European Cloud Service
Data Protection Certification

# AUDITOR-Kriterienkatalog

**- Entwurfsfassung 0.7 -**

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], Ayşe Necibe Batman[a], Sebastian Lins[b], Natalie Maier[a], Heiner Teigeler[b]

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

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

# Inhaltsverzeichnis

# Abkürzungsverzeichnis

| | |
|---|---|
| Abs. | Absatz |
| AGB | Allgemeine Geschäftsbedingungen |
| Art. | Artikel |
| BDSG n.F. | Bundesdatenschutzgesetz neue Fassung (Geltung ab 25.5.18) |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| C5 | Cloud Computing Compliance Controls Catalogue des BSI |
| 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 |
| Nr. | Nummer |
| PIN | Persönliche Identifikationsnummer |
| S. | Siehe |
| SDM | Standard-Datenschutzmodell der Aufsichtsbehörden v.1.1 vom 26.4.2018 |
| SLA | Service Level Agreements |
| Sog. | Sogenannt |
| TAN | Transaktionsnummer |
| TCDP | Trusted Cloud Datenschutz-Profil |
| TOM | technische und organisatorische Maßnahmen |
| Vgl. | Vergleiche |
| Z.B. | Zum Beispiel |
| 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

Die Datenschutz-Zertifizierung ermöglicht es Anbietern von Cloud-Diensten des privaten Sektors, die Vereinbarkeit ihrer Datenverarbeitungsvorgänge mit datenschutzrechtlichen Anforderungen nachzuweisen. Der AUDITOR-Kriterienkatalog beschreibt die datenschutzrechtlichen Anforderungen an die Verarbeitung von personenbezogenen Daten auf der Seite des Auftragnehmers (Cloud-Anbieter). Jedoch werden die datenschutzrechtlichen Anforderungen an den Auftraggeber (Cloud-Nutzer) nicht adressiert.

**Zertifizierungsgegenstand AUDITOR**

Der Zertifizierungsgegenstand des AUDITOR-Kriterienkatalogs sind Datenverarbeitungsvorgänge mit personenbezogenen Daten in Cloud-Diensten. Eine Datenverarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie 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. Die Datenverarbeitungsvorgänge können in Produkten oder Diensten oder mit Hilfe von (auch mehreren) Produkten und Diensten erbracht werden. Sie müssen eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen, innerhalb derer die spezifischen Datenschutzrisiken des jeweiligen Cloud-Dienstes vollständig erfasst werden können. Ein Datenverarbeitungsvorgang kann sowohl technische und automatisierte als auch nicht-technische Vorgangsschritte enthalten. Der gesamte Verarbeitungsvorgang muss den Anforderungen der DSGVO entsprechen. Insofern sind auch alle technischen und organisatorischen Vorkehrungen zu erfassen, die diese Konformität sicherstellen. Hierzu gehören auch Datenschutzkonzepte und -Managementsysteme.

Weiterführende Informationen zum Zertifizierungsgegenstand AUDITOR sind dem Begleitdokument „Zertifizierungsgegenstand“ zu entnehmen.

**Personenbezogene Daten als hohes Schutzgut**

Schutzbedürftig nach diesem Katalog sind alle *personenbezogenen Daten* im Sinne des Art. 4 Abs. 1 DSGVO, also alle Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Im Cloud-Kontext können dies beispielsweise Anmeldedaten, Bestands- und Vertragsdaten, Nutzungsdaten, Protokollierungsdaten oder Metadaten sein, soweit sie dem Verantwortlichen oder dem Auftragsverarbeiter die Identifizierung oder Identifizierbarkeit einer natürlichen Person ermöglichen (siehe Tabelle 1 und Kapitel 3. Die Schutzklassen des AUDITOR-Kriterienkatalogs).

| Datenart | Beschreibung | Beispiele |
|---|---|---|
| Anwendungsdaten des Nutzers | Die Nutzung eines Cloud-Dienstes impliziert, dass ein Cloud-Nutzer seine Daten zur Verarbeitung oder Speicherung an den Cloud-Dienst übermittelt. | Geschäftsdaten, Produkt- und Artikeldaten, Kommunikationsdaten |
| Stammdaten des Nutzers | Zur Nutzung des Cloud-Dienstes muss der Cloud-Nutzer persönliche Informationen über seine Person und/oder das Unternehmen dem Cloud-Anbieter mitteilen, sodass dieser den Cloud-Nutzer identifizieren kann. | Namen, Kontaktdaten, Adressen sowie Daten über die Art und Umfang der Dienstnutzung |
| Abrechnungsdaten des Nutzers | Zur Abrechnung der in Anspruch genommenen Dienstleistung erhebt ein Cloud-Anbieter Abrechnungsinformationen. | Kreditkarteninformationen oder Kontodaten |
| Identifizierungs-/ Authentifizierungsdaten | Um den Zugriff auf den Cloud-Dienst zu ermöglichen, erhebt ein Cloud-Anbieter Identifizierungs- und Authentifizierungsdaten. | Benutzernamen, IDs und E-Mail-Adressen |
| Technische Daten zur Dienstbereitstellung | Es kann erforderlich sein, dass ein Cloud-Anbieter spezifische Informationen erhebt, um den Dienst bereitstellen oder auf die Besonderheiten des Nutzers individuell zuschneiden / konfigurieren zu können. | Browser- und Gerätetyp, Betriebssystem, eindeutige Gerätekennungen |
| Standortdaten | Zur Erbringung des Dienstes kann es notwendig oder förderlich sein, dass Informationen über den tatsächlichen Standort erfasst werden. | GPS-Daten, WLAN-Zugangspunkte |
| Nutzungsdaten | Bei der Nutzung des Cloud-Dienstes können verschiedene Informationen protokolliert werden. Diese Informationen sind meist dem Nutzer direkt zuordenbar oder ermöglichen gar eine Identifikation des Nutzers. | IP-Adressen, durchgeführte Aktivitäten, Dienstzugriffe, aktive Logins, Suchanfragen |
| Meta-Daten | Beim Betrieb des Cloud-Dienstes können eine Vielzahl von weiteren strukturierten Daten mit Personenbezug erzeugt werden. | Log Files, welche Datenmigrationsvorgänge protokollieren |

Tabelle 1. Beispielhafte personenbezogene Daten, welche in der Cloud verarbeitet werden könnten.

### Cloud-Anbieter als Adressat

Antragsteller im AUDITOR-Zertifizierungsverfahren können der Verantwortliche oder der Auftragsverarbeiter eines Datenverarbeitungsvorgangs sein. In den meisten Fällen wird allerdings nur der Cloud-Anbieter als Auftragsverarbeiter eine Zertifizierung anstreben. Der Cloud-Nutzer möchte als Verantwortlicher Kenntnis von einer Zertifizierung des Cloud-Anbieters haben, um seinen Pflichten zur Auswahl, Weisung und Kontrolle gemäß Art. 28 Abs. 1 DSGVO nachkommen zu können.

*Cloud-Anbieter* im Sinne dieses Katalogs ist jedes Unternehmen, das einen Cloud-Dienst am Markt anbietet und sich nach dem AUDITOR-Kriterienkatalog zertifizieren lassen möchte.

### Cloud-Nutzer als Nutznießer

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

Aufgrund der Zertifizierung der Datenverarbeitungsvorgänge eines Cloud-Dienstes kann der Cloud-Nutzer darauf vertrauen, dass der von ihm verwendete Cloud-Dienst datenschutzkonform ist. Das Anwendungsgebiet 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 DSGVO 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, da ein Zertifikat gemäß Art. 28 Abs. 5 DSGVO als Faktor herangezogen werden kann, 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.

# 2. Fortentwicklung von TCDP gemäß der Datenschutz-Grundverordnung

Die Zertifizierung nach dem alten Bundesdatenschutzgesetz wurde im Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ durch das im September 2016 finalisierte TCDP untersucht. Da bei der Entwicklung der Zertifizierungskriterien nach TCDP noch nicht alle einschlägigen internationalen Normen, neu entwickelten relevanten Kriterienwerke – z. B. Cloud Computing Compliance Controls Catalogue (C5) – und insbesondere die Anforderungen der DSGVO berücksichtigt werden konnten, muss mit dem Geltungsbeginn der DSGVO 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 DSGVO und konkretisiert diese zu prüffähigen Kriterien. Wichtig ist darauf hinzuweisen, dass der Regelfall des Cloud Computing eine Auftragsverarbeitung gemäß Art. 28 DSGVO darstellt. Der Vertrag über die Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO regelt die für die hier vorzunehmende Zertifizierung relevante Zuständigkeitsabgrenzung zwischen beiden Parteien und stellt eine (gesetzlich vorausgesetzte) Rechtsgrundlage für die Auftragsverarbeitung dar. Der Auftragsverarbeiter hat die Datenverarbeitung gemäß Art. 28 und 29 DSGVO nur weisungsgebunden durchzuführen. Bei der Auftragsverarbeitung fungiert der Cloud-Nutzer nach Art. 4 Nr. 7 DSGVO als Verantwortlicher und der Cloud-Anbieter als Auftragsverarbeiter gemäß Art. 4 Nr. 8 DSGVO. Der Cloud-Nutzer bleibt damit stets „Herr der Daten“, der Cloud-Anbieter ist sein „verlängerter Arm“.

# B. Aufbau und Nutzung des AUDITOR-Kriterienkatalogs

Der AUDITOR-Kriterienkatalog unterscheidet wie auch bereits TCDP zwischen „Kriterien“, „Umsetzungshinweisen“ und „Erläuterungen“. Zusätzlich enthält der AUDITOR-Kriterienkatalog noch die Kategorie der „Nachweise“.

Die *„Kriterien“* bezeichnen die normativen Voraussetzungen, die zu erfüllen sind, um ein Zertifikat auf der Grundlage des AUDITOR-Kriterienkatalogs zu erhalten. Sie stellen die Prüfanforderungen dar und können sich auf unterschiedliche Prüfobjekte beziehen wie Tabelle 2 zu entnehmen ist. So bildet beispielsweise in Kapitel 1 dieses Kriterienkatalogs der Cloud-Vertrag das Prüfobjekt, während in Kapitel 2 bei der Gewährleistung der Datensicherheit nach Nr. 2 regelmäßig vorwiegend Softwarearchitektur, Infrastruktur und Prozesse eine Rolle spielen werden. Abbildung 1 stellt schematisch die Einordnung von Prüfobjekten dar. Da die DSGVO verpflichtende Anforderungen stellt, sind auch die Kriterien des AUDITOR-Kriterienkatalogs als verpflichtende Anforderungen formuliert.

| **Prüfobjekt** | **Beschreibung** |
|---|---|
| Vertrag | Die zu überprüfenden Objekte sind Eigenschaften und Inhalte von Verträgen mit Cloud-Nutzern oder Subauftragsverarbeitern. |
| Prozess | Das zu prüfende Objekt ist ein Prozess oder eine entsprechende und realitätsnahe Prozessdokumentation. |
| Anbietereigenschaften | Es werden Eigenschaften und Ausprägungen des Cloud-Anbieters geprüft, z.B. die zugrundeliegende Organisationsstruktur. |
| Diensteigenschaften | Zu den Diensteigenschaften gehören insbesondere Cloud-Dienst-Features und Funktionen, die für den Cloud-Nutzer unmittelbar sichtbar sind. |
| Infrastruktur | Ein Kriterium betrachtet physische Objekte, wie beispielsweise Hardware-Komponenten oder die Rechenzentrumsinfrastruktur. |
| Softwarearchitektur | Ein Kriterium untersucht virtuelle Objekte, z.B. Software oder den Quellcode sowie die Zusammenstellung und Interaktionen der einzelnen Komponenten des Cloud-Dienstes. |
| Personal | Ein Kriterium erfordert die Betrachtung von Personalressourcen, z.B. die Auswahl geeigneter Personen oder die Durchführung von Mitarbeiterschulungen. |

Tabelle 2. Übersicht über mögliche Prüfobjekte innerhalb eines Datenverarbeitungsvorgangs.

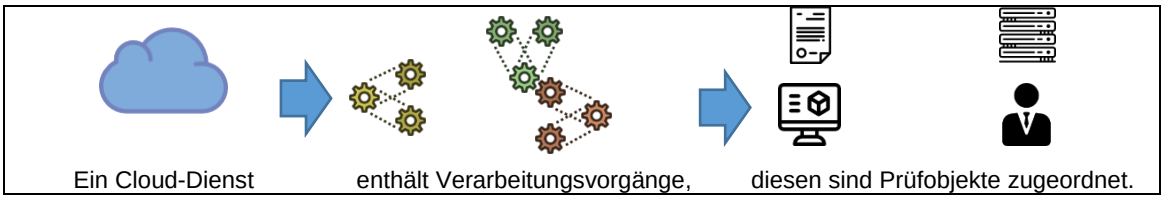


Abbildung 1. Schematische Darstellung zur Einordnung von Prüfobjekten.

