbeschreibung des Cloud-Anbieters hervorgehen.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, wie er den Cloud-Nutzer durch einschlägige Informationen unterstützen kann. Er sollte darlegen, dass diese Informationen vorliegen oder von ihm in kurzer Zeit generiert werden können.

Kapitel III: Datenschutz-Managementsystem des Cloud-Anbieters

Erläuterung

Der Cloud-Anbieter muss seine Datenschutzmaßnahmen in einem Datenschutz-Managementsystem organisieren. Die Einrichtung eines Datenschutz-Managementsystems indizieren die Art. 24 und 25, 32, 33, 34 sowie 37 bis 39 DSGVO. Die Sicherstellung eines Datenschutz-Managementsystems sollte der fortwährenden Sicherstellung des Datenschutzniveaus des zertifizierten Cloud-Dienstes dienen.

Nr. 8 – Datenschutz-Managementsystem

Nr. 8.1 – Benennung, Stellung und Aufgaben eines Datenschutzbeauftragten (Art. 37-39 DSGVO, § 38 BDSG)

Kriterium

(1) Ist der Cloud-Anbieter zur Benennung eines Datenschutzbeauftragten (DSB) verpflichtet, benennt er diesen auf Grund seiner beruflichen Qualifikation und insbesondere seines Fachwissens, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf Grundlage seiner Fähigkeit zur Erfüllung der in Art. 39 DSGVO genannten Aufgaben.

(2) Der Cloud-Anbieter stellt sicher, dass der DSB unmittelbar der höchsten Managementebene berichtet.

(3) Der Cloud-Anbieter stellt sicher, dass der DSB bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält.

(4) Der Cloud-Anbieter stellt sicher, dass der DSB ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

(5) Der Cloud-Anbieter stellt die Anerkennung der Person und Funktion des DSB im Organisationsgefüge sicher und unterstützt ihn bei seinen Aufgaben, insbesondere mit angemessenen Ressourcen.

(6) Der Cloud-Anbieter stellt sicher, dass der DSB seinen Aufgaben nach Art. 39 Abs. 1 DSGVO im angemessenen Umfang nachkommt.

(7) Ist ein Beauftragter für Informationssicherheit benannt, stellt dieser die Einhaltung der datenschutzrechtlich gebotenen TOM sicher. Der Cloud-Anbieter stellt sicher, dass der DSB und der Beauftragte für Informationssicherheit in angemessener Weise kooperieren (gegenseitige Information und Unterstützung).

Erläuterung

Sofern Cloud-Anbieter die Pflicht haben, einen DSB zu benennen, müssen sie ihn sorgfältig auswählen, ausstatten, schützen und ihm in der Betriebsorganisation einen gebührenden Platz zuweisen.

Die Benennung eines Beauftragten für Informationssicherheit wird durch die Datenschutz-Grundverordnung nicht verlangt. Der Cloud-Anbieter kann jedoch aufgrund anderweitiger Verpflichtungen zur Benennung verpflichtet sein oder die Benennung freiwillig vornehmen.

Erfolgt die Benennung eines DSB, so muss dieser seinen gesetzlichen Pflichten in Bezug auf alle durchgeführten Datenverarbeitungsvorgänge nachkommen, unabhängig davon, ob der Cloud-Anbieter als Auftragsverarbeiter oder Verantwortlicher der Datenverarbeitung agiert.

Umsetzungshinweis

Der Cloud-Anbieter sollte eine schriftliche Dokumentation der für den jeweiligen Cloud-Dienst eingesetzten Systeme, Verfahren und Prozesse (Software, Hardware, beteiligte Organisationseinheiten, Rollen und Dienstleister) und eine möglichst exakte Beschreibung der Gesamtheit der getroffenen TOM führen (z.B. in einem Datensicherheitskonzept) und dem DSB sowie (auf Anfrage) der Aufsichtsbehörde zugänglich machen.

Ist der DSB bei einem anderen Unternehmen beschäftigt (externer DSB des Cloud-Anbieters) oder gleichzeitig DSB anderer Unternehmen, gilt seine Weisungsfreiheit auch gegenüber seinem Arbeitgeber und seinen anderen Auftraggebern. Die Anforderung der Abwesenheit von Interessenskonflikten ist primär eine Benennungsvoraussetzung und in sekundärer Hinsicht eine Organisationspflicht des Cloud-Anbieters. Der Cloud-Anbieter weist dem DSB keine zusätzlichen Aufgaben zu, die ihn in einen Interessenskonflikt bringen könnten. Interessenskonflikte sind im Rahmen folgender Tätigkeiten anzunehmen: Tätigkeiten, im Rahmen derer der DSB sich selbst kontrollieren müsste, z.B. Stellung als Geschäftsführer, IT- oder Personalabteilungsleiter, Informationssicherheitsbeauftragter, wirtschaftliche Interessen des DSB am Unternehmenserfolg, zu große Nähe zur benennenden Stelle.

Die Verschwiegenheitspflicht des DSB umfasst insbesondere die Identität des Beschwerdeführers oder der betroffenen Person(en), alle datenschutzrechtlich relevanten Informationen sowie alles, was zur Identifizierung eines Hinweisgebers führen könnte. Auch gegenüber der ihn benennenden Stelle ist der DSB zur umfassenden Verschwiegenheit verpflichtet. Das Kriterium fördert das Gewährleistungsziel der Vertraulichkeit (SDM 6.2.3).

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er einen DSB benannt hat und durch Einträge auf seiner Webseite seine direkte Ansprechbarkeit der Öffentlichkeit vorstellt. Zur Beurteilung der fachlichen und persönlichen Eignung kann er einschlägige Zeugnisse und Beurteilungen vorlegen. Mit den regelmäßig durchzuführenden internen Audits des DSB kann der Nachweis über seine Tätigkeiten, seine Unabhängigkeit sowie seine Einbindung und Wirksamkeit im Organisationsgefüge des Cloud-Anbieters nachgewiesen werden.

Nr. 8.2 – Meldung von Datenschutzverletzungen (Art. 33 Abs. 2 und Art. 28 Abs. 3 lit. f DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch geeignete Maßnahmen sicher, dass er dem Cloud-Nutzer Datenschutzverletzungen und deren Ausmaß unverzüglich meldet.

(2) Der Cloud-Anbieter bestimmt, wer zuständig ist, über die Mitteilung an den Cloud-Nutzer zu entscheiden und diese vorzunehmen. Die zuständigen Stellen sind für Mitarbeiter und Subauftragsverarbeiter in einer Weise erreichbar, dass Mitteilungen über etwaige Verstöße zeitnah entgegengenommen und bearbeitet werden können.

(3) Die zuständigen Stellen verfügen über ausreichend Ressourcen, um eine rasche Bearbeitung von Meldungen sicher zu stellen. Die Mitarbeiter in den zuständigen Stellen sind ausreichend geschult, um Verstöße beurteilen und eine Folgeabschätzung durchführen zu können.

Erläuterung

Der Cloud-Anbieter ist nach Art. 33 Abs. 2 DSGVO zur unverzüglichen Meldung von Datenschutzverstößen an den Cloud-Nutzer verpflichtet, damit dieser seiner Meldepflicht gegenüber der Aufsichtsbehörde aus Art. 33 Abs. 1 DSGVO und seiner Unterrichtungspflicht gegenüber den betroffenen Personen aus Art. 34 Abs. 1 DSGVO nachkommen kann. Diese Pflicht bezieht sich auch auf Verstöße von Subauftragnehmern in der gesamten Subauftragsverarbeiterkette. Das Kriterium fördert das Gewährleistungsziel der Integrität und Transparenz (SDM 6.2.2 und 6.2.5).

Umsetzungshinweis

Die Meldung von Datenschutzverletzungen kann über geeignete Informationssysteme innerhalb des Dienstes wie über Nachrichtensysteme oder Newsmeldungen geschehen.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er in seinem Datensicherheitskonzept dokumentiert, wie er die Meldung von Datenschutzverletzungen gewährleistet.

Nr. 8.3 – Führen eines Verarbeitungsverzeichnisses (Art. 30 Abs. 2 DSGVO)

Kriterium

(1) Cloud-Anbieter, die mehr als 250 Mitarbeiter beschäftigen, führen ein Verarbeitungsverzeichnis. Der Cloud-Anbieter führt unabhängig von der Beschäftigtenzahl ein Verarbeitungsverzeichnis, wenn die Verarbeitung für die betroffenen Personen mit Risiken für ihre Rechte und Freiheiten verbunden ist.

(2) Im Verzeichnis führt der Cloud-Anbieter alle Kategorien von Verarbeitungsvorgänge auf, die er im Auftrag eines Verantwortlichen durchführt. Das Verzeichnis enthält außerdem die in Art. 30 Abs. 2 DSGVO aufgelisteten Inhalte.

(3) Für jeden einzelnen Cloud-Nutzer ist jeweils ein eigenes Verarbeitungsverzeichnis zu führen.

(4) Das Verarbeitungsverzeichnis ist schriftlich oder in einem elektronischen Format zu führen. Es ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Transparenz (SDM 6.2.5).

Risikobehaftet ist ein Verarbeitungsvorgang i.S.d. Art. 30 Abs. 5 DSGVO, wenn er Risiken für die Rechte und Freiheiten von betroffenen Personen birgt oder besondere Kategorien von personenbezogenen Daten gemäß Art. 9 DSGVO oder Art. 10 DSGVO zum Gegenstand hat. Auch Cloud-Anbieter mit weniger als 250 Mitarbeitern werden in der Regel ein Verarbeitungsverzeichnis führen müssen, da sich bereits aus der Menge der verarbeiteten Daten Risiken ergeben und die Datenverarbeitung nicht nur gelegentlich erfolgt, sodass die Ausnahme aus Art. 30 Abs. 5 DSGVO im Regelfall nicht anwendbar ist.

Umsetzungshinweis

Das für jeden Cloud-Nutzer jeweils zu führende Verarbeitungsverzeichnis sollte auch die für jeden Cloud-Nutzer jeweils eingesetzten TOM zur Gewährleistung der Datensicherheit bei der Datenverarbeitung dokumentieren. Bei standardisierten Massengeschäften sollte das Verarbeitungsverzeichnis automatisiert erstellt werden.

Das Verfahrensverzeichnis kann für alle Dokumentationspflichten als Nachweis oder Nachweisbekräftigung herangezogen werden. Dieses Verzeichnis ist jedoch nicht öffentlich und richtet sich nicht an betroffene Personen, sondern ist ausschließlich nach innen und auf das Verhältnis zur Aufsichtsbehörde gerichtet. Der Cloud-Nutzer sollte jedoch – etwa zur Auftragskontrolle nach Art. 28 Abs. 3 Satz 2 lit. h DSGVO – einen Einblick in das seinen Auftrag betreffende Verzeichnis erhalten.

Die Umsetzungshinweise aus ISO/IEC 27018 Ziff. A5.2 sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er die (eine repräsentative Stichprobe der) Verarbeitungsverzeichnisse vorlegt.

Nr. 8.4 – Rückgabe von Datenträgern und Löschung von Daten (Art. 28 Abs. 3 lit. h DSGVO)

Kriterium

Der Cloud-Anbieter stellt durch geeignete Maßnahmen sicher, dass die Rückgabe überlassener Datenträger, die Rückführung von Daten und die Löschung der beim Cloud-Anbieter gespeicherten Daten nach Abschluss der Auftragsverarbeitung oder nach Weisung des Cloud-Nutzers erfolgen.

Umsetzungshinweis

Auf ISO/ IEC 27018 Ziff. A 9.3. wird hingewiesen.

