European Cloud Service
Data Protection Certification

AUDITOR-Kriterienkatalog

Fassung 1.0

Stand 05.06.2024

Weitere AUDITOR-Dokumente:

- Zertifizierungsgegenstand (Kurz- und Langfassung)
- Konformitätsbewertungsprogramm
- Modularitätskonzept
- Schutzklassenkonzept

Online verfügbar: https://www.trusted-cloud.de

Empfohlene Zitation:

Roßnagel, A., Sunyaev, A., Maier-Reinhardt, N., Müller, J., Lins, S., & Teigeler, H. (2024). AUDITOR-Kriterienkatalog – Fassung 1.0. Online verfügbar: https://www.trusted-cloud.de

Beitrag zum Forschungsprojekt „European Cloud Service Data Protection Certification (AUDITOR)“, das aufgrund eines Beschlusses des Deutschen Bundestages vom Bundesministerium für Wirtschaft und Klimaschutz gefördert wird (FKZ 01MT17003A).

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Autoren

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

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

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

UNIKASSEL VERSITÄT

provet

Karlsruher Institut für Technologie

CRITICAL INFORMATION INFRASTRUCTURES RESEARCHGROUP

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
Anf.	Anforderung
Art.	Artikel
Alt.	Alternative
BDSG	Bundesdatenschutzgesetz (vom 30.6.2017)
BSI	Bundesamt für Sicherheit in der Informationstechnik
DSB	Datenschutzbeauftragter
DSGVO	EU-Datenschutz-Grundverordnung (Geltung ab 25.5.18)
EG	Erwägungsgrund
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
i.S.v.	Im Sinne von
i.V.m.	In Verbindung mit
lit.	litera (Buchstabe)
Nr.	Nummer
s.	siehe
TCDP	Trusted Cloud Datenschutz-Profil
TOM	technische und organisatorische Maßnahmen
Ziff.	Ziffer

Hinweis zur geschlechtsneutralen Formulierung:

Alle personenbezogenen Bezeichnungen im AUDITOR-Kriterienkatalog sind geschlechtsneutral zu verstehen. Zum Zweck der besseren Lesbarkeit wird daher auf die geschlechtsspezifische Schreibweise verzichtet, sodass die grammatikalisch maskuline Form kontextbezogen jeweils als Neutrum zu lesen ist (z.B. ist bei der Bezeichnung *Datenschutzbeauftragter* die Funktionsbezeichnung als Neutrum zu lesen und meint nicht einen ausschließlich maskulinen Personenbezug).

A. Gegenstand und Ziele des AUDITOR-Kriterienkatalogs

Der AUDITOR-Kriterienkatalog ist ein Prüfstandard für die Datenschutz-Zertifizierung von Cloud-Diensten gemäß den Anforderungen der EU-Datenschutz-Grundverordnung (DSGVO). Die AUDITOR-Zertifizierung stellt eine nationale Datenschutz-Zertifizierung gemäß Art. 42 DSGVO dar.[1]

1. Adressaten und Funktionen des AUDITOR-Kriterienkatalogs

Durch die AUDITOR-Datenschutz-Zertifizierung können Anbieter von Cloud-Diensten des privaten Sektors die Vereinbarkeit ihrer Datenverarbeitungsvorgänge mit datenschutzrechtlichen Anforderungen nachweisen. Der AUDITOR-Kriterienkatalog beschreibt die datenschutzrechtlichen Anforderungen an die Verarbeitung von personenbezogenen Daten auf der Seite des Auftragnehmers (Cloud-Anbieter). Dagegen werden die datenschutzrechtlichen Anforderungen an den Auftraggeber (Cloud-Nutzer) nicht adressiert.

Zertifizierungsgegenstand AUDITOR

Den Zertifizierungsgegenstand des AUDITOR-Verfahrens bilden Verarbeitungsvorgänge von personenbezogenen Daten im Kontext von Cloud-Diensten. Eine Datenverarbeitung ist nach Art. 4 Nr. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe. Dazu zählen das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten.

