

European Cloud Service Data Protection Controls Catalogue

European Cloud Service Data Protection Controls Catalogue

Catalogue européen des mécanismes de protection des données dans le nuage

Dieser Entwurf mit Erscheinungsdatum 2019-07-05 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Spezifikation von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an info@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an das DIN e. V., 10772 Berlin, Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Zur Erstellung einer DIN SPEC können verschiedene Verfahrensweisen herangezogen werden:
Das vorliegende Dokument wurde nach den Verfahrensregeln einer PAS erstellt.

Gesamtumfang 70 Seiten

Dieses Dokument wurde durch die im Vorwort genannten Verfasser erarbeitet und verabschiedet.

Inhalt

	Seite
Vorwort	4
1 Anwendungsbereich	5
2 Normative Verweisungen	5
3 Begriffe	5
4 Symbole und Abkürzungen	6
5 Elemente dieser DIN SPEC	7
6 Schutzklassen	7
6.1 Allgemeines	7
6.2 Das Schutzklassenkonzept	7
6.3 Die Schutzklassen	8
7 Nichtanwendbarkeit von Kriterien	14
8 Kriterien und Umsetzungsempfehlungen für die Auftragsverarbeitung	14
8.1 Rechtsverbindliche Vereinbarung zur Auftragsverarbeitung	14
8.1.1 Allgemeines	14
8.1.2 Wirksame und eindeutige Vereinbarung zwischen Cloud-Anbieter und Cloud-Nutzer (Art. 28 Abs. 3 DSGVO)	15
8.2 Rechte und Pflichten des Cloud-Anbieters	20
8.2.1 Sicherstellung der Datensicherheit durch geeignete TOM nach dem Stand der Technik	20
8.2.2 Sicherstellung der Weisungsbefolgung (Art. 28 Abs. 3 Satz 2 lit. a; 29 DSGVO)	33
8.2.3 Hinweispflicht des Cloud-Anbieters	34
8.2.4 Sicherstellung der Vertraulichkeit beim Personal (Art. 28 Abs. 3 Satz 2 lit. b DSGVO)	35
8.2.5 Unterstützung des Cloud-Nutzers bei der Wahrung der Betroffenenrechte	36
8.3 Datenschutz-Managementsystem des Cloud-Anbieters	41
8.3.1 Allgemeines	41
8.3.2 Datenschutz-Managementsystem	41
8.4 Datenschutz durch Systemgestaltung und datenschutzfreundliche Voreinstellungen	46
8.4.1 Datenschutz durch Systemgestaltung (Art. 25 Abs. 1 DSGVO i.V.m. Art. 5 Abs. 1 lit. f DSGVO)	46
8.4.2 Datenschutz durch Voreinstellungen (Art. 25 Abs. 2 DSGVO)	46
8.5 Subauftragsverarbeitung	47
8.5.1 Allgemeines	47
8.5.2 Subauftragsverhältnisse	47
8.6 Datenverarbeitung außerhalb der EU und des EWR	50
8.6.1 Datenübermittlung	50
9 Kriterien und Umsetzungshinweise für Verarbeitung als Verantwortlicher	51
9.1 Allgemeines	51
9.2 Der Cloud-Anbieter als Verantwortlicher	51
9.2.1 Sicherstellung der Datenschutzgrundsätze (Art. 5 Abs. 1 und 2 i.V.m. Art. 24 DSGVO)	51
9.2.2 Rechtsgrundlage für die Datenverarbeitung (Art. 6 Abs. 1 UAbs. 1 lit. b. sowie lit. c i.V.m. Abs. 2 DSGVO)	52
9.2.3 Gewährleistung der Datensicherheit durch geeignete TOM nach dem Stand der Technik	53
9.2.4 Wahrung von Betroffenenrechten	61
9.2.5 Verpflichtung zur Vertraulichkeit (Art. 5 Abs. 1 lit. a, Abs. 2 i.V.m. Art. 24 Abs. 1 DSGVO)	63
9.2.6 Meldung von Datenschutzverletzungen (Art. 33 Abs. 1, 3 und 5 DSGVO)	64