Die Umsetzungshinweise aus ISO/IEC 27040:2017-03 Ziff. 6.8.1 zur Datenlöschung sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welches Verfahren er vorgesehen hat, nach dem er die Herausgabe der Datenträger, die Rückführung von Daten und die Löschung von Daten nach Beendigung des Auftrags durchführt. Auch kann er die Quittierung von Rückgaben oder die automatisierte Benachrichtigung über tatsächliche Löschungen der für die Auftragsverarbeitung nicht mehr benötigten personenbezogenen Daten vorlegen.

Nr. 8.5 – Einrichtung eines internen Kontrollsystems (Art. 24 DSGVO)

Kriterium

(1) Der Cloud-Anbieter überprüft die Umsetzung aller in diesem Katalog geprüften Kriterien regelmäßig in einem internen Revisionsverfahren. Hierfür legt der Cloud-Anbieter Kontrollverfahren und Zuständigkeiten fest.

(2) Der Cloud-Anbieter stellt durch geeignete TOM sicher, dass bei der (Weiter-)Entwicklung oder Änderung des Cloud-Dienstes die in diesem Katalog geprüften Kriterien weiterhin eingehalten werden.

Erläuterungen

Der Cloud-Anbieter hat sicherzustellen, dass die Maßnahmen zur Erfüllung der datenschutzrechtlichen Pflichten nach diesem Katalog nicht nur einmalig implementiert werden, sondern während der Gültigkeit eines Zertifikats aufrechterhalten werden.

Umsetzungshinweis

Der Cloud-Anbieter sollte vor allem die internen Audits des DSB zu Datenschutzfragen heranziehen. Des Weiteren wird auf die Umsetzungshinweise zur regelmäßigen Überprüfung durch die oberste Leitung beim Cloud-Anbieter nach ISO/IEC 27002:2017-06, Ziff. 18.2. hingewiesen.

Der Cloud-Anbieter sollte die Wirksamkeit der internen Kontrollaktivitäten regelmäßig überprüfen. Dazu gilt es zunächst zu definieren, wie die Wirksamkeit der internen Kontrollaktivitäten gemessen werden kann. Es ist empfohlen ein standardisiertes Vorgehensmodell (z. B. ITIL oder COBIT) für die IT-Prozesse des angebotenen Cloud-Dienstes zu definieren und einzuhalten. Wird ein interner Prüfer/Auditor eingesetzt, sollte er über eine geeignete Qualifikation verfügen, objektiv und unparteiisch und nicht an der Erstellung der Prüfobjekte beteiligt sein.

Bei der Bereitstellung eines Cloud-Dienstes sollten Prozesse für ein sicheres Änderungs- und Release-Management etabliert werden. Im Rahmen dieser Prozesse sollte ein Cloud-Anbieter u.a. eine dokumentierte Eignungsprüfung und einen Abnahmeprozess bei der (Weiter-)Entwicklung und Änderung (insb. Patches und System-Updates) an seinem Dienst durchführen, um nachteilige Auswirkungen aufgrund der Änderungen zu vermeiden und die Konformität zur Datenschutz-Grundverordnung fortlaufend sicherzustellen. Die Geltungsbereiche, Rollen und Verbindlichkeiten im Rahmen des Änderungs- und Release-Managements sollten zwischen Cloud-Anbieter und -Nutzer klar definiert und aufeinander abgestimmt sein.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welches interne Kontrollsystem er eingerichtet hat.

Nr. 8.6 – Auswahl und Einsatz geeigneter Personen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO)

Kriterium

(1) Der Cloud-Anbieter betraut nur Mitarbeiter mit der Durchführung von Verarbeitungsvorgängen, die fachlich für die Erfüllung ihrer jeweiligen Aufgaben befähigt sind, die nötige Zuverlässigkeit aufweisen und sowohl im Datenschutz als auch in der Datensicherheit sensibilisiert und geschult sind.

(2) Der Cloud-Anbieter stellt sicher, dass bei den Mitarbeitern keine Interessenkonflikte hinsichtlich der Ausübung ihrer jeweiligen Aufgaben bestehen.

Erläuterungen

Der Einsatz geeigneter Mitarbeiter ist die Voraussetzungen dafür, dass der Cloud-Anbieter seinen zahlreichen Pflichten überhaupt nachkommen kann. Das Kriterium steht zudem in enger Verbindung mit dem Kriterium Nr. 8.1, da der DSB für die Sensibilisierung und Schulung von an Verarbeitungsvorgängen beteiligten Mitarbeitern zuständig ist und die diesbezüglichen Überprüfungen vornimmt.

Umsetzungshinweis

Um die fachliche Kompetenz der Mitarbeiter zu erhalten, sollte der Cloud-Anbieter regelmäßige Mitarbeiterschulungen (ca. 1 Mal pro Jahr) zu datenschutzrechtlichen und informationssicherheitstechnischen Themen durchführen – auch zur konkreten Technik des Cloud-Dienstes.

Nachweis

Der Cloud-Anbieter kann den Nachweis der erforderlichen Fachkunde seiner Mitarbeiter durch einschlägige Qualifikationsnachweise erbringen. Sensibilisierungs- und Schulungsmaßnahmen von Mitarbeitern kann er durch die Dokumentation erfolgter Schulungen nachweisen.

Kapitel IV: Datenschutz durch Systemgestaltung

Nr. 9 – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Nr. 9.1 – Datenschutz durch Systemgestaltung (Art. 25 Abs. 1 DSGVO i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

(1) Der Cloud-Anbieter setzt im Rahmen des angebotenen Dienstes die Grundsätze des Art. 5 DSGVO (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckfestlegung und Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Systemdatenschutz und Verantwortlichkeit) praktikabel und zielführend um.

(2) Der Cloud-Anbieter verfügt über Prozesse zur Transparenz und zur aktiven Verfolgung des Stands der Technik auf den Ebenen der konzeptionellen Zielsetzung, der Architektur, der Systemgestaltung und der Implementierung.

(3) Der Cloud-Anbieter stellt sicher, dass zu jedem Zeitpunkt durch seine Systemgestaltung in den angebotenen Anwendungen und durch die Konzeption der Dienstleistung die Nachvollziehbarkeit und Transparenz der Datenverarbeitungen, auch in den verlängerten Leistungsketten durch etwaige Subauftragsverhältnisse, gewährleistet ist.

Erläuterung

Der Cloud-Nutzer muss als Verantwortlicher die Gestaltungspflicht aus Art. 25 Abs. 1 DSGVO erfüllen. Sobald er einen Cloud-Dienst nutzt, muss er einen Cloud-Anbieter auswählen, der diese Pflicht erfüllt. Technik und Organisation des Cloud-Dienstes sind daher so zu gestalten, dass sie die Datenschutzgrundsätze des Art. 5 DSGVO bestmöglich unterstützen.

Nachweis

Der Cloud-Anbieter legt Dokumentationen vor, aus denen hervorgeht, welche Maßnahmen er ergriffen hat, um die Datenschutzgrundsätze bei der Gestaltung des Cloud-Dienstes umzusetzen. Die Dokumentationen schildern auch die Abwägungen, die unternommen wurden, um die Maßnahmen festzulegen.

Nr. 9.2 – Datenschutz durch Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch seine Voreinstellungen im jeweiligen Dienst sicher, dass der Zugang zu den personenbezogenen Daten auf das Maß beschränkt wird, das erforderlich ist, um den Verarbeitungszweck des Cloud-Nutzers zu erfüllen.

(2) Der Cloud-Anbieter stellt durch Voreinstellungen sicher, dass personenbezogene Daten nicht ohne Eingreifen der betroffenen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden und hierbei keine Risiken für die betroffenen Personen durch eine zu umfassende Zugänglichmachung von personenbezogenen Daten entstehen.

Erläuterung

Der Verantwortliche muss die Pflichten aus Art. 25 Abs. 2 DSGVO erfüllen. Sobald er eine Datenverarbeitung im Auftrag ausführen lässt, muss der Cloud-Nutzer einen Cloud-Anbieter auswählen, der diese Pflichten erfüllt. Die Voreinstellungen des Cloud-Dienstes sind daher so zu wählen, dass sie die Pflicht des Art. 25 Abs. 2 Satz 1 DSGVO erfüllen.

Umsetzungshinweis

Die Voreinstellungen sollten so konzipiert sein, dass nach diesen nur personenbezogene Daten erhoben, gespeichert und zugänglich gemacht werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Soweit der Cloud-Anbieter eine Datenschutz-Folgenabschätzung durchgeführt hat, können sich Anforderungen an die Voreinstellungen aus der Pflicht ergeben, die festgestellten Risiken zu minimieren.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Voreinstellungen er aus welchen Erwägungen gewählt hat.

Kapitel V: Subauftragsverarbeitung

Erläuterung

Für die Auftragsverarbeitung gilt grundsätzlich das Prinzip der höchstpersönlichen Leistungserbringung. Unter bestimmten Voraussetzungen kann der Cloud-Anbieter weitere Subauftragsverarbeiter in Anspruch nehmen. Soweit auch Subauftragsverarbeiter ihrerseits auf Subauftragsverarbeiter zugreifen, ergeben sich mehrstufige Unterauftragsverhältnisse.

Der Cloud-Anbieter als Hauptauftragsverarbeiter hat allerdings dafür Sorge zu tragen, dass auch der Subauftragsverarbeiter alle Pflichten erfüllt, die der Cloud-Anbieter als Hauptauftragsverarbeiter erfüllen muss, soweit er hiervon nicht gesetzlich befreit ist. Schließlich bleibt der Cloud-Anbieter gegenüber dem Cloud-Nutzer durchgängig für die Auftragsausführung verantwortlich.

Nr. 10 – Subauftragsverhältnisse

Nr. 10.1 – Weitere Auftragsverarbeiter des Cloud-Anbieters (Subauftragsverarbeitung) (Art. 28 Abs. 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass ein Cloud-Dienst unter Einbeziehung von Subauftragsverarbeitern nur dann erbracht wird, wenn und soweit der Cloud-Nutzer vorher in diese Subauftragsverarbeitung in Schrift- oder Textform eingewilligt hat. Zustimmungsbedürftig sind nur solche Subaufträge, bei denen der weitere Auftragsverarbeiter eine Möglichkeit hat, die zu verarbeitenden personenbezogenen Daten zur Kenntnis zu nehmen.

(2) Der Cloud-Anbieter stellt sicher, dass auch der Subauftragsverarbeiter alle TOM im Rahmen seiner Auftragsverarbeitung gewährleistet und alle Pflichten erfüllt, die auch der Cloud-Anbieter als Hauptauftragsverarbeiter erfüllen muss, soweit er hiervon nicht gesetzlich befreit ist. Der Subauftragsverarbeiter muss dieselben Garantien nachweisen können wie der Hauptauftragsverarbeiter.

Erläuterung

Die Qualitätssicherung und die Einhaltung des Datenschutzes in der Leistungskette sind durch den Cloud-Anbieter zu gewährleisten. Insbesondere darf der Subauftrag nicht dazu führen, dass die Wahrung der Betroffenenrechte erschwert wird.

Umsetzungshinweis

Bei standardisierten Massengeschäften können die Cloud-Nutzer bei Änderungen in den Subauftragsverarbeitungen automatisiert, z.B. über eine automatisch generierte E-Mail, informiert werden. In den AGB von Cloud-Anbietern im Massengeschäft kann z.B. auch vorab eine Generalzustimmung für etwaige Änderungen in der Subauftragsverarbeitung, die vorbehalten werden, eingeholt werden. Dabei ist infolge der o.g. automatisierten Information jedem Cloud-Nutzer ein jederzeitiges Kündigungsrecht zuzugestehen, da ein Einspruch (i.S.d. Art. 28 Abs. 2 Satz 2 Hs. 2 DSGVO) von einem einzelnen Cloud-Nutzer im Massengeschäft die Beauftragung eines weiteren oder anderen Auftragsverarbeiters durch den Cloud-Anbieter nicht verhindert.