Den Zertifizierungsgegenstand bilden Datenverarbeitungsvorgänge, die in Produkten oder Diensten oder mit Hilfe von (auch mehreren) Produkten und Diensten erbracht werden. Schwerpunktmäßig werden im AUDITOR-Verfahren die Datenverarbeitungsvorgänge betrachtet, die der Cloud-Anbieter als Auftragsverarbeiter im Rahmen der Auftragsverarbeitung gemäß Art. 28 DSGVO durchführt. Es werden aber auch Datenverarbeitungsvorgänge betrachtet, die der Cloud-Anbieter als Verantwortlicher vornimmt, um den Vertrag mit dem Cloud-Nutzer über die Bereitstellung des Cloud-Dienstes schließen und diesen durchführen zu können und damit er rechtliche Pflichten erfüllen kann. Das Begleitdokument „AUDITOR-Zertifizierungsgegenstand“ erläutert, beschreibt und veranschaulicht Datenverarbeitungsvorgänge in Cloud-Diensten und führt typische Beispiele auf (siehe Abschnitt B. 2.2 des Dokuments).

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

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

- solche zur Durchführung: Daten, die sich aus der Verarbeitung der in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung vereinbarten Daten ergeben, um den Dienst im Hinblick auf das konzeptionelle Ziel des Dienstes zu erhalten, sowie Nutzungsdaten[2], um entsprechend die Dienstnutzung abrechnen zu können. Zu den Daten, die verarbeitet werden können, gehören beispielsweise Zahlungsinformationen (z. B. Bankverbindung), Benutzernamen und Passwörter für die Anmeldung beim Cloud-Dienst oder nutzerspezifische Qualitätsindikatoren (z. B. für die Überwachung oder die Erbringung von Dienstleistungen). Dazu zählen etwa der Name, eine Telefonnummer, eine Adresse, eine E-Mail-Adresse, um eine Rechnung übersenden zu können.

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

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

[1] Die AUDITOR-Zertifizierung allein stellt daher keine isolierte, geeignete Garantie für die Datenübermittlung gem. Art. 46 Abs. 2 lit. f DSGVO dar.
[2] "Nutzungsdaten" sind zusätzliche personenbezogene Daten wie z.B. Login-/Logout-Daten für Nutzerkonten, IP-Adressen, die genutzten Servicemodule und der Umfang der Nutzung, die sich aus der Nutzung des Dienstes ergeben.

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

Sobald der Cloud-Anbieter sich entschließt die Zertifizierung zu erlangen, wird er mit der Zertifizierungsstelle ausführliche Gespräche führen, um den Umfang der Zertifizierung und die konkreten Datenverarbeitungsvorgänge, die zertifiziert werden sollen, festzulegen. Das AUDITOR-Konformitätsbewertungsprogramm spezifiziert diese Prozesse und die Zertifizierungsstellen sind verpflichtet, die entsprechenden Prozesse zu befolgen und anzuwenden.[3] Beispiele für Datenverarbeitungsvorgänge, die ***nicht*** unter der AUDITOR-Zertifizierung zertifiziert werden können sind: a) Datenverarbeitungsvorgänge, die ausschließlich für die Verarbeitung als Verantwortlicher durchgeführt werden, um den Vertrag mit dem Cloud-Nutzer über die Erbringung des Cloud-Dienstes abzuschließen und zu erfüllen, OHNE dass die Datenverarbeitungsvorgänge in seiner Rolle als Auftragsverarbeiter zertifiziert werden; b) Datenverarbeitungsvorgänge, die der Durchführung rechtswidriger Tätigkeiten dienen; oder c) wenn die den Cloud-Anbieter betreffenden Rechtsvorschriften ihn daran hindern würden, die Grundsätze der DSGVO einzuhalten.

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

Datenverarbeitungsvorgänge müssen eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen, innerhalb derer die spezifischen Datenschutzrisiken des jeweiligen Cloud-Dienstes vollständig erfasst werden können. Dies bedeutet, dass auch Schnittstellen des zu zertifizierenden Cloud-Dienstes zu anderen Diensten betrachtet werden müssen, um Datenflüsse zu identifizieren, aus denen datenschutzrechtliche Risiken erwachsen können. Weiterführende Informationen zum Zertifizierungsgegenstand von AUDITOR und Beispiele für Datenverarbeitungsvorgänge sind dem Begleitdokument „AUDITOR-Zertifizierungsgegenstand“ zu entnehmen.