9.2.7 Benachrichtigung der betroffenen Person bei Datenschutzverletzungen (Art. 34 Abs. 1 und 2 DSGVO).....	64
9.2.8 Führen eines Verarbeitungsverzeichnisses (Art. 30 Abs. 1 DSGVO)	65
9.2.9 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen	65
9.2.10 Auftragsverarbeitung des Cloud-Anbieters.....	66
Literaturhinweise.....	70

Vorwort

Diese DIN SPEC wurde nach dem PAS-Verfahren erarbeitet. Die Erarbeitung von DIN SPEC nach dem PAS-Verfahren erfolgt in DIN SPEC (PAS)-Konsortien und nicht zwingend unter Einbeziehung aller interessierten Kreise.

Die Erarbeitung und Verabschiedung des Dokuments erfolgten durch die nachfolgend genannten Initiator(en) und Verfasser:

- Karlsruher Institut für Technologie: Sebastian Lins, Heiner Teigeler
- Fachgebiet Öffentliches Recht mit Schwerpunkt Recht der Technik und des Umweltschutzes, Universität Kassel: Natalie Maier
- Cleopa GmbH: Dipl. Ing. Detlef Olschewski
- IBM Technical Relations Europe: Dipl. Ing. Volker M. Smoljko
- EuroCloud Deutschland_eco e.V., eco – Verband der Internetwirtschaft: Andreas Weiss

Für dieses Thema bestehen derzeit keine Normen im Deutschen Normenwerk.

DIN SPEC (PAS) sind nicht Teil des Deutschen Normenwerks.

Trotz großer Anstrengungen zur Sicherstellung der Korrektheit, Verlässlichkeit und Präzision technischer und nicht-technischer Beschreibungen kann das DIN SPEC (PAS)-Konsortium weder eine explizite noch eine implizite Gewährleistung für die Korrektheit des Dokuments übernehmen. Die Anwendung dieses Dokuments geschieht in dem Bewusstsein, dass das DIN SPEC (PAS)-Konsortium für Schäden oder Verluste jeglicher Art nicht haftbar gemacht werden kann. Die Anwendung der vorliegenden DIN SPEC (PAS) entbindet den Nutzer nicht von der Verantwortung für eigenes Handeln und geschieht damit auf eigene Gefahr.

Die kostenfreie Bereitstellung dieses Dokuments als PDF-Version über den Beuth WebShop wurde im Vorfeld finanziert.

1 Anwendungsbereich

Diese DIN SPEC legt datenschutzrechtliche Anforderungen an die Verarbeitung von personenbezogenen Daten auf der Seite des Auftragnehmers (Cloud-Anbieter) fest. Dagegen werden die datenschutzrechtlichen Anforderungen an den Auftraggeber (Cloud-Nutzer) nicht adressiert. In dieser DIN SPEC werden die Datenverarbeitungsvorgänge betrachtet, die der Cloud-Anbieter als Auftragsverarbeiter im Rahmen der Auftragsverarbeitung gemäß Art. 28 DSGVO durchführt. Weiterhin werden Datenverarbeitungsvorgänge betrachtet, die der Cloud-Anbieter als Verantwortlicher vornimmt, um den Vertrag mit dem Cloud-Nutzer über die Bereitstellung des Cloud-Dienstes schließen und durchführen zu können sowie um rechtliche Pflichten zu erfüllen.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

DIN und DKE stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- DIN-TERMinologieportal: verfügbar unter <https://www.din.de/go/din-term>
- DKE-IEV: verfügbar unter <http://www.dke.de/DKE-IEV>

3.1

Verarbeitung

jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten

Anmerkung 1 zum Begriff: Dazu zählen das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten.

[QUELLE: Art. 4 Nr. 2 DSGVO]

3.2

Inhaltsdaten

Anwendungsdaten

personenbezogene Daten, die in der Cloud verarbeitet werden

Anmerkung 1 zum Begriff: Im B2B-Bereich werden Inhaltsdaten häufig personenbezogene Daten von Kunden, Mitarbeitern oder anderen betroffenen Personen sein, mit denen der Cloud-Nutzer in Vertragsbeziehungen steht. Sie können aber auch personenbezogene Daten des Cloud-Nutzers sein.