Die Umsetzungshinweise aus ISO/IEC 27002 Ziff. 15 sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis über die rechtskonforme weitere Datenverarbeitung dadurch erbringen, dass er die erteilte Zustimmung der Cloud-Nutzer und die Verträge zu den weiteren Auftragsverarbeitungen (Sub-Cloud-Verträge) mitsamt der für die Konformitätsprüfung erforderlichen Angaben (Dauer, Art und Zweck, Ort der weiteren Verarbeitung, Angaben über den weiteren Auftragsverarbeiter und dessen Dienstbeschreibung) vorlegt.

Nr. 10.2 – Rechtsverbindliche Vereinbarung als Grundlage der Subauftragsverarbeitung (Art. 28 Abs. 4 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass seine Subauftragsverarbeiter nur auf Grundlage einer rechtsverbindlichen Vereinbarung zur Subauftragsverarbeitung tätig werden, die mit der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung zwischen dem Cloud-Anbieter und Cloud-Nutzer in Einklang steht.

(2) Der Cloud-Anbieter verpflichtet seine Subauftragsverarbeiter sicherzustellen, dass ihre Subauftragsverarbeiter ebenfalls auf Grundlage einer rechtsverbindlichen Vereinbarung zur Subauftragsverarbeitung tätig werden und auf ihre Sub-Subauftragsverarbeiter dieselbe Verpflichtung übertragen.

Nachweis

Der Cloud-Anbieter kann den Nachweis über die rechtskonforme weitere Datenverarbeitung dadurch erbringen, dass er die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung und die rechtsverbindliche Vereinbarung über die Sub-Auftragsverarbeitung mitsamt der für die Konformitätsprüfung erforderlichen Angaben (Dauer, Art und Zweck, Ort der weiteren Verarbeitung, Angaben über den weiteren Auftragsverarbeiter und dessen Dienstbeschreibung) vorlegt.

Nr. 10.3 – Information des Cloud-Nutzers (Art. 28 Abs. 2 Satz 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter informiert den Cloud-Nutzer über die Identität aller von ihm eingeschalteten Subauftragsverarbeiter (einschließlich ladungsfähiger Anschrift).

(2) Der Cloud-Anbieter informiert den Cloud-Nutzer immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Subauftragsverarbeiter und gewährleistet, dass der Cloud-Nutzer auf jeder Stufe der Auftragsverarbeitung Gebrauch von seinem Einspruchsrecht machen kann.

Erläuterung

Dem Cloud-Nutzer muss es zu jedem Zeitpunkt der Auftragsverarbeitung möglich sein zu erfahren, welcher Subauftragsverarbeiter sich in welchem Verarbeitungsschritt befindet und welche Anwendungen und Dienste in Bezug auf personenbezogene Daten durch welchen Subauftragsverarbeiter auf welcher Stufe der Auftragsverarbeitung ausgeführt werden.

Umsetzungshinweis

Der Cloud-Anbieter als Hauptauftragsverarbeiter sollte für jede Verlängerung der Auftragsverarbeitungsleistungskette eine detaillierte Dokumentation über die involvierten Subauftragsverarbeiter unter Angabe von Identität inklusive ladungsfähiger Anschrift und der ausgeführten Tätigkeiten verfassen, sodass nachvollzogen werden kann, welcher (Sub-)Auftragsverarbeiter jeweils in den datenschutzkritischen Dienstteilen involviert ist und welche Verarbeitungsvorgänge jeweils von wem ausgeführt werden. Dies setzt voraus, dass der Subauftragsverarbeiter den Cloud-Anbieter über seine eingebundenen Subauftragsverarbeiter informiert und die notwendigen Informationen bereitstellt.

Zur Darstellung der involvierten Subauftragsverarbeiter eignen sich Informationsportale innerhalb oder außerhalb des angebotenen Cloud-Dienstes. Diese sollten fortlaufend gepflegt und aktualisiert werden.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, wie er den Cloud-Nutzer bei beabsichtigter Änderung von Subauftragsverarbeitern informiert. Außerdem kann er seine detaillierte Dokumentation über die involvierten Subauftragsverarbeiter unter Angabe von Identität, ladungsfähiger Anschrift und der ausgeführten Tätigkeiten vorlegen, mit deren Hilfe nachvollzogen werden kann, welcher (Sub-)Auftragsverarbeiter jeweils in den datenschutzkritischen Dienstteilen involviert ist und welche Verarbeitungsvorgänge jeweils von wem ausgeführt werden.

Nr. 10.4 – Auswahl und Kontrolle der Subauftragsverarbeiter (Art. 28 Abs. 4 Satz 1 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass nur solche Subauftragsverarbeiter in die Auftragsverarbeitung einbezogen werden, die die Gewähr für die Einhaltung der datenschutzrechtlichen Anforderungen an die von ihnen zu erbringende Leistung bieten.

(2) Der Cloud-Anbieter überzeugt sich davon, dass seine Subauftragsverarbeiter die datenschutzrechtlichen Anforderungen an die von ihnen zu erbringende Leistung erfüllen.

Umsetzungshinweis

Soweit der Cloud-Anbieter nicht auf Zertifikate seiner Subauftragsverarbeiter vertrauen kann, muss er sich selbst von der Einhaltung der datenschutzrechtlichen Anforderungen durch die Subauftragsverarbeiter überzeugen. Insoweit sind die Umsetzungshinweise von ISO/IEC 27017 Ziff. 15.1.2, 15.1.3 und ISO/IEC 27002 Ziff. 15 anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er Zertifikate der Subauftragnehmer oder sonstige Unterlagen vorlegt, aus denen sich die Gewähr zur Einhaltung der Datenschutz-Grundverordnung ergibt. Hierbei kann eine transparente Dienstbeschreibung des jeweiligen Subauftragsverarbeiters hilfreich sein.

Nr. 10.5 – Gewährleistung der Unterstützungsfunktionen (Art. 28 Abs. 4 Satz 1 i.V.m. Art. 28 Abs. 3 Satz 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass auch bei der Einschaltung von (mehreren) Subauftragsverarbeitern seine Unterstützungsfunktionen im vereinbarten Umfang sowie seine Pflichten als Hauptauftragsverarbeiter erfüllt werden.

(2) Der Cloud-Anbieter stellt durch geeignete Verfahren und Vorkehrungen sicher, dass die Verlängerung der Leistungskette in der Auftragsverarbeitung nicht zur Minderung der Achtung von datenschutzrechtlichen Standards und Verpflichtungen führt.

Umsetzungshinweis

Der Cloud-Anbieter sollte wegen des gesteigerten Risikos bei weiteren Auftragsverarbeitungen interne Dokumentationen führen und die Verarbeitungsprozesse protokollieren. Dies dient auch der Selbstkontrolle des Cloud-Anbieters bei der Pflichtenerfüllung auf den weiteren Auftragsstufen.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er eine Dokumentation vorlegt, aus der sich ergibt, in welche Pflichten er weitere Auftragsverarbeiter einbindet. Protokolle zur Pflichterfüllung infolge der Einschaltung von weiteren Auftragsverarbeitern sind hilfreich.

Kapitel VI: Datenverarbeitung außerhalb der EU und des EWR

Nr. 11 – Datenübermittlung

Nr. 11.1 – Geeignete Garantien für die Datenübermittlung (Art. 46 Abs. 2 lit. f i.V.m. Art. 42 Abs. 1 und 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter übermittelt personenbezogene Daten in Drittstaaten oder an internationale Organisationen nur, sofern für den Empfängerstaat oder die internationale Organisation ein Beschluss der Europäischen Kommission nach Art. 45 Abs. 3 DSGVO vorliegt, dass dort ein angemessenes Datenschutzniveau gilt.

(2) Alternativ kann die Übermittlung stattfinden, wenn der Empfänger geeignete Garantien im Sinne des Art. 46 Abs. 2 DSGVO vorweist und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe in dem Drittstaat oder gegenüber der Internationalen Organisation zur Verfügung stehen. Geeignete Garantien sind auch bei einem Zertifikat nach Art. 42 Abs. 2 DSGVO gegeben, wenn außerdem rechtsverbindliche und durchsetzbare Verpflichtungen des Cloud-Anbieters in dem Drittstaat bestehen, geeignete Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, anzuwenden.

Erläuterung

Verarbeitungen (sowohl Auftragsverarbeitungen als auch Datenverarbeitungen in eigener Verantwortlichkeit) von personenbezogenen Daten von betroffenen Personen in der EU oder im EWR sind außerhalb der EU und des EWR nur unter den in Art. 44 ff. DSGVO genannten Voraussetzungen zulässig. Das Gleiche gilt für die Übermittlung von personenbezogenen Daten in ein EU-Drittland oder an eine Internationale Organisation, für die kein angemessenes Datenschutzniveau anerkannt ist.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er Dokumente über ausreichende Garantien nach Art. 46 Abs. 2 DSGVO vorlegt. Eine Zertifizierung nach Art. 42 Abs. 2 DSGVO, die diesem oder einem vergleichbaren anerkannten Kriterienkatalog entspricht, kann ebenfalls als Nachweis dienen.

Nr. 11.2 – Vertreterbenennung (Art. 27 i.V.m. Art. 3 Abs. 2 DSGVO)

Kriterium

(1) Cloud-Anbieter ohne Niederlassung in der EU oder im EWR, für die dennoch gemäß Art. 3 Abs. 2 DSGVO die Datenschutz-Grundverordnung gilt, benennen schriftlich einen Vertreter in der EU oder im EWR. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen sich die betroffenen Personen befinden, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird.

(2) Der Cloud-Anbieter beauftragt den Vertreter als Ansprechpartner für sämtliche Fragen im Zusammenhang mit der Datenverarbeitung zur Gewährleistung der Einhaltung der Datenschutz-Grundverordnung und erteilt dem Vertreter die notwendigen Vollmachten, damit dieser im Namen des Cloud-Anbieters und an dessen Stelle tätig werden kann, um die Pflichten der Datenschutz-Grundverordnung zu erfüllen.

Erläuterung

Der Cloud-Anbieter kann bei der Beauftragung entscheiden, ob der Vertreter ergänzend zu ihm oder allein als Ansprechpartner auftreten soll; dies ist entsprechend im Außenverhältnis zu kommunizieren. Bietet der Cloud-Anbieter ohne Niederlassung in der EU oder im EWR seine Dienstleistung in mehreren Mitgliedstaaten an, muss er nicht in jedem Mitgliedstaat einen Vertreter benennen, vielmehr ist auch ein

Vertreter in einem Mitgliedstaat mit Zuständigkeit für mehrere Mitgliedstaaten zulässig, solange sich in diesem betroffene Personen befinden.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er die schriftliche Benennung eines Vertreters vorlegt.

D. Kriterien und Umsetzungshinweise für Verarbeitung als Verantwortlicher

Kapitel VII: Der Cloud-Anbieter als Verantwortlicher

Nr. 12 – Sicherstellung der Datenschutzgrundsätze
(Art. 5 Abs. 1 und 2 i.V.m. Art. 24 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt bei der Verarbeitung von personenbezogenen Daten, die für die Durchführung des Auftrags über die Erbringung des Cloud-Dienstes oder zur Erfüllung rechtlicher Verpflichtungen erforderlich sind, dem Cloud-Nutzer alle Informationen zur Verfügung, die dieser benötigt, um die Rechtmäßigkeit der Verarbeitung überprüfen zu können (Grundsatz der Transparenz).