Cloud-Anbieter als Adressat

Cloud-Anbieter im Sinne dieses Katalogs ist jedes privatwirtschaftliche Unternehmen, das einen Cloud-Dienst am Markt anbietet und sich nach dem AUDITOR-Kriterienkatalog als Auftragsverarbeiter gemäß Art. 4 Nr. 8 DSGVO zertifizieren lassen möchte.

Cloud-Anbieter sind die Antragsteller im AUDITOR-Zertifizierungsverfahren und werden durch den AUDITOR-Kriterienkatalog in zweierlei Hinsicht adressiert:

1) *Als Auftragsverarbeiter* von Datenverarbeitungsvorgängen (siehe Kapitel C). Die Cloud-Anbieter können sowohl B2B[4]- als auch B2C[5]-Anbieter sein. Wichtig ist nur, dass sie hinsichtlich der Daten, die in der Cloud

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

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

[5] Business to Consumer (B2C) bedeutet, dass der Kunde eine natürliche und private Person ist und daher keine personenbezogenen Daten im Rahmen seiner Geschäftstätigkeit verarbeitet. Siehe auch „Cloud-Nutzer als Nutznießer“ (S. 8) in Bezug auf den Cloud-Nutzer als natürliche Person, die unter die „Haushaltsausnahme“ fällt. Ein „Verbraucher“ ist jede natürliche Person, die bei Verträgen zu Zwecken handelt, die nicht ihrer gewerblichen oder

verarbeitet werden (**„Inhalts- oder Anwendungsdaten“**[6]), als Auftragsverarbeiter und nicht als Verantwortliche tätig sind und die Datenschutzkonformität ihrer Datenverarbeitungsvorgänge durch ein Zertifikat bestätigen lassen möchten. Gerade im B2B-Bereich werden die Inhalts- und Anwendungsdaten häufig personenbezogene Daten von Kunden, Mitarbeitern oder anderen betroffenen Personen sein, mit denen der Cloud-Nutzer in Vertragsbeziehungen steht. Jedoch können Inhalts- und Anwendungsdaten auch personenbezogene Daten des Cloud-Nutzers sein.

2) *Als Verantwortlicher* von Datenverarbeitungsvorgängen (siehe Kapitel D). Der Cloud-Anbieter wird auch als Verantwortlicher von Datenverarbeitungsvorgängen adressiert, die erforderlich sind, um den Vertrag mit dem Cloud-Nutzer über die Bereitstellung des Cloud-Dienstes schließen und diesen durchführen zu können. Wird der Cloud-Dienst im B2C-Bereich angeboten, stellt der Cloud-Nutzer häufig auch die betroffene Person dar, deren Daten erforderlich sind, um den Cloud-Dienst bereitzustellen, sodass der Cloud-Anbieter seine datenschutzrechtlichen Pflichten (z.B. Informationspflichten) gegenüber dem Cloud-Nutzer erfüllen muss.

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

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

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

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

   Um dem Cloud-Nutzer die Inanspruchnahme des Cloud-Dienstes zu ermöglichen und diese abzurechnen, muss der Cloud-Anbieter weitere personenbezogene Daten wie beispielsweise Ein- und Auslogdaten zu Nutzkonten, IP-Adressen, die genutzten Dienstmodule und den Umfang der Nutzung verarbeiten. Diese

---

beruflichen Tätigkeit zugerechnet werden können. Es ist jedoch zu beachten, dass ein Verbraucher nicht automatisch unter die sogenannte „Haushaltsausnahme“ gemäß Art. 2 Abs. 2 lit.c DSGVO fällt. Diese Ausnahme ist der Nichtanwendbarkeit in Bezug auf die Verarbeitung personenbezogener Daten durch eine natürliche Person im Rahmen einer rein persönlichen oder häuslichen Tätigkeit vorbehalten. Die Datenverarbeitung eines Verbrauchers kann also entweder unter diese Ausnahmeregelung fallen oder nicht, was zur Folge hat, dass seine Datenverarbeitung entweder privilegiert ist oder nicht. Im letzteren Fall ist der Verbraucher als für die Verarbeitung Verantwortlicher zu behandeln.

