European Cloud Service
Data Protection Certification

AUDITOR-Kriterienkatalog

- Fassung 0.99 -

Stand 30.1.2020

Weitere AUDITOR-Dokumente:

- Zertifizierungsgegenstand (Kurz- und Langfassung)
- Konformitätsbewertungsprogramm
- Modularitätskonzept
- Schutzklassenkonzept
- DIN SPEC 27557

Online verfügbar: www.auditor-cert.de

Empfohlene Zitation:

Roßnagel, A., Sunyaev, A., Maier, N., Lins, S., & Teigeler, H. (2019). AUDITOR-Kriterienkatalog – Fassung 0.99. DOI: 10.5445/IR/1000105506. 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], Natalie Maier[a], Sebastian Lins[b], 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

UNIKASSEL VERSITÄT

provet

Karlsruher Institut für Technologie

CRITICAL INFORMATION INFRASTRUCTURES RESEARCHGROUP

Inhaltsverzeichnis

Abkürzungsverzeichnis 4
A. Gegenstand und Ziele des AUDITOR-Kriterienkatalogs 5
1. Adressaten und Funktionen des AUDITOR-Kriterienkatalogs 5
2. Fortentwicklung vom TCDP gemäß der Datenschutz-Grundverordnung 8
B. Aufbau und Nutzung des AUDITOR-Kriterienkatalogs 9
1. Elemente des Kriterienkatalogs 9
2. Schutzklassen 9
2.1 Das Schutzklassenkonzept 9
2.2 Die Schutzklassen des AUDITOR-Kriterienkatalogs 10
3. Nichtanwendbarkeit von Kriterien 13
C. Kriterien und Umsetzungsempfehlungen für die Auftragsverarbeitung 15
Kapitel I: Rechtsverbindliche Vereinbarung zur Auftragsverarbeitung 15
Kapitel II: Rechte und Pflichten des Cloud-Anbieters 21
Kapitel III: Datenschutz-Managementsystem des Cloud-Anbieters 51
Kapitel IV: Datenschutz durch Systemgestaltung 57
Kapitel V: Subauftragsverarbeitung 59
Kapitel VI: Datenverarbeitung außerhalb der EU und des EWR 63
D. Kriterien und Umsetzungshinweise für Verarbeitung als Verantwortlicher 65
Kapitel VII: Der Cloud-Anbieter als Verantwortlicher 65
E. Referenzen 83

Abkürzungsverzeichnis

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
Anf.	Anforderung
Art.	Artikel
Alt.	Alternative
BDSG	Bundesdatenschutzgesetz neue Fassung (Geltung ab 25.5.18)
BSI	Bundesamt für Sicherheit in der Informationstechnik
DSB	Datenschutzbeauftragter
DSGVO	EU-Datenschutz-Grundverordnung (Geltung ab 25.5.18)
EG	Erwägungsgrund
EWR	Europäischer Wirtschaftsraum
i.S.v.	Im Sinne von
i.V.m.	In Verbindung mit
lit.	litera (Buchstabe)
Nr.	Nummer
s.	siehe
SDM	Standard-Datenschutzmodell v.1.1 vom 26.4.2018
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 bilden Verarbeitungsvorgänge von personenbezogenen Daten im Kontext von Cloud-Diensten. Eine Datenverarbeitung ist nach Art. 4 Nr. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe. Dazu zählen das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten.

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

Bei der Bestimmung des Zertifizierungsgegenstands sind drei Komponenten wichtig, die Cloud-Anbieter als Adressaten des AUDITOR-Zertifizierungsverfahrens beachten müssen: 1. personenbezogene Daten, 2. technische Systeme (Infrastruktur, Hardware und Software, die genutzt werden, um personenbezogene Daten zu verarbeiten) und 3. Prozesse und Verfahren, die mit Verarbeitungsvorgängen in Verbindung stehen. Somit besteht ein Datenverarbeitungsvorgang in der Regel sowohl aus technischen und automatisierten als auch aus nicht-technischen organisatorischen Komponenten, die zu Datenschutzkonzepten und -managementsystemen zusammengefasst sind. Der gesamte Datenverarbeitungsvorgang muss den Anforderungen der Datenschutz-Grundverordnung entsprechen.

Datenverarbeitungsvorgänge müssen eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen, innerhalb derer die spezifischen Datenschutzrisiken des jeweiligen Cloud-Dienstes vollständig erfasst werden können. Dies bedeutet, dass auch Schnittstellen des zu zertifizierenden Cloud-Dienstes zu anderen Diensten betrachtet werden müssen, um Datenflüsse zu identifizieren, aus denen datenschutzrechtliche Risiken erwachsen können. Weiterführende Informationen zum Zertifizierungsgegenstand von AUDITOR sind dem Begleitdokument *„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 (siehe Kapitel C). 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 (siehe Kapitel D). Der Cloud-Anbieter wird auch als Verantwortlicher von Datenverarbeitungsvorgängen adressiert, die erforderlich sind, um den Vertrag mit dem Cloud-Nutzer über die Bereitstellung des Cloud-Dienstes schließen und diesen durchführen zu können. Wird der Cloud-Dienst im B2C-Bereich angeboten, stellt der Cloud-Nutzer häufig auch die betroffene Person dar, deren Daten erforderlich sind, um den Cloud-Dienst bereitzustellen, sodass der

Cloud-Anbieter seine datenschutzrechtlichen Pflichten (z.B. Informationspflichten) gegenüber dem Cloud-Nutzer erfüllen muss.

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

Schließt der Cloud-Nutzer einen Vertrag mit dem Cloud-Anbieter über die Bereitstellung und Nutzung des Cloud-Dienstes ab, wird der Cloud-Anbieter vor allem durch handels- und steuerrechtliche Aufzeichnungs- und Aufbewahrungspflichten zur Verarbeitung personenbezogener Daten verpflichtet, sodass die Datenverarbeitung zur Erfüllung rechtlicher Pflichten ebenfalls in den Anwendungsbereich der AUDITOR-Zertifizierung fällt.

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

Um den Vertrag mit dem Cloud-Nutzer über die Nutzung des Cloud-Dienstes abzuschließen und durchzuführen, entscheidet der Cloud-Anbieter, welche personenbezogenen Daten er erhebt und verarbeitet. In der Regel werden hier Daten wie Namen, Adressen, Zahlungsdaten wie beispielsweise Bankverbindungen, Rufnummern, Benutzernamen und Passwörter fürs Einloggen in den Cloud-Dienst verarbeitet. Diese können unter dem Begriff **„Bestandsdaten“** zusammengefasst werden. Gerade im B2B-Bereich können neben den Daten des Cloud-Nutzers auch Daten anderer betroffener Personen wie beispielsweise von Mitarbeitern des Cloud-Nutzers erforderlich sein, um den Vertrag über die Nutzung des Cloud-Dienstes mit dem Cloud-Nutzer schließen und durchführen zu können. So werden z.B. Namen und Kontaktdaten von Mitarbeitern des Cloud-Nutzers verarbeitet, die dem Cloud-Anbieter als Ansprechpartner dienen sollen. Da der Cloud-Anbieter den Vertrag über die Cloud-Nutzung nicht mit dem Mitarbeiter schließt, kann Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO nicht die Verarbeitung der Mitarbeiterdaten legitimieren. Stattdessen kann sich der Cloud-Anbieter auf Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO und seine berechtigten Interessen an der Datenverarbeitung stützen, solange wie die Daten zur Begründung und Erfüllung des Vertrags mit dem Cloud-Nutzer erforderlich sind.

Um dem Cloud-Nutzer die Inanspruchnahme des Cloud-Dienstes zu ermöglichen und diese abzurechnen, muss der Cloud-Anbieter weitere personenbezogene Daten wie beispielsweise Ein- und Auslogdaten zu Nutzkonten, IP-Adressen, die genutzten Dienstmodule und den Umfang der Nutzung verarbeiten. Diese Daten können unter dem Begriff **„Nutzungsdaten“** 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 aus der Privatwirtschaft, 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 *personenbezogene 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 die Verarbeitung personenbezogener Daten des Cloud-Nutzers oder anderer betroffener Personen wie beispielsweise der Mitarbeiter des Cloud-Nutzers geht, die erforderlich ist, um den Cloud-Dienst zu erbringen und um dessen Nutzung und Abrechnung zu ermöglichen und soweit die Datenverarbeitung zur Erfüllung rechtlicher Pflichten dient, denen der Cloud-Anbieter unterliegt.

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

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

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 liegen. Der Auftragsverarbeiter muss sich jedoch als Hauptauftragsverarbeiter davon überzeugen, dass auch diese fremden, von ihm genutzten Plattformen, Infrastrukturen und sonstigen Subauftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten und darf nur solche für die Erbringung seines Cloud-Dienstes einsetzen.

Ein Cloud-Anbieter darf daher nur solche Subauftragsverarbeiter auswählen, die gemäß Art. 28 Abs. 1 DSGVO ebenfalls *„geeignete Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den*

Schutz der Rechte der betroffenen Personen gewährleistet". Subauftragsverarbeiter können die geforderten geeigneten Garantien ihrerseits beispielsweise durch den Nachweis durchlaufener Zertifizierungsverfahren oder durch die Befolgung von anerkannten Verhaltensregeln (‚Code of Conduct') gemäß Art. 40 DSGVO erbringen. Kapitel V dieses Kriterienkatalogs regelt insbesondere die Subauftragsverarbeitung.

2. Fortentwicklung vom 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. ISO/IEC 27701 – und insbesondere die Anforderungen der Datenschutz-Grundverordnung berücksichtigt werden konnten, muss mit dem Geltungsbeginn der Datenschutz-Grundverordnung ab dem 25.5.2018 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. Auch sind Umsetzungshinweise nicht abschließend, sondern beschreiben zentrale Umsetzungen für die Kriterien. Die Umsetzungshinweise orientieren sich dabei, wo es angemessen ist, an bestehenden Industriestandards, Normen und Best-Practices. So wird bspw. insbesondere bei den Kriterien unter Nr. 2 zur Gewährleistung der Datensicherheit auf die ISO/IEC 27002 und das BSI C5 verwiesen und es werden entsprechende Textabschnitte zitiert. Zudem finden sich zu jedem Kriterium *„Nachweise“*, die eine Antwort auf die Frage liefern, 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. Dabei wird bspw. die Vorlage von Dokumentationen zur Prüfung durch die Zertifizierungsstelle vorgeschlagen, oder die Durchführung einer Vor-Ort-Auditierung durch die Zertifizierungsstelle als Nachweis zur Umsetzung von dokumentierten Maßnahmen vorausgesetzt. 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. Das Begleitdokument *„Schutzklassenkonzept“* fasst die Konzeption und Abgrenzung der Schutzklassen ausführlich zusammen.

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 zu **erkennen geben**, für welche Art und Kategorien von Daten und **für welche Schutzklasse 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 in diesem AUDITOR-Kriterienkatalog nicht weiter erläutert, weil sie vornehmlich den Cloud-Nutzer und nicht die Zertifizierung des Cloud-Anbieters als solche betreffen. Für weiterführende Informationen wird auf das Begleitdokument *„Schutzklassenkonzept“* verwiesen.

Zu beachten gilt jedoch, dass für die Datenverarbeitung zur Durchführung des Auftrags mit dem Cloud-Nutzer und zur Erfüllung rechtlicher Pflichten, 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);
- Arbeitszeitdaten;
- 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-Anbieter 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 die 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 Datensicherheit 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 Datensicherheit 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. 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 ausreichende 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. In der Regel werden nicht alle Kriterien des AUDITOR-Kriterienkatalogs für jeden Zertifizierungsgegenstand anwendbar sein. 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. 6.2 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 (bspw. im Falle eines Infrastructure-as-a-Service-Dienstes). 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.

Auch sind Kriterien nicht anwendbar, wenn die Datenschutz-Grundverordnung oder die sie konkretisierenden Gesetze die Anwendbarkeit nicht absolut fordern, sondern von gewissen Voraussetzungen oder „Schwellen“ abhängig machen, welche vom Cloud-Anbieter nicht erfüllt werden. Dies ist beispielsweise bei der Benennung eines Datenschutzbeauftragten (Art. 37 Abs. 1 und 4 DSGVO i.V.m. § 38 BDSG) oder beim Führen eines Verarbeitungsverzeichnisses der Fall (Art. 30 Abs. 5 DSGVO).

Ebenfalls sind Kriterien nicht anwendbar, wenn die Erfüllung des Kriteriums verhindert, einen legitimen Datenverarbeitungszweck zu erreichen. So kann beispielsweise ein Anbieter eines E-Mail-Dienstes die Mailheader nicht anonymisieren, da ansonsten die Zustellung von E-Mails nicht mehr ordnungsgemäß gewährleistet werden kann, sodass er zu einer solchen Anonymisierung auch nicht verpflichtet werden kann.

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 TOM sicher, dass der Dienst erst nach dem Abschluss einer rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung mit dem Cloud-Nutzer erbracht wird.

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

(3) Diese Vereinbarung muss die Kriterien dieses Kapitels (1.2 bis 1.8) erfüllen, wobei die in diesen Kriterien geforderten Festlegungen auch in sonstigen Dokumenten getroffen werden können, wenn diese als Bestandteile der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung einbezogen worden sind.

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 TOM, die einen automatischen Vereinbarungsschluss vor der eigentlichen Dienstnutzung sicherstellen. Hierzu kann dem potentiellen Cloud-Nutzer während der (elektronischen) Registrierung eine entsprechende Vereinbarung angezeigt werden, die dieser vor der Dienstnutzung bestätigen muss.

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

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 8.2 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann im Rahmen der Zertifizierung die Muster-Vereinbarung sowie alle oder eine repräsentative Stichprobe von rechtsverbindlichen Vereinbarungen vorlegen, die er mit den Cloud-Nutzern schließt. Außerdem kann er anhand einer geeigneten Dokumentation (z.B. Prozessdokumentation, Funktionsdokumentation, Protokolldateien oder Logs) nachweisen, dass TOM getroffen wurden, die eine Dienstnutzung erst nach Abschluss der Vereinbarung sicherstellen (bspw. in Bezug auf einen Vereinbarungs- oder Registrierungsprozess mit potenziellen

[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.

Cloud-Nutzern). Der Cloud-Anbieter kann durch eine testweise Durchführung eines entsprechenden Vereinbarungs- oder Registrierungsprozesses nachweisen, dass die in der Dokumentation angegebenen Konzepte auch im Cloud-Dienst realisiert wurden.

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.

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 Auftragsgegenstand sollten auch die abgegrenzten Verantwortungsbereiche zwischen Cloud-Nutzer und Cloud-Anbieter abbilden.

Auf die Umsetzungshinweise zur transparenten Systembeschreibung im BSI C5 Anf. UP-01 sowie zur Verantwortungsverteilung in Anf. OIS-03 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 8.2 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er Dokumentationen zur rechtsverbindlichen Vereinbarung mit diesen Angaben vorlegt (bspw. Vertragsmuster, -vorlagen oder -instanzen). Durch eine testweise Dienstnutzung (insb. Einsicht, ob Inhalte bei der Registrierung für die Dienstnutzung angezeigt werden) kann der Cloud-Anbieter nachweisen, dass er ein Verfahren implementiert hat, wonach die Vereinbarung mit diesen Festlegungen geschlossen wird.

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

Kriterium

In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung werden Art und 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.

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 8.2 und ISO/IEC 27018 Ziff. A10.11 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er Dokumentationen zur rechtsverbindlichen Vereinbarung mit diesen Angaben vorlegt (bspw. Vertragsmuster, -vorlagen oder -instanzen). Durch eine testweise Dienstnutzung (insb. Einsicht, ob Inhalte bei der Registrierung für die Dienstnutzung angezeigt werden) kann der Cloud-Anbieter nachweisen, dass er 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 Cloud-Nutzers – auch in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation – verarbeitet werden, sofern der Cloud-Anbieter nicht durch Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet ist.

(2) Für den Fall, dass der Cloud-Anbieter durch Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet ist, sieht die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung die Pflicht des Cloud-Anbieters vor, dem Cloud-Nutzer die rechtlichen Anforderungen vor der Verarbeitung mitzuteilen, sofern das jeweilige Recht die Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(3) Für den Fall, dass die Auftragsverarbeitung weisungsgebundene Übermittlungen personenbezogener Daten an Drittländer oder internale Organisationen vorsieht, legt die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung fest, welche Instrumente nach Art. 45 DSGVO oder Art. 46 Abs. 2 und 3 DSGVO für die Übermittlungen genutzt werden sollen, um ein angemessenes Schutzniveau sicherzustellen.

(4) 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) und stellt das Wesensmerkmal der Auftragsverarbeitung dar.

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.

Nach Art. 28 Abs. 3 S. 2 lit. a DSGVO kann die Weisungsbefolgung den Cloud-Anbieter jedoch nicht von der Gesetzestreue entbinden, sodass der Cloud-Anbieter nicht weisungsgedeckte Verarbeitungen durchführen darf, wenn er durch Unionsrecht oder mitgliedstaatliches Recht hierzu verpflichtet wird. Mit dieser Regelung soll Interessenkonflikten auf Seiten des Cloud-Anbieters vorgebeugt werden.

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.

In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung des Cloud-Anbieters sollten die technisch ausführbaren Dienstleistungen und Weisungsbefugnisse des Cloud-Nutzers aufgeführt werden. 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 (bspw. API-Aufrufe oder Softwarebefehle). 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.

Aus der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung sollte hervorgehen, ob weisungsgebundene Datenübermittlungen an Drittländer oder internationale Organisationen im Rahmen der Auftragsverarbeitung durchgeführt werden sollen und wie dort ein angemessenes Schutzniveau sichergestellt werden soll. Geeignete Garantien für die Datenübermittlung sind z.B. Standarddatenschutzklauseln der Kommission nach Art. 46 Abs. 2 lit. b DSGVO oder genehmigte Zertifizierungsverfahren nach Art. 46 Abs. 2 lit. f i.V.m. Art. 42 DSGVO.

Auf die Umsetzungshinweise zur transparenten Systembeschreibung im BSI C5 Anf. UP-01 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27018 Ziff. A2.1 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 8.5.1 und 8.5.2 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er entsprechende Regelungen zur Weisungserteilung, zur nicht weisungsgebundenen Verarbeitung aufgrund rechtlicher Pflichten aus Unions- oder mitgliedstaatlichem Recht und zur Festlegung geeigneter Garantien für die Datenübermittlung in Drittländer oder internationale Organisationen in rechtsverbindlichen Vereinbarungen offenlegt (bspw. Bereitstellung von Vertragsmuster, -vorlagen oder -instanzen). Ggf. kann er vorhandene Dokumentationen von Einzelanweisungen vorzeigen. Durch eine testweise Dienstnutzung (insb. Einsicht, ob Inhalte bei der Registrierung für die Dienstnutzung angezeigt werden) kann er nachweisen, dass er ein Verfahren implementiert hat, wonach die Vereinbarung mit diesen Festlegungen geschlossen wird.

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 ändert, der Cloud-Anbieter diese Änderung dem Cloud-Nutzer unverzüglich mitteilt.

Erläuterung

Das konkrete Land, in dem die personenbezogenen Daten verarbeitet werden sollen, ist nur bei einer Datenverarbeitung in einem Drittland anzugeben; jedoch nicht, wenn die Datenverarbeitung in der Europäischen Union oder dem Europäischen Wirtschaftsraum stattfinden soll.

Umsetzungshinweise

Auf die Umsetzungshinweise der ISO/IEC 27018 Ziff. A11.1 und ISO/IEC 27701 Ziff. 8.5 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er entsprechende Dokumentationen vorlegt (bspw. Vertragsmuster, -vorlagen oder -instanzen). Durch eine testweise Dienstnutzung (insb. Einsicht, ob Inhalte bei der Registrierung für die Dienstnutzung angezeigt werden) kann er nachweisen, dass der Ort der Datenverarbeitung (innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums oder das konkrete Drittland) und die Verpflichtung zur Meldung bei Änderungen des Ortes dem Cloud-Nutzer auf geeignete Weise kommuniziert werden.

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 C1.4).

Umsetzungshinweis

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 6.10.2.4 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er entsprechende Dokumentationen vorlegt (bspw. Vertragsmuster, -vorlagen oder -instanzen), in denen ersichtlich wird, dass 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. Durch eine testweise Dienstnutzung (insb. Einsicht, ob Inhalte bei der Registrierung für die Dienstnutzung angezeigt werden) kann er nachweisen, dass er ein Verfahren implementiert hat, wonach die Vereinbarung mit diesen Festlegungen geschlossen wird.

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 dem Schutzniveau der ausgelagerten Datenverarbeitung angemessenen TOM werden in einer rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt.

(2) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung enthält die Angabe, ob der Cloud-Anbieter 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.

(3) Der Cloud-Anbieter legt in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung fest, auf welchem Niveau 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, welches Schutzniveau der Cloud-Dienst bietet.

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.

Der Cloud-Anbieter kann einen Wiederherstellbarkeitszeitraum in der rechtsverbindlichen Vereinbarung angeben sowie auf die jeweilige Wiederherstellbarkeitsklasse der Zertifizierung verweisen.

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, bspw. 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.

Auf die Umsetzungshinweise der ISO/IEC 27018 Ziff. A1.1 und A10.11 und ISO/IEC 27701 6.13.1.5, 8.2.1, 8.2.5 und 8.3.1 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er entsprechende Dokumentationen vorlegt (bspw. Vertragsmuster, -vorlagen oder -instanzen). Durch eine testweise Dienstnutzung (insb. Einsicht, ob Inhalte bei Dienstnutzung angezeigt werden) kann er nachweisen, dass er ein Verfahren implementiert hat, wonach die Vereinbarung mit diesen Festlegungen geschlossen wird. Dabei ist insbesondere die Vollständigkeit und der hinreichende Detailgrad zur Beschreibung der TOMs nachzuweisen (bspw. Angabe der TOM ausgerichtet an den Gewährleistungszielen).

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 irreversiblen 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 aus nationalem oder Unionsrecht zur Speicherung oder Aufbewahrung von Daten verpflichtet, sind diese nicht zu löschen.

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 sollte zwischen den Abwicklungsmodalitäten wählen können.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er entsprechende Dokumentationen vorlegt (bspw. Vertragsmuster, -vorlagen oder -instanzen). Durch eine testweise Dienstnutzung (insb. Einsicht, ob Inhalte bei der Registrierung für die Dienstnutzung angezeigt werden) kann der Cloud-Anbieter nachweisen, dass er seine Pflichten zur Rückgabe von Datenträgern und zur Rückführung und Löschung von Daten nach Ende der Auftragsverarbeitung dem Cloud-Nutzer auf geeignete Weise kommuniziert.

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 und Abs. 2 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) Die in Nr. 2 geforderten Angaben können außer im Datensicherheitskonzept auch in sonstigen Dokumenten getroffen werden, solange diese als rechtsverbindlich für die Auftragsverarbeitung zwischen Cloud-Anbieter und Cloud-Nutzer vereinbart worden sind. Die Anforderungen an das Datensicherheitskonzept gelten auch für diese sonstigen Dokumente.

(3) 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.

(4) Das Datensicherheitskonzept ist schriftlich oder in einem elektronischen Format zu dokumentieren.

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

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

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

(8) Soweit das Datensicherheitskonzept Sicherheitsmaßnahmen des Cloud-Nutzers verlangt, sind diese dem Cloud-Nutzer schriftlich 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 Richtlinien und Schutzmaßnahmen beinhalten sowie Ressourcen, Verantwortlichkeiten und Priorisierungen für den Umgang mit Datensicherheitsrisiken spezifizieren. Mitarbeiter des Cloud-Anbieters sollten über diese Richtlinien und Schutzmaßnahmen zur Datensicherheit fortlaufend informiert werden. 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 denkbarer 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 (mindestens jährlich) aktualisiert und verbessert werden. Dabei sollten Risikobewertungen, das mögliche Schadensausmaß und die identifizierten akzeptablen Risiken regelmäßig unter Berücksichtigung des technischen und organisatorischen Wandels, erkannten Bedrohungen, der Auswirkung der implementierten Schutzmaßnahmen und externen Ereignisse überprüft werden. Zudem sollten angemessene und für den Cloud-Anbieter relevante Kontakte zu Behörden und Interessenverbänden hergestellt werden, um stets über aktuelle Risiken, Bedrohungslagen und mögliche Gegenmaßnahmen informiert zu sein.