(2) Der Cloud-Anbieter legt für die Verarbeitung der Daten zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen die Zwecke der jeweiligen Datenverarbeitungen eindeutig und präzise fest (Grundsätze der Zweckfestlegung und Zweckbindung).

(3) Der Cloud-Anbieter verarbeitet nur personenbezogene Daten des Cloud-Nutzers, soweit diese zur Erreichung der festgelegten Verarbeitungszwecke erforderlich sind (Grundsatz der Datenminimierung).

(4) Der Cloud-Anbieter verfügt über TOM zur Prüfung, Korrektur und Löschung unzutreffender oder unvollständiger personenbezogener Daten, die er für die Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen verarbeitet (Grundsatz der Datenrichtigkeit).

(5) Der Cloud-Anbieter stellt bei der Datenverarbeitung den Personenbezug nur solange her, wie dies für die Erreichung der festgelegten Zwecke zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes oder zur Erfüllung rechtlicher Verpflichtungen unverzichtbar ist und löscht nicht erforderliche Daten frühestmöglich (Grundsatz der Speicherbegrenzung).

Erläuterung

Der Zweck stellt die zu steuernde Größe für die Datenauswahl und die Prozessschritte der Verarbeitung dar. Da eine weite Zweckfestlegung kaum steuernde Wirkung entfaltet, reicht es nicht aus, wenn lediglich die Vertragserfüllung aus Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO oder die Erfüllung rechtlicher Verpflichtungen aus Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO als Zweck der Datenverarbeitung festgelegt wird. Vielmehr muss bei der Zweckfestlegung der präzise und konkrete Geschäfts- oder Verarbeitungszweck festgelegt werden. Erst nach dieser Zweckfestlegung können die anderen Datenschutzgrundsätze ihre Wirkung entfalten.

Umsetzungshinweis

Der Transparenzgrundsatz wird erfüllt, wenn der Cloud-Anbieter seinen Informations- und Auskunftspflichten über die Datenverarbeitung (Nr. 15.1 und Nr. 15.2) nachkommt. Außerdem kann Transparenz durch datenschutzgerechte Systemgestaltung und datenschutzfreundliche Voreinstellungen (Nr. 20.1 und Nr. 20.2) erreicht werden.

Zur Einhaltung der Speicherbegrenzung sollte der Cloud-Anbieter für alle Daten oder Datenkategorien Speicherfristen festlegen, die auf das erforderliche Mindestmaß beschränkt sind. Zudem sollten Fristen bestimmt werden, wann personenbezogene Daten gelöscht werden oder der Personenbezug beseitigt wird. Müssen Daten aufgrund gesetzlicher Vorschriften aufbewahrt werden, sollten sie pseudonym aufbewahrt werden und der Personenbezug erst bei Bedarf wiederhergestellt werden.

Nachweis

Der Cloud-Anbieter legt eine Dokumentation vor, aus der sich die TOM ergeben, die er ergriffen hat, um die Einhaltung der Datenschutzgrundsätze sicherzustellen.

Nr. 13 – Rechtsgrundlage für die Datenverarbeitung (Art. 6 Abs. 1 UAbs. 1 lit. b. sowie lit. c i.V.m. Abs. 2 DSGVO)

Kriterium

Der Cloud-Anbieter verarbeitet personenbezogene Daten für die Erfüllung eines Vertrags zur Datenverarbeitung im Auftrag des Cloud-Nutzers oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage des Cloud-Nutzers erfolgen oder zur Erfüllung einer rechtlichen Verpflichtung, der er unterliegt.

Erläuterung

AUDITOR betrachtet die Datenverarbeitungsvorgänge des Cloud-Anbieters in seiner Rolle als Verantwortlicher nur, soweit diese erforderlich sind, um den Auftrag mit dem Cloud-Nutzer über die Erbringung des Cloud-Dienstes zu erfüllen. Die Rechtsgrundlage der Datenverarbeitung bildet daher Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO. Die Norm erlaubt die Datenverarbeitung, soweit diese für die Erfüllung eines Vertrags oder für vorvertragliche Maßnahme erforderlich ist. Der Datenumgang für das Zustandekommen eines Vertrags, für Vertragsänderungen und -beendigungen gehört zur Vertragserfüllung. Auch Daten, die für die Ermöglichung der Inanspruchnahme des Cloud-Dienstes oder die Abrechnung der Nutzung des Cloud-Dienstes erforderlich sind, sind Teil der Vertragserfüllung und fallen somit unter Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO.

Schließen Cloud-Anbieter und Cloud-Nutzer einen Vertrag über die Bereitstellung eines Cloud-Dienstes, wird der Cloud-Anbieter u.a. aufgrund handels- und steuerrechtlicher Aufbewahrungspflichten zur Verarbeitung personenbezogener Daten des Cloud-Nutzers verpflichtet. Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO erlaubt die Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt. Die eigentlichen Rechtsgrundlagen für solche Verarbeitungen folgen aus nationalen oder europarechtlichen Vorschriften, da Art. 6 Abs. 2 DSGVO eine Öffnungsklausel zur Anwendung solcher Vorschriften enthält.

Über die Rechtsgrundlage einer Datenverarbeitung hat der Cloud-Anbieter den Cloud-Nutzer im Rahmen seiner Informationspflicht nach Art. 13 Abs. 1 lit. c DSGVO (Nr. 15.1) zu informieren.

Nachweis

Der Cloud-Anbieter kann im Rahmen der Zertifizierung alle oder eine repräsentative Stichprobe von rechtsverbindlichen Vereinbarungen vorlegen, die er mit den Cloud-Nutzern über die Bereitstellung eines Cloud-Dienstes geschlossen hat.

Der Cloud-Anbieter legt im Rahmen der Zertifizierung eine Übersicht vor, aus der hervorgeht, welchen rechtlichen Verpflichtungen er zur Datenverarbeitung unterliegt.

Nr. 14 – Gewährleistung der Datensicherheit durch geeignete TOM nach dem Stand der Technik

Erläuterungen

Auch für die Datenverarbeitung zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes gegenüber dem Cloud-Nutzer und zur Erfüllung rechtlicher Verpflichtungen gilt, dass der Cloud-Anbieter durch TOM sicherstellen muss, dass Daten entsprechend ihrer Schutzbedürftigkeit vor allem vor sicherheitsrelevanter Vernichtung, vor Verlust und unbefugter Offenlegung geschützt werden.

Da der Cloud-Anbieter durch Durchführung des Auftrags mit dem Cloud-Nutzer und zur Erfüllung rechtlicher Verpflichtungen regelmäßig keine personenbezogenen Daten der Schutzklasse 3 verarbeiten wird, werden Kriterien nur für die Schutzklassen 1 und 2 angegeben.

Nr. 14.1 – Datensicherheitskonzept
(Art. 24, 25, 32 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

(1) Der Cloud-Anbieter führt eine Risikoanalyse in Bezug auf die Datensicherheit durch und verfügt über ein Datensicherheitskonzept entsprechend seiner Schutzklasse, das den spezifischen Risiken seiner Datenverarbeitungsvorgänge zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen angemessen ist.

(2) Im Datensicherheitskonzept stellt der Cloud-Anbieter dar, welche Datensicherheitsmaßnahmen er ergriffen hat, um die bestehenden Risiken abzustellen oder einzudämmen. Der Cloud-Anbieter schildert auch die Abwägungen, die er vorgenommen hat, um zu diesen Maßnahmen zu gelangen.

(3) Das Datensicherheitskonzept ist schriftlich zu dokumentieren.

(4) Das Datensicherheitskonzept ist in regelmäßigen Abständen auf Aktualität und Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren.

(5) Sofern der Cloud-Anbieter Auftragsverarbeiter zur Durchführung des Auftrags mit dem Cloud-Nutzer einsetzt, beschreibt das Datensicherheitskonzept welche Datenverarbeitungsvorgänge ausgelagert sind und daher den TOM des Auftragsverarbeiters unterliegen.

(6) Soweit das Datensicherheitskonzept Sicherheitsmaßnahmen des Cloud-Nutzers verlangt, sind diese dem Cloud-Nutzer in Schriftform oder in einem elektronischen Format mitzuteilen.

Erläuterung

Auch hinsichtlich der Datenverarbeitung zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen müssen Risiken insbesondere gegen unbeabsichtigte und unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugten Zugang zu personenbezogenen Daten ausgeschlossen oder zumindest minimiert werden. Bei der Festlegung der konkreten Maßnahmen berücksichtigt der Cloud-Anbieter nicht nur die Modalitäten der Verarbeitung und die Eintrittswahrscheinlichkeit und Schwere des Schadens, sondern auch den Stand der Technik sowie die Implementierungskosten der Maßnahmen. Die dabei getroffenen Abwägungen müssen aus dem Datensicherheitskonzept ersichtlich werden.

Umsetzungshinweis

Auch für die Datenverarbeitungsvorgänge zur Durchführung des Auftrags mit dem Cloud-Nutzer und zur Erfüllung rechtlicher Verpflichtungen sollte eine Risikoanalyse durchgeführt werden, bei der der Risikobewertungsansatz und die Risikobewertungsmethodik dokumentiert werden. Jedem Risiko sollte durch eine oder mehrere Schutzmaßnahmen begegnet werden.

Bei der Analyse von Risiken können folgende Merkmale analysiert und evaluiert werden:

1) Evaluierung der Auswirkungen auf die Organisation, Technik oder Dienstbereitstellung aufgrund eines Sicherheitsausfalls und Berücksichtigung der Konsequenzen des Verlusts von Vertraulichkeit, Integrität oder Verfügbarkeit;

2) Evaluierung der realistischen Wahrscheinlichkeit eines solchen Sicherheitsausfalls unter Berücksichtigung aller denkbaren Bedrohungen und Sicherheitslücken;

3) Abschätzung des möglichen Schadensausmaßes für die Grundrechte und Freiheiten der betroffenen Personen;

4) Prüfung, ob alle möglichen Optionen für die Behandlung der Risiken identifiziert und evaluiert sind;

5) Bewertung, ob das verbleibende Risiko akzeptierbar oder eine Gegenmaßnahme erforderlich ist.

Das Datensicherheitskonzept sollte unter Berücksichtigung neu auftretender Sicherheitsherausforderungen kontinuierlich aktualisiert und verbessert werden. Dabei sollten Risikobewertungen, das mögliche Schadensausmaß und die identifizierten akzeptablen Risiken regelmäßig unter Berücksichtigung des Wandels der Organisation, der Technologien, von Geschäftszielen und -prozessen, von erkannten Bedrohungen, der Auswirkungen der implementierten Kontrollen und der externen Ereignisse überprüft werden.

Nachweis

Das Datensicherheitskonzept und seine Angemessenheit kann der Cloud-Anbieter dadurch nachweisen, dass er dieses vorlegt.

Nr. 14.2 – Sicherheitsbereich und Zutrittskontrolle (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter sichert Räume und Anlagen gegen Schädigung durch Naturereignisse4 und verwehrt Unbefugten den Zutritt zu Räumen und Datenverarbeitungsanlagen, um unbefugte Kenntnisnahmen personenbezogener Daten und Einwirkungsmöglichkeiten auf die Datenverarbeitungsanlagen auszuschließen. Die TOM müssen geeignet sein, um im Regelfall den Zutritt Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert.

Schutzklasse 2

(2) Die Kriterien von Schutzklasse 1 sind erfüllt.