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

Daten können unter dem Begriff **„Nutzungsdaten“**[7] zusammengefasst werden. Auch die Verarbeitung von Telemetrie- und Diagnosedaten fällt unter diesen Begriff, sofern die Daten für die Durchführung des Vertrags mit dem Cloud-Nutzer erforderlich sind.

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

Ein Cloud-Anbieter sollte davon absehen, eine Zertifizierung zu beantragen, wenn er weiß, dass die ihn betreffenden Rechtsvorschriften ihn daran hindern würden, die in diesem Zertifizierungsprogramm verankerten Grundsätze der DSGVO einzuhalten.

Cloud-Nutzer als Nutznießer

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

Da es sich bei einem Cloud-Nutzer um eine juristische Person handeln kann, ist zu beachten, dass seine Entscheidung, die Datenverarbeitung an einen Cloud-Anbieter auszulagern, im Allgemeinen bedeutet, dass personenbezogene Daten natürlicher Personen, die für ihn arbeiten, in Abhängigkeit von dem gewählten Dienst wahrscheinlich auch vom Cloud-Anbieter verarbeitet werden, um den Vertrag mit dem Cloud-Nutzer zu erfüllen. Folglich wird ein Cloud-Anbieter, der als für die Verarbeitung Verantwortlicher (Kapitel D) auftritt, Daten des Cloud-Nutzers, mit dem er einen Vertrag geschlossen hat, und der Personen, die für den Cloud-Nutzer arbeiten, verarbeiten, um die Erfüllung des Vertrags zu ermöglichen. Als weitere Folge bedeutet dies, dass der Begriff „Cloud-Nutzer“ in Kapitel D juristische und natürliche Personen sowie betroffene Personen umfasst, für die die Verarbeitung durch den Cloud-Anbieter als für die Verarbeitung Verantwortlicher vollständig DSVGO-konform sein muss.

Da ein Cloud-Nutzer auch eine natürliche Person sein kann, kann seine Datenverarbeitung als privilegiert zu behandeln sein.

Die Verarbeitung personenbezogener Daten durch den Cloud-Nutzer kann gemäß Art. 2 Abs. 2 lit. c DSGVO unter die sogenannte „Haushaltsausnahme“ fallen, wenn sie durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten erfolgt. Im Hinblick auf diese Verarbeitungen findet die DSGVO keine Anwendung. Da die Verarbeitung personenbezogener Daten im Rahmen der Haushaltsausnahme eher begrenzt ist, die Übergänge zur nicht privilegierten Verarbeitung fließend[8] sind und die Ausnahme von den Aufsichtsbehörden sehr restriktiv gehandhabt wird, findet das grundsätzliche Konzept des Cloud-Anbieters nach dem Bild der DSGVO als Auftragsverarbeiter auch in dieser Situation Anwendung.[9] So gilt die DSGVO weiterhin für den Cloud-Anbieter, der als Auftragsverarbeiter fungiert und die Mittel für eine solche Verarbeitung bereitstellt.[10]

Eine Verarbeitung einer natürlichen Person „im Rahmen ausschließlich persönlicher oder familiärer Tätigkeit“ kann z. B. anhand der folgenden allgemeinen Kriterien nachgewiesen werden[11]:

- Damit die Ausnahmeregelung gilt, muss eine „natürliche Person“ die Daten verarbeiten. Die Verarbeitung durch juristische Personen, unabhängig von ihrer Form (einschließlich NRO, Stiftungen, Treuhändlern und dergleichen), fällt nicht unter die Ausnahmeregelung
- Eine „persönliche oder familiäre Tätigkeit“ bezieht sich auf das „Privat“-Leben der verarbeitenden natürlichen Person. Die Abgrenzung zwischen „Privatleben“ und „Nicht-Privatleben“ kann aus der bestehenden Rechtsprechung abgeleitet werden:
    - Der Begriff „privat“ ist so auszulegen, dass er nur Tätigkeiten umfasst, die im Rahmen des Privat- oder Familienlebens des Einzelnen ausgeübt werden: „Insofern kann eine Tätigkeit nicht als ausschließlich persönlich oder familiär … angesehen werden, wenn sie zum Gegenstand hat, personenbezogene Daten einer unbegrenzten Zahl von Personen zugänglich zu machen,