Auf die Umsetzungshinweise im BSI C5 Anf. OIS-03, OIS-05, OIS-06, OIS-07, SA-01, SA-02, SA-03, RB-17, SIM-01 wird hingewiesen.

Auf die Richtlinien zum Risikomanagement in der ISO 31000, die Risikobewertungstechniken in der IEC 31010, und auf die Richtlinien zur Erfassung von Gefahren für die Privatsphäre in der ISO/IEC 29134 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 5.1.1, 5.1.2, 8.2, 12.1 bis 12.6, 18.1, 18.2, ISO/IEC 27018 Ziff. 5.1.1, 5.4.1 und 27701 Ziff. 5.2.1, 5.2.2, 5.4.1, 6.3.1, 6.5.2.1, 6.5.2.2, 6.12 und 6.15.1 wird hingewiesen.

Nachweis

Der Cloud-Anbieter legt das Datensicherheitskonzept sowie ggf. alle sonstigen Dokumente vor, welche ausführliche Informationen über das Verfahren zur Risikobeurteilung enthalten. Diese Dokumente führen alle identifizierten Risiken mit Angabe ihrer jeweiligen Schwere und Eintrittswahrscheinlichkeit auf. Die Dokumente enthalten auch die Abwägungen, die der Cloud-Anbieter bei der Wahl der Datensicherheitsmaßnahmen vorgenommen hat und beschreiben die Datensicherheitsmaßnahmen zur Adressierung der Risiken (beispielsweise Dokumentation von geplanten Maßnahmen im internen Ticketsystem des Unternehmens und Verweis auf durch diese Maßnahmen adressierte Risiken). Der Cloud-Anbieter kann insbesondere auch Dokumente über Prozesse im Falle der Risikorealisierung (z.B. in Form von Unternehmensrichtlinien) vorlegen. Zudem sollten Dokumentationen über die Trennung des Verantwortungsbereichs zwischen Cloud-Anbieter und Subauftragsverarbeiter und Cloud-Anbieter und Cloud-Nutzer vorgelegt werden.

Soweit das Datensicherheitskonzept Sicherheitsmaßnahmen des Cloud-Nutzers verlangt, kann der Cloud-Anbieter bspw. vorhandene Protokolle, Verträge, Prozessspezifikationen zur Mitteilung an den Cloud-Nutzer vorlegen. Wird der Cloud-Nutzer elektronisch informiert, bspw. während des Online-Registrierungsprozesses für den Cloud-Dienst, kann der Cloud-Anbieter ebenfalls die konforme Mitteilung des Cloud-Nutzers durch eine testweise Dienstnutzung nachweisen.

Der Cloud-Anbieter muss sicherstellen, dass aus den vorgelegten Dokumenten die Aktualität des Datensicherheitskonzepts hervorgeht und dass es fortlaufend weiterentwickelt wird (bspw. durch Zeitstempel, Versionierungshistorie oder Protokolle der Weiterentwicklung).

Unterstützend kann der Cloud-Anbieter eine Befragung von Mitarbeitern ermöglichen, um die oben genannten Punkte auf Vollständigkeit und Umsetzung im Unternehmen nachzuweisen.

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) Der Cloud-Anbieter überprüft den Zutritt zu Räumen und Datenverarbeitungsanlagen durch eine Zwei-Faktor-Authentifizierung.

[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.

(3) Die Maßnahmen sind geeignet, um 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.

(4) Der Cloud-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zutritt zu Räumen und Anlagen in regelmäßigen Abständen auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

Schutzklasse 2

(5) Die Kriterien von Schutzklasse 1 sind erfüllt.

(6) Zusätzlich ergreift der Cloud-Anbieter geeignete Maßnahmen, um Schädigungen nicht nur durch Naturereignisse, sondern auch durch fahrlässige Handlungen Befugter auszuschließen. Der Zutritt ist vor vorsätzlichen Handlungen Unbefugter hinreichend sicher geschützt, was Schutz gegen Zutrittsversuche durch bekannte Angriffsszenarien, Täuschung und Gewalt einschließt.

(7) Jeder unbefugte Zutritt und jeder Zutrittsversuch sind nachträglich feststellbar.

Schutzklasse 3

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

(9) Jeder befugte 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 Verfügbarkeit, Integrität, Vertraulichkeit (SDM C1.2 – C1.4) 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

Schutzklasse 1

Um sicherzustellen, dass Unbefugte keinen Zutritt zu Räumen und Datenverarbeitungsanlagen erhalten, sollte der Zutritt ins Rechenzentrum über Videoüberwachungssysteme, Bewegungssensoren, Alarmsysteme und von geschultem Sicherheitspersonal fortlaufend überwacht werden. Der Zutritt zu Bereichen, in denen personenbezogene Daten verarbeitet werden, sollte mit einem geeigneten Zwei-Faktor-Authentifizierungsmechanismus gesichert sein, bspw. bestehend aus einer Zutrittskarte und einer geheimen PIN (s. ISO/IEC 27002 Ziff. 11.1.2). Zutrittsrechte sollten regelmäßig (mindestens jährlich) überprüft und aktualisiert sowie, sofern erforderlich, wieder entzogen werden.

Einrichtungen sollten durch bauliche, technische und organisatorische Maßnahmen vor Feuer, Wasser, Erdbeben, Explosionen, zivilen Unruhen und anderen Formen natürlicher und von Menschen verursachter Bedrohungen geschützt werden (s. BSI C5 Anf. PS-03). Dazu zählen unter anderem Brandfrüherkennungs- und Löschanlagen, die Durchführung von regelmäßigen Brandschutzübungen und Brandschutzbegehungen, um die Einhaltung der Brandschutzmaßnahmen zu prüfen, die Einbettung von Sensoren zum Überwachen von Temperatur und Luftfeuchtigkeit und die Ausstattung aller Gebäude mit Blitzschutzeinrichtungen. Es kann eine fachliche Beratung in Anspruch genommen werden, um mögliche Schäden zu verhindern (s. ISO/IEC 27002 Ziff. 11.1.4).

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

Der Zutrittsschutz sollte durch Errichtung mehrerer physischer Barrieren rund um das Gelände des Cloud-Anbieters und die Einrichtungen zur Datenverarbeitung erreicht werden, da der Ausfall einer Barriere keine unmittelbare Beeinträchtigung der Datensicherheit zur Folge hat (s. ISO/IEC 27002 Ziff. 11.1.1).

Physische Zutrittssteuerungen sollte insbesondere vor bösartigen Angriffen oder Unfällen konzipiert und angewendet werden, und gleichzeitig an die technischen und wirtschaftlichen Bedingungen des Cloud-Anbieters angepasst werden, die im Datensicherheitskonzept dargelegt sind. Die Gebäudestruktur des Standorts sollte stabil gebaut sein, und alle Außentüren sollten ausreichend mit Hilfe von Kontrollmechanismen (bspw. Schranken, Alarmvorrichtungen, Verriegelungen) vor unbefugtem Zutritt geschützt sein (s. ISO/IEC 27002 Ziff. 11.1.1). Bei den äußeren Türen und Fenstern sollten einbruchhemmendes Material (bspw. nach DIN EN 1627 Widerstandsklasse RC 2) und entsprechende Schließvorrichtungen verbaut sein (s. BSI C5 Anf. PS-01). Alle Außentüren und alle zugänglichen Fenster sollten mit Einbruchmeldeanlagen überwacht werden.

Besuchern sollte der beaufsichtigte Zutritt nur für spezifische Zwecke und für abgegrenzte Bereiche gestattet werden (s. ISO/IEC 27002 Ziff. 11.1.2). Zusätzlich sollten sie in die Sicherheitsanforderungen des betreffenden Bereichs sowie in die Notfallmaßnahmen eingewiesen werden. Alle Beschäftigten und externen Parteien sollten dazu verpflichtet werden, eine gut sichtbare Kennzeichnung ihrer Zutrittsberechtigung zu tragen und unverzüglich das Sicherheitspersonal zu benachrichtigen, wenn sie auf unbegleitete Besucher oder sonstigen Personen treffen, die keine erkennbare Kennzeichnung tragen.

Zur Unterbindung böswilliger Handlungen sollten unbeaufsichtigte Tätigkeiten in Sicherheitsbereichen vermieden werden (s. ISO/IEC 27002 Ziff. 11.1.5). Das Mitführen von Foto-, Video-, Audio- und sonstigen Aufzeichnungsgeräten wie Mobiltelefonen sollte untersagt und nur nach ausdrücklicher Genehmigung gestattet werden.

Auf die Umsetzungshinweise im BSI C5 Anf. OIS-04, PS-01, PS-02, PS-03, PS-04 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 11.1.1, 11.1.2, 11.1.3, 11.1.4, ISO/IEC 27018 Ziff. 11 und ISO/IEC 27701 Ziff. 6.8 und 6.10.2 wird hingewiesen.

Schutzklasse 3

Es gelten die Umsetzungshinweise für Schutzklasse 1 und 2.

Zur Protokollierung der Zutritte sollte ein physisches Protokollbuch oder ein elektronischer Prüfpfad existieren, der sicher aufbewahrt und überwacht wird (s. ISO/IEC 27002 Ziff. 11.1.2). An- und Abmeldung von Besuchern sollten mit Datum und Uhrzeit vermerkt werden.

Nachweis

Der Cloud-Anbieter legt zum Nachweis die relevanten Dokumentationen zum Schutz vor Schädigungen durch Naturereignisse und zur Zutrittskontrolle vor. Dazu zählen unter anderem die Dokumentation der TOM im Datensicherheitskonzept, Berechtigungskonzepte und Verfahrensanweisungen/Konzepte/Richtlinien zu z.B. Wachschutz, Videoüberwachung, Besucherregelungen, Einbruchsmeldeanlagen, Schließsysteme und Berechtigungen.

Die Implementierung, die Angemessenheit und der (fortlaufende) Betrieb von Zutrittskontrollen müssen im Rahmen von Vor-Ort-Prüfungen nachgewiesen werden. Dabei muss der Cloud-Anbieter die Verfügbarkeit und Zuverlässigkeit von definierten Zutrittskontrollen und die Bekanntheit von Anweisungen bei Mitarbeitern nachweisen. Zudem muss er die tatsächliche Umsetzung der Maßnahmen vor Ort gemäß der Dokumentation nachweisen (z.B. Wachschutz aktiv, Videoüberwachung vorhanden, Aufzeichnungen und Protokolle vorhanden).

Der Cloud-Anbieter sollte zudem die Befragung von Mitarbeitern ermöglichen, um nachzuweisen, dass Schulungen und Sensibilisierungsmaßnahmen (bspw. zur Social Engineering Prävention) durchgeführt werden und Mitarbeiter Kenntnis über entsprechende Verhaltensregeln haben (z.B. Umgang mit betriebsfremden Personen). Die Pflege und Aktualität der Maßnahmendokumentation sollte durch entsprechende Dokumentationen nachgewiesen werden (z.B. Zeit-/Datumstempel von Schlüsselbüchern).

Für Schutzklasse 2 und 3 sollte ein Cloud-Anbieter die Prozessdokumentation zur Protokollierung von unbefugten Zutritten und Zutrittsversuchen vorlegen, um nachzuweisen, ob eine fortlaufende Protokollierung vorgenommen wird. Die tatsächliche Protokollierung kann durch die Vorlage von Zutritts- und Ereignisprotokollen oder mittels elektronischer Prüfpfade nachgewiesen werden. Im Rahmen einer Vor-Ort-Prüfung kann nachgewiesen werden, dass unbefugte Zutritte und Zutrittsversuche nachträglich festgestellt werden. Für Schutzklasse 3 gelten diese Nachweise analog zur Feststellung, ob auch jeder autorisierte Zutritt protokolliert wurde.

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 Zwei-Faktor- Authentifizierung. 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 Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) 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

Schutzklasse 1

Zugangssteuerungsregeln, Zugangsrechte und -beschränkungen sollten auf Grundlage der risiko- und sicherheitsrelevanten Anforderungen erstellt, dokumentiert und überprüft werden (s. ISO/IEC 27002 Ziff. 9.1.1). Zugangssteuerungen sind sowohl logischer (bspw. hinsichtlich des Zugangs zu Systemprogrammen) als auch physischer Art (bspw. hinsichtlich des Zugangs zu Hardwareschnittstellen) und beide Arten sind zusammen zu berücksichtigen.

Zugangsberechtigungen für Benutzer unter Verantwortung des Cloud-Anbieters (interne und externe Mitarbeiter) werden in einem formalen Genehmigungsverfahren mit festgelegten Verantwortlichkeiten erteilt (s. ISO/IEC 27002 Ziff. 9.2.2). Organisatorische und/oder technische Maßnahmen stellen sicher, dass eindeutige Benutzerkennungen vergeben werden, die jeden Benutzer eindeutig identifizieren (s. ISO/IEC 27002 Ziff. 9.2.1).

Regeln sollten auf der Grundlage festgelegt werden, dass grundsätzlich alles verboten ist, was nicht ausdrücklich gestattet wird („Least-Privilege-Prinzip“) (s. ISO/IEC 27002 Ziff. 9.1.1). Man erhält nur Zugang zu den Datenverarbeitungssystemen (IT-Ausrüstung, Anwendungen, Verfahren, Räume), die zur Ausführung der eigenen Aufgaben/Tätigkeiten/Funktionen benötigt werden („Need-to-know-Prinzip“).

Das Verfahren zur Anmeldung an einem System/einer Anwendung sollte so gestaltet sein, dass die Gefahr eines unbefugten Zugangs möglichst gering ist (s. ISO/IEC 27002 Ziff. 9.4.2). Das Anmeldeverfahren sollte daher so wenige Informationen wie möglich über das System/die Anwendung preisgeben, um einem unbefugten Benutzer keine Hilfestellung zu geben. Systeme sollten erst nach Abmeldung verlassen oder mit einer Bildschirm- und Tastensperre geschützt werden, die durch eine Benutzerauthentifizierung gesichert ist, wenn sie unbeaufsichtigt sind oder nicht genutzt werden (s. ISO/IEC 27002 Ziff. 11.2.9).

Eine regelmäßige Überprüfung der Zugangsrechte sollte durchgeführt werden. Dabei sollte insbesondere eine Anpassung der Zugangsrechte der Benutzer bei Änderung ihrer Funktionen oder Tätigkeiten erfolgen. Zudem sollte eine unverzügliche Entziehung von Benutzerberechtigungen durchgeführt werden, wenn die Benutzer die Organisation verlassen haben.

Alle Anlagen des Cloud-Anbieters sollten korrekt gewartet werden, damit ihre fortgesetzte Verfügbarkeit und Integrität gewährleistet werden können.

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

Der Zugang sollte ausreichend überwacht und geschützt werden, um Angriffe zu erkennen. Dazu sollten u.a. Viren-Schutz- und Reparaturprogramme eingesetzt werden, die eine signatur- und verhaltensbasierte Erkennung und Entfernung von Schadprogrammen ermöglichen (s. BSI C5 Anf. RB-05).

Die Zuteilung geheimer Authentifizierungsinformationen (z. B. Passwörter, Zertifikate, Sicherheitstoken) an Mitarbeiter des Cloud-Anbieters oder den Cloud-Nutzer sollte, soweit diese organisatorischen oder technischen Verfahren des Cloud-Anbieters unterliegt, in einem geordneten Verfahren erfolgen, das die Vertraulichkeit der Informationen sicherstellt (s. BSI C5 Anf. IDM-07). Soweit die Authentifizierungsinformationen initial vergeben werden, sollten diese nur temporär, höchstens aber 14 Tage lang gültig sein. Benutzer sollten ferner gezwungen werden, diese bei der ersten Verwendung zu ändern. Es sollten interaktive Systeme zur Verwaltung von Kennwörtern genutzt werden sowie starke Kennwörter gemäß dem Stand der Technik (s. ISO/IEC 27002 Ziff. 9.4.3).

Ein gutes Anmeldeverfahren sollte insbesondere während des Anmeldeverfahrens keine Hilfetexte anzeigen, die sich Unbefugte zunutze machen könnten (s. ISO/IEC 27002 Ziff. 9.4.2). Die Anmeldedaten sollten erst nach Eingabe aller Daten geprüft, und bei Auftreten eines Fehlers sollte nicht angezeigt werden, welcher Teil der eingegebenen Daten richtig oder falsch war. Vor Brute-Force-Anmeldeversuchen sollte geschützt und bei Erkennung einer möglicherweise versuchten oder erfolgreichen Umgehung der Anmeldesteuerung sollte ein Sicherheitsereignis ausgelöst werden. Erfolglose und erfolgreiche Anmeldeversuche sollten protokolliert werden. Inaktive Sitzungen sollten nach einer vorgegebenen Zeitspanne automatisch beendet werden.

Die Zugangsberechtigung für netzübergreifende Zugriffe sollte auf einer Sicherheitsbewertung auf Grundlage von Kundenanforderungen basieren (s. BSI C5 Anf. KOS-03). Administrative Berechtigungen sollten mindestens halbjährlich überprüft werden (s. BSI C5 Anf. IDM-05).

Auf die Umsetzungshinweise im BSI C5 Anf. OIS-04, RB-05, RB-17 bis RB-22, IDM-01 bis IDM-13, KOS-03, KOS-04 und SIM-01 bis SIM07 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 9, 12.1.4, 12.4.2, ISO/IEC 27018 Ziff. 9 und ISO/IEC 27701 Ziff. 6.6 wird hingewiesen.

Schutzklasse 3

Es gelten die Umsetzungshinweise für Schutzklasse 1 und 2.

Der Zugang sollte ausreichend überwacht und geschützt werden, um Angriffe zu erkennen. Dazu sollten u.a. Schwachstellen-Scanner und Intrusion-Detection- and Prevention-Systeme eingesetzt und jährliche Penetrationstests durchgeführt werden, um Schwachstellen zu identifizieren und zu beheben. Systemkomponenten, welche für die Erbringung des Cloud-Dienstes verwendet werden, sollten gemäß allgemein etablierter und akzeptierter Industriestandards gehärtet werden (s. BSI C5 Anf. RB-22).

Die Verwendung von Notfallbenutzern (für Aktivitäten, die mit personalisierten, administrativen Benutzern nicht durchgeführt werden können) sollte dokumentiert, begründet und von der Genehmigung einer autorisierten Person, deren Benennung unter Berücksichtigung des Prinzips der Funktionstrennung erfolgt, abhängig gemacht werden. (s BSI C5 Anf. IDM-09). Die Freischaltung des Notfallbenutzers sollte nur so lange erfolgen, wie es für die Aufgabenwahrnehmung notwendig ist.

Die Verwendung von Dienstprogrammen und Managementkonsolen (z. B. zur Verwaltung des Hypervisors oder virtueller Maschinen), die weitreichenden Zugriff auf die Daten der Cloud-Nutzer ermöglichen, sollte auf autorisierte Personen beschränkt werden (s. BSI C5 Anf. IDM-12). Vergabe und Änderung entsprechender Zugriffsberechtigungen sollten gemäß der Richtlinie zur Verwaltung von Zugangsberechtigungen erfolgen .

Der Zugang zu Dienst-Quellcode und zugehörigen Objekten (wie Entwürfen, Spezifikationen, Verifizierungs- und Validierungsplänen) sollte geregelt und überwacht werden, um die Hinzufügung nicht berechtigter Dienst-Funktionen zu verhindern und unbeabsichtigte Änderungen zu vermeiden (s. ISO/IEC 27002 Ziff. 9.4.5). Dies kann bspw. durch kontrollierte zentrale Speicherung, vorzugsweise in Software-Quellcode-Bibliotheken, erreicht werden.

Jeder befugte und unbefugte Zugang und entsprechende Zugangsversuche sollten protokolliert werden. Die Verbindungszeiten sollten beschränkt werden, um zusätzliche Sicherheit und möglichst wenige Gelegenheiten für unbefugte Zugangsversuche zu bieten (s. ISO/IEC 27002 Ziff. 9.4.2).

Auf die Umsetzungshinweise in der ISO/IEC 29146 „Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Zugangssteuerung“ wird hingewiesen.

Nachweis

Der Cloud-Anbieter legt als Nachweis die Dokumentation zur Zugangskontrolle vor, darunter bspw. Dokumentation der TOM im Datensicherheitskonzept, Berechtigungskonzepte, Verfahrensanweisungen, Richtlinien/Konzepte zu Kennwörtern, Dokumentation zu Authentifizierungs- und Verschlüsselungskonzepten bei dem Zugriff (berechtigter

Mitarbeiter) und zu Zugangsberechtigungen. Aus der Dokumentation muss ersichtlich werden, dass das Zugangskonzept und die Berechtigungen aktuell sind und fortlaufend aktualisiert werden (bspw. durch Zeitstempel, Versionierungshistorie oder Protokolle der Aktualisierung).

Die Implementierung, die Angemessenheit und der (fortlaufende) Betrieb von Zugangskontrollen werden im Rahmen eines Vor-Ort-Audits nachgewiesen. Durch eine Befragung des Personals im Rahmen des Audits sollte nachgewiesen werden, ob dieses Kenntnis über entsprechende Verhaltensregeln (z.B. das Verbot der Weitergabe von Passwörtern) hat, und ob Maßnahmen auch gemäß der Dokumentation durchgeführt werden (z.B. Prüfung des Entzuges von Zugangsrechten nach Austritt von Mitarbeitern aus der Organisation). Im Rahmen einer Prüfung können auch Zugangsschnittstellen auf Sicherheit überprüft werden (bspw. Sperrung von Computern von Mitarbeitern).

Für Schutzklasse 2 und 3 legt der Cloud-Anbieter die Prozessdokumentation zur Feststellung von unbefugten Zugängen als Nachweis vor. Der Nachweis über die tatsächliche Feststellung im Regelfall kann durch die Vorlage von Zugangs- und Ereignisprotokollen oder durch elektronische Prüfpfade durchgeführt werden, sofern unbefugte Zugänge stattgefunden haben. Im Rahmen des Vor-Ort-Audits und einer Befragung oder Prüfung kann der Cloud-Anbieter nachweisen, dass unbefugte Zugänge im Regelfall nachträglich festgestellt werden können. Für Schutzklasse 3 weist der Cloud-Anbieter analog nach, dass jeder unbefugte Zugang und entsprechende Versuche nachträglich feststellbar sind.

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 überprüft die Erforderlichkeit der Berechtigungen für den Zugriff auf personenbezogene Daten in regelmäßigen Abständen auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

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

(4) 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.

(5) Für Zugriffe von Befugten auf personenbezogene Daten über das Internet ist eine Zwei Faktor-Authentifizierung erforderlich.

(6) 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.

(7) 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

(8) Die Kriterien von Schutzklasse 1 sind erfüllt.

(9) 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.

(10) Der Cloud-Anbieter ermöglicht es dem Cloud-Nutzer, dass dieser verschiedene zweckbezogene Nutzerrollen für seine Mitarbeiter festlegen kann, um nicht zweckgemäße Zugriffe auf personenbezogene Daten logisch auszuschließen.

(11) Sofern ein privilegierter Zugriff vorliegt, darf dieser nur in Rollen erfolgen, die von der Administration und vom Rechenzentrumsbetrieb unabhängig sind. Der privilegierte Zugriff ist mit Zwei-Faktor-Authentifizierung abzusichern und die Anzahl der Mitarbeiter mit privilegiertem Zugriff ist so gering wie möglich zu halten.

Schutzklasse 3

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

(13) Unbefugte Zugriffe auf Daten sind hinreichend sicher ausgeschlossen. Dies schließt regelmäßig manipulationssichere technische Maßnahmen zur Prävention und aktiven Erkennung von Angriffen ein. Jeder unbefugte Zugriff und entsprechende Versuche sind 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 Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen. Dies setzt ein Berechtigungskonzept für den Zugriff auf personenbezogenen Daten voraus.