(3) Die TOM sind geeignet, um Schädigungen durch fahrlässige Handlungen Befugter im Regelfall auszuschließen. Sie schließen unbefugten Zutritt durch fahrlässige und vorsätzliche Handlungen hinreichend sicher aus. Dies gilt auch für Zutrittsversuche durch Täuschung oder Gewalt. Die TOM gewährleisten einen hinreichenden Schutz gegen bekannte Angriffsszenarien.

(4) Jeder unbefugte Zutritt und Zutrittsversuch wird nachträglich festgestellt.

Erläuterung

Dieses Kriterium konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Art. 5 Abs. 1 lit. f DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Integrität, Vertraulichkeit und Verfügbarkeit (SDM 6.2.1 – 6.2.3) von personenbezogenen Daten und Diensten auf Dauer zu gewährleisten. Dies setzt ein Berechtigungskonzept für den Zutritt zu Datenverarbeitungsanlagen voraus. Die Zutrittskontrolle gewährleistet den Zutrittsschutz nicht nur im Normalbetrieb, sondern auch im Zusammenhang mit Naturereignissen.

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27001 Ziff. A11 und ISO/IEC 27018 Ziff. 11 sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Datensicherheitskonzept die TOM zur Zutrittskontrolle darlegt.

[4] Naturereignisse stellen ungewöhnliche, in der Natur ablaufende Vorgänge dar, die vom Menschen nicht beeinflusst werden können und zeitlich begrenzt sind. Beispiele sind Blitze, Hochwasser, Trockenheit.

Nr. 14.3 – Zugangskontrolle
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter stellt sicher, dass Unbefugte keinen Zugang zu Datenverarbeitungssystemen erhalten und auf diese einwirken können. Dies gilt auch für Sicherungskopien, soweit diese personenbezogene Daten enthalten.

(2) Der Cloud-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zugang zu Datenverarbeitungssystemen in regelmäßigen Abständen auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

(3) Der Cloud-Anbieter schützt Zugänge von Befugten über das Internet mit einer starken Authentifizierung, die mindestens zwei Elemente der Kategorie Wissen, Besitz oder Inhärenz verwendet. Die Elemente müssen voneinander unabhängig sein, sodass die Überwindung eines Elements die Zuverlässigkeit des anderen nicht beeinflusst. Sie müssen so konzipiert sein, dass die Vertraulichkeit der Authentifizierungsdaten gewährleistet ist. Der Zugang über das Internet hat über einen verschlüsselten Kommunikationskanal zu erfolgen.

(4) Die Maßnahmen zur Zugangskontrolle sind geeignet, um im Regelfall den Zugang zu Datenverarbeitungssystemen durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert.

Schutzklasse 2

(1) Die Kriterien von Schutzklasse 1 sind erfüllt.

(2) Gegen zu erwartenden vorsätzlichen unbefugten Zugang ist ein Schutz vorzusehen, der zu erwartende Zugangsversuche hinreichend sicher ausschließt. Die TOM gewährleisten einen hinreichenden Schutz gegen bekannte Angriffsszenarien und stellen einen unbefugten Zugang im Regelfall nachträglich fest.

Erläuterungen

Das Kriterium der Zugangskontrolle konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele der Integrität, Vertraulichkeit und Verfügbarkeit (SDM 6.2.1 – 6.2.3) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen. Dies setzt ein Berechtigungskonzept für den Zugang zu Datenverarbeitungssystemen voraus.

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27001 Ziff. A12.1.4, A12.4.2 sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er im Datensicherheitskonzept die TOM zur Zugangskontrolle darlegt.

Nr. 14.4 – Zugriffskontrolle
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter stellt durch TOM sicher, dass Berechtigte nur im Rahmen ihrer Berechtigungen auf personenbezogene Daten zugreifen können und schließt unbefugte Einwirkungen auf Datenverarbeitungsvorgänge aus. Dies gilt auch für Sicherungskopien, soweit sie personenbezogene Daten enthalten.

(2) Zugriffe auf personenbezogene Daten sind zu kontrollieren.

(3) Die TOM sind geeignet, um im Regelfall den Zugriff auf Daten durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen. Gegen vorsätzliche Eingriffe besteht ein Mindestschutz, der diese erschwert.

(4) Der Cloud-Anbieter schützt Zugriffe von Befugten über das Internet durch eine starke Authentifizierung, die mindestens zwei Elemente der Kategorie Wissen, Besitz oder Inhärenz verwendet, die insofern voneinander unabhängig sind, als die Überwindung eines Elements die Zuverlässigkeit des anderen nicht in Frage stellt, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten gewährleistet ist.

Schutzklasse 2

(1) Die Kriterien von Schutzklasse 1 sind erfüllt.

(2) Gegen zu erwartenden vorsätzlichen unbefugten Zugriff ist ein Schutz vorzusehen, der zu erwartende Zugriffsversuche hinreichend sicher ausschließt. Die TOM gewährleisten einen hinreichenden Schutz gegen bekannte Angriffsszenarien und stellen einen unberechtigten Zugriff im Regelfall nachträglich fest.

Erläuterungen

Das Kriterium der Zugriffskontrolle konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Integrität, Vertraulichkeit und Verfügbarkeit (SDM 6.2.1 – 6.2.3) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen. Dies setzt ein Berechtigungskonzept für den Zugriff auf personenbezogenen Daten voraus.

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27002 Ziff. 13.2 sind anwendbar.

Ein geeigneter Managementprozess für die Zugriffskontrolle sollte etabliert werden, der die Erforderlichkeit der Berechtigungen in regelmäßigen Abständen auf Angemessenheit überprüft, die Vergabe, Aktualisierung, Kontrolle und den Entzug von Berechtigungen regelt, Zugriffspolitiken überwacht und aktualisiert sowie Passwortrichtlinien überprüft und die Einhaltung sicherstellt.

Der Cloud-Anbieter sollte angemessene Sicherheitsmaßnamen gegen sowohl interne auch gegen externe Angriffe implementieren, um einen unbefugten Zugriff zu verhindern. Hierzu zählen beispielsweise sämtliche Standardmaßnahmen für den Schutz des Cloud-Hosts, d. h. Host Firewalls, Network-Intrusion-Prevention-Systeme, Applikationsschutz, Antivirus, regelmäßige Integritätsüberprüfungen wichtiger Systemdateien und Host-based Intrusion-Detection-Systeme. Der Cloud-Anbieter sollte seinen Dienst ununterbrochen auf Angriffe und Sicherheitsvorfälle überwachen, um verdächtige Aktivitäten (bspw. Extraktion großer Datenmengen), Angriffe und Sicherheitsvorfälle rechtzeitig erkennen und angemessene und zeitnahe Reaktionen einleiten zu können.

Um vorsätzliche Eingriffe auf Datenverarbeitungsvorgänge durch Mitarbeiter zu erschweren, sollten der Cloud-Anbieter Zugriffsberechtigungen restriktiv vergeben, um den Kreis der Berechtigten klein zu halten. Mitarbeiter sollten nur Zugriff auf die Daten und Datenverarbeitungsvorgänge haben, die sie für ihre Aufgabenerledigung benötigen. Eine weitere Maßnahme, um vorsätzliche Eingriffe durch Mitarbeiter zu erschweren, kann die Implementierung eines Vier-Augen-Prinzips sein, das bestimmte Aktionen an Datenverarbeitungsvorgängen nur zulässt, wenn mindestens ein weiterer Mitarbeiter der Aktion zugestimmt hat. Der Cloud-Anbieter sollte die Zugriffe protokollieren, um Zugriffe durch befugte Mitarbeiter nachträglich nachverfolgen zu können.

Der Cloud-Anbieter sollte sämtliche relevanten Sicherheitsereignisse einschließlich aller Sicherheitslücken oder -vorfälle erfassen, protokollieren, revisionssicher archivieren und auswerten. Ein handlungsfähiges Team für Security-Incident-Handling und Trouble-Shooting sollte ununterbrochen erreichbar sein, damit Sicherheitsvorfälle gemeldet und zeitnah bearbeitet werden können.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er im Datensicherheitskonzept die TOM zur Zugriffskontrolle darlegt.

Nr. 14.5 – Übertragung von Daten und Transportverschlüsselung (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f und Abs. 2 DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter setzt bei Datenübertragungsvorgängen eine Transportverschlüsselung nach dem Stand der Technik oder gleichermaßen angemessene Maßnahmen ein oder fordert dies durch entsprechende Konfiguration von Schnittstellen. Die eingesetzte Transportverschlüsselung gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Bei verschlüsselter Übertragung sind die Schlüssel sicher aufzubewahren.

(2) Der Cloud-Anbieter schließt im Regelfall solche Handlungen Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter aus. Die TOM verhindern im Regelfall die fahrlässige Weitergabe von Daten an Unbefugte durch den Cloud-Anbieter und seine Mitarbeiter. Gegen vorsätzliche Eingriffe besteht ein Mindestschutz, der diese erschwert.

(3) Der Cloud-Anbieter protokolliert automatisiert die Metadaten aller Datenübertragungsvorgänge, einschließlich der Empfänger, auch solche vom und an den Cloud-Nutzer oder an Subauftragsverarbeiter.

(4) Die Kriterien gelten auch für die Übertragung von Daten im eigenen Netzwerk des Cloud-Anbieters und seiner Auftragsverarbeiter und zwischen diesen.

(5) Der Cloud-Anbieter verhindert beim Transport von Datenträgern durch TOM, dass personenbezogene Daten unbefugt gelesen, kopiert, verändert oder entfernt werden können. Der Cloud-Anbieter dokumentiert die Transporte.

Schutzklasse 2

(6) Die Kriterien von Schutzklasse 1 sind erfüllt.

(7) Der Cloud-Anbieter schützt personenbezogene Daten gegen vorsätzliches unbefugtes Lesen, Kopieren, Verändern oder Entfernen und schließt zu erwartende Versuche hinreichend sicher aus. Er schützt gegen bekannte Angriffsszenarien und stellt ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen im Regelfall (nachträglich) fest.

Erläuterungen

Das Kriterium der Übertragungs- und Transportkontrolle konkretisiert die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Integrität, Vertraulichkeit und Verfügbarkeit (SDM 6.2.1 – 6.2.3) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen und personenbezogene Daten gegen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugten Zugang oder unbefugte Offenlegung während der elektronischen Übertragung, des Transports oder der Speicherung auf Datenträgern zu schützen.

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27018 Ziff. 10.1.1, ISO/IEC 27002 Ziff. 12.4, ISO/IEC 27040:2017-03 Ziff. 6.7.1 und ISO/IEC 27040:2017-03 Ziff. 7.7.1 sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Datensicherheitskonzept die TOM zur Übertragungs- und Transportkontrolle darlegt.

Nr. 14.6 – Nachvollziehbarkeit der Datenverarbeitung (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. c, e, f und Abs. 2 DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter protokolliert Eingaben, Veränderungen und Löschungen an Daten, die zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen erforderlich sind, um eine nachträgliche Prüfbarkeit und Nachvollziehbarkeit der Datenverarbeitung sicherzustellen. Bei Protokollierungen sind die Grundsätze der Erforderlichkeit, Zweckbindung und Datenminimierung zu beachten. Die Protokolldaten sind sicher aufzubewahren.

(2) Der Cloud-Anbieter kann Dateneingaben, -veränderungen oder -löschungen, die bei der bestimmungsgemäßen Nutzung des Cloud-Dienstes durch den Cloud-Nutzer wie bei administrativen Maßnahmen des Cloud-Anbieters erfolgen, jederzeit nachvollziehen.