[7] "Nutzungsdaten" sind zusätzliche personenbezogene Daten wie z.B. Login-/Logout-Daten für Nutzerkonten, IP-Adressen, die genutzten Servicemodule und der Umfang der Nutzung, die sich aus der Nutzung des Dienstes ergeben.
[8] Die Hürde einer Verarbeitung personenbezogener Daten als „ausschließlich persönliche oder familiäre Tätigkeit“ dürfte leicht überschritten werden, was zur Folge hat, dass die Privilegierung des Cloud-Nutzers durch die DSVGO endet. Er muss dann also seinen Pflichten als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO erfüllen.
[9] D.h. der Cloud-Anbieter muss alle Anforderungen erfüllen, die in Teil "C. Kriterien und Umsetzungshinweise für die Verarbeitung als Verantwortlicher" vorgesehen sind.
[10] Erwägungsgrund 18 DSGVO.
[11] https://gdprhub.eu/Article_2_GDPR#(c)_Processing_by_a_natural_person_in_the_course_of_purely_personal_or_household_activity. Siehe auch die Randnummern 11-14 der “EDSA-Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte“.

oder wenn sie sich auch nur teilweise auf den öffentlichen Raum erstreckt und dadurch auf einen Bereich außerhalb der privaten Sphäre desjenigen gerichtet ist, der die Daten verarbeitet“[12].

- Auch die Veröffentlichung personenbezogener Daten auf einer Blogging-Seite, die einer unbegrenzten Anzahl von Personen zugänglich ist, könnte daher nicht unter die Haushaltsausnahme fallen[13]. Dies gilt auch für ein Kamerasystem, das in einem Einfamilienhaus zum Schutz des Eigentums installiert ist, da es auch einen öffentlichen Raum erfasst[14].

- Der Unterschied zwischen „privatem“ und „nicht privatem“ Leben lässt sich auch aus Erwägungsgrund 18 der Datenschutz-Grundverordnung ableiten:
  - Persönlicher Schriftverkehr,
  - Vorhalten von Anschriftenverzeichnissen oder
  - die Nutzung von Social Networks und Online-Tätigkeiten solange es sich um ausschließlich persönliche oder familiäre Aktivitäten handelt, was bedeutet, dass der Austausch von Informationen mit einer begrenzten Anzahl von engen Freunden immer noch als rein persönliche Aktivität angesehen werden kann.

Die Feststellung, ob eine natürliche Person unter die Haushaltsausnahme fällt, wird in der Praxis nicht von Cloud-Anbietern durchgeführt werden, da sie einen Dienst anbieten müssen, der auf der Grundlage der Vorschrift vollständig DSGVO-konform ist, d. h. nicht auf der Annahme der Ausnahmeregelung beruht. Da der Dienst des Cloud-Anbieters also mit diesem Kriterienkatalog konform sein muss, da er sich ausschließlich an ihn und nicht an die betroffene Person richtet, könnte es dennoch von Interesse sein zu wissen, wie man feststellt, ob in der Praxis die Haushaltsausnahme gilt. Es gibt drei grundlegende Faktoren, die bei der Feststellung der Anwendung der Haushaltsausnahme berücksichtigt werden können:[15]

- der Raum, in dem die Verarbeitung stattfindet, ist zu bewerten. Tätigkeiten, die in einem privaten Raum stattfinden, können als „persönlich“ betrachtet werden. Öffentliche Orte oder allgemein zugängliche Websites sind von der Anwendung der Haushaltsausnahme ausgeschlossen.
- die Bewertung des sozialen Aspekts der Verarbeitung ist durchzuführen. Es ist zu prüfen, welche Beziehung zwischen der natürlichen Person, die die Verarbeitung vornimmt, und den betroffenen Personen besteht und wie groß der Kreis der Personen ist, die Zugang zu den personenbezogenen Daten haben.
- der von dem für die Verarbeitung Verantwortlichen verfolgten Zweck ist zu bestimmen. Nach Erwägungsgrund 18 dürfen diese Tätigkeiten keinen Bezug zu „beruflichen“ oder „wirtschaftlichen“ Zwecken haben. Werden mit den Tätigkeiten solche Zwecke verfolgt, gilt die Ausnahmeregelung folglich nicht.