3.3

Cloud-Anbieter

jedes privatwirtschaftliche Unternehmen, das einen Cloud-Dienst am Markt anbietet

Anmerkung 1 zum Begriff: Die Cloud-Anbieter können sowohl B2B- als auch B2C-Anbieter sein. Wichtig ist nur, dass sie hinsichtlich der Daten, die in der Cloud verarbeitet werden („Inhalts- oder Anwendungsdaten“), als Auftragsverarbeiter und nicht als Verantwortliche tätig sind.

3.4

Cloud-Nutzer

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

3.5

Personenbezogene Daten

alle Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen

[QUELLE: Art. 4 Abs. 1 DSGVO]

Anmerkung 1 zum Begriff: Im Cloud-Kontext können dies beispielsweise Anwendungsdaten des Cloud-Nutzers sein, soweit sie dem jeweiligen Datenverarbeiter die Identifizierung oder Identifizierbarkeit einer natürlichen Person ermöglichen.

3.6

Nutzungsdaten

Personenbezogene Daten vom Cloud-Anbieter, welche für die Inanspruchnahme des Cloud-Dienstes und dessen Abrechnung erhoben werden müssen

Anmerkung 1 zum Begriff: Nutzungsdaten können beispielsweise Ein- und Auslogdaten zu Nutzkonten, IP-Adressen, die genutzten Dienstmodule oder der Umfang der Nutzung sein.

Anmerkung 2 zum Begriff: Da die Datenschutz-Grundverordnung die Unterscheidung in Bestands- und Nutzungsdaten nicht kennt, werden diese Daten im Rahmen dieser DIN SPEC ebenfalls als personenbezogene Daten bezeichnet, die ihm Rahmen der Durchführung des Auftrags über die Erbringung des Cloud-Dienstes anfallen.

3.7

Bestandsdaten

Vom Cloud-Anbieter erhobene Daten die für den Vertragsabschluss notwendig sind

Anmerkung 1 zum Begriff: Bestandsdaten sind typischerweise Daten wie Namen, Adressen, Zahlungsdaten wie beispielsweise Bankverbindungen, Rufnummern.

Anmerkung 2 zum Begriff: Da die Datenschutz-Grundverordnung die Unterscheidung in Bestands- und Nutzungsdaten nicht kennt, werden diese Daten im Rahmen dieser DIN SPEC ebenfalls als personenbezogene Daten bezeichnet, die ihm Rahmen der Durchführung des Auftrags über die Erbringung des Cloud-Dienstes anfallen.

4 Symbole und Abkürzungen

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
Art.	Artikel
Alt.	Alternative
BDSG	Bundesdatenschutzgesetz neue Fassung (Geltung ab 25.05.18)
DSB	Datenschutzbeauftragter
DSGVO	EU-Datenschutz-Grundverordnung (Geltung ab 25.05.18)
EG	Erwägungsgrund

EWK	Europäischer Wirtschaftsraum
Hs.	Halbsatz
i.S.v.	Im Sinne von
i.V.m.	In Verbindung mit
lit.	litera (Buchstabe)
Nr.	Nummer
TOM	technische und organisatorische Maßnahmen
Ziff.	Ziffer

5 Elemente dieser DIN SPEC

Diese DIN SPEC enthält „Kriterien“, „Anmerkungen“, „Umsetzungshinweise“ und „Nachweise“. Die „Kriterien“ bezeichnen die normativen Voraussetzungen, die zu erfüllen sind, um Konformität mit dieser DIN SPEC zu erlangen. Die „Anmerkungen“ sollen das Verständnis der Kriterien und ihre Herleitung aus der Datenschutz-Grundverordnung erleichtern.