(3) Der Cloud-Anbieter gestaltet die Protokollierung der administrativen Aktivitäten und der Nutzer-Aktivitäten so, dass die Nachvollziehbarkeit von Eingaben, Veränderungen und Löschungen im Regelfall auch bei technischen oder organisatorischen Fehlern, einschließlich Bedienfehlern des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter gewahrt bleibt. Er sieht gegen vorsätzliche Manipulationen an den Maßnahmen zur Nachvollziehbarkeit einen Mindestschutz vor, der diese Manipulationen erschwert.

Schutzklasse 2

(4) Die Kriterien von Schutzklasse 1 sind erfüllt.

(5) Der Cloud-Anbieter sieht gegen zu erwartende vorsätzliche Manipulationen der Protokollierungsinstanzen und gegen vorsätzlichen Zugriff auf oder Manipulationen von Protokollierungsdateien (Logs) durch Unbefugte einen Schutz vor, der zu erwartende Manipulationsversuche hinreichend und sicher ausschließt. Zu diesen Schutzmaßnahmen gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die eine Manipulation im Regelfall (nachträglich) festgestellt werden kann.

Erläuterung

Das Kriterium der Nachvollziehbarkeit konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Integrität, Vertraulichkeit und Verfügbarkeit (SDM 6.2.1 – 6.2.3) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen und personenbezogene Daten gegen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugten Zugang oder unbefugte Offenlegung zu schützen. Hierzu muss nachträglich überprüft und festgestellt werden können, ob, wann und von wem und mit welchen inhaltlichen Auswirkungen personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, um gegebenenfalls Zugriffsrechte für die Zukunft anders zu gestalten. Zur sicheren Aufbewahrung der Protokolldaten gehört auch, dass die Auswertbarkeit der Protokolldaten sichergestellt ist.

Da im Rahmen von Protokollierungen regelmäßig personenbezogene Daten anfallen, unterliegt der Umgang mit Protokollierungsdaten ebenfalls datenschutzrechtlichen Anforderungen. Auf die Datenschutzgrundsätze aus Art. 5 DSGVO wird Bezug genommen. Auf das Gewährleistungsziel der Datenminimierung und der Zweckbindung aus Art. 5 Abs. 1 lit. c und b DSGVO ist besonderes Augenmerk zu legen.

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27018 Ziff. 12.4.1, 12.4.2 und ISO/IEC 27002 Ziff. 12.4 sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er im Datensicherheitskonzept dokumentiert, wie er durch Festlegung von Gegenstand und Umfang der Protokollierung, Aufbewahrung und Verwendung der Protokolldaten, Integritätsschutz und Löschung von Protokollen, die Datenschutzziele sicherstellt.

Nr. 14.7 – Verschlüsselung gespeicherter Daten (Art. 32 Abs. 1 lit. a DSGVO)

Kriterium

Schutzklasse 1 und 2

(1) Der Cloud-Anbieter stellt sicher, dass Anmeldedaten zur Nutzung des Cloud-Dienstes in einer Weise verschlüsselt gespeichert werden, dass auch er intern keinen Zugriff darauf hat.

(2) Der Cloud-Anbieter verschlüsselt personenbezogene Daten, die zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen gespeichert werden müssen, und speichert sie verschlüsselt.

(3) Der Cloud-Anbieter verfolgt laufend die technische Entwicklung im Bereich der Verschlüsselung und setzt Verschlüsselungsverfahren ein, die den aktuellen technischen Empfehlungen (best practice) entsprechen.

(4) Eingesetzte Verschlüsselungsverfahren sind durch andere Verschlüsselungsverfahren zu ersetzen, wenn sie nicht mehr den aktuellen technischen Empfehlungen (best practice) entsprechen.

Erläuterung

Die Verschlüsselung wird neben der Pseudonymisierung in Art. 32 Abs. 1 lit. a DSGVO explizit als eine einzusetzende Sicherheitsmaßnahme benannt. Zweck der Verschlüsselung ist es, die Gewährleistungsziele der Vertraulichkeit und Integrität (SDM 6.2.2 und 6.2.2) sicherzustellen. Die Schwelle, ab der zu verschlüsseln ist, ist niedrig, sodass personenbezogene Daten bereits bei niedrigem Risiko verschlüsselt werden sollten, soweit dies möglich ist.

Umsetzungshinweis

Der Stand der Technik ergibt sich aus aktuellen technischen Normen für kryptographische Verfahren und deren Anwendung. Die Umsetzungshinweise aus ISO/IEC 27018 Ziff. 10 und ISO/IEC 27002, Z. 10 sind anwendbar.

Die Schlüsselerzeugung bei der Verschlüsselung sollte in einer sicheren Umgebung und unter Einsatz geeigneter Schlüsselgeneratoren erfolgen. Kryptografische Schlüssel sollten möglichst nur einem Einsatzzweck dienen und generell nie in klarer Form, sondern grundsätzlich verschlüsselt im System gespeichert werden. Die Speicherung muss stets redundant gesichert und wiederherstellbar sein, um einen Verlust eines Schlüssels auszuschließen. Schlüsselwechsel müssen regelmäßig durchgeführt werden. Der Zugang zum Schlüsselverwaltungssystem sollte eine separate Authentisierung erfordern.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Datensicherheitskonzept dokumentiert, dass die angewandten Verschlüsselungsverfahren den aktuellen technischen Anforderungen entsprechen. Er legt Prozessdokumentationen vor, wie er die technische Entwicklung im Bereich der Verschlüsselung verfolgt und die Geeignetheit des Verfahrens fortdauernd prüft und es gegebenenfalls aktualisiert. Er weist in seinem Datensicherheitskonzept nach, dass er die eingesetzten Verschlüsselungstechniken durch geeignete technische Tests geprüft hat.

Nr. 14.8 – Getrennte Verarbeitung (Art. 5 Abs. 1 lit. b i.V.m. Art. 24, 25, 32 Abs. 1 lit. b und Abs. 2 DSGVO)

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter verarbeitet personenbezogene Daten, die zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Pflichten verarbeitet werden, getrennt nach den jeweiligen Verarbeitungszwecken.

(2) Die Datentrennung muss im Regelfall auch bei technischen oder organisatorischen Fehlern, einschließlich Bedienfehlern, des Cloud-Anbieters oder seiner Mitarbeiter gewahrt ein. Der

Cloud-Anbieter realisiert einen Mindestschutz, der vorsätzliche Verstöße gegen das Trennungsgebot verhindert.

Schutzklasse 2

(3) Die Kriterien von Schutzklasse 1 sind erfüllt.

(4) Der Cloud-Anbieter schließt zu erwartende vorsätzliche Verstöße hinreichend sicher aus. Zu den dafür erforderlichen TOM gehört im Rahmen der Datenspeicherung die Verschlüsselung mit individuellen Schlüsseln. Er stellt vorsätzliche Verstöße gegen das Trennungsgebot im Regelfall (nachträglich) fest.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Verfügbarkeit, Integrität, Vertraulichkeit und Nichtverkettung (SDM 6.2.1 – 6.2.4) und zielt damit auch auf die Sicherstellung des Zweckbindungsgrundsatzes aus Art. 5 Abs. 1 lit. b DSGVO.

Umsetzungshinweis

Die Umsetzungshinweise aus ISO/IEC 27002 Ziff. 12.1.4, 13.1.3 sind anwendbar.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er im Datensicherheitskonzept dokumentiert, welche TOM er ergriffen hat, um Datenbestände nach den Verarbeitungszwecken voneinander zu trennen.

Nr. 15 – Wahrung von Betroffenenrechten

Nr. 15.1 – Informationspflicht (Art. 13 i.V.m. Art. 12 Abs. 1 und Art. 5 Abs. 1 lit. a DSGVO)

Kriterium

Der Cloud-Anbieter stellt durch TOM sicher, dass er den Cloud-Nutzer zum Zeitpunkt der Erhebung seiner personenbezogenen Daten zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen über die Umstände der Verarbeitung und über seine Betroffenenrechte verständlich und in klarer und einfacher Sprache informiert. Er informiert den Cloud-Nutzer über alle in Art. 13 Abs. 1 und 2 DSGVO geforderten Angaben.

Erläuterung

Der Cloud-Anbieter ist nach Art. 13 DSGVO verpflichtet, die betroffene Person über die Umstände der Direkterhebung zu informieren. Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM 6.2.5 und 6.2.6).

Nachweis

Der Cloud-Anbieter legt das Muster seiner Datenschutzerklärung mit den Informationen nach Art. 13 Abs. 1 und 2 DSGVO vor, das der Cloud-Nutzer bei Vertragsschluss über die Erbringung des Cloud-Dienstes erhält. Findet der Vertragsschluss online statt, kann im Rahmen eines (Test-)Vertragsabschlusses getestet werden, ob der Cloud-Anbieter alle Informationen nach Art. 13 Abs. 1 und 2 DSGVO bereitstellt.

Nr. 15.2 – Auskunftserteilung (Art. 15 i.V.m. Art. 5 Abs. 1 lit. a 3. Alt. DSGVO)

Kriterium

Der Cloud-Anbieter stellt durch TOM sicher, dass er dem Cloud-Nutzer auf Antrag Auskunft über die Datenverarbeitung erteilt, die er als Verantwortlicher über ihn zur Durchführung des Auftrags

> über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen durchführt. Er stellt dem Cloud-Nutzer eine Kopie dieser Daten zur Verfügung.

Erläuterung

Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM 6.2.5 und 6.2.6).

Umsetzungshinweise

Der Cloud-Anbieter hat der betroffenen Person nach Art. 12 Abs. 3 DSGVO die Auskunft unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zu erteilen. Die Antragstellung sollte möglichst einfach sein, weshalb Kontaktformulare oder Customer-Self-Services via Webportal bereitgestellt werden sollten. Nach Art. 15 Abs. 3 DSGVO hat die betroffene Person einen Anspruch auf eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er dokumentiert, welche Maßnahmen er ergriffen hat, um dem Cloud-Nutzer zeitgerecht Auskunft zu erteilen. Auch können anhand einer Prozessdokumentation die tatsächlich durchgeführten Auskunftserteilungen nachgewiesen werden.

Nr. 15.3 – Berichtigung und Vervollständigung (Art. 16 i.V.m. Art. 5 Abs. 1 lit. d DSGVO)

Kriterium

> Der Cloud-Anbieter stellt durch TOM sicher, dass er dem Cloud-Nutzer die Möglichkeit einräumt, seine in Zusammenhang mit der Durchführung des Auftrags über die Erbringung des Cloud-Dienstes stehenden unvollständigen oder unrichtigen personenbezogenen Daten selbst zu korrigieren oder zu löschen. Alternativ führt der Cloud-Anbieter die (berechtigte) Korrektur oder Löschung durch.

Erläuterung

Der Cloud-Anbieter ist nach Art. 16 DSGVO verpflichtet, auf Antrag unrichtige personenbezogene Daten zu berichtigen und unvollständige personenbezogene Daten von betroffenen Personen zu vervollständigen. Die Berichtigung gemäß Art. 16 DSGVO fördert das Gewährleistungsziel der Intervenierbarkeit (SDM 6.2.6).

Umsetzungshinweise

Auch unabhängig vom Antrag betroffener Personen ist der Cloud-Anbieter aus Art. 5 Abs. 1 lit. d DSGVO zur Datenrichtigkeit verantwortlich, weshalb er Fristen für die regelmäßige Überprüfung und Löschung von Daten festlegen sollte.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er dokumentiert, welche Maßnahmen er ergriffen hat, um Cloud-Nutzern die (direkte) Berichtigung und Vervollständigung von Daten zu ermöglichen oder um die Berichtigung und Vervollständigung selbst vorzunehmen.