Während die Anwendbarkeit der Haushaltsausnahme die Verpflichtungen des Cloud-Anbieters als Auftragsverarbeiter nicht berührt, unterliegt der Cloud-Nutzer nicht den Verpflichtungen der Datenschutz-Grundverordnung. Vor diesem Hintergrund werden die in Art. 28 (3) GDPR wie folgt unterschieden:

Soweit Art. 28 Abs. 3 DSGVO Pflichten enthält, die sich unmittelbar an den Auftragsverarbeiter richten, sind diese Pflichten vom Auftragsverarbeiter zu erfüllen. Insoweit ergibt sich aus der Anwendbarkeit der Haushaltsausnahme kein Änderungsbedarf. Dies gilt für die in Art. 28 Abs. 3 lit. a, b, c, d und h DSGVO aufgeführten Anforderungen.

Soweit Art. 28 Abs. 3 DSGVO jedoch an Pflichten nach der DSGVO anknüpft, denen ein für die Verarbeitung Verantwortlicher unterliegt und aus denen sich die Verpflichtung des Auftragsverarbeiters zur Unterstützung des für die Verarbeitung Verantwortlichen ableitet, muss die Anwendbarkeit der Haushaltsausnahme berücksichtigt werden. Aufgrund der Haushaltsausnahme unterliegt der Cloud-Nutzer nicht den Pflichten, die einem für die Verarbeitung Verantwortlichen obliegen (z. B. Art. 12 ff. GDPR, Art. 33 und 34 GDPR, Art. 35 und Art. 36 DSGVO). Es gibt also keinen „Anknüpfungspunkt“ für die Verpflichtung des Auftragsverarbeiters, den Verantwortlichen zu unterstützen. Dies gilt für die in Art. 28 Abs. 3 lit. e, f und g DSGVO aufgeführten Anforderungen. Ein diesbezüglicher Hinweis findet sich weiter unten unter den betroffenen Kriterien.

Vor einer Auslagerung seiner Verarbeitungen an einen Cloud-Anbieter sollte der Cloud-Nutzer prüfen, ob eine Auftragsverarbeitung bei seinen Verarbeitungsvorgängen zulässig ist oder an besondere Voraussetzungen (z.B. Verschwiegenheitspflichten von Rechtsanwälten [§§ 43a Abs. 2; 43e Bundesrechtsanwaltsordnung] und Ärzten [§ 9

[12] CJEU - C-25/17 - Jehovan todistajat, ECLI:EU:C:2018:551.
[13] CJEU - C-101/01 - Bodil Lindqvist, ECLI:EU:C:2003:596.
[14] CJEU- C-212/13 - František Ryneš, ECLI:EU:C:2014:2428.
[15] https://gdprhub.eu/Article_2_GDPR#(c)_Processing_by_a_natural_person_in_the_course_of_purely_personal_or_household_activity.

der (Muster-)Berufsordnung der Ärztekammer], die durch § 203 StGB geschützt sind) außerhalb der DSGVO geknüpft ist. Zu beachten gilt jedoch, dass sich die AUDITOR-Zertifizierung nicht an Cloud-Nutzer und Cloud-Anbieter aus dem öffentlichen Bereich richtet.

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

Cloud-Nutzer sollten unabhängig vom Vorhandensein der AUDITOR-Zertifizierung dennoch eine Bewertung der Rechtsvorschriften des Landes vornehmen, in dem die Daten gehostet werden, bevor sie Daten an einen nicht nach der DSGVO zertifizierten Auftragsverarbeiter übermitteln. Falls die Rechtsvorschriften kein angemessenes Schutzniveau vorsehen, sollten zusätzliche Maßnahmen ergriffen werden.