Für jedes Kriterium werden „Umsetzungshinweise“ als exemplarische Leitlinien und Hilfestellungen für das Verständnis und die Umsetzung der Kriterien gegeben, die jedoch keinen verpflichtenden Charakter haben. Zudem finden sich zu jedem Kriterium „Nachweise“. Die „Nachweise“ liefern die Antwort auf die Frage, wie das Vorliegen der Kriterien bei einer Überprüfung nachgewiesen werden kann. Sie stellen analog zu den Umsetzungshinweisen exemplarische Leitlinien und informative Hilfestellungen dar, die Cloud-Anbieter, Zertifizierungsstellen, Prüfer und weitere Interessierte bei der Beurteilung der Einhaltung von Kriterien unterstützen sollen. Es besteht keine Verpflichtung, die Nachweise gemäß diesem Dokument zu erbringen.

Diese DIN SPEC unterscheidet zwischen Kriterien, Anmerkungen, Umsetzungshinweisen und Nachweisen für die Auftragsverarbeitung von Anwendungsdaten (Abschnitt 8) und für die Verarbeitung von Bestands- und Nutzungsdaten, für die ein Cloud-Anbieter verantwortlich ist (Abschnitt 9).

6 Schutzklassen

6.1 Allgemeines

Anforderungen an Technisch-organisatorische Maßnahmen (TOM) des Cloud-Dienstes werden in dieser DIN SPEC nach Schutzklassen differenziert.

6.2 Das Schutzklassenkonzept

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

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

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

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

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

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

Die Unterscheidung von Schutzbedarfs- und Schutzanforderungsklasse korrespondiert mit den Rollen und Verantwortungen von Cloud-Nutzer und Cloud-Anbieter in der Auftragsverarbeitung. Der Cloud-Anbieter beansprucht im Rahmen des Zertifizierungsverfahrens für jeden Dienst auf Grundlage der Prüfung und anhand der konkreten TOM eine bestimmte Schutzanforderungsklasse.

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

6.3 Die Schutzklassen

Diese DIN SPEC beruht auf der Unterscheidung von drei Schutzklassen (1, 2, 3), für die jeweils Schutzbedarf (Schutzbedarfsklassen) und Schutzanforderungen (Schutzanforderungsklassen) beschrieben werden.

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

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

Nicht abschließende Beispiele für Daten mit extrem hohem Schutzbedarf:

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

Auch Datenverarbeitungsvorgänge mit individuell stark divergierenden Umständen werden in dem Schutzklassenkonzept und damit in dieser DIN SPEC nicht betrachtet, weil sie der Generalisierung, die mit dem Schutzklassenkonzept einhergeht, nicht zugänglich sind.

a) Die Ermittlung der Schutzbedarfsklasse

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

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

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

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

Schutzbedarfsklassen nach Datenart (Abstrakter Schutzbedarf — Schritt 1)

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

Datenarten mit normalem Schutzbedarf (Schutzbedarfsklasse 1)

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

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

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

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

Datenarten mit hohem Schutzbedarf (Schutzbedarfsklasse 2)

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

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

- Name, Anschrift eines Vertragspartners;
- Geburtsdatum;
- Familienstand;
- verwandtschaftliche Beziehungen und Bekanntenkreis;
- Daten über Geschäfts- und Vertragsbeziehungen;
- Kontext zu einem Vertragspartner (z. B. Gegenstand einer vereinbarten Leistung);
- Verarbeitungen nicht veränderbarer Personendaten, die lebenslang als Anker für Profilbildungen dienen können wie genetische Daten i.S.v. Art. 4 Nr. 13 DSGVO oder biometrische Daten i.S.v. Art. 4 Nr. 14 DSGVO;
- Daten über die rassische und ethnische Herkunft;
- Daten über politische Meinungen;
- religiöse oder weltanschauliche Überzeugungen;
- Gewerkschaftsangehörigkeit;
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person;

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

ANMERKUNG 1 Kommunikationsinhalte, insbesondere Schrift- oder Sprachaufzeichnungen jeder Art, können sehr unterschiedlichen Schutzbedarf, von niedrig bis sehr hoch aufweisen. Die Festlegung des Schutzbedarfs erfordert eine objektive Bewertung, in der das Ausmaß des Risikos der Datenverarbeitung beurteilt wird. Sofern der Cloud-Nutzer keine Kenntnis vom subjektiven Schutzbedarf der Kommunizierenden hat (Beispiel: allgemeiner Kollaborations-Service mit Datenablage, Videokonferenz und Mailfunktion) oder seine Dienste für besonders schutzbedürftige Kommunikationen anbietet (Beispiel: Konferenzservice für Rechtsanwälte und Mandanten, hier: Schutzklasse 3) darf er von Schutzbedarfsklasse 2 ausgehen.