Die *„Umsetzungshinweise“* sollen exemplarische Leitlinie und Hilfestellung für das Verständnis und die Umsetzung der Kriterien geben, sind selbst aber keine verpflichtenden Anforderungen. Die Umsetzungshinweise zu den einzelnen AUDITOR-Kriterien sind grundsätzlich an den Schutzklassen nach Maßgabe des AUDITOR-Schutzklassenkonzepts ausgerichtet. Fehlt in einem AUDITOR-Kriterium eine solche Einteilung nach Schutzklassen, bedeutet dies, dass die Umsetzungshinweise gleichermaßen für alle Schutzklassen gelten.

Die *„Erläuterungen“* sollen das Verständnis der Kriterien und ihre Herleitung aus dem Gesetz erleichtern.

Die *„Nachweise“* liefern die Antwort auf die Frage, wie das Vorliegen der *„Kriterien“* im konkreten Zertifizierungsverfahren erwiesen werden kann. Die Nachweismöglichkeiten wurden – soweit möglich – in Bezug auf Einzel- wie Massengeschäfte in Cloud-Diensten differenziert dargestellt. Nachweise stellen analog zu den Umsetzungshinweisen exemplarische Leitlinien und informative Hilfestellungen dar, die Cloud-Anbieter, Zertifizierungsstellen, Prüfer und weitere Interessierte bei der Beurteilung der Einhaltung von Kriterien unterstützen sollen. Es besteht keine Verpflichtung, die Nachweise gemäß des AUDITOR-Kriterienkatalogs zu erbringen.

Ferner kann unter *„Nachweise“* auch eine mögliche Auditierungsmethode angegeben werden, um die Transparenz der Zertifizierung zu steigern und die Glaubwürdigkeit und Akzeptanz eines Zertifikates zu stärken. Auch wird dadurch einem Cloud-Anbieter deutlich gemacht, mit welchem Aufwand zum Nachweis zu rechnen ist. Die folgende Tabelle 3 listet die im AUDITOR-Katalog umfassten Methoden auf.

| Auditierungsmethode | Beschreibung |
|---|---|
| Interview | Ein Kriterium wird durch Interviews mit Mitarbeitern des Cloud-Anbieters überprüft, z.B. Befragung von Systemadministratoren oder Softwareentwicklern. Interviews kommen häufig zum Einsatz, um zu überprüfen, ob bestimmte Prozesse nicht nur in einem Dokument definiert sind, sondern im Unternehmen auch wirklich gelebt werden. |
| Dienstnutzung | Ein Kriterium wird überprüft, indem der Cloud-Dienst durch einen Prüfer genutzt und getestet wird, beispielsweise Login in den Cloud-Dienst und Testen von speziellen Features. |
| Technische Prüfung | Ein Kriterium wird durch die Verwendung von computergestützten Auditierungssystemen und -Software überprüft, z.B. Penetrationstests. |
| Prozessprüfung | Ein Kriterium wird geprüft, indem z.B. ein Prozess angestoßen und die Ausführung überwacht oder das Ergebnis überprüft wird. Alternativ können Protokolle oder Log-Dateien mit Prozessmeilensteinen überprüft werden. |
| Assetprüfung | Ein Kriterium wird überprüft, indem ein Asset (z.B. Hardware oder Software und ggf. die dazugehörige Dokumentation), in Begleitung oder unter Anweisung eines Mitarbeiters des Cloud-Anbieters untersucht wird. |
| Dokumentationsprüfung | Ein Kriterium wird überprüft, indem der Cloud-Anbieter entsprechende Dokumente, Protokolle oder Testate vorlegt. Eine bloße Selbstauskunft durch den Cloud-Anbieter ist nicht ausreichend. |
| Vor-Ort-Auditierung (Inaugenscheinnahme) | Das Kriterium erfordert von einem Prüfer, das zu prüfende Objekt vor Ort beim Cloud-Anbieter zu auditieren, beispielsweise durch eine Begehung des Rechenzentrums. |
| Kontinuierliche Auditierung | Das Kriterium wird durch einen Prüfer kontinuierlich überwacht, um die Einhaltung dauerhaft sicherzustellen und zu verbessern/zu optimieren. |

Tabelle 3. Übersicht über mögliche Auditierungsmethoden.

# C. Schutzklassen

Anforderungen an TOM 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 Datenschutzaufsichtsbehörden.

## 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 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 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 festzustellen, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt. Diese Risikoabstufungen werden mit dem AUDITOR-Schutzklassenkonzept umgesetzt.

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

Ziel des Schutzklassenkonzepts ist es, den individuellen Maßstab der DSGVO – 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 in den Datenverarbeitungsvorgängen verarbeiteten personenbezogenen Daten, zum anderen die Anforderungen an die TOM. Um die unterschiedlichen Funktionen deutlich zu machen, unterscheidet das Schutzklassenkonzept Schutzbedarfsklassen und 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.

## 2. Verantwortung von Cloud-Nutzer und Cloud-Anbieter

Die Unterscheidung von Schutzbedarf und Schutzanforderungen 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 Dienstes für eine konkrete Schutzanforderungsklasse zum Ausdruck gebracht.

Der Cloud-Nutzer als Verantwortlicher und Auftraggeber hat die Aufgabe, den Schutzbedarf seiner Datenverarbeitung festzulegen und für seine Datenverarbeitung einen Cloud-Dienst auszuwählen, der mindestens die entsprechende Schutzanforderungsklasse erfüllt.

# 3. Die Schutzklassen des AUDITOR-Kriterienkatalogs

Der AUDITOR-Kriterienkatalog beruht auf der Unterscheidung von drei Schutzklassen (I, II, III), für die jeweils Schutzbedarfe (Schutzbedarfsklassen) und Schutzanforderungen (Schutzanforderungsklassen) beschrieben werden. Zusätzlich gibt es die Klasse III+, bei der die Datenverarbeitung mit einem so hohen Risiko verbunden ist, dass sie nicht in einer Schutzklasse beschrieben werden kann und damit einer Zertifizierung nicht zugänglich ist.

**a) Die Ermittlung der Schutzbedarfsklasse**

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

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

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

**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 diesen 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 Verhältnisse der betroffenen Person enthalten, erzeugen, unterstützen oder solche ermöglichen. Die unbefugte Verwendung dieser Daten kann von der betroffenen Person leicht durch Aktivitäten verhindert oder abgestellt werden oder lässt keine besonderen Beeinträchtigungen erwarten.

Beispiele (nicht abschließend) (ohne Kontext, soweit nicht Schutzbedarfsklasse 2 oder 3):

- Name, Anschrift;
- Beruf;
- Geburtsjahr;
- Titel;
- Adressbuchangaben;
- Telefonverzeichnisse;
- Bankverbindungen;
- 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 Erhebung, Verarbeitung oder Nutzung 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.

Beispiele (nicht abschließend) (soweit aufgrund des Verarbeitungskontextes nicht Schutzbedarfsklasse 3 oder 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 ethische Herkunft;
- Daten über politische Meinungen;
- Religiöse oder weltanschauliche Überzeugungen;
- Gewerkschaftsangehörigkeit;
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person;
- Verarbeitungen eindeutig identifizierender, hoch verknüpfbarer Daten wie Krankenversichertennummern oder Steuernummern;
- Daten, die mögliche Auswirkungen auf das Ansehen/die Reputation der betroffenen Person haben;
- Daten über den geschützten inneren Lebensbereich der betroffenen Person (z.B. Tagebücher);
- Gesundheitsdaten i.S.v. Art. 4 Nr. 15 DSGVO;
- Grad der Behinderung;
- Verarbeitung von Daten mit inhärenter Intransparenz für die betroffene Person (Schätzwerte beim Scoring, Anwendung von Algorithmen);
- Einkommen;
- Sozialleistungen;
- Steuern;
- Ordnungswidrigkeiten;
- Daten über Mietverhältnisse;
- Patientenverwaltungsdaten (mit Ausnahme von besonders sensiblen Diagnosedaten und dergleichen);
- Arbeitszeitzeitdaten;
- Mitgliederverzeichnisse;
- Melderegister;
- Zeugnisse und Prüfungsergebnisse;
- Versicherungsdaten;
- Personalverwaltungsdaten aus Beschäftigungsverhältnissen (mit Ausnahme von dienstlichen Beurteilungen und beruflicher Laufbahn);
- Verkehrsordnungswidrigkeiten;
- einfache Bewertungen eher geringer Bedeutung (z.B. Ja/Nein-Entscheidung bei Einstufung im Mobilfunkvertrag etc.);
- Zugangsdaten zu einem Dienst;
- Kommunikationsinhalte einer Person (z.B. E-Mail-Inhaltsdaten, Brief, Telefonat);
- (genauer) Aufenthaltsort einer Person;
- Finanzdaten einer Person (z.B. Kontostand, Kreditkartennummer, einzelne Zahlung);
- Kreditauskünfte;
- Verkehrsdaten der Telekommunikation.

Hinweis: Kommunikationsinhalte, insbesondere Schrift- oder Sprachaufzeichnungen jeder Art, können sehr unterschiedlichen Schutzbedarf, von niedrig bis sehr hoch aufweisen. Die Festlegung des Schutzbedarfs erfordert eine objektive Bewertung, in der das Ausmaß des Risikos der Datenverarbeitung beurteilt wird. Sofern der Cloud-Nutzer keine Kenntnis vom subjektiven Schutzbedarf der Kommunizierenden hat (Beispiel: allgemeiner Kollaborations-Service mit Datenablage, Videokonferenz und Mailfunk-

tion) oder seine Dienste für besonders schutzbedürftige Kommunikationen anbietet (Beispiel: Konferenzservice für Rechtsanwälte und Mandanten, hier: Schutzklasse 3) darf er von der 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 Erhebung, Verarbeitung oder Nutzung 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.

Beispiele (nicht abschließend):

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

**Datenarten mit extrem hohem Schutzbedarf (Schutzbedarfsklasse 3 plus)**

Datenarten, die eine erhebliche Aussagekraft über die Persönlichkeit oder Lebensumstände der betroffenen Person haben oder sonst für die Verhältnisse der betroffenen Person von erheblicher Bedeutung sind. Die unbefugte Erhebung, Verarbeitung oder Nutzung dieser Daten kann zu einer konkreten Gefahr für eine wesentliche Beeinträchtigung von Leben, Gesundheit oder Freiheit der betroffenen Person führen.

Beispiele (nicht abschließend):

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

**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 Risiken des Dienstes angemessen zu schützen.

**Schutzanforderungsklasse 1**

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

Die TOM müssen geeignet sein, um im Regelfall solche Vorgänge 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. Jeder Eingriff muss nachträglich festgestellt werden können.

**Schutzanforderungsklasse 2**

Ein hoher Schutzbedarf führt dazu, dass zusätzliche risikoangemessene TOM ergriffen werden müssen, um die Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit von personenbezogenen Daten sicherzustellen (siehe auch Gewährleistungsziele aus dem SDM). Für die Informationssicherheit bedeutet dies, dass die Daten, insbesondere gegen Vernichtung, Verlust, Veränderung, unbefugten Zugang und unbefugte Offenlegung, zu schützen sind. 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 einer Zwei-Faktor-Authentifizierung oder 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 auszuschließen. 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 3 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.

# D. Kriterien und Umsetzungsempfehlungen

## Kapitel I: Cloud-Vertrag

**Erläuterung**

Der Cloud-Anbieter muss sicherstellen, dass die Leistungen gegenüber dem Cloud-Nutzer aufgrund eines Vertrages (Cloud-Vertrag)[1] erbracht werden, der die gesetzlichen Anforderungen der DSGVO an die Auftragsverarbeitung erfüllt. Dieses Ziel soll durch die nachfolgenden Kriterien und Umsetzungshinweise gesichert werden.

Die Nummern 1.1 bis 1.9 des AUDITOR-Katalogs können dadurch erfüllt werden, dass der Cloud-Anbieter einen Vertrag anbietet, der die genannten Anforderungen erfüllt und durch technische und organisatorische Vorkehrungen gewährleistet, dass der Cloud-Dienst nur auf der Grundlage und nach Abschluss eines entsprechenden Cloud-Vertrags erbracht wird.

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

### Nr. 1.1 – Dienstleistung aufgrund eines Vertrages (Art. 28 Abs. 3 Satz 1 DSGVO)

**Kriterium**

Der Cloud-Anbieter stellt durch geeignete technische oder organisatorische Vorkehrungen sicher, dass der Cloud-Dienst erst nach dem Abschluss eines Vertrages mit dem Cloud-Nutzer erbracht wird. Dieser Vertrag muss die Anforderungen dieses Kapitels (Nr. 1.1 – Nr. 1.9) erfüllen.