Technische Maßnahmen sind manipulationssicher, wenn sie nur durch das Zusammenwirken von mehreren unabhängigen Parteien verändert werden können.

Umsetzungshinweis

Schutzklasse 1

Zugriffsberechtigungskonzepte sollten sowohl für die Cloud-Nutzer als auch für die Mitarbeiter des Cloud-Anbieters bestehen. Ein formaler Prozess für die Registrierung und Deregistrierung von Benutzern sollte umgesetzt werden, um die Zuordnung und Entziehung von Zugriffsrechten zu ermöglichen (s. ISO/IEC 27002 Ziff. 9.2.1). Zugriffssteuerungsregeln, Zugriffsrechte und -beschränkungen sollten auf Grundlage des Datensicherheitskonzepts erstellt, dokumentiert und überprüft werden. Regeln sollten auf der Grundlage festgelegt werden, dass grundsätzlich alles verboten ist, was nicht ausdrücklich gestattet wird („Least-Privilege-Prinzip“) (s. ISO/IEC 27002 Ziff. 9.1.1). Man sollte nur Zugriff auf personenbezogene Daten erhalten, die zur Ausführung der eigenen Aufgaben/Tätigkeiten/Funktionen benötigt werden („Need-to-know-Prinzip“). Zugriffsberechtigungen für Benutzer unter Verantwortung des Cloud-Anbieters (interne und externe Mitarbeiter) sollten in einem formalen Genehmigungsverfahren mit festgelegten Verantwortlichkeiten erteilt werden (s. ISO/IEC 27002 Ziff. 9.2.2). Organisatorische und/oder technische Maßnahmen sollten sicherstellen, dass eindeutige Benutzerkennungen vergeben werden, die jeden Benutzer eindeutig identifizieren (s. ISO/IEC 27002 Ziff. 9.2.1). Es sollte eine Funktionstrennung zwischen operativen und kontrollierenden Funktionen („Separation of Duties“) vorgenommen werden (s. BSI C5 Anf. IDM-01).

Ein geeigneter Managementprozess für die Zugriffskontrolle sollte etabliert werden, der neben der Prüfung der Erforderlichkeit der Berechtigungen auch die Vergabe, Aktualisierung, Kontrolle und den Entzug von Berechtigungen regelt, Zugriffspolitiken überwacht und aktualisiert sowie Passwortrichtlinien überprüft und ihre Einhaltung sicherstellt.

Es sollten angemessene Sicherheitsmaßnamen gegen interne und 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-Detection-Systeme, Applikationsschutz, Antivirus und regelmäßige Integritätsüberprüfungen wichtiger Systemdateien. Alle Zugriffe auf personenbezogene Daten sollten protokolliert werden.

Vergabe und Änderung von Zugriffsberechtigungen für Benutzer mit administrativen oder weitreichenden Berechtigungen unter Verantwortung des Cloud-Anbieters sollten gemäß dokumentierten Zugriffsrichtlinien erfolgen (s. BSI C5 Anf. IDM-06). Die Zuweisung sollte personalisiert und nach dem für die Aufgabenwahrnehmung notwendigen Maß erfolgen („Need-to-know-Prinzip“). Organisatorische und/oder technische Maßnahmen sollten sicherstellen, dass durch die Vergabe dieser Berechtigungen keine ungewollten, kritischen Kombinationen entstehen, die gegen das Prinzip der Funktionstrennung verstoßen (z. B. Zuweisen von Berechtigungen zur Administration der Datenbank wie auch des Betriebssystems). Soweit dies in ausgewählten Fällen nicht möglich ist, sollten angemessene, kompensierende Kontrollen eingerichtet werden, um einen Missbrauch dieser Berechtigungen zu identifizieren (z. B. Protokollierung und Überwachung durch eine SIEM-Lösung).

Zuteilung und Gebrauch von privilegierten Zugangsrechten sollten eingeschränkt und gesteuert werden (s. ISO/IEC 27002 Ziff. 9.2.3). Die Zuteilung von privilegierten Zugangsrechten sollte durch einen offiziellen Genehmigungsprozess kontrolliert werden. Normale Geschäftsaktivitäten sollten nicht mit Benutzerkennungen ausgeführt werden, die über privilegierte Zugangsrechte verfügen. Die Kompetenzen von Benutzern mit privilegierten Zugangsrechten sollten regelmäßig überprüft werden, um sicherzustellen, dass sie dem Aufgabenprofil entsprechen.

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

Sicherheitsparameter auf Netzwerk, Betriebssystem- (Host und Gast), Datenbank- und Anwendungsebene (soweit für den Cloud-Dienst relevant) sollten angemessen konfiguriert werden, um unautorisierte Zugriffe zu

verhindern (s. BSI C5 Anf. IDM-11). 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, sollten der Kreis der Berechtigten klein gehalten und Zugriffsberechtigungen restriktiv vergeben werden. Mitarbeiter sollten nur Zugriff auf die Daten und Datenverarbeitungsvorgänge haben, die sie zur Erfüllung ihrer Aufgaben 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, sollten Zugriffe protokolliert werden.

Der Prozess zur Verwaltung der Benutzerkennungen sollte folgende Punkte umfassen (s. ISO/IEC 27002 Ziff. 9.2.1):

a) Verwendung eindeutiger Benutzerkennungen, damit Benutzer mit ihren Handlungen in Verbindung gebracht und verantwortlich gemacht werden können;
b) Regelmäßige Prüfung der Zugriffsberechtigungen (mindestens jährlich);
c) Anpassung oder Löschung der Benutzerkennungen und der Rechte von Benutzern, deren Funktionen oder Tätigkeit sich geändert haben;
d) Regelmäßige Identifizierung, Löschung oder Deaktivierung überflüssiger Benutzerkennungen;
e) die Gewährung von privilegierten Zugangsrechten sollte in regelmäßigen Abständen überprüft werden, um sicherzustellen, dass keine unbefugten Rechte erworben wurden;
f) Sicherstellung, dass ehemals genutzte Kennungen nicht an andere Benutzer vergeben werden.

Die Zuteilung geheimer Authentifizierungsinformationen (z. B. Passwörter, Zertifikate, Sicherheitstoken) an Mitarbeiter des Cloud-Anbieters oder den Cloud-Nutzer sollte, soweit diese organisatorischen oder technischen Verfahren des Cloud-Anbieters unterliegt, in einem geordneten Verfahren erfolgen, das die Vertraulichkeit der Informationen sicherstellt (s. BSI C5 Anf. IDM-07). Soweit die Authentifizierungsinformationen initial vergeben werden, sollten diese nur temporär, höchstens aber 14 Tage lang gültig sein. Benutzer sollten ferner gezwungen werden, diese bei der ersten Verwendung zu ändern. Es sollten interaktive Systeme zur Verwaltung von Kennwörtern und starke Kennwörter gemäß dem Stand der Technik genutzt werden (s. ISO/IEC 27002 Ziff. 9.4.3).

Richtlinien und Anweisungen mit TOM für die ordnungsgemäße Verwendung mobiler Endgeräte im Verantwortungsbereich des Cloud-Anbieters, die Zugriffe auf IT-Systeme zur Entwicklung und zum Betrieb des Cloud-Dienstes ermöglichen, sollten dokumentiert, kommuniziert und bereitgestellt werden (s. BSI C5 Anf. MDM-01).

Auf die Umsetzungshinweise im BSI C5 Anf. OIS-04, RB-05, RB-17 bis RB-22, IDM-01 bis IDM-13 und KOS-01, KOS-03, KOS-04, MDM-01 und SIM-01 bis SIM07 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 6.2, 9, 12.4.1, 13.2, ISO/IEC 27018 Ziff. 9, A10.13 und ISO/IEC 27701 Ziff. 6.3.2, 6.6, 6.9.1, 6.9.2, 8.2 wird hingewiesen.

Schutzklasse 3

Es gelten die Umsetzungshinweise für Schutzklasse 1 und 2.

Der Zugriff auf personenbezogene Daten sollte umfassend überwacht und geschützt werden, um Angriffe zu erkennen. Dazu sollten u.a. Schwachstellen-Scanner und Intrusion-Detection- and Prevention-Systeme eingesetzt werden und jährliche Penetrationstests durchgeführt werden, um Schwachstellen zu identifizieren und zu beheben. Zudem sollten manipulationssichere technische Maßnahmen zur Prävention und aktiven Erkennung von Angriffen eingesetzt werden. Manipulationssicher ist eine Maßnahme, wenn sie beispielsweise nur durch Zusammenwirken von Cloud-Nutzer und Cloud-Anbieter ausgeführt werden kann.

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.

Auf die Umsetzungshinweise in der ISO/IEC 24760-1 bis ISO/IEC 24760-3 wird hingewiesen.

Nachweis

Der Cloud-Anbieter legt als Nachweis die Dokumentation zur Zugriffskontrolle vor, darunter Dokumentation der TOM im Datensicherheitskonzept, Berechtigungskonzepte, Verfahrensanweisungen, Regelungen für privilegierte Zugriffe, Zugriffsrichtlinien, und Protokolle von administrativen Zugängen und Tätigkeiten. Aus den vorgelegten Dokumenten muss ersichtlich sein, dass das Zugriffskonzept und die Berechtigungen aktuell sind und fortlaufend aktualisiert werden (bspw. durch Zeitstempel, Versionierungshistorie oder Protokolle der Aktualisierung).

Sofern ein privilegierter Zugriff der Mitarbeiter des Cloud-Anbieters auf personenbezogene Daten auf Weisung des Cloud-Nutzers gegeben ist, legt ein Cloud-Anbieter eine repräsentative Stichprobe von rechtverbindlichen Vereinbarungen mit dem Cloud-Nutzer oder andere Dokumente zur Weisungsbeauftragung durch den Cloud-Nutzer vor, um nachzuweisen, dass die Weisungen hierzu dokumentiert und geregelt sind.

Die Implementierung und Angemessenheit von TOM zur Zugriffskontrolle werden im Rahmen von Prüfungen und einem Vor-Ort-Audit nachgewiesen. Der Cloud-Anbieter ermöglicht die Durchführung von Sicherheitstests (bspw. Prüfung auf Verschlüsselung, Sicherung der administrativen Tätigkeiten, Firewallkonfiguration etc.), um die Sicherheit und Angemessenheit der technischen Zugriffsschutzmaßnahmen nachzuweisen. Auch können testweise administrative Tätigkeiten durchgeführt und ihre Protokollierung nachgewiesen werden.

Durch eine Befragung des Personals während des Audits sollte der Cloud-Anbieter nachweisen, dass diese Kenntnis über entsprechende Verhaltensregeln haben (z.B. Verbot der Weitergabe von Passwörtern) und dass Maßnahmen auch gemäß der Dokumentation durchgeführt werden (z.B. Prüfung des Entzuges von Zugriffsrechten nach Austritt von Mitarbeitern aus der Organisation).

Für Schutzklasse 2 und 3 legt ein Cloud-Anbieter die Prozessdokumentation zur Feststellung von unbefugten Zugriffen vor. Die tatsächliche Feststellung im Regelfall kann durch das Vorlegen von Zugriffs- und Ereignisprotokollen oder durch elektronische Prüfpfade nachgewiesen werden, sofern unbefugte Zugriffe stattgefunden haben. Im Rahmen des Vor-Ort-Audits und einer Befragung oder Prüfung kann nachgewiesen werden, ob unbefugte Zugriffe im Regelfall nachträglich festgestellt werden können. Für Schutzklasse 3 weist ein Cloud-Anbieter analog nach, dass jeder unbefugte Zugriff und entsprechende Versuche nachträglich feststellbar sind.

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) Der 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.

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 Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) 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

Schutzklasse 1

Auf den Technischen Report BSI TR-02102-2 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2 – Verwendung von Transport Layer Security (TLS)“ in der jeweils aktuellen Fassung wird hingewiesen. Die Verwendung von SSL (einschließlich der Version 3.0) ist kein sicheres Verfahren.

Datenträger, die personenbezogene Daten enthalten, sollten während des Transports vor unbefugtem Zugriff, Missbrauch oder Verfälschung geschützt werden, indem u.a. nur zuverlässige Transport- bzw. Kurierdienstleister beauftragt werden (s. ISO/IEC 27002 Ziff. 8.3.3). Die Transportbehältnisse sollten ausreichend sein, um Datenträger vor Umweltfaktoren wie Hitze, Feuchtigkeit oder elektromagnetischen Feldern zu schützen. Die Daten sollten verschlüsselt und die Transporte und Transferzeiten dokumentiert werden.

Auf die Umsetzungshinweise im BSI C5 Anf. KRY-01, KRY-02, KOS-01, KOS-02, KOS-05 und KOS-07 wird hingewiesen.

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

Formale Übertragungsrichtlinien, -verfahren und -maßnahmen sollten vorhanden sein, um die Übertragung von Information für alle Arten von Kommunikationseinrichtungen zu schützen (s. ISO/IEC 27002 Ziff. 13.2.1). Hierzu zählen Verfahren, um zu verhindern, dass übertragene Informationen abgefangen, kopiert, verändert, umgeleitet oder zerstört werden; Verfahren zur Erkennung von und zum Schutz vor Schadsoftware, die durch die Verwendung elektronischer Kommunikationseinrichtungen übertragen werden; Maßnahmen und Beschränkungen in Verbindung mit der Nutzung von Kommunikationseinrichtungen, z. B. automatische Weiterleitung von E-Mails an externe E-Mail-Adressen und Maßnahmen zur Sicherstellung der Zuverlässigkeit und Verfügbarkeit des Dienstes (bspw. Maßnahmen gegen Denial-of-Service-Attacken).

Vereinbarungen sollten die sichere Übertragung von personenbezogenen Daten zwischen dem Cloud-Anbieter und externen Parteien behandeln.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 8.3.3, 10.1.1, 10.1.2, 12.4, 13.1.2, 13.2, 14.1.3, ISO/IEC 27018 Ziff. 10.1.1, A.10.6, A.10.9, ISO/IEC 27701 Ziff. 6.7, 6.5.3.3, 6.10, 6.11.1.2 und 8.4.3, ISO/IEC 27040:2017-03 Ziff. 6.7.1 und 7.7.1 wird hingewiesen.

Schutzklasse 3

Es gelten die Umsetzungshinweise für Schutzklasse 1 und 2.

Die Übertragung von personenbezogenen Daten sollte umfassend überwacht und geschützt werden, um Angriffe zu erkennen. Dazu sollten u.a. Schwachstellen-Scanner und Intrusion-Detection- and Prevention-Systeme eingesetzt werden und jährliche Penetrationstests durchgeführt werden, um Schwachstellen zu identifizieren und zu beheben.

Nachweis

Der Cloud-Anbieter legt als Nachweis die Dokumentation zur Übertragung von Daten und Transportverschlüsselung vor, darunter bspw. die der TOM im Datensicherheitskonzept, Verfahrensanweisungen, Richtlinien, Protokoll- und Logdaten, Ergebnisprotokolle interner/externer Audits, Übersicht zu eingesetzten Sicherheitsscannern, Dokumentation des Infrastrukturzugriffs via APIs, Dokumente zum Schlüsselmanagement (insb. Zugriff und Verwahrung der Schlüssel), Dokumente zum Transport von Datenträgern und Dokumentation der Prozesse zur Datenweitergabe.

Durch Prüfungen muss der Cloud-Anbieter nachweisen, dass die Dokumentation mit der tatsächlichen Umsetzung der Maßnahmen übereinstimmt sowie die Maßnahmen wirksam und aktuell sind. Auch eine Befragung der Mitarbeiter z.B. im Hinblick auf die Kenntnis der relevanten Richtlinien und Anweisungen und eine Stichprobenprüfung der Reaktion relevanter Mitarbeiter zur Umsetzung festgelegter Richtlinien und Anweisungen kann als Nachweis angebracht werden.

Für Schutzklasse 2 und 3 legt ein Cloud-Anbieter die Dokumentation zur Feststellung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen von personenbezogenen Daten vor. Die tatsächliche Feststellung im Regelfall kann durch die Prüfung von Ereignisprotokollen, Protokollen zur Abwehr und Erkennung von Angriffen oder elektronischer Prüfpfade nachgewiesen werden, sofern unbefugte Tätigkeiten stattgefunden haben. Für Schutzklasse 3 weist ein Cloud-Anbieter analog nach, ob jedes unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten und entsprechende Versuche nachträglich feststellbar sind.

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 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 Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) 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

Schutzklasse 1

Protokollierungseinrichtungen und Protokollinformation sollten vor Manipulation und unbefugtem Zugriff geschützt sein (s. ISO/IEC 27002 Ziff. 12.4.2). Die Maßnahmen sollten auf den Schutz vor unbefugten Änderungen der Protokollinformationen und Problemen im Betriebsablauf im Zusammenhang mit der Protokollierungseinrichtung abzielen, darunter:

a) Änderungen der aufgezeichneten Nachrichtentypen;
b) bearbeitete oder gelöschte Protokolldateien;
c) Überschreitung der Speicherkapazität der Protokolldatenträger mit dem Ergebnis, dass Ereignisse nicht mehr aufgezeichnet oder frühere Ereignisse überschrieben werden.

Die erstellten Protokolle sollten auf zentralen Protokollierungsservern aufbewahrt werden, wo sie vor unautorisierten Zugriffen und Veränderungen geschützt sind (s. BSI C5 Anf. RB-13). Protokolldaten sollten unverzüglich gelöscht werden, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind.

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

Zwischen den zentralen Protokollierungsservern und den protokollierten (virtuellen) Servern sollte eine Authentisierung erfolgen, um die Integrität und Authentizität der übertragenen und gespeicherten Informationen zu schützen (s. BSI C5 Anf. RB-13). Die Übertragung sollte nach einer dem Stand der Technik entsprechenden Verschlüsselung oder über ein eigenes Administrationsnetz (Out-of-Band-Management) erfolgen.

Der Zugriff und die Verwaltung der Protokollierungs- und Überwachungsfunktionalitäten sollten auf ausgewählte und autorisierte Mitarbeiter des Cloud-Anbieters beschränkt werden. Änderungen der Protokollierungen und Überwachungen sollten vorab durch unabhängige und autorisierte Mitarbeiter überprüft und freigegeben werden (s. BSI C5 Anf. RB-15).

Ein Angriffserkennungssystem, das außerhalb des Einflussbereichs der System- und Netzwerkadministratoren verwaltet wird, kann zur Überwachung der Einhaltung der System- und Netzwerkadministrationsaktivitäten verwendet werden (s. ISO/IEC 27002 Ziff. 12.4.3).

Auf die Umsetzungshinweise im BSI C5 Anf. RB-10 und RB-11 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 12.4, ISO/IEC 27018 Ziff. 12.4.1, 12.4.2 und ISO/IEC 27701 Ziff. 6.9.4 wird hingewiesen.

Schutzklasse 3

Es gelten die Umsetzungshinweise für Schutzklasse 1 und 2.

Der Zugriff und die Verwaltung der Protokollierungs- und Überwachungsfunktionalitäten sollten eine Multi-Faktor-Authentifizierung erfordern.

Die Verfügbarkeit der Protokollierungs- und Überwachungssoftware sollte unabhängig überwacht werden(s. BSI C5 Anf. RB-16). Bei einem Ausfall der Protokollierungs- und Überwachungssoftware sollten die verantwortlichen Mitarbeiter umgehend informiert werden. Die Protokollierungs- und Überwachungssoftware sollte redundant vorhanden sein, um auch bei Ausfällen die Protokollierung und Überwachung durchführen zu können.

Die erstellten Protokolle erlauben eine eindeutige Identifizierung von Benutzerzugriffen auf Tenant-Ebene, um (forensische) Analysen im Falle eines Sicherheitsvorfalls zu unterstützen (s. BSI C5 Anf. RB-14).

Auf die Umsetzungshinweise im BSI C5 Anf. RB-13 bis RB-16 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Datensicherheitskonzept dokumentiert, wie ein Cloud-Anbieter durch Festlegung von Gegenstand und Umfang der Protokollierung, Aufbewahrung, Integritätsschutz und Löschung von Protokollen und der Verwendung der Protokolldaten die Datenschutzgrundsätze sicherstellt. Weitere Dokumente als Nachweise können Berechtigungskonzepte (insb. Nutzer- und Administratorenberechtigungen), Verfahrensanweisungen, Richtlinien, Protokoll- und Logdaten, Ergebnisprotokolle interner/externer Audits und Risikoanalysen sein.

Die Implementierung und Angemessenheit dieses Protokollierungskonzepts sollten durch repräsentative Stichproben im Rahmen des laufenden Betriebs nachgewiesen werden (bspw. Nachweis, dass Protokolleinträge bei Eingaben, Veränderungen und Löschungen personenbezogener Daten erzeugt werden). Durch die Verwendung von Sicherheitstests können auch angewendete Schutzmaßnahmen von Protokollen gegen Manipulation nachgewiesen werden.

Für Schutzklasse 2 und 3 legt ein Cloud-Anbieter die Dokumentation zur Feststellung von Manipulationen der Protokollierungen vor. Die tatsächliche Feststellung im Regelfall kann durch das Vorlegen von Ereignisprotokollen, Protokollen zur Abwehr und Erkennung von Manipulationen oder mittels elektronischer Prüfpfade nachgewiesen werden, sofern Manipulationen stattgefunden haben. Für Schutzklasse 3 weist ein Cloud-Anbieter analog nach, ob jede Manipulation und möglichst auch jeder entsprechende Versuch nachträglich feststellbar sind.

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) Soweit mit dem Cloud-Nutzer vereinbart (Nr. 1.7), stellt der Cloud-Anbieter sicher, dass die Daten pseudonymisiert verarbeitet werden. Entsprechend der rechtsverbindlichen Vereinbarung 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) Ist die Pseudonymisierung der Daten auf Weisung des Cloud-Nutzers nicht gegenüber allen Mitarbeitern des Cloud-Anbieters wirksam, ist der Kreis der privilegierten Mitarbeiter auf das unbedingt Erforderliche zu begrenzen.

(5) 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.

(6) Der Cloud-Anbieter gewährleistet, dass er die technische Entwicklung im Bereich der Pseudonymisierungsverfahren laufend verfolgt und seine Verfahren den aktuellen technischen Empfehlungen (best practices) 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 C1.5) 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

Schutzklasse 1

Der Cloud-Anbieter sollte durch TOM sicherstellen, dass eine Pseudonymisierung der personenbezogenen Daten nicht aufgehoben werden kann (bspw. Sicherstellung, dass der Schlüssel des Cloud-Nutzers nicht bekannt ist).

Schutzklasse 2 und 3

Hinweise zur rechtssicheren Umsetzung von Pseudonymisierungsverfahren können dem Arbeitspapier „Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen“ entnommen werden. Für die Überwachung des Pseudonymisierungsprozesses sollte der Cloud-Anbieter einen geeigneten Fachverantwortlichen bestimmen, der einen einheitlichen Einsatz bei der Pseudonymisierung koordiniert und die Verantwortung für wichtige Entscheidungen übernimmt.

Werden Pseudonyme durch Berechnungsverfahren erstellt, sollten diese dem Stand der Technik entsprechen (z.B. BSI TR-02102-1). Die getrennte Aufbewahrung des Datensatz mit der Zuordnung des Kennzeichens zu einer Person bedarf eines dokumentierten Berechtigungskonzepts und der Zugriff auf diesen Datensatz sollte auf ein absolutes Minimum an vertrauenswürdigen Personen eingeschränkt werden (Need-to-Know-Prinzip). Jeder Zugriff auf den Datensatz mit der Zuordnungsinformation sollte nach dem Vier-Augen-Prinzip erfolgen. Sofern dies nicht möglich ist, sollte jeder Zugriff personenbezogen protokolliert werden.