Weiterhin können durch Prozessdokumentationen die tatsächlich durchgeführten Berichtigungen und Vervollständigungen nachgewiesen werden.

Nr. 15.4 – Löschung (Art. 17 Abs. 1 DSGVO)

Kriterium

> Der Cloud-Anbieter stellt durch TOM sicher, dass er personenbezogene Daten des Cloud-Nutzers, die er zur Erfüllung des Auftrags über die Erbringung des Cloud-Dienstes verarbeitet, auf Antrag des Cloud-Nutzers und von sich aus unverzüglich löscht, wenn die Voraussetzungen von Art. 17 Abs. 1 lit. a, d oder e DSGVO vorliegen.

Erläuterung

Das Kriterium fördert die Gewährleistungsziele der Intervenierbarkeit und Nichtverkettung (SDM 6.2.4 und 6.2.6). Keine Pflicht zur Löschung besteht insbesondere, wenn der Cloud-Anbieter zur Verarbeitung verpflichtet ist, um eine rechtliche Verpflichtung zu erfüllen (Art. 17 Abs. 3 lit. DSGVO).

Umsetzungshinweis

Um seinen Löschungspflichten nachzukommen zu können, sollte der Cloud-Anbieter ein Löschkonzept anfertigen, mit dem er seine Löschverpflichtungen laufend ermitteln und prüfen kann. Das Löschkonzept sollte Kriterien enthalten, anhand derer bestimmt werden kann, ob ein Datensatz gelöscht werden muss oder aufgrund von Aufbewahrungsfristen gespeichert werden muss. Zu jedem Datensatz sollten daher „Metadaten“ wie Zweck der Verarbeitung, Festlegung von Indikatoren für den Wegfall eines Erlaubnistatbestands, Aufbewahrungsfristen und die Rechtsgrundlage der Speicherung niedergelegt werden.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er dokumentiert, welche Maßnahmen er ergriffen hat, um das Löschbegehren des Cloud-Nutzers zu prüfen und durchzuführen. Auch können anhand von Prozessdokumentationen die tatsächlich durchgeführten Löschungen nachgewiesen werden.

Nr. 15.5 – Einschränkung der Verarbeitung (Art. 18 Abs. 1 und 3 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch TOM sicher, dass er die Verarbeitung von personenbezogenen Daten des Cloud-Nutzers, die er durchführt, um den Auftrag mit diesem über die Erbringung des Cloud-Dienstes zu erbringen oder eine rechtliche Verpflichtung zu erfüllen, auf Antrag einschränken kann.

(2) Der Cloud-Anbieter stellt durch TOM sicher, dass er den Cloud-Nutzer informiert, bevor er eine Einschränkung aufhebt.

Erläuterung

Der Cloud-Anbieter ist nach Art. 18 Abs. 1 DSGVO verpflichtet, die Verarbeitung personenbezogener Daten unter bestimmten Voraussetzungen einzuschränken, sodass Daten nicht weiterverarbeitet oder verändert werden können. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM 6.2.6).

Umsetzungshinweis

Eine Einschränkung der Verarbeitung kann beispielsweise durch eine vorübergehende Übertragung in ein anderes Verarbeitungssystem oder durch Sperrung erfolgen.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er dokumentiert, welche Maßnahmen er ergriffen hat, um die Verarbeitung von Daten einzuschränken und den Cloud-Nutzer vor Aufhebung der Einschränkung zu informieren.

Nr. 15.6 – Mitteilungspflicht bei Berichtung, Löschung oder Einschränkung der Verarbeitung (Art. 19 i.V.m. Art. 5 Abs. 1 lit. a 3. Alt. DSGVO)

Kriterium

Soweit der Cloud-Anbieter Empfängern personenbezogene Daten des Cloud-Nutzers zur Durchführung des Auftrags mit diesem über die Erbringung des Cloud-Dienstes oder aufgrund einer rechtlichen Verpflichtung offengelegt hat, stellt er durch TOM sicher, dass er diesen Empfängern, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitteilt und den Cloud-Nutzer auf Verlangen über die Empfänger unterrichtet.

Erläuterung

Der Cloud-Anbieter ist nach Art. 19 DSGVO verpflichtet, Empfängern, denen er personenbezogene Daten offengelegt hat, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitzuteilen und die betroffene Person auf Verlangen über die Empfänger zu unterrichten. Das Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM 6.2.5 und 6.2.6).

Empfänger sind beispielsweise auch Auftragsverarbeiter, die eingesetzt werden, um den Auftrag über die Erbringung des Cloud-Dienstes durchzuführen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er dokumentiert, welche Maßnahmen er ergriffen hat, um seiner Mitteilungspflicht nachzukommen und den Cloud-Nutzer auf Verlangen über die Empfänger der Offenlegung zu unterrichten.

Nr. 16 – Verpflichtung zur Vertraulichkeit (Art. 5 Abs. 1 lit. a, Abs. 2 i.V.m. Art. 24 Abs. 1 DSGVO)

Kriterium

> Der Cloud-Anbieter betraut nur Mitarbeiter mit der Verarbeitung von personenbezogenen Daten des Cloud-Nutzers, die er vor Beginn der Verarbeitung über die Beachtung der datenschutzrechtlichen Anforderungen nach der DSGVO, inklusive des Datengeheimnisses, unterrichtet und hierauf verpflichtet hat.

Erläuterung

Die Unterrichtung über die datenschutzrechtlichen Anforderungen nach der DSGVO und die Verpflichtung der Mitarbeiter auf das Datengeheimnis fördern den Grundsatz von Treu und Glauben und das Gewährleistungsziel der Vertraulichkeit (SDM 6.2.3)

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er ein Muster für die Verpflichtungserklärungen seiner Mitarbeiter oder bereits unterzeichnete Verpflichtungserklärungen der Mitarbeiter vorlegt.

Nr. 17 – Meldung von Datenschutzverletzungen (Art. 33 Abs. 1, 3 und 5 DSGVO)

Kriterium

(1) Der Cloud-Anbieter meldet der Aufsichtsbehörde Datenschutzverletzungen aus der Verarbeitung von Daten, die zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen vorgenommen werden, unverzüglich nach Bekanntwerden, sofern sie voraussichtlich zu einem Risiko für die Rechte und Freiheiten des Cloud-Nutzers führen.

(2) Der Cloud-Anbieter dokumentiert die Datenschutzverletzungen samt aller mit ihnen in Zusammenhang stehenden Fakten, Auswirkungen und ergriffenen Maßnahmen.

(3) Die Meldung an die zuständige Aufsichtsbehörde enthält mindestens die Vorgaben aus Art. 33 Abs. 3 lit. a bis d DSGVO.

(4) Der Cloud-Anbieter bestimmt, welche Faktoren erfüllt sein müssen, damit von einem voraussichtlichen Risiko für die Rechte und Freiheiten des Cloud-Nutzers ausgegangen werden muss und wer für die Meldung zuständig ist. Die zuständigen Mitarbeiter sind ausreichend geschult, um Verstöße beurteilen zu können.

Erläuterung

Der Cloud-Anbieter ist nach Art. 33 DSGVO zur unverzüglichen Meldung von Datenschutzverstößen an die Aufsichtsbehörde verpflichtet, sofern sie voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen. Der Cloud-Anbieter muss Datenschutzverletzungen dokumentieren, damit die Aufsichtsbehörde überprüfen kann, ob der Cloud-Anbieter allen seinen diesbezüglichen Pflichten nachgekommen ist. Das Kriterium fördert das Gewährleistungsziel der Integrität und Transparenz (SDM 6.2.2 und 6.2.5).

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er in seinem Datensicherheitskonzept dokumentiert, wie er die Meldung von Datenschutzverletzungen durchführt.

Nr. 18 – Benachrichtigung der betroffenen Person bei Datenschutzverletzungen (Art. 34 Abs. 1 und 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter unterrichtet den Cloud-Nutzer über Datenschutzverletzungen aus der Verarbeitung von Daten zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen unverzüglich, wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten des Cloud-Nutzers hat.

(2) Die Benachrichtigung enthält mindestens die Informationen nach Art. 33 Abs. 3 lit. b, c und d DSGVO und erfolgt in klarer und einfacher Sprache.

(3) Der Cloud-Anbieter bestimmt, welche Faktoren erfüllt sein müssen, damit von einem voraussichtlich hohen Risiko für die Rechte und Freiheiten des Cloud-Nutzers ausgegangen werden muss und wer für die Benachrichtigung zuständig ist. Die zuständigen Mitarbeiter sind ausreichend geschult, um Verstöße beurteilen zu können.

Erläuterungen

Von einer hohen Bedrohungslage, die eine Benachrichtigung des Cloud-Nutzers nach Art. 34 DSGVO erforderlich macht, ist beispielsweise bei einem Verlust von Bank- und Kreditkarteninformationen auszugehen. Solche Daten werden häufig zur Vertragsdurchführung mit dem Cloud-Nutzer verarbeitet, sodass die Benachrichtigungspflicht bei Datenschutzverletzungen relevant werden kann.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er in seinem Datensicherheitskonzept dokumentiert, wie er den Cloud-Nutzer über Datenschutzverletzungen informiert.

Nr. 19 – Führen eines Verarbeitungsverzeichnisses (Art. 30 Abs. 1 DSGVO)

Kriterium

(1) Cloud-Anbieter, die mehr als 250 Mitarbeiter beschäftigen, führen ein Verarbeitungsverzeichnis. Der Cloud-Anbieter führt unabhängig von der Beschäftigtenzahl ein Verarbeitungsverzeichnis, wenn die Verarbeitung nicht nur gelegentlich erfolgt oder sie ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt.

(2) Das Verarbeitungsverzeichnis bezieht sich auf die Verarbeitungstätigkeiten, die der Cloud-Anbieter durchführt, um den Auftrag über die Erbringung des Cloud-Dienstes zu erfüllen und auf Verarbeitungstätigkeiten zur Erfüllung rechtlicher Verpflichtungen. Das Verzeichnis enthält die in Art. 30 Abs. 1 DSGVO aufgelisteten Inhalte.

(3) Das Verarbeitungsverzeichnis ist schriftlich oder in einem elektronischen Format zu führen. Es ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Transparenz (SDM 6.2.5).

Auch Cloud-Anbieter, die Daten zur Durchführung des Auftrags mit dem Cloud-Nutzer verarbeiten und weniger als 250 Mitarbeitern beschäftigten, werden im Regelfall ein Verarbeitungsverzeichnis führen müssen, da diese Verarbeitungen regelmäßig und nicht nur gelegentlich erfolgen, sodass die Ausnahme aus Art. 30 Abs. 5 DSGVO nicht anwendbar ist.

Risikobehaftet ist ein Verarbeitungsvorgang i.S.d. Art. 30 Abs. 2 DSGVO, wenn er Risiken für die Rechte und Freiheiten von betroffenen Personen birgt oder besondere Kategorien von personenbezogenen Daten gemäß Art. 9 DSGVO oder Art. 10 DSGVO zum Gegenstand hat.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er die (eine repräsentative Stichprobe der) Verarbeitungsverzeichnisse vorlegt.

Nr. 20 – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Nr. 20.1 – Datenschutz durch Systemgestaltung (Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 und 2 DSGVO)

Kriterium

Der Cloud-Anbieter stellt durch TOM im Rahmen der Dienstgestaltung sicher, dass im Cloud-Dienst nur personenbezogene Daten verarbeitet werden, die zur Erfüllung des Auftrags über die Erbringung des Cloud-Dienstes erforderlich sind und dass die übrigen Grundsätze des Art. 5 DSGVO im Cloud-Dienst umgesetzt werden.