**Erläuterung**

Der Vertrag zur Datenverarbeitung im Auftrag, d.h. der Cloud-Vertrag, ist wesentlich, da mit diesem die Rolle des Cloud-Anbieters als Auftragsverarbeiter i.S.v. Art. 4 Nr. 8 DSGVO gegenüber der Rolle des Cloud-Nutzers als Verantwortlichem nochmals ausdrücklich klargestellt wird.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er alle oder eine repräsentative Stichprobe von Verträgen vorlegt, die er mit den Cloud-Nutzern geschlossen hat (Dokumentationsprüfung). Außerdem muss er anhand einer geeigneten Dokumentation (z.B. Prozessdokumentation) nachweisen, dass er technische oder organisatorische Vorkehrungen getroffen hat, die einen automatischen Vertragsschluss vor der eigentlichen Dienstnutzung sicherstellen. Hierzu können auch einzelne Anwendungen des Cloud-Dienstes im Rahmen einer Prüfung mit repräsentativen Stichproben getestet werden, um zu überprüfen, ob diese technischen oder organisatorischen Vorkehrungen tatsächlich umgesetzt und anwendbar sind (Dienstnutzung).

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

**Kriterium**

Der Gegenstand und die Dauer des Auftrags sind im Cloud-Vertrag so konkret wie möglich festzulegen. Zumindest ist der Gegenstand des Auftrags gemäß der in Anspruch genommen Datenverarbeitung zu spezifizieren und die Dauer des Auftrages durch einen Start- und Endpunkt oder den Verweis auf eine unbestimmte Nutzungszeit festzulegen. Die Voraussetzungen einer Kündigung sind aufzunehmen.

[1] Alternativ 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.

**Umsetzungshinweis**

Für beide Vertragsparteien muss anhand dieser Eingrenzung des Auftragsgegenstandes klar hervorgehen, welche Verarbeitungsvorgänge oder Verarbeitungskategorien nach welcher Schutzklasse durch den Cloud-Anbieter für den Cloud-Nutzer durchgeführt werden. Insbesondere soll 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.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen Vertragsentwurf mit diesen Angaben vorhält und ein Verfahren implementiert hat, wonach der Vertrag mit diesen Festlegungen geschlossen wird. Durch eine Dokumentationsprüfung oder Dienstnutzung ist zu prüfen, ob alle im Vertrag enthaltenen Angaben dem Cloud-Nutzer auf geeignete Weise kommuniziert werden.

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

**Kriterium**

Im Cloud-Vertrag werden der Umfang, die Art und der Zweck der vorgesehenen Verarbeitung von Daten im Auftrag, die Art der gemäß dem Schutzklassenkonzept verarbeiteten Daten sowie die Kategorien betroffener Personen festgelegt.

**Umsetzungshinweise**

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

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen Vertragsentwurf mit diesen Angaben vorhält und ein Verfahren implementiert hat, wonach der Vertrag mit diesen Festlegungen geschlossen wird. Durch eine Dokumentationsprüfung oder eine Dienstnutzung ist zu prüfen, ob alle im Vertrag enthaltenen Angaben dem Cloud-Nutzer auf geeignete Weise kommuniziert werden.

### Nr. 1.4 – Weisungsbefugnisse des Cloud-Nutzers (Art. 28 Abs. 3 Satz 2 lit. a DSGVO)

**Kriterium**

(1) Der Cloud-Vertrag sieht vor, dass die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet werden.

(2) Wird im Rahmen standardisierter Massengeschäfte kein individueller Cloud-Vertrag 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 DSGVO an mehreren Stellen genannt (Art. 28 Abs. 3 Satz 2 lit. a; Art. 28 Abs. 3 Satz 3; indirekt in Art. 28 Abs. 10 (Auftragsexzess) und in Art. 29, Art. 32 Abs. 4).

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

**Umsetzungshinweis**

Es sollte aus dem Cloud-Vertrag genau hervorgehen, welche Personen zur Erteilung von Weisungen befugt sind und wer auf Seiten des Cloud-Anbieters mit der Entgegennahme der Weisungen betraut ist. Die zu Weisungen befugten Personen können namentlich im Cloud-Vertrag benannt und deren Authentifizierungsmittel festgelegt werden.

Bei standardisierten Cloud-Diensten werden Weisungen des Cloud-Nutzers häufig mittels Softwarebefehlen automatisiert ausgeführt (bspw. durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeileneingabe), weshalb es erforderlich ist, dass diese Nutzerinteraktionen auch automatisiert protokolliert oder dokumentiert werden.

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

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er bei einer Dokumentenprüfung zeigt, dass er die Weisungserteilung vertraglich vereinbart hat, und durch testweise Dienstnutzung, dass er die Einzelweisungen schriftlich oder in einem elektronischen Format dokumentiert. Weisungen durch Softwarebefehle und ihre Protokollierung kann er durch eine technische Dokumentation und durch Dienstnutzung nachweisen.

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

**Kriterium**

(1) Im Cloud-Vertrag wird festgelegt, in welchen Staaten der Cloud-Anbieter die Daten des Cloud-Nutzers verarbeitet, insbesondere wo sie gespeichert werden.

(2) Sollte sich während des Vertragszeitraums der Ort der Verarbeitung aus Gründen, die im Verantwortungsbereich des Cloud-Anbieters liegen oder für beide Parteien unvorhersehbar sind, ändern, teilt der Cloud-Anbieter diese Änderung dem Cloud-Nutzer unverzüglich mit.

(3) Bei jeder wesentlichen Abweichung von der Festlegung des Ortes der Datenverarbeitung wird dem Cloud-Nutzer im Vertrag ein sofortiges Kündigungsrecht eingeräumt.

**Umsetzungshinweis**

Der Cloud-Vertrag sollte festlegen, dass die Datenverarbeitung im Rahmen der beabsichtigten Auftragsverarbeitung tatsächlich oder potentiell in der EU oder in einem anderen Staat stattfindet und diesen benennen.

Bei Massengeschäften muss ein Kommunikationsprozess, möglichst unterstützt durch ein automatisiertes Informationssystem innerhalb des Dienstes, mindestens jedoch auf der Website des Cloud-Anbieters, eingerichtet werden, wodurch der Cloud-Nutzer bei Ortsänderungen die hinreichende Möglichkeit der Kenntnisnahme erhält.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen Vertragsentwurf mit diesen Angaben vorhält und ein Verfahren implementiert hat, wonach der Vertrag mit diesen Festlegungen geschlossen wird. Hier ist durch eine Dokumentationsprüfung und eine testweise Dienstnutzung zu prüfen, ob alle notwendigen Informationen zur Ortsänderung dem Cloud-Nutzer auf geeignete Weise kommuniziert werden (können).

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

**Kriterium**

(1) Der Cloud-Anbieter verpflichtet sich im Cloud-Vertrag, dass die zur Verarbeitung von personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet werden, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Der Cloud-Anbieter verpflichtet sich, die Verpflichtung zu dokumentieren. Ein organisatorisches Verfahren zur Vornahme der Verpflichtung ist einzurichten und zu dokumentieren.

(3) Bei Änderungen der Zugriffs- und Verarbeitungsbefugnisse ist die Verpflichtungserklärung zu erneuern oder entsprechend anzupassen.

**Umsetzungshinweis**

Die Verpflichtung zur Vertraulichkeit und die Belehrung zur Verschwiegenheit müssen vor Aufnahme der datenverarbeitenden Tätigkeit erfolgen, um das Gewährleistungsziel der Vertraulichkeit (SDM 6.2.3) von vornherein sicherzustellen.

Den Personen (= Mitarbeitern des Cloud-Anbieters) sollte der Cloud-Anbieter eine Ausfertigung des Verpflichtungstextes mitsamt den Hinweisen auf die möglichen 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 immer wieder sensibilisieren. In der Dokumentation des Verfahrens sollte der Cloud-Anbieter 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. Die Hinweise aus DIN EN ISO/IEC 27002:2017 Ziff. 13.2.4 sind anwendbar.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er Belehrungen und Verpflichtungen sowie die zugehörigen Verfahren und Zuständigkeiten dokumentiert. Die Einhaltung dieser Vorgaben in allen Prozesskonstellationen ist durch repräsentativ stichprobenartige Interviews zu überprüfen.

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

**Kriterium**

(1) Die Schutzklasse und die für sie zu treffenden TOM werden im Cloud-Vertrag oder in den Anlagen hierzu festgelegt.

(2) Der Cloud-Vertrag enthält die Angabe, ob der Cloud-Anbieter oder der Cloud-Nutzer eine, Pseudonymisierung, Anonymisierung oder Verschlüsselung (Nr. 2.8, Nr. 2.9 und Nr. 2.10) der zu verarbeitenden personenbezogenen Daten vornimmt.

(3) Der Cloud-Anbieter legt im Cloud-Vertrag fest, auf welchem Niveau und in welchem Zeitraum er nach einem physischen oder technischen Zwischenfall die Daten des Cloud-Nutzers wiederherstellen und dem Cloud-Nutzer Zugang zu ihnen gewährleistet kann (Nr. 2.12).

(4) Der Cloud-Vertrag 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. 5, bei der Durchführung einer Datenschutz-Folgenabschätzung gemäß Nr. 6 und zur Erfüllung der Meldepflicht bei Datenschutzverletzungen nach Nr. 7.1 werden im Cloud-Vertrag festgelegt.

**Umsetzungshinweis**

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

Die Vorgaben des Art. 28 Abs. 3 Satz 2 lit. d sollten im Cloud-Vertrag präzisiert werden, so dass ihre Einhaltung für den Cloud-Nutzer leicht überprüfbar ist.

Bei der Festlegung der Unterstützungspflichten des Cloud-Anbieters im Cloud-Vertrag sollen diese unter Berücksichtigung der Ausgestaltung des konkreten Cloud-Dienstes und der dem Cloud-Anbieter zumutbaren und geeigneten TOM konkretisiert werden. Damit sollen Unsicherheiten hinsichtlich der sich aus dem Vertrag ergebenden Rechte und Pflichten vermieden werden.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen Vertragsentwurf mit diesen Angaben vorhält und ein Verfahren implementiert hat, wonach der Vertrag mit diesen Festlegungen geschlossen wird. Durch eine Dokumentationsprüfung und eine testweise Dienstnutzung ist zu prüfen, ob alle im Vertrag enthaltenen Festlegungen dem Cloud-Nutzer auf geeignete Weise kommuniziert werden.

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

**Kriterium**

Im Cloud-Vertrag werden die Pflichten des Cloud-Anbieters zur Rückgabe von Datenträgern, zur Rückführung von Online-Daten und zur Löschung von Daten nach Ende der Auftragsverarbeitung festgelegt.

**Umsetzungshinweis**

Dies kann auch durch Verweis auf entsprechende Grundsätze des Cloud-Anbieters erfolgen. Der Cloud-Nutzer kann zwischen den Abwicklungsmodalitäten wählen. Die Pflichten des Cloud-Anbieters entfallen, wenn er eine Pflicht zur Speicherung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten hat. Die Umsetzungshinweise aus DIN EN ISO/IEC 27040:2017-03 Ziff. 6.8.1 sowie DIN EN ISO/IEC 27002:2017, Ziff. 8.3 sind anwendbar.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen Vertragsentwurf mit diesen Festlegungen vorhält (Dokumentationsprüfung) und ein Verfahren implementiert hat (testweise Dienstnutzung), wonach der Vertrag mit diesen Festlegungen geschlossen wird.

### Nr. 1.9 – Form des Vertrages (Art. 28 Abs. 9 DSGVO)

**Kriterium**

Der Vertrag ist schriftlich oder in einem elektronischen Format abzufassen.

**Umsetzungshinweis**

Im Rahmen der Vertragserstellung können die Vorgaben aus DIN ISO/IEC 19086-1:2018 Rahmenwerk zur Dienstgütevereinbarung (SLA) – Informationstechnik – Cloud Computing einbezogen werden.

**Nachweis**

Der Cloud-Anbieter kann die Erfüllung des Kriteriums durch eine Dokumentation eines Vertragsentwurfs und eines Verfahrens, wonach der Vertrag in der schriftlichen oder speicherbaren Form abgeschlossen wird, nachweisen. Im Rahmen einer Dokumentationsprüfung oder testweisen Dienstnutzung ist zu prüfen, ob geeignete organisatorische oder technische Verfahren vorhanden sind, die eine schriftliche oder elektronische Vertragsversion verfügbar machen.

# Kapitel II: Rechte und Pflichten des Cloud-Anbieters

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

### Nr. 2.1 – Risiko- und Schutzkonzept (Art. 24, 25, 28, 32, 35 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

**Kriterium**

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

(2) Im Risiko- und Schutzkonzept stellt der Cloud-Anbieter die von ihm ergriffenen Datensicherheitsmaßnahmen dar und schildert auch die Abwägungen, die er vorgenommen hat, um zu diesen Maßnahmen zu gelangen.

(3) Das Risiko- und Schutzkonzept ist schriftlich zu dokumentieren und in regelmäßigen Abständen auf Aktualität und Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren.