Um eine weisungsgetreue De-Pseudonymisierung durchführen zu können, sollten mit dem Cloud-Nutzer dokumentierte Fälle von gewünschten Aufdeckungen definiert werden. Der Vorgang der De-Pseudonymisierung

sollte protokolliert werden. Aus dem Protokoll sollte hervorgehen, wer die De-Pseudonymisierung durchgeführt hat. In ihm sollten jedoch keine Angaben enthalten sein, die Rückschlüsse auf die dem Pseudonym zugrunde liegenden Identitätsdaten erlauben.

Der Cloud-Anbieter sollte öffentlich bekannt geben, welche technischen Standards sein Pseudonymisierungsverfahren erfüllt. Beispielsweise kann zur Pseudonymisierung in der medizinischen Informatik ISO 25237 herangezogen werden.

Nachweis

Für Schutzklasse 1 legt der Cloud-Anbieter Dokumentationen über den Prozess der Datenverarbeitung, insbesondere im Hinblick auf pseudonymisierte Daten vor. Durch eine testweise Dienstnutzung mit pseudonymisierten Daten kann nachgewiesen werden, dass Verarbeitungen unter Wahrung der Pseudonymität durchgeführt werden.

Für Schutzklasse 2 und 3 legt ein Cloud-Anbieter Dokumentationen vor, die nachweisen, wie Pseudonymisierungen vorgenommen, Identifizierungsdaten sicher aufbewahrt und gegen Manipulation geschützt, und pseudonymisierte Daten verarbeitet werden (bspw. Vorlage von Dokumentationen der TOM, Verfahrensanweisungen, Richtlinien, Protokoll- und Logdaten, Ergebnisprotokolle interner/externer Audits und der Risikoanalyse).

Die Implementierung, Angemessenheit und Wirksamkeit der Pseudonymisierungsverfahren und der Maßnahmen zum Schutz der zusätzlichen Informationen zur Identifizierung werden für Schutzklasse 2 und 3 im Rahmen einer (Sicherheits-)Prüfung durch repräsentative Stichproben festgestellt. Auch kann der Cloud-Anbieter die Art der eingesetzten Programme, die Programmierungen zur Pseudonymisierung und ihre Konfiguration im Rahmen einer Assetprüfung darlegen und eine stichprobenartige Prüfung von pseudonymisierten Datensätzen zulassen. Eine Befragung von Mitarbeitern im Rahmen eines Audits kann zusätzlich als Nachweis dienen, indem die in der Dokumentation spezifizierten Maßnahmen mit den tatsächlich durchgeführten Maßnahmen für Schutzklasse 2 und 3 abgeglichen werden (bspw. Befolgung von Richtlinien und Schutzmaßnahmen, Bekanntheit der Weisungen zur De-Pseudonymisierung).

Erfordert die Art des Auftrags mit dem Cloud-Nutzer die De-Pseudonymisierung der Daten, legt ein Cloud-Anbieter die rechtsverbindliche Vereinbarung mit dem Cloud-Nutzer oder andere Dokumente zur Weisungserteilung des Cloud-Nutzers vor.

Zudem legt der Cloud-Anbieter Dokumentationen vor (bspw. Protokolle, Versionierungshistorie), die belegen, dass der Cloud-Anbieter die technische Entwicklung im Bereich der Pseudonymisierungsverfahren laufend verfolgt. Dies kann auch im Rahmen einer Assetprüfung nachgewiesen werden (bspw. Nachweis über Änderungen am Programmcode zur Pseudonymisierung, Aktualisierung von Bibliotheken etc.). Auch kann durch eine Befragung der Mitarbeiter nachgewiesen werden, dass diese die aktuellen Empfehlungen zur Pseudonymisierung kennen und umsetzen.

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 practices) 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 C1.1) zu fördern.

Umsetzungshinweis

Schutzklasse 1

Der Cloud-Anbieter sollte durch TOM sicherstellen, dass eine Anonymisierung der personenbezogenen Daten nicht aufgehoben werden kann.

Schutzklasse 2 und 3

Der Cloud-Anbieter sollte öffentlich bekannt geben, welche technischen Standards sein Anonymisierungsverfahren erfüllt.

Der Cloud-Anbieter sollte anerkannte Verfahren zur Anonymisierung passend zu dem jeweiligen Datenverarbeitungszweck verwenden.

Nachweis

Für Schutzklasse 1 legt ein Cloud-Anbieter Dokumentationen über den Prozess der Datenverarbeitung vor, insbesondere im Hinblick auf anonyme Daten. Im Rahmen einer testweisen Dienstnutzung mit anonymen Daten kann nachgewiesen werden, dass Verarbeitungen unter Wahrung der Anonymität durchgeführt werden.

Für Schutzklasse 2 und 3 legt ein Cloud-Anbieter Dokumentationen vor, welche darlegen, wie der Cloud-Anbieter Anonymisierungen durchführt und anonymisierte Daten verarbeitet sowie welche Anonymisierungsverfahren eingesetzt bzw. angeboten werden (z.B. Dokumentation der TOM, Verfahrensanweisungen, Richtlinien, Protokoll- und Logdaten, Ergebnisprotokolle interner/externer Audits und Risikoanalyse).

Die Implementierung und Angemessenheit der Anonymisierungsverfahren wird für Schutzklasse 2 und 3 im Rahmen einer Prüfung durch repräsentative Stichproben festgestellt. Dazu sollten die Art der eingesetzten Programme, die Programmierungen zur Anonymisierung und ihre Konfiguration im Rahmen einer Assetprüfung überprüft und eine stichprobenartige Prüfung von Datensätzen durchgeführt werden. Eine Befragung von Mitarbeitern kann zusätzlich als Nachweis dienen, indem die in der Dokumentation spezifizierten Maßnahmen mit den tatsächlich durchgeführten Maßnahmen für Schutzklasse 2 und 3 abgeglichen werden (bspw. Befragung hinsichtlich der Richtlinien und Regelungen zur Anonymisierung).

Durch die Vorlage von Dokumentationen (bspw. Protokolle, Versionierungshistorie) weist ein Cloud-Anbieter für Schutzklasse 2 und 3 nach, dass der Cloud-Anbieter die technische Entwicklung im Bereich der Anonymisierung laufend verfolgt. Dies kann auch im Rahmen einer Assetprüfung bei einer Prüfung (bspw. Nachweis über Änderungen am Programmcode zur Anonymisierung, Aktualisierung von Bibliotheken etc.) nachgewiesen werden.

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) Ist die Verschlüsselung des Cloud-Anbieters auf Weisung des Cloud-Nutzers nicht gegenüber allen Mitarbeitern des Cloud-Anbieters wirksam, ist die Anzahl der privilegierten Mitarbeiter auf das unbedingt Erforderliche zu begrenzen.

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

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

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

Schutzklasse 3

(7) Es gelten die Kriterien der Schutzklasse 2. Zusätzlich werden unberechtigte Zugriffe auf den Schlüssel hinreichend sicher durch geeignete TOM ausgeschlossen.

(8) Erfolgt die Verschlüsselung durch den Cloud-Nutzer, unterstützt der Cloud-Anbieter diesen auf dessen Weisung hin bei der Verschlüsslung und Entschlüsselung der Daten. Die Unterstützung erfolgt in Form von Dokumentationen und Hilfsmaßnahmen zur Durchführung von Verschlüsselung.

(9) Der Cloud-Anbieter hält seine unterstützenden Maßnahmen in Form von Dokumentationen und Hilfsmaßnahmen zur Durchführung von Verschlüsselung auf dem Stand der aktuellen technischen Empfehlungen (best practices).

Erläuterung

Das Kriterium bezieht sich auf die Verschlüsselung von gespeicherten Daten, d.h. Daten, die sich im Ruhezustand befinden.

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 2 und 3 bietet der Cloud-Anbieter Verschlüsselungsverfahren an. Die Verschlüsselung kann durch den Cloud-Nutzer erfolgen oder auf dessen Weisung hin durch den Cloud-Anbieter.

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 C1.4 und C1.3) 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

Schutzklasse 1

Der Cloud-Anbieter sollte durch TOM sicherstellen, dass die Verschlüsselung der Daten bei der Speicherung in seinem Cloud-Dienst aufrechterhalten bleibt.

Schutzklasse 2

Der Stand der Technik ergibt sich aus aktuellen technischen Normen für kryptographische Verfahren und deren Anwendung.

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 sollte stets redundant gesichert und wiederherstellbar sein, um einen Verlust eines Schlüssels auszuschließen. Schlüsselwechsel sollten regelmäßig durchgeführt werden. Der Zugang zum Schlüsselverwaltungssystem sollte eine separate Authentisierung erfordern. Cloud-Administratoren sollten keinen Zugriff auf Nutzerschlüssel haben.

Auf die Umsetzungshinweise im BSI C5 Anf. KRY-01, KRY-03 und KRY-04 wird hingewiesen.

Auf die Technischen Reports BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“; BSI TR-02102-3 „Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPSec) und Internet Key Exchange (IKEv2)“; und BSI TR-02102-4 „Kryptographische Verfahren: Verwendung von Secure Shell (SSH)“ in der jeweils aktuellen Fassung wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27002, Ziff. 10.1, ISO/IEC 27018 Ziff. 10.1 und ISO/IEC 27701 Ziff. 6.7 wird hingewiesen. ISO/IEC 11770-2 enthält weitere Informationen zur Schlüsselverwaltung.

Schutzklasse 3

Es gelten die Umsetzungshinweise für Schutzklasse 2. Weiterhin sollte der Cloud-Anbieter durch zusätzliche TOM sicherstellen, dass unberechtigte Zugriffe auf den Schlüssel hinreichend sicher ausgeschlossen werden. Zugriffe auf Schlüssel sollten daher umfassend überwacht und geschützt werden. Um Schwachstellen beim Zugriff auf Schlüssel identifizieren und beheben zu können, sollten u.a. Schwachstellen-Scanner eingesetzt und jährliche Penetrationstests durchgeführt werden.

Nachweis

Für Schutzklasse 1 legt der Cloud-Anbieter Dokumentationen über den Prozess der Datenverarbeitung vor, insbesondere im Hinblick auf die Speicherung verschlüsselter Daten. Im Rahmen einer testweisen Dienstnutzung mit verschlüsselten Daten kann die erfolgreiche Speicherung nachgewiesen werden.

Für Schutzklasse 2 und 3 legt ein Cloud-Anbieter Dokumentationen vor, um nachzuweisen, dass die angebotenen und angewandten Verschlüsselungsverfahren den aktuellen technischen Anforderungen entsprechen (z.B. Dokumentation der TOM, Verfahrensanweisungen, Richtlinien, Protokoll- und Logdaten, Ergebnisprotokolle interner/externer Audits, Risikoanalyse). Die Implementierung und Angemessenheit der Verschlüsselungsverfahren wird für Schutzklasse 2 und 3 im Rahmen einer Prüfung durch repräsentative Stichproben festgestellt. Dazu sollten u.a. die Art der eingesetzten Programme, die Programmierungen zur Verschlüsselung und ihre Konfiguration im Rahmen einer Assetprüfung nachgewiesen und eine stichprobenartige Prüfung von Datensätzen durchgeführt werden. Durch das Vorlegen von Dokumenten (bspw. Protokolle, Versionierungshistorie) weist der Cloud-Anbieter für Schutzklasse 2 und 3 nach, dass er die technische Entwicklung im Bereich der Verschlüsselung laufend verfolgt, die Geeignetheit des Verfahrens fortdauernd prüft und das Verfahren sowie die Dokumentation gegebenenfalls aktualisiert (bspw. Nachweis über Änderungen am Programmcode zur Verschlüsselung, Aktualisierung von Bibliotheken etc.). Durch eine Befragung der Mitarbeiter kann ebenfalls nachgewiesen werden, dass diese die aktuellen Empfehlungen zur Verschlüsselung kennen und umsetzen. Der Cloud-Anbieter sollte Protokolle vorlegen, die nachweisen, dass der Cloud-Anbieter die Verschlüsselungstechniken durch geeignete technische Tests geprüft hat.

Für Schutzklasse 3 legt der Cloud-Anbieter Zugriffs- und Ereignisprotokolle für den Zugriff auf Schlüssel vor. Zudem kann er weitere Dokumente vorlegen, wie bspw. die Nutzerdokumentation zur Ver-/Entschlüsselung, Dokumentation von Verschlüsselungsverfahren oder Protokolle eines qualifizierten (ggf. durch Schulungen nachzuweisenden) IT-Sicherheitsgremiums, in dem auch regelmäßig die technischen Verfahren zur Ver-/Entschlüsselung reflektiert werden.

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 gegen das Trennungsgebot einen Schutz, der diese hinreichend sicher ausschließt. Der Cloud-Anbieter kann vorsätzliche Verstöße gegen das Trennungsgebot im Regelfall (nachträglich) feststellen.

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. Der Cloud-Anbieter erkennt vorsätzliche Verstöße gegen die getrennte Verarbeitung.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Verfügbarkeit, Integrität, Vertraulichkeit und Nichtverkettung (SDM C1.2 – C1.5) 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

Schutzklasse 1

Daten sollten auf gemeinsam genutzten virtuellen und physischen Ressourcen (Speichernetz, Arbeitsspeicher) gemäß einem dokumentierten Konzept sicher und strikt separiert werden (s. BSI C5 Anf. RB-23). Eine techni-

sche Trennung der gespeicherten und verarbeiteten Daten der Cloud-Nutzer in gemeinsam genutzten Ressourcen kann durch Firewalls, Zugriffslisten, Tagging (Auszeichnung des Datenbestandes), VLANs, Virtualisierung und Maßnahmen im Speichernetz (z. B. LUN Masking) erreicht werden.

Auf die Umsetzungshinweise des BSI C5 Anf. RB-23 und KOS-05 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 12.1.4, 13.1.3 und ISO/IEC 27701 Ziff. 6.9.1.4. wird hingewiesen.

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

Im Rahmen der Datenspeicherung sollten eine mandantenspezifische Verschlüsselung mit individuellen Schlüsseln und die Verwendung getrennter Betriebsumgebungen für verschiedene Verarbeitungen oder gleichwertige Verfahren eingesetzt werden. Zugriffe auf Daten sollten protokolliert werden.

Der Cloud-Anbieter sollte technische und organisatorische Überwachungsverfahren und -systeme betreiben, um Angriffe (bspw. Cross-VM Attacks) und böswilliges Verhalten feststellen zu können.

Zur sicheren Segmentierung gemeinsam genutzter Ressourcen bei Webanwendungen, die als SaaS bereitgestellt werden, sollte gemäß BSI C5 Anf. KOS-05 die Session-ID in der Grundstufe

a) zufallsgeneriert sein und eine ausreichende Entropie von mindestens 128 Bit (16 Zeichen) haben, um dem Erraten der Session-ID (zum Beispiel durch einen Brute-Force-Angriff) standzuhalten,
b) bei der Übertragung und clientseitigen Speicherung ausreichend geschützt sein,
c) eine begrenzte Gültigkeit (Timeout) haben, die gemessen an den Anforderungen zur Nutzung der Webanwendung möglichst kurz ist,
d) nach erfolgreicher Authentisierung oder Wechsel von einem ungesicherten Kommunikationskanal (HTTP) auf einen gesicherten Kommunikationskanal (HTTPS) gewechselt werden.

Bei IaaS/PaaS ist die sichere Trennung durch physisch getrennte Netze oder durch stark verschlüsselte VLANs sichergestellt (s. BSI C5 Anf. KOS-05).

Schutzklasse 3

Es gelten die Umsetzungshinweise für Schutzklasse 1 und 2.

Der Cloud-Anbieter sollte technische und organisatorische Überwachungsverfahren und -systeme betreiben, um Angriffe und böswilliges Verhalten feststellen und unterbinden zu können.

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. Darüber hinaus kann er bspw. die Dokumentation der TOM, Verfahrensanweisungen, Richtlinien, Ergebnisprotokolle interner/externer Audits, Risikoanalysen und Produktbeschreibungen als Nachweis vorlegen.

Die tatsächliche Umsetzung der Maßnahmen (bspw. getrennte Datenbanken) sollte durch eine Überprüfung der Trennung (bspw. der eingesetzten Programme oder des Programmcodes, Prüfung auf getrennte Datenbanken) und Sicherheitstests (z.B. Penetrationstests zur Feststellung des Sicherheitsniveaus der Mandantentrennung) nachgewiesen werden. Unterstützend kann eine Befragung relevanter Mitarbeiter im Rahmen eines Audits (z.B. zur Kenntnis über Richtlinien etc.) als Nachweis angeführt werden.

Für Schutzklasse 2 und 3 weist ein Cloud-Anbieter durch Dokumentationen die Erkennung von vorsätzlichen Verstößen gegen das Trennungsgebot nach. Die tatsächliche Feststellung im Regelfall kann durch die Vorlage von Ereignisprotokollen, Protokollen zur Abwehr und Erkennung von Angriffen oder mittels elektronischer Prüfpfade nachgewiesen werden.

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 rasch wiederhergestellt werden und verfügbar sind. 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.

Wiederherstellbarkeitsklasse 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 C1.2). 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. 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

Wiederherstellbarkeitsklasse 1

Zur Wiederherstellung von Daten und Systemen sollte ein Cloud-Anbieter ein wirksames Datensicherungskonzept erstellen, in dem er Systeme zu Datensicherungen, Pläne zur Wiederherstellung und zur Schadensbegrenzung sowie einen Plan zur regelmäßigen Überprüfung und Aktualisierung der vorgesehenen Maßnahmen vorsieht (s. BSI C5 Anf. RB-06). Bei der Datensicherung ist zwischen Backups und Snapshots virtueller Maschinen zu unterscheiden. Snapshots ersetzen kein Backup, können jedoch Teil der Backup-Strategie sein.

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. Die Wiederherstellbarkeit der Sicherheitskopien sollte regelmäßig überprüft werden.

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

Auf die Umsetzungshinweise im BSI C5 Anf. RB-01, RB-02, RB-04, RB-06 bis RB-09 wird hingewiesen.

Für die Aufstellung eines Datensicherungskonzepts sind die Umsetzungshinweise aus ISO/IEC 27002 Ziff. 11.1.4, 11.2.2, 12.1.3, 12.3, 17.1.2, ISO/IEC 27018 Ziff. 12.3.1, A.10.3 und ISO/IEC 27701 Ziff. 6.9.1, 6.9.3, 6.13, 6.14 anwendbar.

Wiederherstellbarkeitsklasse 2

Bei betriebswichtigen Systemen und Diensten sollten die Datensicherungsvorkehrungen alle Systeminformationen, -anwendungen und -daten umfassen, die zur Wiederherstellung des kompletten Systems bei einem Schaden erforderlich sind.

Im Rahmen der Betriebsabläufe sollten die Durchführung von Datensicherungen überwacht und Maßnahmen bei fehlgeschlagenen geplanten Datensicherungen festlegt werden, um die Vollständigkeit der Backups nach der Datensicherungsrichtlinie zu gewährleisten (s. ISO/IEC 27002 Ziff. 12.3.1).

TOM zur Überwachung und Provisionierung bzw. De-Provisionierung von Cloud-Dienstleistungen sind definiert.

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.

Auf die Umsetzungshinweise im BSI C5 Anf. BCM-01 bis BCM-05 wird hingewiesen.

Wiederherstellbarkeitsklasse 3

Die Datensicherungen sollten an einem oder mehreren externen Orten in ausreichender Entfernung redundant aufbewahrt werden, um vor Schäden am Hauptstandort geschützt zu sein (s. ISO/IEC 27002 Ziff. 12.3.1). Datensicherungen sollten mittels Verschlüsselung auf dem aktuellen Stand der Technik geschützt werden.

Der Zugriff auf die gesicherten Daten ist auf autorisiertes Personal beschränkt (s. BSI C5 Anf. RB-06). Wiederherstellungsprozesse beinhalten Kontrollmechanismen, die sicherstellen, dass Wiederherstellungen ausschließlich nach Genehmigung durch hierfür autorisierte Personen gemäß den vertraglichen Vereinbarungen mit dem Cloud-Nutzer oder den internen Richtlinien des Cloud-Anbieters erfolgen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er im Datensicherheitskonzept dokumentiert, 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.

Weitere Dokumente als Nachweis zur Wiederherstellbarkeit können insbesondere die Dokumentation der TOM, Verfahrensanweisungen, Richtlinien, Protokolle zu Testläufen der Datenwiederherstellung, Ergebnisse interner/externer Audits, Risikoanalysen und Produktbeschreibungen sein.

Die Implementierung und die Angemessenheit der geeigneten TOM sollten durch repräsentative Stichproben im Rahmen eines Audits nachgewiesen werden. Durch eine Befragung relevanter Mitarbeiter (z.B. zur Kenntnis über Richtlinien und Verfahrensanweisungen zur Wiederherstellung etc.) kann ebenfalls die Implementierung nachgewiesen werden. Die Prüfung oder Besichtigung von Serverräumen und die Beurteilung getroffener Maßnahmen und eingesetzter Techniken (bspw. redundanter Server) zur Wiederherstellbarkeit können als Nachweise angeboten werden. Ein Ausfall und. eine Wiederherstellung können testweise simuliert und Mitarbeiter dabei beobachtet werden, um die Übereinstimmung mit der Prozessdokumentation nachzuweisen.

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

Kriterium

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

(2) Der Cloud-Anbieter gewährleistet durch TOM, dass die Verarbeitung der Daten des Cloud-Nutzers nur nach Maßgabe der Weisungen des Cloud-Nutzers erfolgt, es sei denn der Auftragsverarbeiter wird durch Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet.

(3) Für den Fall, dass der Auftragsverarbeiter durch Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet ist, worunter auch die Datenübermittlung an ein Drittland oder eine internationale Organisation fällt, stellt der Cloud-Anbieter durch TOM sicher, dass er dem Cloud-Nutzer die rechtlichen

Anforderungen vor der Datenverarbeitung mitteilt, sofern das jeweilige Recht die Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(4) 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.

Umsetzungshinweis

Durch Art. 29 DSGVO wird der Cloud-Anbieter zur Unterweisung aller Mitarbeiter in die vertraglich dokumentierten Weisungen verpflichtet, deren Tätigkeiten im Zusammenhang mit der Verarbeitung von personenbezogenen Daten stehen. Der Cloud-Anbieter sollte die Weisungsbefolgung auch in einer etwaigen Datenverarbeitungskette sicherstellen. Darüber hinaus sollte der Cloud-Anbieter regelmäßig kontrollieren, ob die Weisungen des Cloud-Nutzers eingehalten werden.

Da die Weisungsbefolgung essentiell für die Auftragsverarbeitung ist, sollte der Cloud-Anbieter diese durch TOM sicherstellen. Die Maßnahmen sollten auch gegen technische und organisatorische Fehler und Manipulationsversuche bei der Erteilung von Weisungen absichern. Maßnahmen der Datensicherheit wie beispielsweise die Zugangs- und Zugriffskontrolle (Nr. 2.3 und Nr. 2.4) und die Gewährleistung der Nachvollziehbarkeit der Datenverarbeitung (Nr. 2.6) tragen zur Sicherstellung der Weisungsbefolgung bei, sodass die hierzu angegebenen Umsetzungshinweise ebenfalls berücksichtigt werden sollten.

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.

Der Cloud-Anbieter sollte durch TOM sicherstellen, dass er den Cloud-Nutzer über die rechtlichen Anforderungen einer nicht weisungsgedeckten Verarbeitung zur Erfüllung von Pflichten aus dem Unionsrecht oder aus mitgliedstaatlichem Recht vor deren Durchführung informiert. Auf diese Weise wird sichergestellt, dass auch diese Verarbeitung dem Cloud-Nutzer transparent gemacht wird, sodass er ggf. betroffene Personen informieren kann. Ausnahmen von der Informationspflicht bestehen nach Art. 28 Abs. 3 Satz 2 lit. a DSGVO nur, sofern das betreffende Recht eine solche Mitteilung im wichtigen öffentlichen Interesse verbietet. Beispiele hierfür sind Übermittlungen des Cloud-Anbieters an Ermittlungsbehörden in Strafsachen, Steuerangelegenheiten oder staatsschutz- und geheimdienstrelevante Sachverhalte.