Personenbezogene Daten als das zu schützende Gut

Als *personenbezogene Daten* werden, der gesetzlichen Definition des Art. 4 Abs. 1 DSGVO entsprechend, alle Daten verstanden, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Im Cloud-Kontext können dies beispielsweise Anwendungsdaten des Cloud-Nutzers sein, soweit sie dem jeweiligen Datenverarbeiter die Identifizierung oder Identifizierbarkeit einer natürlichen Person ermöglichen. Die Cloud-Nutzer und Cloud-Anbieter müssen gemäß Art. 28 Abs. 3 UAbs. 1 Satz 1 DSGVO in einer rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung[16] festlegen, welche Arten personenbezogener Daten im Rahmen der Auftragsverarbeitung weisungsgebunden durch den Auftragsverarbeiter verarbeitet werden sollen.

Verantwortungsverteilung zwischen Cloud-Anbieter und Cloud-Nutzer

Da sich der Anwendungsbereich der Datenschutz-Zertifizierung nach AUDITOR auf die Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO erstreckt, adressiert der AUDITOR-Kriterienkatalog schwerpunktmäßig die datenschutzrechtlichen Anforderungen an den Cloud-Anbieter in seiner Funktion als Auftragsverarbeiter. Datenverarbeitungsvorgänge, bei denen der Cloud-Anbieter nicht lediglich weisungsgebunden agiert, sondern als Verantwortlicher über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet, werden im Rahmen der AUDITOR-Zertifizierung nur betrachtet, soweit es um die Verarbeitung personenbezogener Daten des Cloud-Nutzers oder anderer betroffener Personen wie beispielsweise der Mitarbeiter des Cloud-Nutzers geht, die erforderlich ist, um den Cloud-Dienst zu erbringen und um dessen Nutzung und Abrechnung zu ermöglichen und soweit die Datenverarbeitung zur Erfüllung rechtlicher Pflichten dient, denen der Cloud-Anbieter unterliegt.

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

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

Als Faustformel kann festgehalten werden, dass der Cloud-Nutzer regelmäßig für diejenigen personenbezogenen Daten als Verantwortlicher anzusehen ist, die er oder ihm zurechenbare Personen in die Cloud übertragen. Dies

[16] Die „rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung“ ist der Vertrag zwischen dem Cloud-Dienst-Anbieter du dem Kunden, der die Spezifika zur Datenverarbeitung in Übereinstimmung mit den Anforderungen aus Art. 28 Abs. 3 DSGVO beinhaltet.

betrifft die Inhalts- und Anwendungsdaten des Cloud-Nutzers. Der Cloud-Anbieter wird für diejenigen Datenverarbeitungsvorgänge verantwortlich sein, die er vornimmt, um den Cloud-Dienst zu erbringen und um dessen Nutzung und Abrechnung zu ermöglichen. In der Regel betrifft dies Bestands- und Nutzungsdaten.

Verantwortungsverteilung zwischen Cloud-Anbieter und Subauftragsverarbeiter

Der Cloud-Anbieter hat die Möglichkeit, den Cloud-Dienst nicht vollständig selbst zu erbringen, sondern sich für die Leistungserbringung weiterer Subauftragsverarbeiter zu bedienen, soweit der Cloud-Nutzer damit einverstanden ist. In diesem Fall können einzelne Abschnitte oder Teile des Datenverarbeitungsvorgangs an weitere Auftragsverarbeiter delegiert oder ausgelagert werden, sodass eine Leistungskette entsteht.

Die Auslagerung der Datenverarbeitung an weitere Subauftragsverarbeiter darf jedoch nicht dazu führen, dass die Vorgaben der Datenschutz-Grundverordnung in der Leistungskette missachtet werden. Vielmehr muss der Cloud-Anbieter als Hauptauftragsverarbeiter dafür Sorge tragen, dass auf allen Stufen die einschlägigen Vorschriften der Datenschutz-Grundverordnung von allen Subauftragsverarbeitern eingehalten werden. Für die Auftragsdurchführung gegenüber dem Cloud-Nutzer bleibt der Cloud-Anbieter durchgängig verantwortlich.