(4) Das Risiko- und Schutzkonzept grenzt die Verantwortung des Cloud-Anbieters von der Verantwortlichkeit der Cloud-Nutzer ab.

(5) Soweit das Risiko- und Schutzkonzept Sicherheitsmaßnahmen des Cloud-Nutzers verlangt, sind diese dem Cloud-Nutzer in Schriftform oder in einem elektronischen Format mitzuteilen.

**Erläuterung**

Der Cloud-Anbieter hat risikoangemessene TOM festzulegen, um Risiken einer Verletzung der Rechte und Freiheiten von natürlichen Personen zu verhindern. Insbesondere hat er Risiken gegen unbeabsichtigte und unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugten Zugang zu personenbezogenen Daten auszuschließen oder zu minimieren. Bei der Festlegung der konkreten Maßnahmen berücksichtigt er nicht nur die Modalitäten der Verarbeitung und die Eintrittswahrscheinlichkeit und Schwere des Schadens, sondern auch den Stand der Technik sowie die Implementierungskosten der Maßnahmen. Die dabei getroffenen Abwägungen müssen aus dem Risiko- und Schutzkonzept ersichtlich sein. Der Cloud-Nutzer ermittelt den Schutzbedarf für seine Datenverarbeitung und legt dafür eine Schutzbedarfsklasse fest. 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 Risiko- und Schutzkonzept soll die sich aus den spezifischen Umständen des Cloud-Dienstes, seiner Datenverarbeitungsvorgänge und Räumlichkeiten ergebenden Risiken abdecken und zu jedem Risiko eine oder gegebenenfalls mehrere Schutzmaßnahmen beinhalten sowie Ressourcen, Verantwortlichkeiten und Priorisierungen für den Umgang mit Informationssicherheitsrisiken spezifizieren. Alle identifizierten Restrisiken des Cloud-Dienstes, die nicht vollständig behandelt werden können, sollten von der Geschäftsleitung des Cloud-Service-Anbieters zur Kenntnis genommen werden. Der Risikobewertungsansatz und die Risikobewertungsmethodik des Cloud-Service-Anbieters sollten dokumentiert werden.

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

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

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

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

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

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

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

**Nachweis**

Das Risiko- und Schutzkonzept und seine Angemessenheit kann der Cloud-Anbieter dadurch nachweisen, dass er dieses vorlegt (Dokumentenprüfung). Die Angemessenheit der einzelnen darin genannten TOM und ihre Umsetzung werden nach den nachfolgenden Nummern des Katalogs geprüft.

### Nr. 2.2 – Kooperation der Beauftragten für Informationssicherheit und für Datenschutz (Art. 32 DSGVO i.V.m. Art. 37-39 DSGVO)

**Kriterium**

Der Cloud-Anbieter stellt sicher, dass ein bestellter Informationssicherheitsbeauftragter mit einem benannten Datenschutzbeauftragten eng kooperiert.

**Umsetzungshinweis**

Sofern der Cloud-Anbieter einen Beauftragten für Informationssicherheit bestellt hat, muss dieser auch die Einhaltung der datenschutzrechtlich gebotenen TOM sicherstellen.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er eine entsprechende Arbeitsanweisung vorlegt (Dokumentenprüfung). Die Kooperation kann durch Interviews mit dem Beauftragten für Informationssicherheit und dem Datenschutzbeauftragten überprüft werden.

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

**Kriterium**

Der Cloud-Anbieter hat durch risikoangemessene TOM sicherzustellen, dass sich Unbefugte keinen Zutritt zu Datenverarbeitungsanlagen verschaffen können, um unbefugte Kenntnisnahmen personenbezogener Daten und Einwirkungsmöglichkeiten auf die Datenverarbeitungsanlagen auszuschließen.

**Erläuterung**

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

**Umsetzungshinweise zu den Schutzklassen**

Die Umsetzungshinweise aus DIN EN ISO/IEC 27001:2017 Ziff. A.11; DIN EN ISO/IEC 27002:2017 Ziff. 11.1.2 und DIN ISO/IEC 27018:2017 Ziff. 11 sind anwendbar.

**Schutzklasse 1**

Der Cloud-Anbieter gewährleistet durch risikoangemessene TOM, dass Räume und Anlagen gegen Schädigung durch Naturereignisse gesichert werden und Unbefugte keinen Zuritt zu Räumen und Da-

tenverarbeitungsanlagen erhalten. So sollte der Zutritt ins Rechenzentrum über Videoüberwachungssysteme, Bewegungssensoren, Alarmsysteme und von geschultem Sicherheitspersonal permanent überwacht werden.

Die Maßnahmen müssen geeignet sein, um im Regelfall den Zutritt Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert (siehe DIN EN ISO/IEC 27001:2017 Ziff. A.11).

**Schutzklasse 2**

Für Schutzklasse 2 gilt darüber hinaus: Die Maßnahmen müssen auch geeignet sein, Schädigungen durch fahrlässige Handlungen Befugter im Regelfall auszuschließen. Weiterhin muss sichergestellt sein, dass unbefugter Zutritt durch fahrlässige und vorsätzliche Handlungen hinreichend sicher ausgeschlossen ist. Dies schließt Schutz gegen Zutrittsversuche durch Täuschung oder Gewalt ein. Es ist ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die ein unbefugter Zutritt im Regelfall (nachträglich) festgestellt werden kann, vorzusehen.

**Schutzklasse 3**

Für Schutzklasse 3 gilt darüber hinaus: Jeder Zutritt und jeder Zutrittsversuch kann festgestellt werden.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept die TOM zur Zutrittskontrolle darlegt (Dokumentationsprüfung). Die Implementierung von Maßnahmen und Einrichtungen (Assetprüfung) und der (fortlaufende) Betrieb von Zutrittskontrollen werden im Rahmen einer Vor-Ort-Prüfung durch repräsentative Stichproben festgestellt und auf Angemessenheit überprüft.

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

**Kriterium**

(1) Der Cloud-Anbieter hat sicherzustellen, dass Unbefugte keinen Zugang zu Datenverarbeitungsvorgängen erhalten und auf diese einwirken können.

(2) Die Anforderungen nach Abs. 1 gelten auch insbesondere für Sicherungskopien, soweit diese personenbezogene Daten enthalten.

(3) Die Erforderlichkeit der Berechtigungen für den Zugang zu Datenverarbeitungsanlagen sind in regelmäßigen Abständen auf Aktualität und Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren.

**Erläuterungen**

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

**Umsetzungshinweise zu den Schutzklassen**

Die Umsetzungshinweise aus DIN EN ISO/IEC 27001:2017 Ziff. 9 und DIN ISO/IEC 27018:2017 Ziff. 9 sind anwendbar.

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

**Schutzklasse 1**

Der Cloud-Anbieter gewährleistet durch risikoangemessene TOM, dass Unbefugte keinen Zugang zu Datenverarbeitungsvorgängen erhalten. Für Zugänge von Befugten über das Internet ist eine starke

Authentifizierung erforderlich, die mindestens zwei Elemente der Kategorie Wissen, Besitz oder Inhärenz verwendet, die insofern voneinander unabhängig sind, als die Überwindung eines Elements die Zuverlässigkeit des anderen nicht in Frage stellt, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten gewährleistet ist. Darüber hinaus sind VPN und verschlüsselte Verbindungen zu implementieren. Die Maßnahmen zur Zugangskontrolle müssen geeignet sein, um im Regelfall den Zugang zu Datenverarbeitungsvorgängen und 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 ist ein Mindestschutz vorzusehen, der diese erschwert.

**Schutzklasse 2**

Für Schutzklasse 2 gilt darüber hinaus: Gegen zu erwartenden vorsätzlichen unbefugten Zugang ist ein Schutz vorzusehen, der zu erwartende Zugangsversuche hinreichend sicher ausschließt. Dazu gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die ein unbefugter Zugang im Regelfall nachträglich festgestellt werden kann.

**Schutzklasse 3**

Für Schutzklasse 3 gilt darüber hinaus: Es muss sichergestellt sein, dass unbefugter Zugang zu Datenverarbeitungsvorgängen hinreichend sicher ausgeschlossen sind. Dies schließt regelmäßig Maßnahmen zur aktiven Erkennung von Angriffen ein. Jeder unbefugte Zugang und entsprechende Versuche müssen nachträglich festgestellt werden können.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept die TOM zur Zugangskontrolle darlegt (Dokumentationsprüfung). Ihre Implementierung und der Betrieb werden im Rahmen einer Vor-Ort-Prüfung durch repräsentative Stichproben festgestellt und auf Angemessenheit überprüft. Wird ein Fernzugang über das Internet ermöglicht, so wird dieser gesondert auf Sicherheit und Angemessenheit geprüft.

### Nr. 2.5 – Zugriffskontrolle (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

**Kriterium**

(1) Der Cloud-Anbieter stellt durch TOM sicher, dass Berechtigte nur im Rahmen ihrer Berechtigungen Zugriff auf Datenverarbeitungsvorgänge nehmen können und unbefugte Einwirkungen auf Datenverarbeitungsvorgänge ausgeschlossen werden.

(2) Die Anforderungen nach Abs. 1 gelten auch insbesondere für Sicherungskopien, soweit sie personenbezogene Daten enthalten.

**Erläuterungen**

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

**Umsetzungshinweise zu den Schutzklassen**

Die Umsetzungshinweise aus DIN EN ISO/IEC 27002:2017 Ziff. 13.2 und DIN ISO/IEC 27018 Ziff. 9.2, 9.2.1, 9.4.2 sind anwendbar.

Berechtigungskonzepte müssen sowohl für die Nutzer des Dienstes als auch für die Mitarbeiter des Cloud-Anbieters bestehen. Die Erforderlichkeit der Berechtigungen ist in regelmäßigen Abständen auf Aktualität und Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren. Sämtliche relevanten Sicherheitsereignisse einschließlich aller Sicherheitslücken oder -vorfälle sollten erfasst, protokolliert, revisionssicher archiviert und ausgewertet werden.

**Schutzklasse 1**

Der Cloud-Anbieter gewährleistet durch risikoangemessene TOM, dass Berechtigte nur innerhalb ihrer Berechtigungen Zugriff auf personenbezogene Daten nehmen können. Zugriffe sind abzusichern und zu kontrollieren. Für Zugriffe von Befugten über das Internet ist eine starke Authentifizierung erforderlich, die mindestens zwei Elemente der Kategorie Wissen, Besitz oder Inhärenz verwendet, die insofern voneinander unabhängig sind, als die Überwindung eines Elements die Zuverlässigkeit des anderen nicht in Frage stellt, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten gewährleistet ist.

Insbesondere müssen administrative Zugriffe und Tätigkeiten auf kritischen Systemen durch einen entsprechend starken Authentisierungsmechanismus geschützt und protokolliert werden (bspw. das Löschen von Kundendaten). Die Fernadministration des Cloud-Dienstes sollte durch Mitarbeiter des Cloud-Anbieters über einen sicheren Kommunikationskanal erfolgen (bspw. der Benutzung eines VPN und verschlüsselte Verbindungen).

Die Maßnahmen müssen geeignet sein, 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 ist ein Mindestschutz vorzusehen, der diese erschwert.

**Schutzklasse 2**

Für Schutzklasse 2 gilt darüber hinaus: Gegen zu erwartende vorsätzliche unbefugte Zugriffe ist ein entsprechender Schutz vorzusehen, der solche potentiellen Zugriffsversuche hinreichend sicher ausschließt. Dazu gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die ein unberechtigter Zugriff im Regelfall nachträglich festgestellt werden kann.

**Schutzklasse 3**

Für Schutzklasse 3 gilt darüber hinaus: Es muss sichergestellt sein, dass unbefugte Zugriffe auf Daten hinreichend sicher ausgeschlossen sind. Dies schließt regelmäßig Maßnahmen zur aktiven Erkennung von Angriffen ein. Jeder unbefugte Zugriff und entsprechende Versuche müssen nachträglich festgestellt werden können.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept die TOM zur Zugriffskontrolle darlegt. Ihre Implementierung wird im Rahmen einer Vor-Ort-Prüfung durch repräsentative Stichproben festgestellt und auf Angemessenheit überprüft.

### Nr. 2.6 – Übertragung von Daten und Transportverschlüsselung (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

**Kriterium**

(1) Der Cloud-Anbieter setzt bei Datenübertragungen eine Transportverschlüsselung nach dem Stand der Technik oder gleichermaßen angemessene Maßnahmen ein, die geeignet sind zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

(2) Der Transport von Datenträgern ist mit TOM zu schützen, sodass personenbezogene Daten beim Transport der Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

(3) Der Cloud-Anbieter protokolliert die Übertragungsvorgänge und Transporte.