Auf die Umsetzungshinweise zum Schutz des Cloud-Dienstes vor internen und externen Angriffen und Manipulationen im BSI C5 Anf. OIS-04, RB-05, RB-17 bis RB-22, und KOS-01, KOS-03, KOS-04, MDM-01 und SIM-01 bis SIM-07 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 12.2, 12.4, 12.6, 16 und der ISO/IEC 27018 Ziff. A 2.1 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 8.5.4 wird hingewiesen.

Nachweis

Der Cloud-Anbieter legt als Nachweis Dokumentationen zur Weisungsgebundenheit vor, darunter bspw. Dokumentation der TOM, Verfahrensanweisungen (insb. für Administratoren), Richtlinien, Protokollierung der Weisungen und dokumentierte Maßnahmen zum Schutz und zur Manipulationsverhinderung vor.

Bei Einzelvereinbarungen mit Cloud-Nutzern legt der Cloud-Anbieter eine Stichprobe der rechtsverbindlichen Vereinbarungen vor, um die Umsetzung und Befolgung der dokumentierten Weisungen mit dem tatsächlichen Verhalten der Mitarbeiter und des Cloud-Dienstes nachweisen zu können. Hierzu können eine testweise Weisung als Funktion im Cloud-Dienst aufgerufen werden oder entsprechende Mitarbeiter testweise im Rahmen eines Audits zur Durchführung einer Weisung angewiesen werden.

Bei Massengeschäften legt der Cloud-Anbieter eine Dienstbeschreibung zu den technisch ausführbaren Dienstleistungen und Weisungen durch Softwarebefehle vor, sodass diese mit der tatsächlich möglichen Interaktion im Cloud-Dienst verglichen werden können (bspw. im Rahmen einer testweisen Dienstnutzung). Der Cloud-Anbieter sollte Protokolle über die fortlaufende Dokumentierung von erteilten Weisungen und/oder Softwarebefehlen von Cloud-Nutzern (bspw. Logeinträge, Zeitstempel, Versionierung von Logdateien) als Nachweise vorlegen. Im Rahmen eines Audits kann eine Befragung oder Beobachtung relevanter Mitarbeiter (z.B. zur Kenntnis über Weisungen von Cloud-Nutzern und Richtlinien zur Befolgung dieser etc.) als Nachweis durchgeführt werden.

Der Cloud-Anbieter legt als Nachweis erfolgte Mitteilungen an den Cloud-Nutzer über rechtliche Anforderungen zu nicht weisungsgedeckten Verarbeitungen zur Erfüllung rechtlicher Pflichten aus dem Unionsrecht oder dem mitgliedstaatlichen Recht vor, soweit er über solche verfügt. Als Nachweis können auch Dokumentationen dienen,

darunter bspw. Dokumentation der TOM oder Verfahrensanweisungen, z.B., wie mit Anfragen von Ermittlungsbehörden umzugehen ist, die eine Herausgabe von Daten zum Inhalt haben oder wie der Cloud-Nutzer über diese rechtlichen Anforderungen zu informieren ist.

Nr. 4 – Hinweispflicht des Cloud-Anbieters

Nr. 4.1 – Weisungen entgegen datenschutzrechtlicher Vorschriften (Art. 28 Abs. 3 Satz 3 lit. h 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, sollte der Cloud-Anbieter TOM vorsehen, die den Cloud-Nutzer darauf hinweisen, wenn er den Dienst datenschutzwidrig entgegen der Dienstbeschreibung nutzt. Dazu zählt beispielsweise ein Informationstext, der den Cloud-Nutzer warnt, wenn die vom Cloud-Anbieter zur Verfügung gestellten Datensicherungsmaßnahmen wie Verschlüsselung und Pseudonymisierung nicht genutzt werden.

Der Cloud-Anbieter sollte organisatorische Prozesse spezifizieren und dokumentieren, welche die Ansprechpartner, deren Verantwortlichkeiten, Vorgehensweisen und Meldewege im Falle einer Feststellung einer datenschutzwidrigen Weisung regeln. Diese Prozesse können bspw. in bestehende Incident- und Troubleshooting-Management-Prozesse verankert werden.

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 8.2.4 wird hingewiesen.

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. Dazu können die Dokumentation der TOM, Verfahrensanweisungen, Richtlinien, Protokollierung der Weisungen, Dokumentation der relevanten Mechanismen und Meldewege, und dokumentierte Prozesse zur Weisungsüberprüfung zählen. Ein Cloud-Anbieter kann auch stattgefundene und dokumentierte Kommunikationen an Cloud-Nutzer im Falle der Abweichungsvermutung vorlegen.

Eine Befragung relevanter Mitarbeiter (z.B. zur Kenntnis über Richtlinien und Verfahrensschritte im Falle von Zweifeln etc.) im Rahmen eines Audits kann als zusätzlicher Nachweis durchgeführt werden. Darüber hinaus kann mittels einer Beobachtung, bei der testweise eine rechtswidrige Weisung gegeben wird, nachgewiesen werden, dass die Prozesse zur Aufnahme und Bearbeitung der Weisung durchgeführt werden.

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 Datenverarbeitung gegenüber dem in der Vereinbarung festgelegten (Nr. 1.5) ändert.

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.

Auf die Umsetzungshinweise der ISO/IEC 27018 Ziff. A11.1 und ISO/IEC 27701 Ziff. 8.5 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er Dokumente zu Maßnahmen und Zuständigkeiten vorlegt, die er implementiert hat, um den Cloud-Nutzer bei Änderungen des Datenverarbeitungsortes zu informieren (z.B. Dokumentation der TOM, Verfahrensanweisungen, Richtlinien, dokumentierter Prozess zur Kommunikation an den Cloud-Nutzer, Dokumentation der relevanten Mechanismen und Meldewege). Ein Cloud-Anbieter kann zudem bereits erfolgte Informationen an Cloud-Nutzer zu Änderungen von Datenverarbeitungsorten vorlegen.

Durch eine testweise Ausführung der Prozesse im Rahmen eines Audits (bspw. Simulation einer geplanten Ortsänderung) kann nachgewiesen werden, dass dem Cloud-Nutzer alle notwendigen Informationen zur Ortsänderung auf geeignete Weise kommuniziert werden. Eine Befragung relevanter Mitarbeiter (z.B. zur Kenntnis über Richtlinien etc.) kann als weiterer Nachweis durchgeführt werden.

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 C1.4) (s. auch Nr. 1.6).

Die Verpflichtung zur Vertraulichkeit erfolgt bei allen Mitarbeitern, die personenbezogene Daten verarbeiten, unabhängig davon, ob sie Anwendungsdaten oder Bestands- und Nutzungsdaten verarbeiten.

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.

Auf die Umsetzungshinweise im BSI C5 Anf. KOS-08 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 7.1.2 wird hingewiesen.

Nachweis

Ein Cloud-Anbieter legt ein Musterdokuments zur Verpflichtungserklärung und die Prozessdokumentationen zur Verpflichtung auf Vertraulichkeit sowie zur Anpassung von Verpflichtungserklärungen vor (bspw., wenn sich Aufgaben und Verarbeitungsbefugnisse von Mitarbeitern ändern).

Im Rahmen eines Audits kann die Einhaltung dieser Vorgaben in allen Prozesskonstellationen durch Interviews mit Mitarbeitern nachgewiesen werden (bspw. Befragung, ob Mitarbeiter zur Vertraulichkeit verpflichtet wurden und

ihnen bekannt ist, welche Vertraulichkeitspflichten damit einhergehen). Auch kann eine Beobachtung bei einer testweisen Änderung von Verarbeitungsbefugnissen durchgeführt werden, um die Anpassungen von Verpflichtungserklärungen zu simulieren.

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 – Informationserteilung (Art. 13 oder 14 i.V.m. Art. 12 Abs. 1 und Art. 5 Abs. 1 lit. a DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch TOM sicher, dass der Cloud-Nutzer die Möglichkeit hat, die betroffene Person zeitgerecht, verständlich und in klarer und einfacher Sprache über die Datenverarbeitung zu informieren oder dies durch den Cloud-Anbieter vornehmen zu lassen.

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

Erläuterung

Werden personenbezogene Daten direkt bei der betroffenen Person erhoben (Direkterhebung), ist der Cloud-Nutzer nach Art. 13 DSGVO verpflichtet, die betroffene Person zum Zeitpunkt der Erhebung über die Umstände der Datenverarbeitung zu informieren. Nach Art. 14 DSGVO besteht die Informationspflicht für den Cloud-Nutzer auch, wenn die personenbezogenen Daten nicht direkt bei der betroffenen Person erhoben werden (Dritterhebung). Die Angemessenheit der Frist zur Informationserteilung bei der Dritterhebung bemisst sich nach den spezifischen Verarbeitungsumständen. Gemäß Art. 14 Abs. 3 lit a DSGVO beträgt die Frist längstens einen Monat nach Erlangung der personenbezogenen Daten. Es gelten kürzere Fristen, wenn die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet oder anderen Empfängern offengelegt werden sollen. Im ersten Fall verpflichtet Art. 14 Abs. 3 lit. b DSGVO den Cloud-Nutzer dazu, seiner Informationspflicht spätestens bei der ersten Mitteilung an die betroffene Person nachzukommen. Im zweiten Fall kann gemäß Art. 14 Abs. 3 lit. c DSGVO die Information spätestens zum Zeitpunkt der ersten Offenlegung der Daten an den Empfänger erfolgen.

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 C1.6 und C1.7).

Umsetzungshinweis

Soweit dem Cloud-Nutzer eine Umsetzung seiner Informationspflicht selbst nicht möglich ist, sollte für ihn eine organisatorische Kontaktstelle vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung dieser veranlassen kann. Mit Hilfe eines Ticketsystems können die Weisungen des Cloud-Nutzers dokumentiert werden.

Werden Weisungen zur Umsetzung der Informationspflicht automatisiert (z.B. mittels Softwarebefehlen durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeilenangabe) ausgeführt, sollten diese Nutzerinteraktionen automatisiert protokolliert werden, um nachzuweisen, dass der Cloud-Anbieter weisungsgebunden handelt.

Auf die Umsetzungshinweise der ISO/IEC 27018 Ziff. A1.1 und 27701 Ziff. 8.3 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er Dokumente zu Maßnahmen vorlegt, die er ergriffen hat, um dem Cloud-Nutzer die Informationserteilung gegenüber einer betroffenen Person zu ermöglichen oder die Information durch den Cloud-Anbieter mitteilen zu lassen (z.B. Mechanismen und Meldewege, Dienstbeschreibungen). Auch können anhand von Prozessdokumentationen und Protokollen die tatsächlich durchgeführten Informationserteilung nachgewiesen werden.

Im Rahmen einer Prüfung kann der Cloud-Anbieter eine Probeinformationserteilung durchführen, um nachzuweisen, dass diese möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support).

Der Cloud-Anbieter sollte Protokolle über die fortlaufende Dokumentierung von erteilten Weisungen und/oder Softwarebefehlen von Cloud-Nutzern zur Umsetzung der Informationserteilung (bspw. Logeinträge, Zeitstempel, Versionierung von Logdateien) als Nachweise vorlegen. Im Rahmen eines Audits kann auch eine Befragung oder Beobachtung relevanter Mitarbeiter (z.B. zur Kenntnis über Weisungen von Cloud-Nutzern und Richtlinien zur Befolgung dieser etc.) als Nachweis durchgeführt werden.

Nr. 6.2 – 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 des Auskunftsrechts.

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 C1.6 und C1.7).

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. Mit Hilfe eines Ticketsystems können die Weisungen des Cloud-Nutzers dokumentiert werden.

Werden Weisungen zur Umsetzung des Auskunftsrechts automatisiert (z.B. mittels Softwarebefehlen durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeilenangabe) ausgeführt, sollten diese Nutzerinteraktionen automatisiert protokolliert werden, um nachzuweisen, dass der Cloud-Anbieter weisungsgebunden handelt.

Auf die Umsetzungshinweise der ISO/IEC 27018 Ziff. A1.1 und 27701 Ziff. 8.3 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er Dokumente zu Maßnahmen vorlegt, die 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 (z.B. Mechanismen und Meldewege, Dienstbeschreibungen). Auch können anhand von Prozessdokumentationen und Protokollen die tatsächlich durchgeführten Auskunftserteilungen nachgewiesen werden.

Im Rahmen einer Prüfung kann eine Probeauskunft durchgeführt werden, um nachzuweisen, dass Auskunftserteilung und Bereitstellung von Daten möglich sind (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support).

Der Cloud-Anbieter sollte Protokolle über die fortlaufende Dokumentierung von erteilten Weisungen und/oder Softwarebefehlen von Cloud-Nutzern zur Umsetzung der Auskunftserteilung (bspw. Logeinträge, Zeitstempel, Versionierung von Logdateien) als Nachweise vorlegen.

Nr. 6.3 – 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 des Rechts auf Berichtigung und Vervollständigung.

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 C1.7).

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. Mit Hilfe eines Ticketsystems können die Weisungen des Cloud-Nutzers dokumentiert werden.

Werden Weisungen zur Umsetzung des Rechts auf Berichtigung und Vervollständigung automatisiert (z.B. mittels Softwarebefehlen durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeilenangabe) ausgeführt, sollten diese Nutzerinteraktionen automatisiert protokolliert werden, um nachzuweisen, dass der Cloud-Anbieter weisungsgebunden handelt.

Auf die Umsetzungshinweise der ISO/IEC 27018 Ziff. A1.1 und 27701 Ziff. 8.3 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem 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 (z.B. Dokumentation der relevanten Mechanismen und Meldewege, Dienstbeschreibungen). Auch können anhand von Prozessdokumentationen und Protokollen die tatsächlich durchgeführten Berichtigungen und Vervollständigungen nachgewiesen werden.

Im Rahmen einer Prüfung kann eine Probeberichtigung und -vervollständigung durchgeführt werden, um nachzuweisen, dass eine Berichtigung und Vervollständigung von Daten möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support).

Der Cloud-Anbieter sollte Protokolle über die fortlaufende Dokumentierung von erteilten Weisungen und/oder Softwarebefehlen von Cloud-Nutzern zur Umsetzung der Berichtigung und Vervollständigung (bspw. Logeinträge, Zeitstempel, Versionierung von Logdateien) als Nachweise vorlegen.

Nr. 6.4 – 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, sodass die personenbezogenen Daten irreversibel gelöscht sind und aus ihnen auch mit verhältnismäßig hohen Aufwand keine Informationen über die betroffene Person gewonnen werden können.

(2) Der Cloud-Anbieter stellt sicher, dass die Löschung von personenbezogenen Daten nicht nur im aktiven Datenbestand vorgenommen wird, sondern auch in Kopien und Datensicherungen.

(3) Der Cloud-Anbieter hat sicherzustellen, dass nach einer Wiederherstellung von Daten, die bereits im aktiven Datenbestand, aber noch nicht in der Datensicherung gelöscht waren, eine erneute Löschung der betroffenen Daten erfolgt.

(4) Der Cloud-Anbieter dokumentiert Weisungen zur Umsetzung des Rechts auf Löschung.

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 C1.7 und C1.5).

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. Mit Hilfe eines Ticketsystems können die Weisungen des Cloud-Nutzers dokumentiert werden.

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.

Da Art. 17 DSGVO auf eine irreversible Löschung abstellt, sind Maßnahmen der logischen Löschung wie bspw. das Austragen von personenbezogenen Daten aus Verzeichnissen durch Löschbefehle nicht ausreichend, um die Anforderungen von Art. 17 DSGVO zu erfüllen.

Auf die Umsetzungshinweise der ISO/IEC 27018 Ziff. A1.1 und 27701 Ziff. 8.3 wird hingewiesen.

Da die Löschung von Daten in Backup- und Ausfallsicherungssystemen im Vergleich zur Löschung im aktiven Datenbestand aufwändiger ist, können Kopien und Daten aus Sicherungssystemen auch zu späteren Zeitpunkten als im aktiven Datenbestand gelöscht werden, z.B. im Zuge der Überschreibung oder Vernichtung der betroffenen Datenträger. Regelhaft sollte die Löschung in den Sicherungsdateien spätestens ein Jahr nach der Löschung im aktiven Datenbestand erfolgen, wobei kürzere Fristen angestrebt werden sollten. Die Löschung in Backup- und Ausfallsicherungssystemen sollte alle Vorgängerversionen der Daten, temporäre Daten, Metadaten und Dateifragmente umfassen.

Die Maßnahmen aus DIN 66398 zur Erstellung eines Löschkonzepts können hinzugezogen werden.

Nachweis

Der Cloud-Anbieter legt Dokumentationen über Maßnahmen zur Löschung von Daten vor (z.B. Dokumentation der relevanten Mechanismen und Meldewege, Löschkonzepte, Dienstbeschreibungen. Zudem können Protokolle zu getätigten Weisungen und darauffolgenden Löschungen vorgewiesen werden.

Im Rahmen einer Prüfung kann eine Probelöschung durchgeführt werden, um nachzuweisen, dass eine (vollständige) Löschung von Daten möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support). Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen nachgewiesen werden, dass eine Löschung durchgeführt werden kann.

Nr. 6.5 – 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 des Rechts auf Einschränkung der Verarbeitung.

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 C1.7).

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. Mit Hilfe eines Ticketsystems können die Weisungen des Cloud-Nutzers dokumentiert werden.

Auf die Umsetzungshinweise der ISO/IEC 27018 Ziff. A1.1 und 27701 Ziff. 8.3 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem 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. Er kann Protokolle zu getätigten Weisungen und darauffolgenden Einschränkungen vorlegen.

Im Rahmen einer Prüfung kann eine testweise Einschränkung durchgeführt werden, um nachzuweisen, dass eine Einschränkung der Datenverarbeitung möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support). Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen nachgewiesen werden, ob eine Einschränkung durchgeführt werden kann.

Nr. 6.6 – 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 Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung.

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 C1.6 und C1.7).

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. Mit Hilfe eines Ticketsystems können die Weisungen des Cloud-Nutzers dokumentiert werden.

Auf die Umsetzungshinweise der ISO/IEC 27018 Ziff. A1.1 und 27701 Ziff. 8.3 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem 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 (z.B. Dokumentation der relevanten Mechanismen und Meldewege, Dienstbeschreibungen). Er kann Protokolle zu getätigten Weisungen und darauffolgenden Mitteilungen vorlegen.

Im Rahmen einer Prüfung kann eine testweise Weisung zur Mitteilung durchgeführt werden, um nachzuweisen, dass diese möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support). Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen nachgewiesen werden, ob eine Weisung zur Mitteilung durchgeführt werden kann.

Nr. 6.7 – 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 des Rechts auf Datenübertragbarkeit.

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 diesbezüglich 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 C1.7).

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. Mit Hilfe eines Ticketsystems können die Weisungen des Cloud-Nutzers dokumentiert werden.

Auf die Umsetzungshinweise im BSI C5 Anf. PI-01 bis PI-04 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27018 Ziff. A1.1, A9.3 und ISO/IEC 27701 Ziff. 6.5.3.3, 8.3 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 19941 zur Portabilität wird hingewiesen.

Nachweis

Der Cloud-Anbieter legt Dokumentationen über Maßnahmen zur Datenübertragung vor (z.B. Dokumentation der relevanten Mechanismen, Exportformate, Dienstbeschreibungen. Er kann Protokolle zu getätigten Weisungen und darauffolgenden Datenübertragungen vorlegen.

Im Rahmen einer Prüfung kann eine testweise Datenübertragung mit Testdaten durchgeführt werden, um nachzuweisen, dass diese möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support). Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen nachgewiesen werden, ob eine Datenübertragung durchgeführt werden kann.

Nr. 6.8 – 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 des Widerspruchsrechts.

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 C1.7).

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.

Auf die Umsetzungshinweise der ISO/IEC 27018 Ziff. A1.1 und 27701 Ziff. 8.3 wird hingewiesen.

Nachweis

Der Cloud-Anbieter legt Dokumentationen über Maßnahmen zur Entgegennahme von Widersprüchen sowie Beendigung der Verarbeitung (z.B. Dokumentation der relevanten Mechanismen und Meldewege, Dienstbeschreibungen). Ein Cloud-Anbieter kann Protokolle zu getätigten Weisungen und ggf. darauffolgender Beendigung der Verarbeitung vorlegen.

Im Rahmen einer Prüfung kann ein testweiser Widerspruch durchgeführt werden, um nachzuweisen, dass der Cloud-Anbieter dem Cloud-Nutzer alle Daten zur Entscheidungsfindung bereitstellen kann und ggf. eine Beendigung der Verarbeitung möglich ist (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support). Im Rahmen eines Audits kann auch anhand von Befragungen

(z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen nachgewiesen werden, ob und wie eine Widerspruchsweisung durchgeführt werden kann.

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.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 18.1 und 27701 Ziff. 8.2.5 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 29134 zur Datenschutzfolgeabschätzung wird hingewiesen.

Nachweis

Ein Cloud-Anbieter sollte insbesondere die Dokumentation zu Informationspflichten vorlegen, darunter Dokumente zur Hilfestellung für Cloud-Nutzer (bspw. Dienstbeschreibungen, TOM, Datenflussmodelle und -analysen), durchgeführte Datenschutz-Folgenabschätzungen und entsprechende Gesprächsprotokolle, Dokumentation der getroffenen Vorkehrungen, Verfahrensverzeichnisse, Verfahrensanweisungen und Richtlinien. Insbesondere muss der Cloud-Anbieter nachweisen, dass notwendige Informationen vorliegen oder vom Cloud-Anbieter in kurzer Zeit generiert werden können.

Eine Befragung relevanter Mitarbeiter im Rahmen eines Audits (z.B. zur Kenntnis über Richtlinien etc.) kann als Nachweis angeführt werden. Durch eine Beobachtung kann nachgewiesen werden, ob und wie Mitarbeiter eine testweise Anfrage eines Cloud-Nutzers zur Datenschutz-Folgenabschätzung bearbeiten.

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.

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.

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, wirtschaftliche Interessen des DSB am Unternehmenserfolg oder 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 C1.4).

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 6.3.1 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er einen DSB benennt und die Kontaktdaten des DSB der zuständigen Aufsichtsbehörde meldet sowie ihn auf seiner Webseite als Ansprechpartner der Öffentlichkeit vorstellt. Auch interne Dokumente wie z.B. die Vorlage der Stellenbeschreibung des DSB oder von Benen-

nungsurkunden, Fachkundenachweisen (bspw. Zeugnissen, Schulungsnachweisen), Aufgaben- und Verfahrensbeschreibungen, Richtlinien, oder Organigrammen, die die Einordnung des DSB beschreiben, können geeignete Nachweise sein. Gleiches gilt für die Bereitstellung von Protokollen über die Mitarbeiterinformation zur Rolle des DSB; für Gesprächsprotokolle mit dem DSB zur Überprüfung der Anforderungserfüllung und für Tätigkeitsberichte.

Zur Beurteilung der fachlichen und persönlichen Eignung kann der Cloud-Anbieter einschlägige Zeugnisse und Beurteilungen des DSB vorlegen. Eine Befragung des DSB kann während einer Vor-Ort-Auditierung ebenfalls Aufschluss über seine Eignung und Stellung im Unternehmen geben. Auch kann im Rahmen einer Vor-Ort-Auditierung nachgewiesen werden, dass der DSB über die erforderliche Ausstattung und Unterstützung verfügt.

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. Hierzu sollten entsprechende Auditprotokolle zur Prüfung vorgelegt werden. Mittels Protokollen und sonstigen Dokumenten sowie einer Befragung des Managements kann nachgewiesen werden, ob der DSB der obersten Managementebene direkt berichtet. Eine Befragung des DSB zu seinen Aufgaben ist geeignet um nachzuweisen, dass er keinem Interessenkonflikt unterliegt. Zusätzlich können Dokumente vorgelegt werden, die Auskunft über die geleisteten Arbeitsstunden des DSB geben.

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 C1.3 und C1.6).