Datenarten mit sehr hohem Schutzbedarf (Schutzbedarfsklasse 3)

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

ANMERKUNG 2 Als Datenarten in diesem Sinne werden auch Datenmehrheiten, insbesondere verkettete Daten (z. B. Persönlichkeitsprofile) angesehen, aus denen sich ein neuer Informationsgehalt ergibt.

Nicht abschließende Beispiele für Daten mit sehr hohem Schutzbedarf:

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

b) Schutzanforderungsklassen

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

Schutzanforderungsklasse 1

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

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

Schutzanforderungsklasse 2

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

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

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

Schutzanforderungsklasse 3

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

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

7 Nichtanwendbarkeit von Kriterien

Im Rahmen des Zertifizierungsverfahrens stellt der Cloud-Anbieter der Zertifizierungsstelle ausreichend Informationen zur Beurteilung, Abgrenzung und abschließenden Festlegung des Zertifizierungsgegenstands zur Verfügung. Dies schließt insbesondere die Dokumentation von Verantwortlichkeiten und –insofern anwendbar – die Einbindung von Subauftragsverarbeitern in die zu zertifizierenden Datenverarbeitungsvorgänge ein. Bei der Festlegung des Zertifizierungsgegenstands oder im Rahmen des Prüfprozesses kann die Zertifizierungsstelle feststellen, dass einzelne Kriterien für den betrachteten Datenverarbeitungsvorgang nicht anwendbar sind.

Nichtanwendbar sind Kriterien insbesondere dann, wenn der Cloud-Anbieter diese nicht erfüllen kann, weil sie außerhalb seines Verantwortungsbereichs liegen. So wird der Cloud-Anbieter beispielsweise nach Kriterium in 8.2.4.2 zur Unterstützung des Cloud-Nutzers bei der Auskunftserteilung verpflichtet. Das Kriterium ist jedoch auf die Datenverarbeitungsvorgänge des Cloud-Anbieters nicht anwendbar und der Cloud-Anbieter somit von der Auskunftserteilung entbunden, wenn der Verantwortungsbereich für die betreffenden Daten beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt. Das gleiche gilt, wenn nicht der Cloud-Anbieter, sondern Subauftragsverarbeiter für den Zugang zu Datenverarbeitungssystemen nach 8.2.1.3 verantwortlich sind. In diesem Fall ist Kriterium 8.2.1.3 auf den Cloud-Anbieter nicht anwendbar. Der Cloud-Anbieter muss sich jedoch davon überzeugen, dass die Subauftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten (siehe 8.5.2.4) und somit ihrerseits das Kriterium 8.2.1.3 erfüllen.

Weiterhin sind Kriterien beispielsweise nicht anwendbar, wenn der Cloud-Anbieter die in den Kriterien adressierten Handlungen nicht vornimmt. Setzt der Cloud-Anbieter beispielsweise keine Subauftragsverarbeiter ein oder findet keine Datenverarbeitung außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums statt, sind die Kriterien aus 8.5 und 8.6 nicht anwendbar.

8 Kriterien und Umsetzungsempfehlungen für die Auftragsverarbeitung

8.1 Rechtsverbindliche Vereinbarung zur Auftragsverarbeitung

8.1.1 Allgemeines

Der Cloud-Anbieter muss sicherstellen, dass die Leistungen gegenüber dem Cloud-Nutzer aufgrund einer rechtsverbindlichen Vereinbarung¹ erbracht werden, die die gesetzlichen Anforderungen der Datenschutz-Grundverordnung an die Auftragsverarbeitung erfüllt. Die gesetzlichen Anforderungen an diese Vereinbarung werden durch die nachfolgenden Kriterien in 8.1.2.1 bis 8.1.2.8 konkretisiert.