**Erläuterungen**

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

**Umsetzungshinweis zu den Schutzklassen**

Die Umsetzungshinweise aus DIN ISO/IEC 27018:2017 Ziff. 10.1.1, A.10.6, A.10.9; DIN EN ISO/IEC 27002:2017 Ziff. 10 und Ziff. 18.1.5; DIN EN ISO/IEC 27040:2017-03 Ziff. 6.7.1, Ziff. 7.7.1 sind anwendbar.

**Schutzklasse 1**

Der Cloud-Anbieter gewährleistet durch risikoangemessene TOM, dass Unbefugte personenbezogene Daten bei der Übertragung oder ihrem Transport nicht lesen, kopieren, verändern oder entfernen können. Im Regelfall ist eine Transportverschlüsselung nach dem Stand der Technik einzusetzen.

Die Maßnahmen müssen geeignet sein, um 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 auszuschließen. Die Maßnahmen müssen ferner geeignet sein, die fahrlässige Weitergabe von Daten an Unbefugte durch den Cloud-Anbieter und seine Mitarbeiter im Regelfall auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert. Es muss dokumentiert sein, an welche Empfänger eine Weitergabe personenbezogener Daten durchgeführt wurde. Datenübertragungen, auch solche vom und an den Cloud-Nutzer oder an Subauftragsverarbeiter, müssen automatisiert protokolliert werden. Diese Anforderungen gelten auch für die Übertragung von Daten im eigenen Netzwerk des Cloud-Anbieters und seiner Subauftragsverarbeiter und zwischen diesen.

**Schutzklasse 2**

Für Schutzklasse 2 gilt darüber hinaus: Gegen vorsätzliches unbefugtes Lesen, Kopieren, Verändern oder Entfernen ist ein Schutz vorzusehen, der zu erwartende Versuche hinreichend sicher ausschließt. Dazu 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. Bei verschlüsselter Übertragung sind die Schlüssel sicher aufzubewahren.

**Schutzklasse 3**

Für Schutzklasse 3 gilt darüber hinaus: Es muss sichergestellt sein, dass unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Daten durch den Cloud-Anbieter, seine Mitarbeiter oder Dritte hinreichend sicher ausgeschlossen ist. Dies schließt regelmäßig Maßnahmen zur aktiven Erkennung und Abwehr von Angriffen ein. Jedes unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten und auch jeder entsprechende Versuch müssen nachträglich festgestellt werden können. Bei verschlüsselter Übertragung ist durch TOM sicherzustellen, dass der Cloud-Anbieter und seine Mitarbeiter keinen Zugriff auf die Schlüssel haben.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept die TOM zur Übertragungskontrolle darlegt (Dokumentationsprüfung). Ihre Implementierung wird durch eine technische Prüfung (bspw. Testen auf Verschlüsselung der Verbindung) oder im Rahmen einer Vor-Ort-Prüfung durch repräsentative Stichproben festgestellt und auf Angemessenheit überprüft.

### Nr. 2.7 – Nachvollziehbarkeit der Datenverarbeitung (Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. c, e und f DSGVO)

**Kriterium**

Der Cloud-Anbieter hat durch Maßnahmen, die der Schutzbedürftigkeit der verarbeiteten Daten nach dem Schutzklassenkonzept angemessen sind, sicherzustellen, dass Eingaben, Veränderungen und Löschungen personenbezogener Daten protokolliert werden, um eine nachträgliche Prüfbarkeit und Nachvollziehbarkeit der Datenverarbeitung sicherzustellen. Bei Protokollierungen sind die Grundsätze der Erforderlichkeit, Zweckbindung und Datenminimierung zu beachten.

**Erläuterung**

Das Kriterium der Nachvollziehbarkeit konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Integrität, Vertraulichkeit und Verfügbarkeit (SDM 6.2.1 – 6.2.3) von personenbezogenen Daten und Diensten auf

Dauer sicherzustellen und personenbezogene Daten gegen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugten Zugang oder unbefugte Offenlegung zu schützen. Hierzu muss nachträglich überprüft und festgestellt werden können, ob, wann und von wem und mit welchen inhaltlichen Auswirkungen personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, um gegebenenfalls Zugriffsrechte für die Zukunft anders zu gestalten. Die Protokolldaten müssen sicher aufbewahrt werden, damit sie als Nachweis zur Verfügung stehen. Zusätzlich ist zu beachten, 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 Zweckbindung und der Datenminimierung aus Art. 5 Abs. 1 lit. b und c DSGVO ist besonders zu achten.

**Umsetzungshinweise zu den Schutzklassen**

Die Umsetzungshinweise aus DIN ISO/IEC 27018-2017 Ziff. 12.4.1, 12.4.2 und DIN EN ISO/IEC 27002:2017 Ziff. 12.4 sind anwendbar.

**Schutzklasse 1**

Der Cloud-Anbieter gewährleistet durch risikoangemessene TOM, dass nachträglich überprüft und festgestellt werden kann, ob, wann, von wem und mit welchen inhaltlichen Auswirkungen personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die Maßnahmen müssen geeignet sein, um Dateneingaben, -veränderungen oder -löschungen, die bei der bestimmungsgemäßen Nutzung des Dienstes durch den Cloud-Nutzer wie bei administrativen Maßnahmen des Cloud-Anbieters erfolgen, jederzeit nachvollziehen zu können.

Die dafür eingesetzten Maßnahmen, etwa Protokollierung der administrativen Aktivitäten und der Nutzer-Aktivitäten, müssen so gestaltet sein, 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 fahrlässigen Handlungen des Cloud-Nutzers oder Dritter gewahrt bleibt. Gegen vorsätzliche Manipulationen an den Maßnahmen zur Nachvollziehbarkeit ist ein Mindestschutz vorzusehen, der diese Manipulationen erschwert.

**Schutzklasse 2**

Für Schutzklasse 2 gilt darüber hinaus: Gegen zu erwartende vorsätzliche Manipulationen der Protokollierungsinstanzen und gegen vorsätzlichen Zugriff auf oder Manipulationen von Protokollierungsdateien (Logs) durch Unbefugte ist ein Schutz vorzusehen, der solche potentiellen Manipulationsversuche hinreichend und sicher ausschließt. Dazu gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die eine Manipulation im Regelfall (nachträglich) festgestellt werden kann.

**Schutzklasse 3**

Für Schutzklasse 3 gilt darüber hinaus: Es muss sichergestellt sein, dass Manipulationen von Protokollierungsinstanzen und -dateien (Logs) hinreichend sicher ausgeschlossen sind. Dies schließt regelmäßig Maßnahmen zur aktiven Erkennung von Manipulationen ein. Jede Manipulation und möglichst auch jeder entsprechende Versuch müssen nachträglich festgestellt werden können.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept dokumentiert, wie er durch Festlegung von Gegenstand und Umfang der Protokollierung, Aufbewahrung, Integritätsschutz und Löschung von Protokollen und der Verwendung der Protokolldaten die Datenschutzziele sicherstellt (Dokumentationsprüfung). Die Implementierung dieses Protokollierungskonzepts wird durch repräsentative Stichproben im Rahmen des laufenden Betriebs festgestellt und auf Angemessenheit überprüft. Die angemessene Protokollierung kann mittels einer technischen Prüfung nachgewiesen werden.

## Nr. 2.8 – Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO)

### Kriterium

Soweit der Cloud-Anbieter einen Dienst anbietet, der eine Pseudonymisierung personenbezogener Daten umfasst, hat er sicherzustellen, dass er auf Weisung des Cloud-Nutzers personenbezogene Daten pseudonymisieren kann. Bei der Pseudonymisierung hat der Cloud-Anbieter sicherzustellen, dass die zusätzlichen Informationen zur Identifizierung der betroffenen Person gesondert aufbewahrt werden und TOM unterliegen, die eine Zuordnung zur betroffenen Person und damit ihre Re-Identifizierung gegenüber Dritten verhindern.

### Erläuterung

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

### Umsetzungshinweise

Der Cloud-Anbieter hat zu prüfen, ob es bereichsspezifische technische Standards für die Pseudonymisierung gibt, die als verpflichtend vorgeschrieben sind oder empfohlen werden. Der Cloud-Anbieter sollte öffentlich bekannt geben, welche dieser technischen Standards sein Pseudonymisierungsverfahren erfüllt. Beispielsweise kann zur Pseudonymisierung in der Medizinischen Informatik DIN EN ISO 25237:2017 herangezogen werden.

### Umsetzungshinweise zu den Schutzklassen

#### Schutzklasse 1

Der Cloud-Anbieter bietet selbst keinen Pseudonymisierungsdienst an, ermöglicht es dem Cloud-Nutzer jedoch, die von diesem selbst pseudonymisierten Daten zu verarbeiten.

#### Schutzklasse 2

Der Cloud-Anbieter hat sicherzustellen, dass die Daten pseudonymisiert verarbeitet werden. Entsprechend der vertraglichen Vereinbarung (Nr. 1.7) pseudonymisiert der Cloud-Nutzer die personenbezogenen Daten selbst oder der Cloud-Anbieter führt die Pseudonymisierung durch. Wird die Pseudonymisierung vom Cloud-Anbieter durchgeführt, so stellt dieser sicher, dass nur der Cloud-Nutzer Zugang zum Datensatz mit den Identifizierungsdaten hat. Der Datensatz mit der Zuordnung des Kennzeichens zu einer Person muss so geschützt werden, dass zu erwartende Manipulationsversuche hinreichend und sicher ausgeschlossen werden. Der Cloud-Anbieter gewährleistet darüber hinaus, dass er die technische Entwicklung im Bereich der Pseudonymisierungsverfahren laufend verfolgt und seine Verfahren den aktuellen technischen Empfehlungen (best practice) entsprechen.

#### Schutzklasse 3

Der Cloud-Anbieter verfügt über einen Dienst, der die Verarbeitung von durch den Cloud-Nutzer pseudonymisierten Daten ermöglicht. Der Cloud-Anbieter hat keinen Zugang zu den Identifizierungsdaten.

### Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept dokumentiert, wie er selbst Pseudonymisierungen durchführt, Identifizierungsdaten sicher aufbewahrt und pseudonymisierte Daten verarbeitet. Die Implementierung der Pseudonymisierungsverfahren wird durch repräsentative Stichproben festgestellt und auf Angemessenheit überprüft. Ebenso wird die korrekte Verarbeitung der pseudonymen Daten festgestellt.

### Nr. 2.9 – Anonymisierung (Art. 5 Abs. 1 lit. c DSGVO)

**Kriterium**

Soweit der Cloud-Anbieter einen Dienst anbietet, der eine Anonymisierung personenbezogener Daten umfasst, hat er sicherzustellen, dass er auf Weisung des Cloud-Nutzers personenbezogene Daten anonymisieren kann. Die Anonymisierung muss nach dem Stand der Technik eine Re-Identifizierung der betroffenen Person ausschließen.

**Erläuterung**

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

**Umsetzungshinweise**

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

**Umsetzungshinweise zu den Schutzklassen**

**Schutzklasse 1**

Der Cloud-Anbieter bietet selbst keinen Anonymisierungsdienst an, ermöglicht es dem Nutzer jedoch, die von diesem pseudonymisierten Daten zu verarbeiten.

**Schutzklasse 2 und 3**

Soweit mit dem Cloud-Nutzer vereinbart (Nr. 1.7), stellt der Cloud-Anbieter sicher, dass die Daten anonymisiert verarbeitet werden. Entsprechend der vertraglichen Vereinbarung anonymisiert der Cloud-Nutzer oder der Cloud-Anbieter die personenbezogenen Daten. Der Cloud-Anbieter gewährleistet, dass er die technische Entwicklung im Bereich der Anonymisierungsverfahren laufend verfolgt und seine Verfahren den aktuellen technischen Empfehlungen (best practice) entsprechen.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept dokumentiert, wie er selbst Anonymisierungen durchführt und anonymisierte Daten verarbeitet. Die Implementierung der Anonymisierungsverfahren wird durch repräsentative Stichproben festgestellt und auf Angemessenheit überprüft.

### Nr. 2.10 – Verschlüsselung gespeicherter Daten (Art. 32 Abs. 1 lit. a DSGVO)

**Kriterium**

Soweit der Cloud-Anbieter bei Schutzklasse 2 oder 3 einen Dienst anbietet, der eine Verschlüsselung gespeicherter personenbezogener Daten umfasst, hat er sicherzustellen, dass dem Cloud-Nutzer die Verschlüsselung personenbezogener Daten ermöglicht wird oder der Cloud-Anbieter selbst auf Weisung des Cloud-Nutzers personenbezogene Daten verschlüsseln kann. Der Cloud-Anbieter hat dabei Verschlüsselungstechniken nach dem Stand der Technik einzusetzen. Er hat die Geeignetheit des Verfahrens fortdauernd zu prüfen und es gegebenenfalls zu aktualisieren.

**Erläuterung**

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

**Umsetzungshinweise**

Der Stand der Technik ergibt sich aus aktuellen technischen Normen für kryptographische Verfahren und deren Anwendung. Die Umsetzungshinweise aus DIN ISO/IEC 27018:2017 Ziff. 10 sind anwendbar.