Umsetzungshinweis

Der Cloud-Anbieter sollte entsprechende Prozesse etablieren und dokumentieren, sowie Ansprechpartner, Verantwortlichkeiten und Meldewege festlegen. Die Meldung von Datenschutzverletzungen kann über geeignete Informationssysteme innerhalb des Dienstes wie über Nachrichtensysteme oder Newsmeldungen geschehen. Die Meldung von Datenschutzvorfällen sollte in das Incident- und Troubleshooting-Management des Cloud-Anbieters integriert werden, um eine rasche Bearbeitung zu ermöglichen.

Auf die Umsetzungshinweise im BSI C5 Anf. SIM-01 bis SIM-07 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 16.1.1, 16.1.2, ISO/IEC 27018 Ziff. A9.1 und 27701 Ziff. 6.13.1, 8.2.5 und 8.3 wird hingewiesen.

Nachweis

Ein Cloud-Anbieter legt das Datensicherheitskonzept und die darin beschriebenen TOMs zur Gewährleistung der Meldung von Datenschutzverletzungen vor. Er kann zudem weitere Dokumentationen zu Informations- und Meldepflichten vorlegen, darunter bspw. Prozessdokumentationen für die Information von Nutzern, Verfahrensverzeichnisse, Verfahrensanweisungen, Richtlinien und Schulungsunterlagen.

Die Implementierung dieses Konzepts kann durch Prüfung oder Beobachtung einer Probemeldung eines Datenschutzvorfalls bei einem simulierten Cloud-Nutzers nachgewiesen werden. Auch können Protokolle über vergangene Meldungen von Datenschutzvorfällen an Nutzer als Nachweis dienen. Im Rahmen einer Vor-Ort-Auditierung sollte nachgewiesen werden, dass ausreichend Ressourcen vorliegen, um eine rasche Bearbeitung von Meldungen sicherzustellen.

Die Kompetenz der Mitarbeiter sollte durch Dokumentationen von Fähigkeiten wie Zeugnissen oder erfolgten Schulungen und durch Mitarbeiterbefragungen nachgewiesen werden. Auch können ein Organigramm oder eine Übersicht zur Personalsituation in verantwortlichen Bereichen mit entsprechend dokumentierten Qualifikationen des Personals vorgelegt werden. Dabei kann auch durch Befragungen nachgewiesen werden, dass Verantwortlichkeiten klar geregelt und kommuniziert sind (bspw. wer verantwortlich ist über die Meldung des Datenschutzvorfalls an den Cloud-Nutzer zu entscheiden und diese vorzunehmen).

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

Kriterium

(1) Ist der Cloud-Anbieter zur Führung eines Verarbeitungsverzeichnisses verpflichtet, führt er in diesem alle Kategorien von Verarbeitungsvorgängen auf, die er im Auftrag von Verantwortlichen vornimmt. Das Verzeichnis enthält außerdem die in Art. 30 Abs. 2 DSGVO aufgelisteten Inhalte.

(2) 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 C1.6).

In der Regel sind Verantwortliche und Auftragsverarbeiter ab 250 beschäftigten Mitarbeitern zur Führung eines Verarbeitungsverzeichnisses verpflichtet. Jedoch muss der Cloud-Anbieter auch bei weniger Mitarbeitern ein Verarbeitungsverzeichnis führen, wenn gemäß Art. 30 Abs. 5 DSGVO die vorgenommene Verarbeitung Risiken für die Rechte und Freiheiten von betroffenen Personen birgt, besondere Kategorien von personenbezogenen Daten gemäß Art. 9 oder. 10 DSGVO verarbeitet werden oder die Verarbeitung nicht nur gelegentlich erfolgt.

Umsetzungshinweis

Bei standardisierten Massengeschäften sollte das Verarbeitungsverzeichnis automatisiert erstellt werden. Hierzu haben sich bereits am Markt verschiedene Systemwerkzeuge etabliert.

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.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 18.1, ISO/IEC 27018 Ziff. A5.2 und ISO/IEC 27701 Ziff. 8.2.6 wird hingewiesen.

Nachweis

Der Cloud-Anbieter legt die Verarbeitungsverzeichnisse vor und weist ihre Vollständigkeit und Aktualität nach (bspw. Zeitstempel, Versionierungshistorie). Ist eine standardisierte Vereinbarung mit dem Cloud-Nutzer geschlossen, wird das zugrundeliegende standardisierte Verarbeitungsverzeichnis vorgelegt. Sollten keine standardisierten Vereinbarungen mit einem Cloud-Nutzer geschlossen worden sein, legt ein Cloud-Anbieter alle oder eine repräsentative Stichprobe von Verarbeitungsverzeichnissen von Cloud-Nutzern vor. Unterstützend können im Rahmen eines Audits Befragungen der Mitarbeiter durchgeführt werden, um die Verzeichnisse auf Vollständigkeit und Aktualität zu prüfen.

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

Die Erstellung eines Löschkonzepts, z.B. nach DIN 66398-2016, wird empfohlen. Dieses kann die Festlegung von Löschverfahren beinhalten, mit denen es dem Cloud-Anbieter ermöglicht wird, seinen Löschungspflichten nachzukommen. Das Löschkonzept sollte auch Backup- und Ausfallsicherungssysteme umfassen, einschließlich aller Vorgängerversionen der Daten, temporäre Dateien, Metadaten und Dateifragmente.

Da die Löschung von Daten in Backup- und Ausfallsicherungssystemen im Vergleich zur Löschung im aktiven Datenbestand aufwändiger ist, können Kopien und Daten aus Sicherungssystemen auch zu späteren Zeitpunkten

als im aktiven Datenbestand gelöscht werden, z.B. im Zuge der Überschreibung oder Vernichtung der betroffenen Datenträger. Regelhaft sollte die Löschung in den Sicherungsdateien spätestens ein Jahr nach der Löschung im aktiven Datenbestand erfolgen, wobei kürzere Fristen angestrebt werden sollten. Die Löschung in Backup- und Ausfallsicherungssystemen sollte alle Vorgängerversionen der Daten, temporäre Daten, Metadaten und Dateifragmente umfassen.

Da Art. 17 DSGVO auf eine irreversible Löschung abstellt, sind Maßnahmen der logischen Löschung wie bspw. das Austragen von personenbezogenen Daten aus Verzeichnissen durch Löschbefehle nicht ausreichend, um die Anforderungen von Art. 17 DSGVO zu erfüllen. Auch das Löschen von Verknüpfungen oder Verlinkungen auf Datensätze ist nicht ausreichend, da die Datensätze weiterhin vorhanden sind. Eingesetzten Methoden zur Datenlöschung (z. B. durch mehrfaches Überschreiben der Daten) sollten eine Wiederherstellung mit forensischen Mitteln verhindern.

Alle Datenträger des Cloud-Anbieters sollten nach Abschluss der Auftragsvereinbarung oder auf Weisung des Cloud-Nutzers nach einem formalen Managementverfahren sicher und geschützt entsorgt werden. Richtlinien und Anweisungen sollten folgende Aspekte berücksichtigen (s. ISO/IEC 27002 Ziff. 8.3):

a) Sichere und unwiderrufliche Löschung der Daten und Entsorgung/Vernichtung der Datenträger,
b) Verschlüsselung von Wechseldatenträgern,
c) Übertragung der Daten auf neue Datenträger bei Austausch eines Mediums.

Die Maßnahmen aus DIN 66398 zur Erstellung eines Löschkonzepts sowie DIN 66399 und ISO/IEC 21964-1 zur Vernichtung von Datenträgern können hinzugezogen werden.

Auf die Umsetzungshinweise im BSI C5 Anf. AM-04, AM-07, AM-08 und PI-05 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 11.2.7, ISO/IEC 27040-03 Ziff. 6.8.1, ISO/IEC 27018 Ziff. A 9.3 und ISO/IEC 27701 Ziff. 6.5.3, 6.5.3.3, 6.8.2.7, 8.4.2 zur Datenlöschung wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er Dokumente vorlegt, die seine Verfahren zur Herausgabe der Datenträger und zur Rückführung und Löschung von Daten nach Beendigung des Auftrags beschreiben. Geeignete Dokumente können Dokumentation vom TOM, Datenlöschkonzepte, Verfahrensverzeichnisse, Prozessdokumentation für die Daten(träger)behandlung, Verfahrensanweisungen, Richtlinien oder dokumentierte Weisungen sein. Auch kann er die Quittierung von Rückgaben oder die automatisierte Benachrichtigung über tatsächliche Löschungen der für die Auftragsverarbeitung nicht mehr erforderlichen personenbezogenen Daten vorlegen.

Durch eine Prüfung (bspw. Quellcodeanalyse oder Analyse von Datenbanken) oder testweise Löschung und Rückführung kann nachgewiesen werden, ob eine Löschung und Rückführung der personenbezogenen Daten nach Abschluss der Auftragsverarbeitung oder auf Weisung des Cloud-Nutzers erfolgt. Eine Befragung relevanter Mitarbeiter im Rahmen eines Audits (z.B. zur Kenntnis über Richtlinien etc.) kann als weiterer Nachweis über die Durchführung der Maßnahmen dienen. Unterstützend können Sicherheitstests durchgeführt werden, um nachzuweisen, dass Daten hinreichend sicher gelöscht wurden.

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 Ziff. 18.1 und 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.

Auf die Umsetzungshinweise im BSI C5 Anf. BEI-01 bis BEI-12 in Hinblick auf die Einbettung des Revisionsprozesses in das Change-Management sowie Anf. SPN-01 bis SPN-03, COM-02 und COM-3 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 5.1.2, 9.2.5, 14.2.3, 15.2.1 und ISO/IEC 27701 Ziff. 5.7, 6.9.7, 6.15.2 wird hingewiesen.

Nachweis

Der Cloud-Anbieter legt Dokumentationen zur Durchführung von Revisionen vor (z.B. TOM, Verfahrensverzeichnisse, Verfahrensanweisungen, Richtlinien, Rollenbeschreibungen, Revisions- und Ergebnisprotokolle oder Terminpläne für interne Revisionen). Ob interne Kontrollen durchgeführt werden, kann durch Befragungen des DSB, der zuständigen Mitarbeiter und des Managements im Rahmen eines Audits nachgewiesen werden. Dabei sollte insbesondere auch nachgewiesen werden, dass Mitarbeiter um ihre zugeteilte und dokumentierte Verantwortlichkeit wissen und ihre Aufgaben im Hinblick auf die Durchführung von Kontrollverfahren wahrnehmen.

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 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.

(3) Der Cloud-Anbieter stellt sicher, dass Mitarbeiter fortlaufend im Themenfeld Datenschutz und Datensicherheit geschult werden.

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 datensicherheitstechnischen Themen durchführen – auch zur konkreten Technik des Cloud-Dienstes. Die Schulung von Mitarbeitern obliegt dem DSB.

Auf die Umsetzungshinweise im BSI C5 Anf. HR-01, HR-02 und HR-03 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 7.1.2, 7.2.1, 7.2.2 und 7.3 und ISO/IEC 27701 Ziff. 6.4.2.2, 6.8.2.9 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis der erforderlichen Fachkunde seiner Mitarbeiter durch einschlägige Qualifikationsnachweise erbringen (z.B. Zeugnisse, Dokumentation über Eignungsvoraussetzungen, Schulungsunterlagen, Teilnahmenachweise, Rollen- und Berechtigungsbeschreibungen und -konzepte, Verfahrensanweisungen und Richtlinien). Sensibilisierungs- und Schulungsmaßnahmen von Mitarbeitern kann er durch die Dokumentation erfolgter Schulungen nachweisen.

Die Feststellung der Umsetzung von Regeln kann im Rahmen einer Vor-Ort-Prüfung (z.B. Clean Desk Grundsatz, Bildschirmsperren) und Befragungen der Mitarbeiter (bspw. Prüfung auf Fachkunde, Bekanntheit der Richtlinien, potenzielle Interessenkonflikte) nachgewiesen werden.

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.

Umsetzungshinweis

Zur Erfüllung der Anforderungen von Art. 25 Abs. 1 DSGVO ist es unablässig, diese bereits bei der Modellierung von Datenverarbeitungssystemen und Verarbeitungsvorgängen auf allen Ebenen zu berücksichtigen. Der Grundsatz der datenschutzfördernden Systemgestaltung („Data Protection by Design“) verlangt eine Beachtung operativer Datenschutzanforderungen bereits während der Planungsphase, damit nicht-datenschutzkonforme Funktionen gar nicht erst implementiert und nachträglich abgestellt werden müssen. Nach dem SDM können zur datenschutzgerechten Gestaltung der Verarbeitungsvorgänge die Gewährleistungsziele des SDM als Design-Prinzipien oder -Strategien interpretiert werden. Es sind ausgereifte Changemanagement-Prozesse erforderlich, um auf Änderungen der rechtlichen Rahmenbedingungen reagieren und um neue, datenschutzfreundliche Techniken in vorhandene Verarbeitungssystemen einsetzen zu können. Hierzu zählen bspw. Privacy Enhancing Technologies (PETs), welche im Cloud-Dienst zum Einsatz kommen können.

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 verarbeiteten Daten bis hin zu Löschkonzepten für die Löschung dieser Daten. Auch Maßnahmen, die es der betroffenen Person ermöglichen, ihre Betroffenenrechte möglichst einfach auszuüben, zählen hierzu, da sie Transparenz und Kontrollmöglichkeiten für diese 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

Auf die Umsetzungshinweise der ISO/IEC 29101 „Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Datenschutzarchitektur“ wird hingewiesen.

Auf die Umsetzungshinweise im BSI C5 Anf. BEI-01 und BEI-02 wird hingewiesen.

Auf die Umsetzungshinweise im SDM D1.1 bis D1.8 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 6.11, 8.4 wird hingewiesen.

Auf die Umsetzungshinweise in den Guidelines 4/2019 des EDPB zu Art. 25 DSGVO wird hingewiesen.

Nachweis

Zum Nachweis von Datenschutz durch Systemgestaltung kann ein Cloud-Anbieter eine Vielzahl an Maßnahmen durchführen.

Der Cloud-Anbieter kann Dokumente vorlegen, aus denen hervorgeht, welche Gestaltungsprinzipien und -maßnahmen er vorgesehen hat und welche Erwägungen ihn dabei geleitet haben. Relevante Dokumentationen umfassen Dienstbeschreibungen, das Datensicherheitskonzept mit den TOM, Rollen- und Berechtigungskonzepte, Prozessbeschreibungen, Verfahrensanweisungen, Richtlinien, Musterverträge für Subauftragsverarbeiter, Ergebnisprotokolle von internen Audits und Subauftragsverarbeiterkontrollen, Risikoanalysen, Dokumentationen des Information Security Management Systems, Incident-Response-Management Dokumentationen und Datenschutz-Folgenabschätzungen.

Der Abgleich der Dokumentation mit der tatsächlichen Umsetzung der Maßnahmen sollte durch Prüfungen und (Vor-Ort-)Auditierungen nachgewiesen werden. Im Rahmen einer Prüfung können unter anderem eine Dienstnutzung (bspw. Überprüfung der Funktionen und Maßnahmen gemäß Dienstbeschreibung), eine Vorgangsüberwachung (bspw. Sicherstellung von Verschlüsselung) und eine Assetprüfung (bspw. Quellcodeanalyse, Analyse von Systemschnittstellen und Hardwarekomponenten) durchgeführt werden, um den Nachweis der Umsetzung der Datenschutzgrundsätze bei der eingesetzten Hard- oder Software und der Durchführung der Datenverarbeitungsvorgänge zu erbringen. Auch sollte eine Befragung oder Beobachtung relevanter Mitarbeiter durchgeführt werden, um deren Kenntnis über Richtlinien und Verfahrensschritte sowie deren Kompetenzen und Verantwortlichkeiten nachzuweisen. Zusätzlich sollte das Management befragt werden, um nachzuweisen, dass Datenschutz durch Systemgestaltung als Zielsetzung im Unternehmen verankert ist.

Darüber hinaus kann eine Entwicklungs- und Designprüfung durchgeführt werden, um nachzuweisen, ob die datenschutzrechtlichen Anforderungen bereits bei der Entwicklung des Systems berücksichtigt werden. Hierzu kann der Cloud-Anbieter Dokumente über eingesetzte Entwicklungsmethoden und -verfahren (insb. Abnahmekriterien und Anforderungslisten) vorlegen. Eine Prüfung von Testsystemen und -umgebungen (bspw. auf Angemessenheit und Sicherheit) kann bei Bedarf durchgeführt werden. Bei der Designprüfung können unter anderem Dokumentationen zur gewählten Architektur, Datenbankdiagramme, Datenflussdiagramme, Designentscheidungen, aber auch die Konfiguration und Einstellung des Cloud-Dienstes zur Erbringung des Datenverarbeitungsvorgangs vorgelegt werden.

Der Cloud-Anbieter weist anhand von Prozessdokumentationen (bspw. Protokolle über Entscheidungen, Zeitstempel, Versionierungshistorie, Change-Logs) und Befragungen der Mitarbeiter (bspw. Bekanntheit der Richtlinien und Trennung der Verantwortlichkeiten) nach, dass der Stand der Technik beobachtet und eingehalten wird.

Unterstützend können Sicherheitstests angewendet werden, um bspw. die Sicherheit und Angemessenheit von Gestaltungsmaßnahmen nachweisen zu können.

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 nur personenbezogene Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck erforderlich sind und auch 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 Maßnahmen, um dieses Kriterium umzusetzen, sind sehr vielfältig. Der Cloud-Anbieter sollte durch Voreinstellungen sicherstellen, dass nur personenbezogene Daten verarbeitet werden, die für den jeweilig bestimmten Verarbeitungszweck erforderlich sind. Hierzu sollte nicht nur die Menge der verarbeiteten Daten zu minimiert werden, sondern auch der Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Muss bspw. die Nutzung des Cloud-Dienstes protokolliert werden, um Missbrauch aufzudecken oder die Datensicherheit sicherzustellen, so sollte die Voreinstellung derart gewählt werden, dass die Daten anonymisiert erhoben und verarbeitet werden.

Nutzer können von den datenschutzfreundlichen Voreinstellungen abweichen, wenn sie z.B. umfangreichere Verarbeitungsoptionen wünschen. Hierfür ist eine gute Nutzbarkeit des Cloud-Dienstes ebenso wichtig wie eine Information des Cloud-Nutzers darüber, welche Auswirkungen Änderungen von Voreinstellungen haben können (z.B. über Pop-up-Fenster innerhalb des Dienstes). Art. 25 Abs. 2 DSGVO verpflichtet jedoch dazu, dass die umfangreicheren Verarbeitungsoptionen nicht voreingestellt sind, sondern vom Cloud-Nutzer bei Bedarf eingeschaltet und aktiviert werden können. Soweit der Cloud-Anbieter eine Datenschutz-Folgenabschätzung durchgeführt hat, können sich Anforderungen an die Voreinstellungen aus der Pflicht ergeben, die festgestellten Risiken zu minimieren.

Auf die Umsetzungshinweise der ISO/IEC 29101 „Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Datenschutzarchitektur“ wird hingewiesen.

Auf die Umsetzungshinweise im SDM D1.1 bis D1.8 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 6.11, 8.4 wird hingewiesen.

Auf die Umsetzungshinweise in den Guidelines 4/2019 des EDPB zu Art. 25 DSGVO wird hingewiesen.

Nachweis

Zum Nachweis des Datenschutzes durch Voreinstellungen kann ein Cloud-Anbieter eine Vielzahl an Maßnahmen durchführen.

Der Cloud-Anbieter legt Dokumente vor, die beschreiben, welche Voreinstellungen aus welchen Erwägungen heraus gewählt worden sind. Dabei können die Dokumentationen der einzelnen TOM, das Datensicherheitskonzept, Standardeinstellungen des Cloud-Dienstes, Verfahrensanweisungen, Richtlinien/Konzepte zu Kennwörtern, Authentifizierungen und Zugangs- und Zugriffsberechtigungen vorgelegt werden. Auch können Dokumentationen über die Trennung von Testsystemen, über die Entwicklung des Cloud-Dienstes und Protokolle und andere Nachweise zur Durchführung von technischen Voreinstellungen vorgelegt werden.

Die tatsächliche Umsetzung der Maßnahmen sollte durch Prüfungen und (Vor-Ort-)Auditierungen nachgewiesen werden. Im Rahmen einer Prüfung können unter anderem eine Dienstnutzung (bspw. Überprüfung der Standardwerte und Vorauswahl bei Datenfeldern), eine Vorgangsüberwachung (bspw. Umsetzung der Maßnahmen zur Trennung der Entwicklungssysteme) und eine Assetprüfung (bspw. Quellcodeanalyse, Analyse von Systemschnittstellen und Hardwarekomponenten) durchgeführt werden, um Voreinstellungen nachzuweisen. Auch sollte eine Befragung oder Beobachtung relevanter Mitarbeiter durchgeführt werden, um ihre Kenntnis über Richtlinien und Verfahrensschritte, durchgeführte Sensibilisierungen zu Datenschutz und Datensicherheit sowie ihre Kompetenzen (insb. im Hinblick auf die Erforderlichkeit der Verarbeitung von Daten) nachzuweisen. Zusätzlich sollte das Management befragt werden, um nachzuweisen, dass Datenschutz durch Voreinstellung als Zielsetzung im Unternehmen verankert ist.

Darüber hinaus kann eine Entwicklungs- und Designprüfung durchgeführt werden, um nachzuweisen, dass die datenschutzrechtlichen Anforderungen und Voreinstellungen bereits bei der Entwicklung des Systems berücksichtigt werden. Hierzu kann ein Cloud-Anbieter Dokumente zu eingesetzten Entwicklungsmethoden und -verfahren (insb. Abnahmekriterien und gewählte Voreinstellungen) vorlegen. Eine Prüfung von Testsystemen und -umgebungen (bspw. auf Umsetzung von Voreinstellungen) kann bei Bedarf durchgeführt werden. Bei der Designprüfung können unter anderem Datenflussdiagramme, Designentscheidungen, aber auch die Konfiguration und Einstellung des Cloud-Dienstes zur Erbringung des Datenverarbeitungsvorgangs als Nachweis dienen.

Unterstützend können Sicherheitstests angewendet werden, um bspw. die Sicherheit und Angemessenheit von Gestaltungsmaßnahmen nachweisen zu können.

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 seine vorherige gesonderte oder allgemeine Genehmigung in die Subauftragsverarbeitung erteilt hat. Die Genehmigung bedarf der Schrift- oder Textform. Zustimmungsbedürftig sind nur solche Subaufträge, bei denen der weitere Auftragsverarbeiter eine Möglichkeit hat, die zu verarbeitenden personenbezogenen Daten zur Kenntnis zu nehmen.

(2) Erfolgt eine vorherige gesonderte Genehmigung der Subauftragsverarbeitung, hat der Cloud-Anbieter sicherzustellen, dass alle Subauftragsverarbeiter namentlich und mit ladungsfähiger Anschrift benannt werden sowie die Verarbeitungen, für die sie eingesetzt werden sollen, festgelegt sind.

(3) 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

Nicht jeder eingesetzte Dienstleister ist zugleich ein Subauftragsverarbeiter. So liegt keine Subauftragsverarbeitung vor, wenn es beim Dienstleister an einer Verarbeitung personenbezogener Daten fehlt. Dies ist bspw. der Fall bei der Miete von Räumen in einem Rechenzentrum (Co-Location), wenn dem Dienstleister der Zugriff auf Datenverarbeitungsanlagen und personenbezogene Daten durch TOM verwehrt ist. Werden Subaufträge vergeben, hat der Cloud-Anbieter die Qualitätssicherung und die Einhaltung des Datenschutzes in der Leistungskette zu gewährleisten. Insbesondere darf der Subauftrag nicht dazu führen, dass die Wahrung der Betroffenenrechte erschwert wird.