Erläuterung

Während der Cloud-Anbieter in seiner Rolle als Auftragsverarbeiter nur indirekt von Art. 25 DSGVO adressiert wird, ist er als Verantwortlicher direkter Adressat. Technik und Organisation des Cloud-Dienstes sind so zu gestalten, dass sie die Datenschutzgrundsätze des Art. 5 DSGVO bestmöglich unterstützen. Der Cloud-Anbieter muss im Rahmen der Dienstgestaltung sicherstellen, dass er nur personenbezogene Daten verarbeitet, die für die Diensterbringung gegenüber dem Cloud-Kunden erforderlich sind. Ebenfalls sind Umfang der Verarbeitung und Speicherfrist auf das zur Zweckerreichung erforderliche Maß zu begrenzen.

Umsetzungshinweise

Die Maßnahmen, um dieses Kriterium umzusetzen, sind sehr vielfältig. Sie reichen von der Implementierung eines datensparsamen Logins für den Zugang zum Cloud-Dienst, über Rollen- und Berechtigungskonzepte für die Administration der Daten des Cloud-Nutzers bis hin zu Löschkonzepten für die Löschung dieser Daten. Auch Maßnahmen, die es dem Cloud-Nutzer ermöglichen, seine Betroffenenrechte möglichst einfach auszuüben, zählen hierzu, da sie Transparenz und Kontrollmöglichkeiten für diesen erhöhen. Beispielhafte Maßnahmen sind die Antragstellung auf Auskunft nach Art. 15 Abs. 1 DSGVO auf Knopfdruck innerhalb des Dienstes oder der Onlineabruf von Daten, die zur betroffenen Person gespeichert sind. Der Cloud-Anbieter sollte die Abwägungsvorgänge dokumentieren, die ihn bei der Auswahl der TOM zur Gewährleistung der Datenschutzgrundsätze geleitet haben, da er bei dieser Auswahl den Stand der Technik, die Implementierungskosten, die Eintrittswahrscheinlichkeit und Schwere des Schadens für die Rechte und Freiheiten der betroffenen Personen in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigen darf.

Nachweis

Der Cloud-Anbieter legt Dokumentationen vor, aus denen hervorgeht, welche Maßnahmen er ergriffen hat, um die Datenschutzgrundsätze bei der Gestaltung des Cloud-Dienstes umzusetzen. Die Dokumentationen schildern auch die Abwägungen, die unternommen wurden, um die Maßnahmen festzulegen.

Nr. 20.2 – Datenschutz durch datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 i.V.m. Art. 5 Abs. 1 und 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch Voreinstellungen sicher, dass er bei der Inbetriebnahme und Nutzung des Cloud-Dienstes nur personenbezogene Daten des Cloud-Nutzers verarbeitet, die erforderlich sind, um den Cloud-Dienst erbringen zu können.

(2) Der Cloud-Anbieter stellt durch Voreinstellungen sicher, dass personenbezogene Daten des Cloud-Nutzers nicht ohne dessen Eingreifen einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Umsetzungshinweise

Die Maßnahmen, um dieses Kriterium umzusetzen, sind sehr vielfältig. Wie auch bei Nr. 20.1. spielt die datenschutzarme Protokollierung eine Rolle. Muss die Nutzung des Cloud-Dienstes protokolliert werden, um beispielsweise Missbrauch aufzudecken oder die Datensicherheit sicherzustellen, so sollte die Voreinstellung derart gewählt werden, dass die Daten anonymisiert erhoben und verarbeitet werden.

Nachweise

Der Cloud-Anbieter dokumentiert welche Voreinstellungen er implementiert hat, um dem Cloud-Nutzer eine datenschutzfreundliche Inbetriebnahme und Nutzung des Cloud-Dienstes zu ermöglichen.

Nr. 21 – Auftragsverarbeitung des Cloud-Anbieters

Erläuterung

Die Datenverarbeitung, die erforderlich ist, um den Auftrag mit dem Cloud-Nutzer über die Erbringung und Nutzung des Cloud-Dienstes zu erfüllen, muss vom Cloud-Anbieter nicht höchstpersönlich durchgeführt werden. Vielmehr kann der Cloud-Anbieter die Datenverarbeitung (wie Abrechnung der Dienstnutzung gegenüber dem Cloud-Nutzer) auch an Auftragsverarbeiter auslagern, sodass auch diese Auslagerung in die Zertifizierungsprüfung aufgenommen werden muss.

Nr. 21.1 – Dienstleistung aufgrund einer rechtsverbindlichen Vereinbarung (Art. 28 Abs. 3 UAbs. 1 Satz 2 DSGVO)

Kriterium

(1) Lagert der Cloud-Anbieter die Verarbeitung von Daten zur Erfüllung des Auftrags über die Erbringung des Cloud-Dienstes an einen Auftragsverarbeiter aus, schließt er mit diesem eine rechtsverbindliche Vereinbarung zur Auftragsverarbeitung ab.

(2) Der Cloud-Anbieter stellt durch geeignete technische oder organisatorische Maßnahmen sicher, dass der Auftrag erst nach dem Abschluss einer rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung mit dem Auftragsverarbeiter erbracht wird.

(3) Die rechtsverbindliche Vereinbarung ist schriftlich oder in einem elektronischen Format abzufassen.

(4) Der Cloud-Anbieter stellt sicher, dass die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung die Anforderungen der Kriterien Nr. 1.2 bis 1.6, 1.7 (1), (3)-(4) und 1.8 von Kapitel I erfüllt.

(5) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung enthält die Angabe, ob von Seiten des Cloud-Anbieters oder des Auftragsverarbeiters Pseudonymisierungs-, Anonymisierungs- oder Verschlüsselungsverfahren zum Einsatz kommen.

(6) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung enthält Angaben zur Unterstützung des Cloud-Anbieters bei der Erfüllung der Betroffenenrechte und der Meldepflicht bei Datenschutzverletzungen.

Erläuterung

Da der Cloud-Anbieter eine Zertifizierung seiner Datenverarbeitungsvorgänge anstrebt, hat er sicherzustellen, dass auch in Auftrag gegebene Auftragsverarbeitungen den Anforderungen der Datenschutz-Grundverordnung entsprechen. Dafür muss der Cloud-Anbieter zunächst eine rechtsverbindliche Vereinbarung mit dem Auftragsverarbeiter abschließen, die die Pflichtangaben aus Art. 28 Abs. 3 UAbs. 1 Satz 2 enthält.

Die Kriterien Nr. 1.2. bis 1.6, 1.7 (1), (3)-(4) und 1.8 aus Kapitel I sind so zu lesen, dass der Cloud-Anbieter in seiner Funktion als Verantwortlicher die Rolle des Cloud-Nutzers und der eingesetzte Auftragsverarbeiter die Rolle des Cloud-Anbieters einnimmt.

Nachweis

Der Cloud-Anbieter legt die rechtsverbindliche(n) Vereinbarung(en) zur Auftragsverarbeitung mit den entsprechenden Festlegungen vor, die er mit dem/den Auftragsverarbeiter(n) abgeschlossen hat.

Nr. 21.2 – Sicherstellung ordnungsgemäßer Auftragsverarbeitung

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter personenbezogene Daten nur auf dokumentierte Weisung des Cloud-Anbieters verarbeitet (Art. 28 Abs. 3 Satz 2 lit. a, 29 DSGVO).

(2) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter ihn informiert, wenn er der Ansicht ist, dass seine Weisungen gegen datenschutzrechtliche Pflichten verstoßen (Art. 28 Abs. 3 Satz 2 lit. h DSGVO).

(3) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter bei der ausgelagerten Verarbeitung Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Systeme, die Belastbarkeit der Systeme sowie die Verfügbarkeit der Daten und den Zugang zu ihnen nach einem physischen oder technischen Zwischenfall gewährleistet. Die implementierten TOM müssen vom Auftragsverarbeiter regelmäßig überprüft und gegebenenfalls angepasst werden (Art. 24, 25, 28, 32, 35 i.V.m. Art. 5 Abs. 1 lit. f DSGVO).

(4) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter seine Mitarbeiter vor Beginn der Datenverarbeitung zur Vertraulichkeit verpflichtet, sofern sie nicht einer gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 Satz 2 lit. b DSGVO).

(5) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter nur Mitarbeiter mit der Durchführung von Verarbeitungsvorgängen betraut, die die dafür erforderliche Fachkunde und Zuverlässigkeit aufweisen und die im Datenschutz und der Datensicherheit geschult sind (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO).

(6) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter den Cloud-Anbieter in jenen Fällen informiert, in denen sich der Datenverarbeitungsort unvorhergesehen ändert (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

(7) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter nach Abschluss der Auftragsverarbeitung oder auf Weisung des Cloud-Anbieters überlassene Datenträger zurückgibt, Daten zurückführt und beim ihm gespeicherte Daten löscht (Art. 28 Abs. 3 lit. h DSGVO).

(8) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter dem Cloud-Anbieter die Erfüllung der Betroffenenrechte ermöglicht und alle Weisungen zur Umsetzung der Betroffenenrechte dokumentiert (Art. 28 Abs. 3 lit. e i.V.m. Kapitel III DSGVO).

(9) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter einen DSB benennt, sofern er hierzu gesetzlich verpflichtet ist (Art. 37-39 DSGVO, § 38 BDSG).

(10) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter ein Verarbeitungsverzeichnis führt, wenn er mehr als 250 Mitarbeiter beschäftigt oder wenn die Verarbeitung nicht nur gelegentlich erfolgt oder die Verarbeitung für die betroffenen Personen mit Risiken für ihre Rechte und Freiheiten verbunden ist (Art. 30 Abs. 2 DSGVO).

(11) Der Cloud-Anbieter stellt sicher, dass ihm der Auftragsverarbeiter Datenschutzverletzungen und deren Ausmaß unverzüglich meldet (Art. 33 Abs. 2 und Art. 28 Abs. 3 lit. f).

(12) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter allen Anforderungen aus der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung nach Nr. 21.1 nachkommt und alle Anforderungen nach diesem Kriterium erfüllt (Art. 24 Abs. 1 DSGVO).

(13) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter, wenn er seinerseits Subauftragsverarbeiter einsetzt, gewährleistet, dass diese die Anforderungen nach den Kriterien Nr. 10.1-10.5 aus Kapitel V einhalten.

Erläuterung

Setzt der Cloud-Anbieter für die Datenverarbeitung zur Erfüllung des Auftrags über die Erbringung des Cloud-Dienstes Auftragsverarbeiter ein, muss er nicht nur eine rechtsverbindliche Vereinbarung hierzu abschließen, die die Anforderungen aus Art. 28 Abs. 3 UAbs. 1 Satz 2 DSGVO erfüllt, sondern sich auch vergewissern, dass der Auftragsverarbeiter die in der rechtsverbindlichen Vereinbarung zugesicherten Maßnahmen durchführt und seinen sonstigen Pflichten nach der Datenschutz-Grundverordnung nachkommt.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er Dokumentationen, Prüfungsergebnisse oder ähnliche Nachweise des Auftragsverarbeiters vorlegt, die ihn überzeugt haben anzunehmen, dass der Auftragsverarbeiter allen für ihn geltenden Pflichten nach der Datenschutz-Grundverordnung nachkommt und daher über die geeigneten Garantien nach Art. 28 Abs. 1 DSGVO verfügt.