**Umsetzungshinweise zu den Schutzklassen**

**Schutzklasse 1**

Der Cloud-Anbieter ist nicht verpflichtet, selbst Verschlüsselungsverfahren für die verschlüsselte Speicherung von Daten anzubieten, jedoch muss er dem Cloud-Nutzer die verschlüsselte Speicherung von Daten ermöglichen und die technische Entwicklung im Bereich der Verschlüsselung verfolgen.

**Schutzklasse 2**

Der Cloud-Anbieter bietet Verschlüsselungsverfahren an, um dem Cloud-Nutzer die verschlüsselte Speicherung von Daten zu ermöglichen oder auf dessen Weisung hin, die Daten selbst zu verschlüsseln. Der Cloud-Anbieter verfolgt laufend die technische Entwicklung im Bereich der Verschlüsselung. Die von ihm getroffenen Maßnahmen entsprechen den aktuellen technischen Empfehlungen (best practice). Er überprüft die angemessene Implementierung der Maßnahmen durch geeignete Tests und dokumentiert diese.

**Schutzklasse 3**

Personenbezogene Daten der Schutzklasse 3 werden vom Cloud-Nutzer verschlüsselt. Die Schlüssel werden bei diesem sicher aufbewahrt. Der Cloud-Anbieter unterstützt den Cloud-Nutzer bei der Verschlüsslung und Entschlüsselung der Daten, ohne den Schlüssel zu kennen. Er verfolgt die technische Entwicklung im Bereich der Verschlüsselung und hält seine unterstützenden Maßnahmen auf dem Stand der aktuellen technischen Empfehlungen (best practice).

**Nachweis**

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

### Nr. 2.11 – Getrennte Verarbeitung (Art. 5 Abs. 1 lit. b i.V.m. Art. 24, 25, 32 Abs. 1 lit. b und Abs. 2 DSGVO)

**Kriterium**

(1) Der Cloud-Anbieter gewährleistet durch geeignete TOM, dass Daten von unterschiedlichen Cloud-Nutzern getrennt verarbeitet werden.

(2) Der Cloud-Anbieter gewährleistet durch geeignete TOM, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

**Erläuterung**

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

**Umsetzungshinweise zu den Schutzklassen**

Die Umsetzungshinweise aus DIN EN ISO/IEC 27002:2017 Ziff. 12.1.4, 13.1.3 sind anwendbar.

**Schutzklasse 1**

Der Cloud-Anbieter gewährleistet durch risikoangemessene TOM, dass die Daten des Cloud-Nutzers von den Datenbeständen anderer Cloud-Nutzer und von anderen Datenbeständen des Cloud-Anbieters logisch oder physisch getrennt verarbeitet werden und dass der Cloud-Nutzer die Datenverarbeitung nach verschiedenen Verarbeitungszwecken trennen kann, um die Daten vor unbefugtem Zugang, Veränderungen und Vernichtung zu schützen und eine Verkettung der Daten zu verhindern (sichere Mandantentrennung). Die Maßnahmen müssen so gestaltet sein, dass die Datentrennung 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. Es ist ein Mindestschutz vorzusehen, der vorsätzliche Verstöße gegen das Trennungsgebot verhindert.

**Schutzklasse 2**

Für Schutzklasse 2 gilt darüber hinaus: Der Cloud-Anbieter gewährleistet, dass gegen zu erwartende vorsätzliche Verstöße ein Schutz besteht, der diese hinreichend sicher ausschließt. Dazu gehören im Rahmen von Datenspeicherung die Verschlüsselung mit getrennten Schlüsseln und die Verwendung getrennter Betriebsumgebungen für verschiedene Verarbeitungen oder der Einsatz gleichwertiger Verfahren. Weiterhin sind Maßnahmen zu ergreifen, durch die vorsätzliche Verstöße gegen das Trennungsgebot im Regelfall (nachträglich) festgestellt werden können, z.B. durch Protokollierung der Zugriffe.

**Schutzklasse 3**

Für Schutzklasse 3 gilt darüber hinaus: Der Cloud-Anbieter stellt sicher, dass eine Verletzung der Datentrennung hinreichend sicher ausgeschlossen ist. Dazu gehören im Rahmen von Datenspeicherung die Verschlüsselung mit getrennten Schlüsseln und die Verwendung getrennter Betriebsumgebungen für verschiedene Verarbeitungen. Es ist zudem ein Verfahren zur Erkennung von Missbräuchen vorgesehen.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept dokumentiert, welche TOM er ergriffen hat, um die Daten unterschiedlicher Nutzer sicher voneinander zu trennen und die Daten eines Nutzers nach den Verarbeitungszwecken trennen zu können (Dokumentationsprüfung). Die Implementierung der Mandanten- und Zwecktrennung wird durch technische Prüfungen (z.B. Penetrationstests) festgestellt und auf Angemessenheit überprüft.

### Nr. 2.12 – Wiederherstellbarkeit nach physischem oder technischem Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO)

**Kriterium**

(1) Der Cloud-Anbieter gewährleistet durch risikoangemessene TOM, dass die Daten innerhalb der im Cloud-Vertrag angegebenen Zeiten wiederhergestellt werden können.

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

**Erläuterung**

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

**Umsetzungshinweis**

Da die Verfügbarkeit von personenbezogenen Daten nicht notwendigerweise mit ihrer Schutzbedürftigkeit nach dem Schutzklassenmodell 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 Schutzklassen unterschieden. Stattdessen wird die Möglichkeit der Wiederherstellung in den Wiederherstellbarkeitsniveaus „normale Widerherstellbarkeit“, „hohe Wiederherstellbarkeit“ und „sehr hohe Wiederherstellbarkeit“ 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.

Die Umsetzungshinweise aus DIN ISO/IEC 27018:2017 Ziff. 12.3.1, A.10.3 sowie aus DIN EN ISO/IEC 27002:2017 Ziff. 16 sind anwendbar. Der Cloud-Anbieter sollte ein etabliertes und getestetes Datensicherungskonzept erstellen, in dem er ein System zur Datensicherung, ein Notfallmanagement, Pläne zur Wiederherstellung und zur Schadensbegrenzung sowie einen Plan zur regelmäßigen Überprüfung und Aktualisierung der vorgesehenen Maßnahmen vorsieht.

**Normale Wiederherstellbarkeit**

Es ist ein Schutz zu gewährleisten, der gegen zu erwartende, naheliegende Ereignisse so zuverlässig absichert, dass diese Risiken bei normalem Verlauf nicht zu endgültigem Datenverlust führen. „Zu erwartend, naheliegend“ sind Ereignisse, die nicht vorkommen sollen, nach der Lebenserfahrung aber trotz hinreichender Vorsicht nicht ausgeschlossen werden können und „immer wieder einmal“ vorkommen, wie etwa Unfälle im Straßenverkehr oder dem technischen Defekt von Hardware.

**Hohe Wiederherstellbarkeit**

Es ist ein Schutz zu gewährleisten, der gegen seltene Ereignisse so zuverlässig absichert, dass diese Risiken bei normalem Verlauf der Datenverarbeitung nicht zu endgültigem Datenverlust führen. „Selten“ sind Ereignisse, die nicht vorkommen sollen und nach der Lebenserfahrung bei hinreichender Vorsicht „praktisch nie“ vorkommen, aber gleichwohl in einigen Fällen zu beobachten sind, wie etwa „Jahrhunderthochwasser“ oder gezielte, umfangreiche Angriffe auf den Cloud-Dienst oder ein plötzlich erhöhtes Zugriffsvolumen.

**Sehr hohe Widerherstellbarkeit**

Es ist ein hoher Schutz zu gewährleisten, der außergewöhnliche, aber nicht auszuschließende Ereignisse so zuverlässig absichert, dass diese Risiken bei normalem Verlauf der Datenverarbeitung nicht zu endgültigem Datenverlust führen. „Außergewöhnlich, aber nicht als theoretisch auszuschließen“ sind Ereignisse, die 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.

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

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept dokumentiert, mit welchen Ereignissen er sich auseinandergesetzt hat, die zu einem physischen, organisatorischen oder technischen Zwischenfall führen können, ob sein Cloud-Dienst normale, hohe oder sehr hohe Wiederherstellbarkeit gewährleistet und welche konkreten Maßnahmen zur Wiederherstellbarkeit der Daten nach einem Zwischenfall er ergriffen hat. Die Implementierung der geeigneten TOM wird durch repräsentative Stichproben festgestellt und auf Angemessenheit überprüft.

### Nr. 3 – Weisungsbefolgungspflicht des Cloud-Anbieters (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 risikoangemessene Maßnahmen, dass die Verarbeitung der Daten des Cloud-Nutzers nur nach Maßgabe der Weisungen des Cloud-Nutzers erfolgt.

(3) Sollte der Cloud-Anbieter einen Auftragsverarbeiter heranziehen, hat er sicherzustellen, dass auch der Subauftragsverarbeiter und seine Mitarbeiter die Datenverarbeitung ausschließlich gemäß der Weisung des Cloud-Nutzers ausführen.

(4) Im Rahmen von standardisierten Cloud-Diensten 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**

Der Cloud-Anbieter unterweist alle Mitarbeiter, deren Tätigkeiten im Zusammenhang mit der Verarbeitung von personenbezogenen Daten stehen, in die vertraglich dokumentierten Weisungen (Art. 29 DSGVO) und stellt auch in einer etwaigen Datenverarbeitungskette die Weisungsbefolgung sicher (s. hierzu noch die Kriterien in Nr. 9 (Subauftragsverarbeitung)). Der Cloud-Anbieter hat regelmäßig zu kontrollieren, ob die Weisungen des Cloud-Nutzers eingehalten werden.

In standardisierten Cloud-Diensten werden Weisungen des Cloud-Nutzers insbesondere mittels Softwarebefehlen häufig automatisiert ausgeführt (z.B. durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeileneingabe), weshalb es erforderlich ist, dass diese Nutzerinteraktionen auch automatisiert protokolliert oder dokumentiert werden.

**Umsetzungshinweise zu den Schutzklassen**

**Schutzklasse 1**

Der Cloud-Anbieter gewährleistet durch risikoangemessene TOM, dass die Verarbeitung der Daten des Cloud-Nutzers nur nach Maßgabe von dessen Weisungen erfolgt.

Die Maßnahmen müssen geeignet sein, um im Regelfall Abweichungen von den Weisungen aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen. Gegen vorsätzliche Manipulationen von Weisungen ist ein Mindestschutz vorzusehen, der diese erschwert.

**Schutzklasse 2**

Für Schutzklasse 2 gilt darüber hinaus: Die Maßnahmen müssen ein Abweichen von den Weisungen durch zu erwartende vorsätzliche Eingriffe hinreichend sicher ausschließen und sicherstellen, dass Eingriffe im Regelfall (nachträglich) festgestellt werden können.

**Schutzklasse 3**

Für Schutzklasse 3 gilt darüber hinaus: Es muss sichergestellt sein, dass Abweichungen von den Weisungen des Cloud-Nutzers hinreichend sicher ausgeschlossen sind. Dies schließt regelmäßig eine umfassende Protokollierung von Administratorenzugriffen ein sowie Maßnahmen, die Eingriffe in die zu verarbeitenden Daten und Datenverarbeitungsvorgänge, abweichend von den Weisungen des Nutzers, auch durch Administratoren erheblich erschweren.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er im Risiko- und Schutzkonzept dokumentiert, wie er Weisungen des Cloud-Nutzers empfängt, umsetzt und dokumentiert. Bei Massengeschäften erbringt der Cloud-Anbieter den Nachweis über seine konkrete Dienstbeschreibung zu seinen technisch ausführbaren Dienstleistungen und den Nachweis zur Ausführbarkeit von Weisungen durch Softwarebefehle in Form einer technischen Dokumentation oder durch Dienstnutzung. Die Implementierung der geeigneten Maßnahmen wird durch repräsentative Stichproben im Rahmen von technischen Prüfungen festgestellt und auf Angemessenheit überprüft.

### Nr. 4 – Hinweispflicht des Cloud-Anbieters (Art. 28 Abs. 3 Satz 3 i.V.m Art. 29 DSGVO)

**Kriterium**

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

**Erläuterung**

Die Verantwortung für die Vereinbarkeit einer Weisung mit dem geltenden Datenschutzrecht liegt beim Cloud-Nutzer. Gleichwohl 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 den Cloud-Vertrag und bei jeder nach Vertragsabschluss ergangenen Weisung sollte der Cloud-Anbieter seinen DSB konsultieren, wenn sich die Datenschutzwidrigkeit der Weisung einem datenschutzrechtlich geschulten Mitarbeiter des Cloud-Anbieters aufdrängt. Der Cloud-Anbieter hat keine Pflicht, ohne Anlass eine Weisung zu überprüfen.