Umsetzungshinweis

Nach Art. 28 Abs. 2 Satz 1 DSGVO bedarf es für die Einbindung von Subauftragsverarbeitern der Genehmigung des Cloud-Nutzers. Die Genehmigung kann gesondert oder allgemein erteilt werden. Die gesonderte Genehmigung bietet sich für solche Fälle an, in denen absehbar ist, dass Subauftragsverarbeiter nur ausnahmsweise eingesetzt werden sollen und keine Änderungen zu erwarten sind. Die allgemeine Genehmigung sollte genutzt werden, wenn bereits bei Abschluss der rechtsverbindlichen Vereinbarung über die Auftragsvereinbarung klar ist, dass zahlreiche Subauftragsverarbeiter eingesetzt werden sollen und der Cloud-Anbieter damit einverstanden ist. 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. Da im Massengeschäft ein Einspruch (i.S.d. Art. 28 Abs. 2 Satz 2 Hs. 2 DSGVO) von einem einzelnen Cloud-Nutzer die Beauftragung eines weiteren oder anderen Auftragsverarbeiters durch den Cloud-Anbieter nicht verhindern wird, sollten in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung (Nr. 1.7) die Voraussetzungen und Folgen eines Einspruchs geregelt werden, bspw. ob der Cloud-Nutzer bei Einspruch die Vereinbarung aufkündigen darf.

Auf die Umsetzungshinweise im BSI C5 Anf. DLL-01 und DLL-02 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 15, ISO/IEC 27018 Ziff. A10.12 und ISO/IEC 27701 Ziff. 6.12, 8.5.6 und 8.5.7 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis über die rechtskonforme weitere Datenverarbeitung dadurch erbringen, dass er die erteilte Zustimmung der Cloud-Nutzer vorlegt. Die gesondert erteilte Genehmigung enthält die Identitäten der genehmigten Subauftragsverarbeiter, ihre Anschriften sowie die Beschreibungen der Verarbeitungen, die sie durchführen sollen. Weiterhin können 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) vorgelegt werden.

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.

Umsetzungshinweis

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 15.1.2, 15.1.3, ISO/IEC 27018 Ziff. A10.12 und ISO/IEC 27701 Ziff. 6.12, 8.5.6 und 8.5.7 wird hingewiesen.

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.

Der Cloud-Anbieter kann das Verzeichnis eingesetzter Subauftragsverarbeiter vorlegen, um eine stichprobenartige Prüfung geschlossener Vereinbarungen zu ermöglichen. Für die jeweiligen Subauftragsverarbeiter sollte der Cloud-Anbieter Dokumente der TOM, das Datensicherheitskonzept oder Zertifikate vorlegen. Weitere relevante Dokumente können als Nachweis herangezogen werden, darunter der Mustervertrag zur Auftragsverarbeitung mit Subauftragsverarbeitern, Richtlinien und Anweisungen, weitere Garantien der Subauftragsverarbeiter, interne Kontrollbereiche des Cloud-Anbieters über Subauftragsverarbeiterkontrollen, das Datenschutzkonzept oder die Risikoabschätzung bei der Unterbeauftragung.

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

Kriterium

(1) Wird die Genehmigung zur Subauftragsverarbeitung in allgemeiner Form erteilt, informiert der Cloud-Anbieter den Cloud-Nutzer über die Identität aller von ihm eingeschalteten Subauftragsverarbeiter (einschließlich ladungsfähiger Anschrift) und über die Verarbeitungen, die diese vornehmen sollen.

(2) Der Cloud-Anbieter informiert den Cloud-Nutzer 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

Auch bei allgemeiner Genehmigung von Subauftragsverarbeitern muss es für den Cloud-Nutzer zu jedem Zeitpunkt der Auftragsverarbeitung möglich sein zu erfahren, welcher Subauftragsverarbeiter sich in welchem Verarbeitungsschritt befindet und welche Verarbeitungen durch welchen Subauftragsverarbeiter auf welcher Stufe der Auftragsverarbeitung ausgeführt werden, weshalb dem Cloud-Anbieter eine Informationspflicht zukommt.

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 Verarbeitungen 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 (kaskadierende Informationsbereitstellung).

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

Auf die Umsetzungshinweise der ISO/IEC 27018 Ziff. A7.1 und ISO/IEC 27701 Ziff. 8.5.2, 8.5.6 und 8.5.8 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er Dokumente (wie konkrete rechtsverbindliche Vereinbarungen oder Muster solcher Vereinbarungen) vorlegt, die den Cloud-Nutzer in Kenntnis darüber setzen wie er bei beabsichtigten Änderungen von Subauftragsverarbeitern informiert wird (z.B. per E-Mail oder in Informationsportalen). Zudem sollte der Cloud-Anbieter Dokumentationen darüber vorlegen, wie Einsprüche von Cloud-Nutzer entgegengenommen und bearbeitet werden. Weitere relevante Nachweisdokumente können bspw. Dokumentationen der Einwilligungen von Cloud-Nutzern sowie solche über die Ausübung des Widerspruchsrechts sein. Protokolle über mitgeteilte Änderungen der Einbindung von Subauftragsverarbeitern oder bearbeitete Einsprüche sollten vom Cloud-Anbieter, sofern vorhanden, vorgelegt werden.

Außerdem kann der Cloud-Anbieter seine detaillierte Dokumentation über die involvierten Subauftragsverarbeiter unter Angabe von Identität, ladungsfähiger Anschrift und der ausgeführten Verarbeitungen vorlegen, mit deren Hilfe nachvollzogen werden kann, welcher (Sub-)Auftragsverarbeiter welche Verarbeitungsvorgänge ausführt.

Durch eine Prüfung in Form einer Vorgangsüberwachung oder durch eine Beobachtung im Rahmen eines Audits kann nachgewiesen werden, ob dem Cloud-Nutzer alle notwendigen Informationen zur Einbindung von Subauftragsverarbeiter auf geeignete Weise kommuniziert werden. Hierzu kann testweise eine Information über die Änderung eines Subauftragsverarbeiters simuliert werden. Gleichermaßen kann die Bearbeitung eines Einspruchs durch einen Cloud-Nutzers nachgewiesen werden. Eine Befragung relevanter Mitarbeiter (z.B. zur Kenntnis über Richtlinien, Entgegennahme von Anfragen und Einsprüchen des Cloud-Nutzers etc.) kann als weiterer Nachweis dienen.

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, sollte er sich selbst von der Einhaltung der datenschutzrechtlichen Anforderungen durch die Subauftragsverarbeiter überzeugen.

Auf die Umsetzungshinweise im BSI C5 Anf. DLL-01 und DLL-02 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 15.2.1, ISO/IEC 27018 Ziff. A10.12 und ISO/IEC 27701 Ziff. 8.5.6 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er Zertifikate der Subauftragnehmer oder sonstige Unterlagen vorlegt (bspw. befolgte Verhaltensregeln, rechtsverbindliche Vereinbarungen, Datensicherheitskonzepte, sonstige Garantien), aus denen sich die Gewähr zur Einhaltung der Datenschutz-Grundverordnung ergibt. Hierbei kann eine transparente Dienstbeschreibung des jeweiligen Subauftragsverarbeiters hilfreich sein. Darüber hinaus können Dokumente über die Auswahl (bspw. Protokolle über Auswahlüberlegungen und -entscheidungen) und die Durchführung von eigenen Kontrollen (bspw. Protokolle der Subauftragsverarbeiterkontrollen) als Nachweise dienlich sein.

Unterstützend können im Rahmen eines Audits Befragungen der Mitarbeiter durchgeführt werden, um in Erfahrung zu bringen, wie die Einhaltung datenschutzrechtlicher Anforderungen von Subauftragsverarbeitern überprüft wird (bspw. Bekanntheit von Verfahrensschritten und Garantien der Subauftragsverarbeiter).

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. Abhängig von den jeweiligen ausgelagerten Verarbeitungsprozessen sollten in der rechtsverbindlichen Vereinbarung mit dem Subauftragsverarbeiter die entsprechenden Unterstützungsfunktionen festgehalten werden. Insbesondere sollten Kontaktstellen und die jeweiligen Verantwortlichkeiten bei Subauftragsverarbeitern protokolliert und fortlaufend aktualisiert werden. Es sollten Prozesse, Meldewege und Verfahrensrichtlinien definiert und dokumentiert werden.

Auf die Umsetzungshinweise der ISO/IEC 27002 Ziff. 15.1.3, ISO/IEC 27018 Ziff. A10.12 und ISO/IEC 27701 Ziff. 8.5 wird hingewiesen.

Nachweis

Der Cloud-Anbieter legt Dokumente zu Verfahren und Vorkehrungen zur Einbindung von Subauftragsverarbeitern als Nachweis vor, darunter rechtsverbindliche Vereinbarungen mit Subauftragsverarbeitern, Prozessdokumentationen zur Einbindung, Datensicherheitskonzepte und Informationen über Ansprechpartner der Subauftragsverarbeiter, Risikoanalysen oder Dokumente zur Verantwortlichkeitstrennung für einzelne Verarbeitungsprozesse. Protokolle zur Pflichterfüllung infolge der Einschaltung von weiteren Auftragsverarbeitern können vorgelegt werden.

Unterstützend kann eine Befragung der Mitarbeiter zur Einbindung von Subauftragsverarbeitern als Nachweis durchgeführt werden (bzgl. der Bekanntheit von Verfahrensschritten und Ansprechpartnern der Subauftragsverarbeiter).

Kapitel VI: Datenverarbeitung außerhalb der EU und des EWR

Nr. 11 – Datenübermittlung

Nr. 11.1 – Geeignete Garantien für die Datenübermittlung (Art. 46 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 die in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegten geeigneten Garantien im Sinne des Art. 46 Abs. 2 oder 3 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.

Beinhaltet die Auftragsverarbeitung die weisungsgebundene Datenübermittlung an Drittländer oder an internationale Organisationen, verpflichtet Art. 44 DSGVO zusätzlich zur Einhaltung der Bedingungen von Kapitel 5 DSGVO. Der Cloud-Anbieter darf sich daher für die Datenübermittlung nur auf einen Angemessenheitsbeschluss nach Art. 45 Abs, 3 DSGVO oder die geeigneten Garantien nach Art. 46 Abs. 2 oder 3 DSGVO stützen, die zwischen ihm und dem Cloud-Nutzer nach Nr. 1.4 festgelegt worden sind.

Umsetzungshinweis

Auf die Umsetzungshinweise der ISO/IEC 27018 Ziff. A11.1 und ISO/IEC 27701 Ziff. 6.15, 8.5 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er ein Verzeichnis eingesetzter Subauftragsverarbeiter aus Drittländern mit Angemessenheitsbeschluss nach Art. 45 Abs. 3 DSGVO vorlegt. Liegt kein Angemessenheitsbeschluss vor, können Nachweise durch Dokumente zu den vereinbarten geeigneten Garantien nach Art. 46 Abs. 2 oder 3 DSGVO vorgelegt werden (z.B. Standarddatenschutzklauseln, verbindliche interne Datenschutzvorschriften nach Art. 47 DSGVO). 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.

Umsetzungshinweis

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

Ein Cloud-Anbieter kann verschiedene Dokumente als Nachweise vorlegen, darunter Verträge mit Vertretern, die schriftlichen Benennungsurkunden, Richtlinien, öffentliche Informationen für Cloud-Nutzer (bspw. Kontaktinformationen des Vertreters in der Datenschutzerklärung auf der Website), Verantwortlichkeiten und deren Rollenbeschreibungen. Es kann eine Befragung des Vertreters oder der Vertreter (auch stichprobenartig) durchgeführt werden.

D. Kriterien und Umsetzungshinweise für Verarbeitung als Verantwortlicher

Kapitel VII: Der Cloud-Anbieter als Verantwortlicher

Erläuterung

Wie in A.1. Adressaten und Funktionen des AUDITOR-Kriterienkatalogs erläutert, kann je nachdem wem gegenüber der Cloud-Dienst angeboten wird, es für den Cloud-Anbieter erforderlich sein, neben den Daten des Cloud-Nutzers auch Daten anderer betroffener Personen wie beispielsweise die der Mitarbeiter des Cloud-Nutzers zu verarbeiten (z.B. ihre Namen und Kontaktinformationen), um den Cloud-Dienst gegenüber dem Cloud-Nutzer erbringen zu können. Dies hat zur Folge, dass der Cloud-Anbieter in seiner Rolle als Verantwortlicher seine datenschutzrechtlichen Pflichten nicht nur gegenüber dem Cloud-Nutzer erfüllen muss, sondern auch gegenüber den anderen betroffenen Personen.

Verarbeitet der Cloud-Anbieter Daten des Cloud-Nutzers, um diesem den Cloud-Dienst erbringen zu können, kann er sich hierbei auf Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO berufen, der die Verarbeitung personenbezogener Daten für die Erfüllung eines Vertrags mit der betroffenen Person oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erlaubt. Auf diese Rechtsgrundlage kann er sich bei der Verarbeitung von z.B. Mitarbeiterdaten des Cloud-Nutzers jedoch nicht stützen, weil die Mitarbeiter nicht die Vertragspartner sind. Stattdessen kann sich der Cloud-Anbieter auf Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO und seine berechtigten Interessen an der Datenverarbeitung berufen, solange diese für die Geschäftsbeziehung mit dem Cloud-Nutzer erforderlich ist.

Zur leichteren Lesbarkeit der nachfolgenden Kriterien dieses Abschnitts werden mit Ausnahme von Kriterium Nr. 13 die Datenverarbeitungen, die auf Grundlage von Art. 6 Abs. 1 UAbs. 1 lit b und lit. f DSGVO durchgeführt werden, unter „Verarbeitung von personenbezogenen Daten zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes“ zusammengefasst, da sie gleichermaßen für die Geschäftsbeziehung mit dem Cloud-Nutzer über die Erbringung des Cloud-Dienstes erforderlich sind und daher als Einheit betrachtet werden können.

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, der betroffenen Person alle Informationen zur Verfügung, die diese 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, 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, Nr. 15.3, Nr. 15.3) nachkommt. Außerdem können die Grundsätze der Transparenz und der Datenminimierung durch datenschutzgerechte Systemgestaltung und datenschutzfreundliche Voreinstellungen (Nr. 19.1 und Nr. 19.2) erreicht werden. Der Cloud-Anbieter sollte bei der Datenverarbeitung zur Diensterbringung Überlegungen und Entscheidungen hinsichtlich der hierfür erforderlichen Daten vornehmen und dokumentieren.

Der Cloud-Anbieter sollte TOM zur Prüfung, Korrektur und Löschung unzutreffender oder unvollständiger personenbezogener Daten zur Erfüllung des Grundsatzes der Datenrichtigkeit etablieren und dokumentieren. Hierzu zählen bspw. Prüfverfahren und Löschkonzepte, die Einrichtung einer Kontaktstelle für Cloud-Nutzer zur Entgegennahme von Anfragen, die Festlegung von Verantwortlichkeiten und Verfahrensrichtlinien zur raschen Bearbeitung und die Spezifikation von Meldewegen. Die TOM können auch in die bestehenden Kundensupport-, Troubleshooting-, oder Incident-Management-Systeme eingebettet 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. Auf die Umsetzungshinweise unter Nr. 8.4 zur Datenlöschung wird hingewiesen.

Auf die Umsetzungshinweise im SDM D1.1 bis D1.8 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 6.5.2.1, 6.5.2.2, 7.2.1, 7.2.2 und 7.4 wird hingewiesen.

Nachweis

Grundsätzlich kann ein Cloud-Anbieter als Nachweis der Datenschutzgrundsätze Einblick in TOMs und das Datensicherheitskonzept gewähren.

Für die Erfüllung des Transparenzgrundsatzes wird auf die Nachweise in den Kriterien zu den Informations- und Auskunftspflichten über die Datenverarbeitung (Nr. 15.1 und Nr. 15.3) und zur datenschutzgerechten Systemgestaltung und zu datenschutzfreundlichen Voreinstellungen (Nr. 19.1 und Nr. 19.2) verwiesen.

Zum Nachweis der Einhaltung der Grundsätze der Zweckfestlegung und Zweckbindung sollte ein Cloud-Anbieter eine Datenschutzerklärung vorlegen, um nachzuweisen, dass er die Zwecke für die Datenverarbeitung in eigener Verantwortlichkeit festgelegt, eindeutig und präzise beschrieben und der betroffenen Person kommuniziert hat. Darüber hinaus sollte der Cloud-Anbieter Dokumentationen zu TOM vorlegen, in denen darlegt wird, wie er Daten logisch oder physisch getrennt nach den jeweiligen Verarbeitungszwecken verarbeitet.

Mittels einer testweisen Dienstnutzung (bspw. Registrierung des Cloud-Nutzers) oder Assetprüfung (bspw. Quellcodeanalyse) kann nachgewiesen werden, dass nur die in der Dokumentation angegebenen und erforderlichen Daten zur Zweckerreichung verarbeitet werden. Darüber hinaus können Befragungen der Mitarbeiter und des DSB im Hinblick auf Verfahrensschritte und Richtlinien zur Datenminimierung als Nachweise durchgeführt werden. Unterstützend kann im Rahmen einer Entwicklungs- und Designprüfung nachgewiesen werden, dass während der Anwendung von Entwicklungs- oder Designmethoden bereits die Grundsätze der Datenminimierung, Zweckfestlegung und Zweckbindung einbezogen werden, sodass nur die für die Verarbeitung erforderlichen Daten verarbeitet und bspw. entsprechende Datenfelder in Datenbanken datensparsam designed werden.

Ein Cloud-Anbieter legt Dokumente vor, um die Einhaltung des Grundsatzes der Datenrichtigkeit nachzuweisen. Hierzu zählen insbesondere Prozessdokumentationen zur Prüfung, Korrektur und Löschung unzutreffender oder unvollständiger personenbezogener Daten sowie Dokumentationen über entsprechende (technische) Verfahren (bspw. Einstellungen von Datenbanksystemen). Unterstützend kann eine testweise Korrektur oder Löschung der Daten durchgeführt werden. Eine Befragung oder Beobachtung von Mitarbeitern in Bezug auf die Prüfung, Korrektur und Löschung unzutreffender oder unvollständiger personenbezogener Daten kann zum Nachweis durchgeführt werden (bspw. Bekanntheit der Verfahrensschritte und Richtlinien, klare Verteilung der Verantwortlichkeiten).

Zur Ermittlung des Grundsatzes der Speicherbegrenzung legt der Cloud-Anbieter entsprechende Dokumente vor, bspw. Löschkonzepte (bspw. Fristen und Art der Löschung), Dokumentationen zu Pseudonymisierungsverfahren zur Umsetzung des Speicherbegrenzungsgrundsatzes oder Protokolle über durchgeführte Löschungen und Pseudonymisierungen. Im Rahmen eines Audits sollte eine Befragung der Mitarbeiter zur Speicherbegrenzung durchgeführt werden (bspw. Kenntnis über Speicherfristen, Richtlinien und Verfahrensschritte).

Nr. 13 – Rechtsgrundlage für die Datenverarbeitung (Art. 6 Abs. 1 UAbs. 1 lit. b, c oder f 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, zur Wahrung seiner berechtigten Interessen, solange die Datenverarbeitung zur Erfüllung des Vertrags mit dem Cloud-Nutzer erforderlich ist und nicht die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person gegen die Verarbeitung überwiegen oder zur Erfüllung einer rechtlichen Verpflichtung, der der Cloud-Anbieter 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 Verarbeitung von personenbezogenen Daten des Cloud-Nutzers 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 mit der betroffenen Person 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.

Verarbeitet der Cloud-Anbieter zur Erfüllung des Vertrags mit dem Cloud-Nutzer nicht nur Daten über diesen, sondern auch über andere betroffene Personen wie z.B. die Mitarbeiter des Cloud-Nutzers, so kann er sich bei dieser Datenverarbeitung auf Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO und seine berechtigten Interessen stützen, solange wie die Datenverarbeitung zur Erfüllung des Vertrags mit dem Cloud-Nutzer erforderlich ist und nicht die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person gegen die Verarbeitung überwiegen

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.

Umsetzungshinweis

Art. 13 Abs. 1 lit. c oder 14 Abs. 1 lit. c DSGVO (Nr. 15.1 oder Nr. 15.2) verpflichten den Cloud-Anbieter dazu, die betroffene Person über die Rechtsgrundlage einer Datenverarbeitung zu informieren. Daher sollte die Datenschutzerklärung des Cloud-Anbieters nicht nur die Zwecke der Datenverarbeitungen in eigener Verantwortlichkeit eindeutig und präzise bestimmen, sondern auch die konkreten Rechtsgrundlagen für die Datenverarbeitungen benennen.

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 6.15.1, 7.2.1 und 7.2.2 wird hingewiesen.

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 und Abs. 2 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) Die in Nr. 14 geforderten Angaben können außer im Datensicherheitskonzept auch in sonstigen Dokumenten getroffen werden, solange diese als rechtsverbindlich für die Auftragsverarbeitung zwischen Cloud-Anbieter und Cloud-Nutzer vereinbart worden sind. Die Anforderungen an das Datensicherheitskonzept gelten auch für diese sonstigen Dokumente.

(3) 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.

(4) Das Datensicherheitskonzept ist schriftlich oder in einem elektronischen Format zu dokumentieren.

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

(6) 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.

(7) 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. Der Cloud-Anbieter kann auch für die Verarbeitung von Daten zur Durchführung des Auftrags mit dem Cloud-Nutzer und zur Erfüllung rechtlicher Verpflichtungen die Umsetzungshinweise unter Nr. 2.1 zur Erstellung und Pflege des Datensicherheitskonzepts anwenden.

Nachweis

Für den Nachweis eines angemessenen Datensicherheitskonzepts gelten die Ausführungen in Nr. 2.1 analog.

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 Naturereignisse[4] 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

[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.

Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert.

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

Schutzklasse 2

(3) Die Kriterien von Schutzklasse 1 sind erfüllt.

(4) Zusätzlich ergreift der Cloud-Anbieter geeignete Maßnahmen, um Schädigungen nicht nur durch Naturereignisse, sondern auch durch fahrlässige Handlungen Befugter ausschließen. Der Zutritt ist vor vorsätzlichen Handlungen Unbefugter hinreichend sicher geschützt, was Schutz gegen Zutrittsversuche durch bekannte Angriffsszenarien, Täuschung und Gewalt einschließt.

(5) Alle unbefugten Zutritte und Zutrittsversuche sind nachträglich feststellbar.

Erläuterung

Es wird auf die Erläuterungen in Nr. 2.2 verwiesen.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 2.2 sind anwendbar.

Nachweis

Für den Zutrittsschutz zu Räumlichkeiten und Anlagen gelten die Ausführungen in Nr. 2.2 analog.

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 Zwei-Faktor-Authentifizierung. 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

(5) Die Kriterien von Schutzklasse 1 sind erfüllt.

(6) 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

Es wird auf die Erläuterungen in Nr. 2.3 verwiesen.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 2.3 sind anwendbar.

Nachweis

Für den Nachweis der Zugangskontrolle gelten die Ausführungen in Nr. 2.3 analog.

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) Der Cloud-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zugriff auf personenbezogene Daten in regelmäßigen Abständen auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

(3) Zugriffe auf personenbezogene Daten sind zu kontrollieren.

(4) 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.

(5) Der Cloud-Anbieter schützt Zugriffe von Befugten über das Internet durch eine Zwei Faktor-Authentifizierung.

Schutzklasse 2

(6) Die Kriterien von Schutzklasse 1 sind erfüllt.

(7) 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

Es wird auf die Erläuterungen in Nr. 2.4 verwiesen.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 2.4 sind anwendbar.

Nachweis

Für den Nachweis der Zugriffskontrolle gelten die Ausführungen in Nr. 2.4 analog.

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

Es wird auf die Erläuterungen in Nr. 2.5 verwiesen.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 2.5 sind anwendbar, wobei statt auf Ziff. 8.4.3 der ISO/IEC 27701 auf Ziff. 7.4.9 hingewiesen wird.

Nachweis

Der Cloud-Anbieter kann den Schutz von Daten bei der Übertragung analog wie in Nr. 2.5 angegeben nachweisen.

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 auch 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

Es wird auf die Erläuterungen in Nr. 2.6 verwiesen.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 2.6 sind anwendbar. Auf die Umsetzungshinweise in der ISO/IEC 27701 Ziff. 7.2.8 wird hingewiesen.