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

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

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

8.1.2.1.1 Kriterium

- 1) Der Cloud-Anbieter stellt durch geeignete technische oder organisatorische Vorkehrungen sicher, dass der Dienst erst nach dem Abschluss einer rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung mit dem Cloud-Nutzer erbracht wird.
- 2) Diese Vereinbarung muss die Kriterien in 8.1.2.1 bis 8.1.2.8 erfüllen.
- 3) Die rechtsverbindliche Vereinbarung ist schriftlich oder in einem elektronischen Format² abzufassen.

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

8.1.2.1.2 Umsetzungshinweis

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

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

8.1.2.1.3 Nachweis

Der Cloud-Anbieter kann im Rahmen der Zertifizierung alle oder eine repräsentative Stichprobe von rechtsverbindlichen Vereinbarungen vorlegen, die er mit den Cloud-Nutzern schließt. Außerdem kann er anhand einer geeigneten Dokumentation nachweisen, dass technische oder organisatorische Vorkehrungen getroffen wurden, die eine Dienstnutzung erst nach Abschluss der Vereinbarung sicherstellen.

8.1.2.2 Gegenstand und Dauer der Verarbeitung (Art. 28 Abs. 3 Satz 1 DSGVO)

8.1.2.2.1 Kriterium

- 1) Der Gegenstand und die Dauer des Auftrags sind in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung so konkret wie möglich festzulegen.
- 2) Die Vereinbarung muss die Dauer des Auftrages durch einen Start- und Endpunkt oder den Verweis auf eine unbestimmte Nutzungszeit festlegen.
- 3) Die Voraussetzungen einer Kündigung sind in die Vereinbarung aufzunehmen.

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

8.1.2.2.2 Umsetzungshinweis

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

8.1.2.2.3 Nachweis

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

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

8.1.2.3.1 Kriterium

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

8.1.2.3.2 Umsetzungshinweis

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

8.1.2.3.3 Nachweis

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

8.1.2.4 Festlegung von Weisungsbefugnissen (Art. 28 Abs. 3 Satz 2 lit. a DSGVO)

8.1.2.4.1 Kriterium

- 1) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung sieht vor, dass die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen — auch in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation — verarbeitet werden.
- 2) Wird im Rahmen standardisierter Massengeschäfte keine individuelle rechtsverbindliche Vereinbarung geschlossen, hat der Cloud-Anbieter in seiner Dienstbeschreibung die durch ihn technisch ausführbaren Dienstleistungen auf eine aus der Cloud-Nutzer-Perspektive nachvollziehbare Weise so präzise wie möglich zu benennen, um diesem eine Auswahl nach Art. 28 Abs. 1 DSGVO zu ermöglichen.

ANMERKUNG 1 Die Weisungsgebundenheit wird in der Datenschutz-Grundverordnung an mehreren Stellen genannt (Art. 28 Abs. 3 Satz 2 lit. a, 28 Abs. 3 Satz 3; indirekt in Art. 28 Abs. 10 und 29 und 32 Abs. 4 DSGVO).

ANMERKUNG 2 Überschreitet der Cloud-Anbieter die Maßgaben des Cloud-Nutzers nach dessen Weisungen, so liegt ein Verstoß gegen Art. 28 Abs. 10 und 29 DSGVO vor, und der Cloud-Anbieter hat mit haftungsrechtlichen Konsequenzen zu rechnen.