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

Die Umsetzungshinweise aus DIN ISO/IEC 27018:2017 Ziff. 16.1.1 sind anwendbar.

**Nachweis**

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

### Nr. 5 – Unterstützung des Cloud-Nutzers bei der Wahrung der Betroffenenrechte

**Erläuterung**

Für die Erfüllung der Rechte der betroffenen Person 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. 5.1 – Auskunftserteilung (Art. 28 Abs. 3 lit. e i.V.m. Art. 15 DSGVO)

**Kriterium**

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.

**Erläuterung**

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

**Umsetzungshinweis**

Der Cloud-Anbieter hat Weisungen zur Umsetzung der Betroffenenrechte zu dokumentieren.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er dokumentiert, welche Maßnahmen er ergriffen hat, um dem Cloud-Nutzer die Auskunftserteilung gegenüber einer betroffenen Person zu

ermöglichen oder die Auskunft durch den Cloud-Anbieter erteilen zu lassen. Im Rahmen einer repräsentativen Probeauskunft oder durch Interviews wird geprüft, ob bei einem Antrag Auskunft erteilt werden kann. Auch können anhand einer Prozessdokumentation die tatsächlich durchgeführten Auskunftserteilungen nachgewiesen werden.

### Nr. 5.2– Berichtigung und Vervollständigung (Art. 28 Abs. 3 lit. e i.V.m. Art. 16 DSGVO)

**Kriterium**

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.

**Erläuterung**

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

**Umsetzungshinweis**

Der Cloud-Anbieter hat Weisungen zur Umsetzung der Betroffenenrechte zu dokumentieren.

**Nachweis**

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

### Nr. 5.3 – Löschung (Art. 28 Abs. 3 lit. e i.V.m. Art. 17 Abs. 1 DSGVO)

**Kriterium**

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.

**Erläuterung**

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

**Umsetzungshinweis**

Die 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 muss auch Backup- und Ausfallsicherungssysteme, einschließlich aller Vorgängerversionen der Daten, temporäre Dateien, Metadaten und Dateifragmente umfassen. Die Maßnahmen aus DIN 66398 zur Erstellung eines Löschkonzepts sowie DIN 66993 zur Vernichtung von Datenträgern können hinzugezogen werden. Der Cloud-Anbieter hat Weisungen zur Umsetzung der Betroffenenrechte zu dokumentieren.

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

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Maßnahmen er ergriffen hat, um dem Cloud-Nutzer die Löschung von Daten zu ermöglichen oder diese durch den Cloud-Anbieter vornehmen zu lassen. Im Rahmen einer repräsentativen Probelöschung wird geprüft, ob die bedarfsgerechte Löschung von Daten möglich ist. Auch können anhand einer Prozessdokumentation die tatsächlich durchgeführten Löschungen nachgewiesen werden.

### Nr. 5.4 – Einschränkung der Verarbeitung (Art. 28 Abs. 3 lit. e i.V.m. Art. 18 Abs. 1 DSGVO)

**Kriterium**

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.

**Erläuterung**

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

**Umsetzungshinweis**

Der Cloud-Anbieter hat Weisungen zur Umsetzung der Betroffenenrechte zu dokumentieren.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Maßnahmen er ergriffen hat, um dem Cloud-Nutzer die Einschränkung der Verarbeitung von Daten zu ermöglichen oder dies durch den Cloud-Anbieter vornehmen zu lassen. Im Rahmen einer Probeeinschränkung wird geprüft, ob die Einschränkung der Verarbeitung von Daten möglich ist.

### Nr. 5.5 – Mitteilungspflicht bei Berichtung, Löschung oder Einschränkung der Verarbeitung (Art. 28 Abs. 3 lit. e i.V.m. Art. 19 DSGVO)

**Kriterium**

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.

**Erläuterung**

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

**Umsetzungshinweis**

Der Cloud-Anbieter hat Weisungen zur Umsetzung der Betroffenenrechte zu dokumentieren.

**Nachweis**

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

Anbieter vornehmen zu lassen. Es wird geprüft, ob der Cloud-Anbieter in der Lage ist, die Empfänger personenbezogener Daten zu unterrichten oder dies durch den Cloud-Anbieter vornehmen zu lassen.

### Nr. 5.6– Datenübertragung (Art. 28 Abs. 3 lit. e i.V.m. Art. 20 Abs. 1 und 2 DSGVO)

**Kriterium**

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. Er kann die ihm möglichen Formate im Vertrag festhalten.

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

**Umsetzungshinweis**

Der Cloud-Anbieter stellt geeignete technische Funktionen innerhalb seines angebotenen Dienstes bereit, welche eine Übertragung der Daten in ein strukturiertes, gängiges und maschinenlesbares Format sicherstellen. Hierzu gehören z.B. Exportfunktionen in XML- oder JSON-Formate. Der Cloud-Anbieter hat Weisungen zur Umsetzung der Betroffenenrechte zu dokumentieren.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Maßnahmen er ergriffen hat, um es dem Cloud-Nutzer zu ermöglichen, der betroffenen Person oder einem anderen Verantwortlichen die von dieser betroffenen Person bereitgestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln oder durch den Cloud-Anbieter übermitteln zu lassen. Im Rahmen einer Datenübertragung mit Testdaten im Rahmen einer Dienstnutzung und technischen Prüfung kann geprüft werden, ob die Daten in einem strukturierten, gängigen und maschinenlesbaren Format übermittelt werden können.

### Nr. 5.7 – Widerspruch (Art. 28 Abs. 3 lit. e i.V.m. Art. 21 Abs. 1 und Art. 32 Abs. 1 lit. b DSGVO)

**Kriterium**

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

**Erläuterung**

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

**Umsetzungshinweis**

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

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Maßnahmen er implementiert hat, um dem Cloud-Nutzer die erforderlichen Daten zur Verfügung zu stellen. Mit repräsentativen Testdaten und einem simulierten Widerspruch ist im Rahmen einer Dienstnutzung und technischen Prüfung zu prüfen, ob die richtigen Daten zur Verfügung gestellt werden.

### Nr. 6 – Unterstützung des Cloud-Nutzers 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 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 sind an dem jeweiligen Einflussbereich des Cloud-Anbieters auszurichten, etwa im Bereich der TOM zur Gewährleistung der Datensicherheit. Zur Einschätzung, ob ein oder welches Risiko bei den jeweiligen Datenverarbeitungsvorgängen des Cloud-Dienstes gegeben ist, können Datenflussmodelle und -analysen erstellt werden, wenn diese nicht bereits aus der Dienstbeschreibung des Cloud-Anbieters hervorgehen.

**Nachweis**

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

## Kapitel III: Datenschutz-Managementsystem des Cloud-Anbieters

**Erläuterung**

Der Cloud-Anbieter muss seine Datenschutzmaßnahmen in einem Datenschutz-Managementsystem organisieren. Die Einrichtung eines Datenschutz-Managementsystems indizieren die Art. 24 und 25, 32, 33, 34 sowie 37 bis 39 DSGVO. Die Einrichtung eines Datenschutz-Managementsystems sollte der fortwährenden Sicherstellung und kontinuierlichen Verbesserung des Datenschutzniveaus des zertifizierten Cloud-Dienstes dienen (vgl. auch DIN EN ISO/IEC 27001:2017 Ziff. 10.2).

## Nr. 7– Datenschutz-Managementsystem

### Nr. 7.1 – Benennung, Stellung und Aufgaben eines Datenschutzbeauftragten (Art. 37-39 DSGVO)

**Kriterium**

(1) Der Cloud-Anbieter benennt einen DSB 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. 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.

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

(6) Der Cloud-Anbieter stellt sicher, dass der DSB und der Beauftragte für Informationssicherheit in angemessener Weise kooperieren (gegenseitige Information und Unterstützung).

**Erläuterung**

Sofern ein Cloud-Anbieter gesetzlich verpflichtet ist, einen DSB zu bestellen, muss er ihn sorgfältig auswählen, ausstatten, angemessen schützen und dessen Funktion in der Betriebsorganisation effektiv sicherstellen.

**Umsetzungshinweise**

Der Cloud-Anbieter hat 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 zu führen (z.B. in einem Risiko- und Datenschutzkonzept) und dem DSB sowie (auf Anfrage) der Aufsichtsbehörde zugänglich zu machen.

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

Der Cloud-Anbieter hat sicherzustellen, dass der DSB für die betroffene Person direkt (von außen) erreichbar ist. Den DSB trifft die Pflicht zum Nachgehen und zur Beratung von betroffenen Personen (Art. 38 Abs. 4 DSGVO). Die Verschwiegenheitspflicht des DSB gemäß Art. 38 Abs. 5 DSGVO umfasst insbesondere die Identität des Beschwerdeführers oder der betroffenen Person(en), alle datenschutzrechtlich relevanten Informationen sowie alles, was zur Identifizierung eines Hinweisgebers führen könnte.

Auch gegenüber der ihn benennenden Stelle ist der DSB zur umfassenden Verschwiegenheit verpflichtet. Das Kriterium fördert das Gewährleistungsziel der Vertraulichkeit (SDM 6.2.3). Der DSB ist zudem Anlaufstelle für die Aufsichtsbehörden.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er einen DSB benannt hat und durch Einträge auf seiner Webseite seine direkte Ansprechbarkeit der Öffentlichkeit vorstellt. Zur Beurteilung der fachlichen und persönlichen Eignung kann er einschlägige Zeugnisse und Beurteilungen vorlegen. Ein Interview mit dem DSB kann während einer Vorort-Auditierung ebenfalls Aufschluss über Eignung und Stellung des DSB geben. Eine Vorort-Auditierung ermöglicht auch festzustellen, ob der DSB über die erforderliche Einbindung, Ausstattung und Unterstützung verfügt. Durch eine regelmäßig durchzuführende Dokumentierung der ausgeführten Aufgaben des DSB kann der Nachweis über seine Tätigkeiten, seine Unabhängigkeit sowie seine Einbindung und Wirksamkeit im Organisationsgefüge des Cloud-Anbieters erbracht werden.

### Nr. 7.2 – Meldung von Datenschutzverletzungen (Art. 33 Abs. 2 und Art. 28 Abs. 3 lit. f DSGVO)

**Kriterium**

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

**Erläuterung**

Der Cloud-Anbieter ist zur unverzüglichen Meldung von Datenschutzverstößen an den Cloud-Nutzer verpflichtet, damit dieser seiner Meldepflicht an die Aufsichtsbehörde 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 Subauftragsverarbeitungskette. Das Kriterium fördert das Gewährleistungsziel der Integrität und Transparenz (SDM 6.2.2 und 6.2.5).

**Umsetzungshinweis**

Um eine unverzügliche Mitteilung zu ermöglichen, ist festzulegen, wer zuständig ist, über die Mitteilung an den Cloud-Nutzer zu entscheiden und diese vorzunehmen. Die zuständigen Stellen müssen für Mitarbeiter und Subauftragsverarbeiter in einer Weise erreichbar sein, dass Mitteilungen über etwaige Verstöße zeitnah entgegengenommen und bearbeitet werden können. Die zuständigen Stellen müssen über ausreichende Ressourcen verfügen, um eine rasche Bearbeitung von Meldungen sicher zu stellen. Die Mitarbeiter in den zuständigen Stellen müssen ausreichend geschult sein, um Verstöße beurteilen und eine Folgeabschätzung durchführen zu können.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er in seinem Risiko- und Schutzkonzept dokumentiert, wie er die Meldung von Datenschutzverletzungen gewährleistet. Die Implementierung dieses Konzepts kann im Rahmen einer Dienstnutzung oder technischen Prüfung durch eine Probemeldung an einen Auditor als simulierter Cloud-Nutzer geprüft werden.

### Nr. 7.3 – Führen eines Verarbeitungsverzeichnisses (Art. 30 Abs. 2 DSGVO)

**Kriterium**

(1) Cloud-Anbieter, die mehr als 250 Mitarbeiter beschäftigen, führen ein Verarbeitungsverzeichnis. Der Cloud-Anbieter hat unabhängig von der Beschäftigtenzahl ein Verarbeitungsverzeichnis zu führen, wenn die Verarbeitung risikobehaftet ist.

(2) Im Verzeichnis hat der Cloud-Anbieter alle Kategorien von im Auftrag eines Verantwortlichen durchzuführende Verarbeitungsvorgänge aufzuführen. Das Verzeichnis enthält außerdem die in Art. 30 Abs. 2 DSGVO aufgelisteten Inhalte.

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

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

**Erläuterung**

Risikobehaftet ist ein Verarbeitungsvorgang i.S.d. Art. 30 Abs. 2 DSGVO, wenn er Risiken für die Rechte und Freiheiten von betroffenen Personen birgt oder besondere Kategorien von personenbezogenen Daten gemäß Art. 9 DSGVO oder Art. 10 DSGVO zum Gegenstand hat. Das Kriterium fördert das Gewährleistungsziel der Transparenz (SDM 6.2.5).