Nachweis

Die Nachvollziehbarkeit der Datenverarbeitung kann der Cloud-Anbieter analog wie in Nr. 2.6 angegeben nachweisen.

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 verschlüsselt gespeichert werden.

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

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

(4) Eingesetzte Verschlüsselungsverfahren sind durch andere Verschlüsselungsverfahren zu ersetzen, wenn sie nicht mehr den aktuellen technischen Empfehlungen (best practices) 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 C1.4 und C1.3) 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

Die Umsetzungshinweise unter Nr. 2.9 zur Schutzklasse 2 sind anwendbar.

Nachweis

Für den Nachweis der verschlüsselten Speicherung gelten die Ausführungen unter Nr. 2.9, Schutzklasse 2 analog.

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, logisch oder physisch 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 C1.2 – C1.5) und zielt damit auch auf die Sicherstellung des Zweckbindungsgrundsatzes aus Art. 5 Abs. 1 lit. b DSGVO ab.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 2.10 sind anwendbar. Auf die Umsetzungshinweise in der ISO/IEC 27701 Ziff. 7.2.8 wird hingewiesen.

Nachweis

Die Datentrennung und deren Angemessenheit kann der Cloud-Anbieter analog wie in Nr. 2.10 angegeben nachweisen.

Nr. 15 – Wahrung von Betroffenenrechten

Nr. 15.1 – Informationspflicht bei Direkterhebung (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 die betroffene Person zum Zeitpunkt der Erhebung ihrer personenbezogenen Daten zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen über die Umstände der Verarbeitung und über ihre Betroffenenrechte verständlich und in klarer und einfacher Sprache informiert wird. Die Information an die betroffene Person umfasst 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 C1.6 und C1.7).

Umsetzungshinweis

Der Cloud-Anbieter sollte dem Cloud-Nutzer eine Datenschutzerklärung mit allen Informationen gemäß Art. 13 Abs. 1 und 2 DSGVO bei der Registrierung für die Nutzung des Cloud-Dienstes zur Verfügung stellen (bspw. über die Webseite oder das Informationsportal des Cloud-Dienstes). Der Cloud-Anbieter sollte zudem eine Kontaktstelle einrichten, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann.

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 7.2.1, 7.3. und 7.5. wird hingewiesen.

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 nachgewiesen werden, ob der Cloud-Anbieter alle Informationen nach Art. 13 Abs. 1 und 2 DSGVO bereitstellt. Zur Erfüllung seiner Informationspflicht gegenüber anderen betroffenen Personen wie z.B. den Mitarbeitern des Cloud-Nutzers legt der Cloud-Anbieter ebenfalls das Muster seiner Datenschutzerklärung vor, dass er dem Mitarbeiter z.B. über E-Mail bei Erhebung der Daten übermittelt.

Nr. 15.2 – Informationspflicht bei Dritterhebung (Art. 14 i.V.m. Art. 12 Abs. 1 und Art. 5 Abs. 1 lit. a DSGVO)

Kriterium

Sofern die personenbezogenen Daten der betroffenen Person zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen nicht direkt bei der betroffenen Person erhoben werden (Dritterhebung), stellt der Cloud-Anbieter durch TOM sicher, dass die betroffene Person innerhalb einer angemessenen Frist über die Umstände der Verarbeitung und über ihre Betroffenenrechte verständlich und in klarer und einfacher Sprache informiert wird, sofern die Informationserteilung nicht unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert. Die Information an die betroffene Person umfassen alle in Art. 14 Abs. 1 und 2 DSGVO geforderten Angaben.

Erläuterung

Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

Umsetzungshinweis

Der Cloud-Anbieter sollte die Zuweisung von Verantwortlichkeiten und Meldewege sicherstellen und diese dokumentieren, damit die betroffene Person fristgemäß informiert werden kann. Die Angemessenheit der Frist zur Informationserteilung bemisst sich nach den spezifischen Verarbeitungsumständen. Gemäß Art. 14 Abs. 3 lit a. DSGVO beträgt die Frist längstens einen Monat nach Erlangung der personenbezogenen Daten. Es gelten kürzere Fristen,

wenn die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet oder anderen Empfängern offengelegt werden sollen. Im ersten Fall verpflichtet Art. 14 Abs. 3 lit. b DSGVO den Cloud-Anbieter dazu, seiner Informationspflicht spätestens bei der ersten Mitteilung an die betroffene Person nachzukommen. Im zweiten Fall kann gemäß Art. 14 Abs. 3 lit. c DSGVO die Information spätestens zum Zeitpunkt der ersten Offenlegung der Daten an den Empfänger erfolgen.

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 7.2.1, 7.3 und 7.5 wird hingewiesen.

Nachweis

Der Cloud-Anbieter legt das Muster seiner Datenschutzerklärung mit den Informationen nach Art. 14 Abs. 1 und 2 DSGVO vor, dass er der betroffenen Person zur Verfügung stellt. Darüber hinaus legt er Dokumentationen zum Meldeverfahren vor, bspw. Verfahrensschritte, Meldewege oder Protokolle über durchgeführte Meldungen.

Nr. 15.3 – 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 der betroffenen Person auf Antrag Auskunft über die Datenverarbeitung erteilt, die er als Verantwortlicher über sie zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen durchführt. Er stellt der betroffenen Person eine Kopie dieser Daten zur Verfügung.

Erläuterung

Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

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.

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 7.3.1, 7.3.2, 7.3.3, 7.3.6, 7.3.8 und 7.3.9 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er dokumentiert, welche Maßnahmen er ergriffen hat, um der betroffenen Person zeitgerecht Auskunft zu erteilen (z.B. Mechanismen und Meldewege, Dienstbeschreibungen). Auch können anhand einer Prozessdokumentation die tatsächlich durchgeführten Auskunftserteilungen nachgewiesen werden.

Im Rahmen einer Prüfung kann eine Probeauskunft durchgeführt werden, um nachzuweisen, dass Auskunftserteilung und Bereitstellung von Daten möglich sind (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support).

Nr. 15.4 – 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 der natürlichen Person die Möglichkeit einräumt, ihre 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 C1.7).

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.

Auf die Umsetzungshinweise der ISO/IEC 27701 7.3.1, 7.3.2, 7.3.6 und 7.3.9 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er dokumentiert, welche Maßnahmen er ergriffen hat, um betroffenen Personen die (direkte) Berichtigung und Vervollständigung von Daten zu ermöglichen oder um die Berichtigung und Vervollständigung selbst vorzunehmen (z.B. Dokumentationen der relevanten Mechanismen und Meldewege, Dienstbeschreibungen). Weiterhin können durch Prozessdokumentationen die tatsächlich durchgeführten Berichtigungen und Vervollständigungen nachgewiesen werden.

Im Rahmen einer Prüfung können repräsentative Probeberichtigungen und -vervollständigungen durchgeführt werden. Diese können bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support erfolgen.

Nr. 15.5 – Löschung (Art. 17 Abs. 1 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch TOM sicher, dass er personenbezogene Daten, die er zur Erfüllung des Auftrags über die Erbringung des Cloud-Dienstes verarbeitet, auf Antrag der betroffenen Person hin und von sich aus unverzüglich löscht, wenn die Voraussetzungen von Art. 17 Abs. 1 lit. a, d oder e DSGVO vorliegen. Die Löschung hat irreversibel zu erfolgen, sodass aus den gelöschten personenbezogenen Daten auch mit verhältnismäßig hohem Aufwand keine Informationen über die betroffene Person gewonnen werden können.

(2) Der Cloud-Anbieter stellt sicher, dass die Löschung von personenbezogenen Daten, die er zur Erfüllung des Auftrags über die Erbringung des Cloud-Dienstes verarbeitet werden, nicht nur im aktiven Datenbestand vorgenommen wird, sondern auch in Kopien und Datensicherungen.

(3) Der Cloud-Anbieter hat sicherzustellen, dass nach einer Wiederherstellung von personenbezogenen Daten, die bereits im aktiven Datenbestand, aber noch nicht in der Datensicherung gelöscht waren, eine erneute Löschung der betroffenen Daten erfolgt.

Erläuterung

Das Kriterium fördert die Gewährleistungsziele der Intervenierbarkeit und Nichtverkettung (SDM C1.7 und C1.5). 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).

Da Art. 17 DSGVO auf eine irreversible Löschung abstellt, sind Maßnahmen der logischen Löschung wie bspw. das Austragen von personenbezogenen Daten aus Verzeichnissen durch Löschbefehle nicht ausreichend, um die Anforderungen von Art. 17 DSGVO zu erfüllen.

Auf die Umsetzungshinweise der ISO/IEC 27701 7.3.1, 7.3.6, 7.3.9 und 7.4.7 wird hingewiesen.

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 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.

Da die Löschung von Daten in Backup- und Ausfallsicherungssystemen im Vergleich zur Löschung im aktiven Datenbestand aufwändiger ist, können Kopien und Daten aus Sicherungssystemen auch zu späteren Zeitpunkten als im aktiven Datenbestand gelöscht werden, z.B. im Zuge der Überschreibung oder Vernichtung der betroffenen Datenträger. Regelhaft sollte die Löschung in den Sicherungsdateien spätestens ein Jahr nach der Löschung im aktiven Datenbestand erfolgen, wobei kürzere Fristen angestrebt werden sollten.

Die Umsetzungshinweise unter Nr. 6.4 sind anwendbar.

Nachweis

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

Die Möglichkeiten zum Nachweis unter Nr. 6.4 sind anwendbar.

Nr. 15.6 – 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, die er durchführt, um den Auftrag mit dem Cloud-Nutzer über die Erbringung des Cloud-Dienstes zu erbringen oder eine rechtliche Verpflichtung zu erfüllen, auf Antrag der betroffenen Person einschränken kann.

(2) Der Cloud-Anbieter stellt durch TOM sicher, dass er die betroffene Person 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 C1.7).

Umsetzungshinweis

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

Auf die Umsetzungshinweise der ISO/IEC 27701 7.3.1, 7.3.2, 7.3.3 und 7.3.9 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er dokumentiert, welche Maßnahmen er ergriffen hat, um die Verarbeitung von Daten einzuschränken und die betroffene Person vor Aufhebung der Einschränkung zu informieren. Er kann Protokolle zu getätigten Anfragen von betroffenen Personen und den darauffolgenden Einschränkungen vorlegen.

Im Rahmen einer Prüfung können testweise Einschränkungen (inkl. Mitteilung an die betroffene Person) und die Aufhebungen dieser durchgeführt werden. Die Einschränkung kann bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support erfolgen. Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen nachgewiesen werden, wie Einschränkungen und ihre Aufhebungen durchgeführt werden und wie die betroffene Person benachrichtigt wird.

Nr. 15.7 – 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 zur Durchführung des Auftrags mit dem Cloud-Nutzer 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 die betroffene Person 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 C1.6 und C1.7).

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

Auf die Umsetzungshinweise der ISO/IEC 27701 7.3.1, 7.3.2, 7.3.3, 7.3.7 und 7.3.9 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er dokumentiert, welche Maßnahmen er ergriffen hat, um seiner Mitteilungspflicht nachzukommen und die betroffene Person auf Verlangen über die Empfänger der Offenlegung zu unterrichten (z.B. Dokumentation der relevanten Mechanismen und Meldewege, Dienstbeschreibungen). Ein Cloud-Anbieter kann Protokolle zu getätigten Mitteilungen vorlegen.

Im Rahmen einer Prüfung kann eine testweise Mitteilung durchgeführt werden (bspw. durch eine technische Funktion innerhalb des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support). Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen nachgewiesen werden, ob eine Mitteilung durchgeführt werden kann. Gleichermaßen kann überprüft werden, ob ein Cloud-Nutzer auf Verlangen über die Empfänger der Offenlegung unterrichtet werden kann.

Nr. 16 – 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 der betroffenen Personen 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 von betroffenen Personenausgegangen 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 C1.3 und C1.6).

Umsetzungshinweis

Der Cloud-Anbieter sollte entsprechende Prozesse etablieren und dokumentieren, sowie Ansprechpartner, Verantwortlichkeiten und Meldewege festlegen. Die Meldung von Datenschutzvorfällen sollte in das Incident- und Troubleshooting-Management des Cloud-Anbieters integriert werden, um eine rasche Bearbeitung zu ermöglichen.

Auf die Umsetzungshinweise im BSI C5 Anf. SIM-01 bis SIM-07 wird hingewiesen.

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 6.13.1 wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er in seinem Datensicherheitskonzept dokumentiert, wie er die Meldung von Datenschutzverletzungen durchführt. Der Cloud-Anbieter kann zudem weitere Dokumentationen vorlegen, darunter bspw. Prozessdokumentationen zur Meldung, Verfahrensverzeichnisse und -anweisungen, Richtlinien, Muster und Vorlagen zur Meldung von Datenschutzverletzungen, Entscheidungsregeln zur Beurteilung von Datenschutzverletzungen, Verfahren zur Risikobeurteilung und Faktoren, die bei der Risikoanalyse einbezogen werden, sowie Meldewege und Verantwortlichkeiten/Zuständigkeiten. Auch können dokumentierte Meldungen von Datenschutzverletzungen vorgelegt werden, sofern sie vorhanden sind.

Der Nachweis kann auch durch eine Befragung von Mitarbeitern oder Beobachtung einer Probemeldung erbracht werden. Im Rahmen einer Vor-Ort-Auditierung sollte nachgewiesen werden, dass ausreichend Ressourcen vorliegen, um eine unverzügliche Meldung sicherzustellen.

Auch sollte ein Cloud-Anbieter Unterlagen zur Schulung zuständiger Mitarbeiter vorlegen (bspw. Zeugnisse, Teilnahmebescheinigungen von Workshops) und ihre Befragung im Rahmen eines Audits zulassen (bspw. im Hinblick auf die Bekanntheit von Richtlinien und Verfahrensschritten).

Nr. 17 – Benachrichtigung der betroffenen Person bei Datenschutzverletzungen (Art. 34 Abs. 1 und 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter unterrichtet die betroffene Person 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 ihre Rechte und Freiheiten 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 von betroffenen Personen 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 der betroffenen Person 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.

Umsetzungshinweise

Die Umsetzungshinweise unter Nr. 8.2 sind anwendbar, wobei statt auf die Ziff. 8.2.5 und 8.3 der ISO/IEC 27701 auf die Ziff. 7.3.1 und 7.3.2 hingewiesen wird.

Nachweis

Die Benachrichtigung der betroffenen Person bei Datenschutzverletzungen kann der Cloud-Anbieter wie in Nr. 8.2 angegeben nachweisen.

Nr. 18 – Führen eines Verarbeitungsverzeichnisses (Art. 30 Abs. 1 DSGVO)

Kriterium

(1) Ist der Cloud-Anbieter zur Führung eines Verarbeitungsverzeichnisses verpflichtet, bezieht sich dieses auf die Verarbeitungstätigkeiten, die er 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.

(2) 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 C1.6).

In der Regel ist der Cloud-Anbieter ab 250 beschäftigten Mitarbeitern zur Führung eines Verarbeitungsverzeichnisses verpflichtet. Jedoch müssen auch Cloud-Anbieter mit weniger Mitarbeitern, die Daten zur Durchführung des Auftrags mit dem Cloud-Nutzer verarbeiten im Regelfall ein Verarbeitungsverzeichnis führen, da diese Verarbeitungen regelmäßig und nicht nur gelegentlich erfolgen, sodass die Ausnahme aus Art. 30 Abs. 5 DSGVO nicht anwendbar ist.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 8.3 sind anwendbar.

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 7.2.8 wird hingewiesen.

Nachweis

Das Führen eines Verarbeitungsverzeichnisses kann der Cloud-Anbieter analog wie in Nr. 8.3 angegeben nachweisen.

Nr. 19 – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Nr. 19.1 – 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 Dienster-bringung gegenüber dem Cloud-Nutzer erforderlich sind. Ebenfalls sind Umfang der Verarbeitung und Speicherfrist auf das zur Zweckerreichung erforderliche Maß zu begrenzen.

Umsetzungshinweise

Die Umsetzungshinweise unter Nr. 9.1 sind anwendbar, wobei statt auf Ziff. 8.4 der ISO/IEC 27701 auf die Ziff. 7.4 hingewiesen wird.

Nachweis

Für den Nachweis von Datenschutz durch Systemgestaltung gelten die Ausführung in Nr. 9.1 analog.

Nr. 19.2 – 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 verarbeitet, die erforderlich sind, um den Cloud-Dienst erbringen zu können.

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

Umsetzungshinweise

Die Umsetzungshinweise unter Nr. 9.2 sind anwendbar. Statt der in Nr. 9.2 angegebenen Ziff. 8.4 der ISO/IEC 27701 ist Ziff. 7.4 anwendbar.

Nachweise

Für den Nachweis von Datenschutz durch datenschutzfreundliche Voreinstellungen gelten die Ausführung in Nr. 9.2 analog.

Nr. 20 – 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. 20.1 – 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 TOM 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) Die rechtsverbindliche Vereinbarung zur Auftragsvereinbarung muss die nachfolgenden Anforderungen dieses Kriteriums erfüllen, wobei die geforderten Festlegungen auch in sonstigen Dokumenten getroffen werden können, wenn diese als Bestandteile der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung einbezogen worden sind.

(5) Der Cloud-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung Gegenstand und Dauer der Verarbeitung so konkret wir möglich festgelegt werden.

(6) Der Cloud-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung, Art und Zweck der vorgesehenen Verarbeitung, Art der verarbeiteten Daten sowie die Kategorien betroffener Personen festgelegt werden.

(7) Der Cloud-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festgelegt ist, dass personenbezogene Daten nur auf seine dokumentierte Weisung hin vom Auftragsverarbeiter verarbeitet werden, auch in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation.

(8) Der Cloud-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung der Ort der Datenverarbeitung festgelegt wird. Erfolgt die Datenverarbeitung außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, ist das konkrete Drittland zu benennen.

(9) Der Cloud-Anbieter stellt sicher, dass sich der Auftragsverarbeiter in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung darauf verpflichtet, ihm Änderungen des Datenverarbeitungsortes unverzüglich mitzuteilen.

(10) Der Cloud-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festgelegt wird, dass der Auftragsverarbeiter die zur Verarbeitung von personenbezogenen Daten befugten Personen vor Aufnahme der datenverarbeitenden Tätigkeit zur Vertraulichkeit verpflichtet, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen.

(11) Der Cloud-Anbieter stellt sicher, dass gemäß Art. 32 DSGVO die dem Schutzniveau der ausgelagerten Datenverarbeitung angemessenen TOM in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festgelegt werden.

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

(13) Die Pflichten des Auftragsverarbeiters zur Rückgabe von Datenträgern, Rückführung von Daten und irreversiblen Löschung von Daten nach Ende der Auftragsverarbeitung sind in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festzulegen.

(14) 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.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 1 sind analog für das Schließen einer rechtsverbindlichen Vereinbarung mit einem Subauftragsverarbeiter anwendbar.

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 5.4.1.2, 5.4.1.3, 6.10.2.4, 6.12, 7.2.6 wird hingewiesen.

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. Für die jeweiligen Subauftragsverarbeiter sollten Dokumente wie das Datensicherheitskonzept mit den TOM oder Zertifikate nachgewiesen werden. Weitere relevante Dokumente können als Nachweis einbezogen werden, darunter der Mustervertrag zur Auftragsverarbeitung mit Subauftragsverarbeitern, Richtlinien und Anweisungen, weitere Garantien der Subauftragsverarbeiter, interne Kontrollbereiche des Cloud-Anbieters über Subauftragsverarbeiterkontrollen, das Datenschutzkonzept oder die Risikoabschätzung bei der Unterbeauftragung.

Nr. 20.2 – Sicherstellung ordnungsgemäßer Auftragsverarbeitung

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter personenbezogene Daten nur auf seine dokumentierte Weisung hin 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 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 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 irreversibel 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 verpflichtet den Auftragsverarbeiter darauf, ein Verarbeitungsverzeichnis zu führen, wenn er gesetzlich dazu verpflichtet 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. 20.1 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.

Umsetzungshinweis

Auf die Umsetzungshinweise der ISO/IEC 27701 Ziff. 5.4.1.2, 5.4.1.3, 6.12, 7.2.6 wird hingewiesen.

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. Diese können. befolgte Verhaltensregeln, Zertifikate, rechtsverbindliche Vereinbarungen (insb. im Hinblick auf Weisungen durch den Cloud-Anbieter und Pflichten des Subauftragsverarbeiters), Dienstbeschreibungen, Datensicherheitskonzepte, oder sonstige Dokumente sein. Darüber hinaus kann der Cloud-Anbieter Dokumente über die Auswahl (bspw. Protokolle über Auswahlüberlegungen und -entscheidungen) und die Durchführung von eigenen Kontrollen (bspw. Protokolle der Subauftragsverarbeiterkontrollen) vorlegen.

Unterstützend kann im Rahmen eines Audits eine Befragung der Mitarbeiter zur Durchführung der Kontrolle von Subauftragsverarbeitern durchgeführt werden (bspw. Bekanntheit von Verfahrensschritten und Garantien der Subauftragsverarbeiter). Auch kann im Rahmen eines Audits eine Befragung der Mitarbeiter zur Einbindung von Subauftragsverarbeitern bei den Unterstützungsfunktionen und Pflichten als Hauptauftragsverarbeiter durchgeführt werden (bspw. Bekanntheit von Verfahrensschritten und Ansprechpartner der Subauftragsverarbeiter).

E. Referenzen

BSI C5	Cloud Computing Compliance Controls Catalogue, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Anforderungskatalog/Anforderungskatalog_node.html, Stand 20.11.2019 (alte Fassung)
BSI TR-02102-1	Kryptographische Verfahren: Empfehlungen und Schlüssellängen, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html, Stand 22.02.2019
BSI TR-02102-2	Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2 – Verwendung von Transport Layer Security (TLS), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html, Stand 22.02.2019
BSI TR-02102-3	Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPSec) und Internet Key Exchange (IKEv2), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-3.html, Stand 25.01.2018
BSI TR-02102-4	Kryptographische Verfahren: Verwendung von Secure Shell (SSH), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-4.html, Stand 25.01.2018
DIN EN 1627	Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung. Stand 2011
DIN 66398	Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten. Stand 2016
DIN 66399	Vernichtung von Datenträgern. Stand 2012
EDPB Guidelines 4/2019	Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Stand 13.11.2019
ISO/IEC 11770-2	IT Security techniques — Key management — Part 2: Mechanisms using symmetric techniques. Stand 2018
ISO/IEC 19941	Information technology — Cloud computing — Interoperability and portability. Stand 2017
ISO/IEC 21964-1	Information technology — Destruction of data carriers — Part 1: Principles and definitions. Stand 2018
ISO/IEC 24760-1	IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts. Stand 2019
ISO/IEC 24760-2	Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements. Stand 2015
ISO/IEC 24760-3	Information technology — Security techniques — A framework for identity management — Part 3: Practice. Stand 2016
ISO 25237	Health informatics — Pseudonymization. Stand 2017
ISO/IEC 27002	Information technology — Security techniques — Code of practice for information security controls. Stand 2013
ISO/IEC 27018	Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Stand 2019
ISO/IEC 27040	Information technology — Security techniques — Storage security. Stand 2015
ISO/IEC 27701	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. Stand 2019
ISO/IEC 29101	Information technology — Security techniques — Privacy architecture framework. Stand 2018
ISO/IEC 29134	Information technology — Security techniques — Guidelines for privacy impact assessment. Stand 2017
ISO/IEC 29146	Information technology — Security techniques — A framework for access management. Stand 2016
ISO 31000	Risk management – Guidelines. Stand 2018
IEC 31010	Risk management — Risk assessment techniques. Stand 2019

SDM	Standard-Datenschutzmodell, Version 2.0, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode.pdf, Stand November 2019
Arbeitspapier „Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen“	Schwartmann/Weiß (Hrsg.), Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen, Ein Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2018, https://www.gdd.de/downloads/anforderungen-an-datenschutz-konforme-pseudonymisierung