8.1.2.4.2 Umsetzungshinweis

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

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

8.1.2.4.3 Nachweis

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

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

8.1.2.5.1 Kriterium

- 1) In der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung wird festgelegt, ob sich der Ort der Datenverarbeitung innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums oder in einem Drittland befindet.
- 2) Wird die Datenverarbeitung in einem Drittland durchgeführt, ist dieses konkret in der rechtsverbindlichen Vereinbarung zu benennen.
- 3) In der rechtsverbindlichen Vereinbarung wird festgelegt, dass in den Fällen, in denen sich während ihres Geltungszeitraums der Ort der Verarbeitung aus Gründen ändert, die im Verantwortungsbereich des Cloud-Anbieters liegen oder für beide Parteien unvorhersehbar sind, der Cloud-Anbieter diese Änderung dem Cloud-Nutzer unverzüglich mitteilt.
- 4) Bei jeder wesentlichen Abweichung von der Festlegung des Ortes der Datenverarbeitung wird dem Cloud-Nutzer in der rechtsverbindlichen Vereinbarung ein sofortiges Kündigungsrecht eingeräumt.

8.1.2.5.2 Nachweis

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

8.1.2.6 Verpflichtung zur Vertraulichkeit (Art. 28 Abs. 3 Satz 2 lit. b DSGVO)

8.1.2.6.1 Kriterium

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

ANMERKUNG Die Verpflichtung zur Vertraulichkeit und die Belehrung zur Verschwiegenheit fördern das Gewährleistungsziel der Vertraulichkeit.

8.1.2.6.2 Nachweis

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

8.1.2.7 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)

8.1.2.7.1 Kriterium

- 1) Die Schutzklasse und die für sie zu treffenden TOM werden in einer rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt.
- 2) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung enthält die Angabe, ob der Cloud-Anbieter oder der Cloud-Nutzer eine Pseudonymisierung, Anonymisierung oder Verschlüsselung (Nr. 8.2.1.7, 8.2.1.8 und 8.2.1.9) der zu verarbeitenden personenbezogenen Daten vornimmt und ob diese auch gegenüber den Mitarbeitern des Cloud-Anbieters wirksam sind. Die maximale Anzahl an Personen aus den Mitarbeitern des Cloud-Anbieters und seiner Subauftragsverarbeiter sind anzugeben, für die die Pseudonymisierung oder Verschlüsselung nicht wirksam sind.
- 3) Der Cloud-Anbieter legt in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung fest, auf welchem Niveau und wie rasch (innerhalb welchen Zeitraums) er nach einem physischen oder technischen Zwischenfall die Daten des Cloud-Nutzers und den Cloud-Dienst wiederherstellen und dem Cloud-Nutzer Zugang zum Cloud-Dienst und zu den Daten gewährleisten kann (Nr. 8.2.1.11).
- 4) In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung wird bestimmt, wie der Cloud-Anbieter die Bedingungen gemäß Art. 28 Abs. 2 und 4 DSGVO für die Inanspruchnahme der Dienste weiterer Auftragsverarbeiter einhält.
- 5) Die Verfahren zur Unterstützung des Cloud-Nutzers bei der Erfüllung der Betroffenenrechte nach 8.2.5., bei der Durchführung einer Datenschutz-Folgenabschätzung gemäß 8.2.5.9 und zur Erfüllung der Meldepflicht bei Datenschutzverletzungen nach 8.3.2.2 werden in der rechtsgültigen Vereinbarung über die Auftragsverarbeitung festgelegt.

8.1.2.7.2 Umsetzungshinweis

Angaben zur Umsetzung der Kriterien unter 8.2.1 können an Gewährleistungszielen ausgerichtet werden, während die konkreten Maßnahmen der Zielerreichung dem Cloud-Anbieter überlassen werden können. Für den Cloud-Nutzer ist es wichtig zu wissen, welcher Schutzanforderungsklasse der Cloud-Dienst entspricht.

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

Da dem Cloud-Nutzer bei Änderungen in der Unterbeauftragung ein Einspruchsrecht zusteht (8.5.2.3), sollten in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung die Voraussetzungen und Folgen eines Einspruchs geregelt werden, beispielsweise ob der Cloud-Nutzer bei Einspruch die Vereinbarung aufkündigen darf.