**Umsetzungshinweise**

Das für jeden Cloud-Nutzer jeweils zu führende Verarbeitungsverzeichnis dokumentiert auch die für jeden Cloud-Nutzer jeweils eingesetzten TOM zur Gewährleistung der Datensicherheit bei der Datenverarbeitung. Bei standardisierten Massengeschäften soll das Verarbeitungsverzeichnis automatisiert erstellt werden. Die Voreinstellungen der automatisiert geführten Verzeichnisse müssen die Pflichtangaben aus Art. 30 Abs. 2 DSVGO und dieses Kriteriums enthalten.

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

Die Umsetzungshinweise aus DIN ISO/IEC 27018:2017 Ziff. A.5.2 sind anwendbar.

**Nachweis**

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

### Nr. 7.4 – 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 Online-Daten und die Löschung der beim Cloud-Anbieter gespeicherten Daten nach Abschluss der Auftragsverarbeitung nach Weisung des Cloud-Nutzers erfolgen.

**Umsetzungshinweis**

Auf DIN ISO/ IEC 27018:2017 Ziff. A.9.3. wird hingewiesen.

**Nachweis**

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

### Nr. 7.5 – Einrichtung eines internen Kontrollsystems (Art. 24 DSGVO)

**Kriterium**

(1) Der Cloud-Anbieter stellt sicher, dass die Umsetzung aller in diesem Katalog geprüften Kriterien regelmäßig in einem internen Revisionsverfahren überprüft wird. 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 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 zieht vor allem die Dokumentationen des DSB zu Datenschutzfragen sowie die Berichte des Beauftragten für Informationssicherheit heran. Des Weiteren wird auf die Umsetzungshinweise zur regelmäßigen Überprüfung durch die oberste Leitung beim Cloud-Anbieter nach DIN EN ISO/IEC 27002:2017-06, Ziff. 18.2. hingewiesen.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welches interne Kontrollsystem er eingerichtet hat. Die Praxis der internen Kontrollen kann durch Interviews mit dem DSB und Verantwortlichen festgestellt werden. Zudem soll die Durchführung eines internen Revisionsverfahrens anhand repräsentativer Stichproben und geeigneter Prozessdokumentationen sichergestellt werden.

### Nr. 7.6 – Auswahl und Einsatz geeigneter Personen (Art. 28 Abs. 3 Satz 2 lit. e und f DSGVO)

**Kriterium**

Der Cloud-Anbieter stellt sicher, dass er nur Mitarbeiter mit der Durchführung von Verarbeitungsvorgängen betraut, die fachlich für die Erfüllung ihrer jeweiligen Aufgaben befähigt sind, die nötige Zuverlässigkeit aufweisen und sowohl im Datenschutz als auch in der Datensicherheit geschult und sensibilisiert sind. Zudem stellt er sicher, dass bei den Mitarbeitern keine Interessenkonflikte hinsichtlich der Ausübung ihrer jeweiligen Aufgaben bestehen.

**Umsetzungshinweis**

Die Hinweise aus DIN EN ISO/IEC 27007:2017 Ziff. 7 sind anwendbar.

**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 7.1, da der DSB für die Sensibilisierung und Schulung von an Verarbeitungsvorgängen beteiligten Mitarbeitern zuständig ist und die diesbezüglichen Überprüfungen vornimmt.

**Nachweis**

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

# Kapitel IV: Datenschutz durch Systemgestaltung

## Nr. 8 – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

### Nr. 8.1 – Datenschutz durch Systemgestaltung (Art. 25 Abs. 1 DSGVO i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

**Kriterium**

(1) Der Cloud-Anbieter stellt im Rahmen des angebotenen Dienstes sicher, dass er bei der Auftragsverarbeitung die Grundsätze des Art. 5 DSGVO (Rechtmäßigkeit, Verarbeitung nach Treu

und Glauben, Transparenz, Zweckfestlegung und Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Systemdatenschutz und Verantwortlichkeit) möglichst praktikabel und zielführend umsetzt.

(2) 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 einhalten.

**Umsetzungshinweise**

Zur Umsetzung von Datenminimierung (SDM 7.1) verweist Art. 25 Abs. 1 DSGVO auf das Mittel der Pseudonymisierung (Nr. 2.8). Weitere Mittel sind u.a. die Anonymisierung (Nr. 2.9) und die Verschlüsselung (Nr. 2.10). Datenminimierung kann auch erreicht werden, indem die Menge der erfassten Attribute der betroffenen Personen, Verarbeitungsoptionen in Verarbeitungsprozessschritten und Möglichkeiten der Kenntnisnahme vorhandener Daten reduziert werden. Ein Cloud-Anbieter sollte soweit möglich Verarbeitungsprozesse automatisieren, um eine Kenntnisnahme verarbeiteter Daten und die Einflussnahme zu begrenzen. Es empfiehlt sich auch, automatische Sperr- und Löschroutinen zu implementieren.

Zur Umsetzung der anderen Grundsätze der Datenverarbeitung muss der Cloud-Anbieter andere geeignete Mittel und Gestaltungsprinzipien anwenden. Soweit der Cloud-Anbieter eine Datenschutz-Folgenabschätzung durchgeführt hat, können sich Gestaltungsanforderungen aus der Pflicht ergeben, die festgestellten Risiken zu minimieren. Bei der (Weiter-)Entwicklung seines Dienstes sollten Datenminimierung und Datensicherheit zentrale Bestandteile des Software-Entwicklungsprozesses sein.

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Gestaltungsprinzipien und -maßnahmen er vorgesehen hat und welche Erwägungen bei Ergreifen oder Unterlassen von Gestaltungsmaßnahmen ihn geleitet haben. Auch mit der transparenten Dienstbeschreibung z.B. im Rahmen des (im Massengeschäft einseitig und vorformuliert vorgegebenen) Cloud-Vertrages kann der Cloud-Anbieter seine datenschutzgerechten Systemgestaltungen und Voreinstellungen nachweisen. Die Dokumentationen in den obligatorisch zu führenden Verarbeitungsverzeichnissen nach Art. 30 Abs. 2 DSGVO und Nr. 7.2 dieses Katalogs können als Nachweis für die dort aufgeführten Systemgestaltungen dienen. Die Umsetzung kann durch repräsentative Stichproben geprüft werden.

### Nr. 8.2 – Datenschutz durch Voreinstellungen (Art. 25 Abs. 2 DSGVO)

**Kriterium**

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

(2) Der Cloud-Anbieter muss durch Entwicklung und Voreinstellungen sicherstellen, 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 konfigurieren, dass sie die Pflichtvorgaben des Art. 25 Abs. 2 Satz 1 DSGVO erfüllen.

**Umsetzungshinweise**

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

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er dokumentiert, welche Voreinstellungen er aus welchen Erwägungen gewählt hat. Die Umsetzung kann durch repräsentative Stichproben geprüft werden.

# Kapitel V: Subauftragsverarbeitung

**Erläuterung**

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

Der Cloud-Anbieter als Hauptauftragsverarbeiter hat allerdings dafür Sorge zu tragen, dass auf allen Stufen die Kriterien der Auftragsverarbeitung von allen Auftragsverarbeitern eingehalten werden, da nur er gegenüber dem Cloud-Nutzer für die Auftragsausführung durchgängig verantwortlich bleibt.

## Nr. 9 – Subauftragsverhältnisse

### Nr. 9.1 – Weitere Auftragsverarbeitern des Cloud-Anbieters (Subauftragsverarbeitung) (Art. 28 Abs. 2 DSGVO)

**Kriterium**

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

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

**Erläuterung**

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

**Umsetzungshinweis**

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

Die Umsetzungshinweise aus DIN EN ISO/IEC 27002:2017 Ziff. 15 sind anwendbar.

**Nachweis**

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

### Nr. 9.2 – Vertragliche Grundlage der Subauftragsverarbeitung (Art. 28 Abs. 4 DSGVO)

**Kriterium**

(1) Der Cloud-Anbieter stellt sicher, dass seine Subauftragsverarbeiter nur auf Grundlage eines wirksamen Subauftragsverarbeitungsvertrages tätig werden, der mit dem Cloud-Vertrag zwischen dem Cloud-Anbieter und Cloud-Nutzer in Einklang steht.

(2) Der Cloud-Anbieter verpflichtet seine Subauftragsverarbeiter sicherzustellen, dass ihre Sub-Subauftragsverarbeiter ebenfalls auf Grundlage eines wirksamen Subauftragsverarbeitungsvertrags tätig werden und auf ihre Sub-Subauftragsverarbeiter dieselbe Verpflichtung übertragen.

**Umsetzungshinweis**

Die Anforderungen an den Cloud-Vertrag und an das Hauptauftragsverhältnis sind entsprechend in den Subauftragsverarbeitungen durch den Cloud-Anbieter umzusetzen.

**Nachweis**

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

### Nr. 9.3 – Information des Cloud-Nutzers (Art. 28 Abs. 2 Satz 2 DSGVO)

**Kriterium**

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

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

**Erläuterung**

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

**Umsetzungshinweis**

Der Cloud-Anbieter als Hauptauftragsverarbeiter hat für jede Verlängerung der Auftragsverarbeitungsleistungskette eine detaillierte Dokumentation über die involvierten Subauftragsverarbeiter unter Angabe von Identität inklusiver ladungsfähiger Anschrift und der ausgeführten Tätigkeiten zu verfassen, sodass nachvollzogen werden kann, welcher (Sub-)Auftragsverarbeiter jeweils in den datenschutzkritischen Dienstteilen involviert ist und welche Verarbeitungsvorgänge jeweils von wem ausgeführt werden.

Zur Darstellung aller involvierter Subauftragsverarbeiter eignen sich Informationsportale innerhalb oder außerhalb des angebotenen Cloud-Dienstes. Diese sind fortlaufend zu pflegen und zu aktualisieren.

**Nachweis**

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

### Nr. 9.4 – Auswahl und Kontrolle der Subauftragsverarbeiter (Art. 28 Abs. 4 Satz 1 DSGVO)

**Kriterium**

(1) Der Cloud-Anbieter stellt sicher, dass auf allen Stufen 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, ist er verpflichtet, sich selbst von der Einhaltung der datenschutzrechtlichen Anforderungen durch die Subauftragsverarbeiter zu überzeugen. Insoweit sind die Umsetzungshinweise (implementation guidance) von ISO/IEC 27017:2015 Ziff. 15.1.2, 15.1.3 und DIN EN ISO/IEC 27002:2017 Ziff. 15 anwendbar.

**Nachweis**

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

### Nr. 9.5 – 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 in jedem Stadium der Auftragsverarbeitung sicher, dass durch die Einschaltung von (mehreren) Subauftragsverarbeitern seine Unterstützungsfunktionen im vertraglichen 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.

**Umsetzungshinweise**

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

**Nachweis**

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, dass er eine Dokumentation vorlegt, aus der sich ergibt, in welche Pflichten er weitere Auftragsverarbeiter einbindet. Protokolle zur Pflichterfüllung infolge der Einschaltung von weiteren Auftragsverarbeitern können als Nachweis vorgelegt werden. Die Implementierung der Verfahren und Vorkehrungen ist durch Dienst-, Prozess- und Vorortprüfungen sowie Interviews zu überprüfen.

# Kapitel VI: Auftragsverarbeitung außerhalb der EU und des EWR

## Nr. 10 – Datenübermittlung

### Nr. 10.1 – Geeignete Garantien für die Datenübermittlung (Art. 46 Abs. 2 lit. f i.V.m. Art. 42 Abs. 1 und 2 DSGVO)

**Kriterium**

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

**Erläuterung**

Auftragsverarbeitungen sind außerhalb der EU und des EWR nur unter den in Art. 44 ff. DSGVO genannten Voraussetzungen zulässig. Das Gleiche gilt für die Übermittlung von personenbezogenen Daten in ein EU-Drittland oder an eine Internationale Organisation, für die kein angemessenes Datenschutzniveau anerkannt ist.

**Nachweis**

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

### Nr. 10.2 – Vertreterbenennung (Art. 27 i.V.m. Art. 3 Abs. 2 DSGVO)

**Kriterium**

(1) Der Cloud-Anbieter, der nicht in der EU niedergelassen ist, für den die DSGVO aber dennoch nach Art. 3 Abs. 2 DSGVO gilt, hat einen Vertreter in der EU schriftlich zu benennen.

(2) Der Cloud-Anbieter beauftragt den Vertreter, zusätzlich zu ihm oder an seiner Stelle insbesondere für Aufsichtsbehörden und betroffene Personen bei sämtlichen Fragen im Zusammenhang mit der Verarbeitung zur Gewährleistung der Einhaltung der DSGVO als Anlaufstelle zu dienen.

**Umsetzungshinweis**

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 (Art. 27 Abs. 3 DSGVO).

**Nachweis**

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