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

8.1.2.7.3 Nachweis

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

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

8.1.2.8.1 Kriterium

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

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

8.1.2.8.2 Umsetzungshinweis

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

8.1.2.8.3 Nachweis

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

8.2 Rechte und Pflichten des Cloud-Anbieters

8.2.1 Sicherstellung der Datensicherheit durch geeignete TOM nach dem Stand der Technik

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

8.2.1.1.1 Kriterium

- 1) Der Cloud-Anbieter führt eine Risikoanalyse in Bezug auf die Datensicherheit durch und verfügt über ein Datensicherheitskonzept entsprechend seiner Schutzklasse, das den spezifischen Risiken seiner Datenverarbeitungsvorgänge angemessen ist.
- 2) Im Datensicherheitskonzept stellt der Cloud-Anbieter dar, welche Datensicherheitsmaßnahmen er ergriffen hat, um die bestehenden Risiken abzustellen oder einzudämmen. Der Cloud-Anbieter schildert auch die Abwägungen, die er vorgenommen hat, um zu diesen Maßnahmen zu gelangen.
- 3) Das Datensicherheitskonzept ist schriftlich zu dokumentieren.
- 4) Das Datensicherheitskonzept ist in regelmäßigen Abständen auf Aktualität und Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren.
- 5) Das Datensicherheitskonzept beschreibt, welche Datenverarbeitungsvorgänge in der Verantwortung des Cloud-Anbieters liegen und für welche Datenverarbeitungsvorgänge eingebundene Subauftragsverarbeiter verantwortlich sind.
- 6) Das Datensicherheitskonzept beschreibt, welche Datenverarbeitungsvorgänge in der Verantwortung des Cloud-Anbieters liegen und welche der Verantwortung des Cloud-Nutzers unterliegen.
- 7) Soweit das Datensicherheitskonzept Sicherheitsmaßnahmen des Cloud-Nutzers verlangt, sind diese dem Cloud-Nutzer in Schriftform oder in einem elektronischen Format mitzuteilen.

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

8.2.1.1.2 Umsetzungshinweis

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

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

- 1) Evaluierung der Auswirkungen auf die Organisation, Technik oder Dienstbereitstellung aufgrund eines Sicherheitsausfalls und Berücksichtigung der Konsequenzen des Verlusts von Vertraulichkeit, Integrität oder Verfügbarkeit;
- 2) Evaluierung der realistischen Wahrscheinlichkeit eines solchen Sicherheitsausfalls unter Berücksichtigung aller denkbaren Bedrohungen und Sicherheitslücken;
- 3) Abschätzung des möglichen Schadensausmaßes für die Grundrechte und Freiheiten der betroffenen Personen;
- 4) Prüfung, ob alle möglichen Optionen für die Behandlung der Risiken identifiziert und evaluiert sind;
- 5) Bewertung, ob das verbleibende Risiko akzeptierbar oder eine Gegenmaßnahme erforderlich ist.

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

8.2.1.1.3 Nachweis

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

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

8.2.1.2.1 Kriterium

Schutzklasse 1

- 1) Der Cloud-Anbieter stellt durch risikoangemessene TOM sicher, dass Räume und Anlagen gegen Schädigung durch Naturereignisse gesichert werden und Unbefugten der Zutritt zu Räumen und Datenverarbeitungsanlagen verwehrt wird, um unbefugte Kenntnismöglichkeiten personenbezogener Daten und Einwirkungsmöglichkeiten auf die Datenverarbeitungsanlagen auszuschließen.
- 2) Die Maßnahmen sind geeignet, um im Regelfall den Zutritt Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert.

Schutzklasse 2

- 1) Die Kriterien von Schutzklasse 1 sind erfüllt.
- 2) Die Maßnahmen sind geeignet, Schädigungen durch fahrlässige Handlungen Befugter im Regelfall auszuschließen. Weiterhin ist sichergestellt, dass unbefugter Zutritt durch fahrlässige und vorsätzliche Handlungen hinreichend sicher ausgeschlossen ist. Dies schließt Schutz gegen Zutrittsversuche durch Täuschung oder Gewalt ein. Es besteht ein hinreichender Schutz gegen bekannte Angriffsszenarien.
- 3) Jeder unbefugte Zutritt und Zutrittsversuch ist nachträglich feststellbar.