Setzen die zu zertifizierenden Verarbeitungsvorgänge eines Cloud-Dienstes auf nicht-anbietereigene Plattformen oder Infrastrukturen auf oder setzt der Auftragsverarbeiter sonstige Subauftragsverarbeiter ein, so kann sich das Zertifikat nur auf diejenigen Datenverarbeitungsvorgänge beziehen, die im Verantwortungsbereich des jeweiligen Auftragsverarbeiters liegen. Der Auftragsverarbeiter muss sich jedoch als Hauptauftragsverarbeiter davon überzeugen, dass auch diese fremden, von ihm genutzten Plattformen, Infrastrukturen und sonstigen Subauftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten und darf nur solche für die Erbringung seines Cloud-Dienstes einsetzen.

Ein Cloud-Anbieter darf daher nur solche Subauftragsverarbeiter auswählen, die gemäß Art. 28 Abs. 1 DSGVO ebenfalls *„geeignete Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet“.* Subauftragsverarbeiter können die geforderten geeigneten Garantien ihrerseits beispielsweise durch den Nachweis durchlaufener Zertifizierungsverfahren oder durch die Befolgung von anerkannten Verhaltensregeln (‚Code of Conduct‘) gemäß Art. 40 DSGVO erbringen. Kapitel V dieses Kriterienkatalogs regelt insbesondere die Subauftragsverarbeitung.

2. Fortentwicklung vom TCDP gemäß der Datenschutz-Grundverordnung

Die Zertifizierung nach dem alten Bundesdatenschutzgesetz wurde im Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ durch das im September 2016 finalisierte Trusted Cloud Datenschutz-Profil (TCDP) untersucht. Da bei der Entwicklung der Zertifizierungskriterien nach TCDP noch nicht alle einschlägigen internationalen Normen, neu entwickelten relevanten Kriterienwerke – z. B. ISO/IEC 27701 – und insbesondere die Anforderungen der Datenschutz-Grundverordnung berücksichtigt werden konnten, muss mit dem Geltungsbeginn der Datenschutz-Grundverordnung ab dem 25.5.2018 das TCDP-Kriterienwerk an die neuen Regelungen angepasst werden. Dies geschieht mit dem AUDITOR-Kriterienkatalog.

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

B. Aufbau und Nutzung des AUDITOR-Kriterienkatalogs

1. Elemente des Kriterienkatalogs

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

2. Schutzklassen

Anforderungen an TOM des Cloud-Dienstes werden nach Schutzklassen differenziert. Dabei orientiert sich der AUDITOR-Kriterienkatalog an dem TCDP-Schutzklassenkonzept. Das Begleitdokument *„Schutzklassenkonzept“* fasst die Konzeption und Abgrenzung der Schutzklassen ausführlich zusammen.

2.1 Das Schutzklassenkonzept

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

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

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

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

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

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

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

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

2.2 Die Schutzklassen des AUDITOR-Kriterienkatalogs

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

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

Nicht abschließende Beispiele für Daten mit extrem hohem Schutzbedarf:
- Daten von V-Leuten des Verfassungsschutzes;
- Daten über Personen, die mögliche Opfer von strafbaren Handlungen sein können;
- Adressen von Zeugen in bestimmten Strafverfahren.

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

a) Die Ermittlung der Schutzbedarfsklasse

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

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

Im Ergebnis wird der Schutzbedarf der konkreten Datenverarbeitung nach den Schutzbedarfsklassen kategorisiert. Die Schritte zwei und drei werden in diesem AUDITOR-Kriterienkatalog nicht weiter erläutert, weil sie vornehmlich den Cloud-Nutzer und nicht die Zertifizierung des Cloud-Anbieters als solche betreffen. Für weiterführende Informationen wird auf das Begleitdokument *„Schutzklassenkonzept“* verwiesen.

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

Schutzbedarfsklassen nach Datenart (Abstrakter Schutzbedarf – Schritt 1)

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

Datenarten mit normalem Schutzbedarf (Schutzbedarfsklasse 1)

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

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

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

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

Datenarten mit hohem Schutzbedarf (Schutzbedarfsklasse 2)

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

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

- Name, Anschrift eines Vertragspartners;
- Geburtsdatum;
- Familienstand;
- verwandtschaftliche Beziehungen und Bekanntenkreis;
- Daten über Geschäfts- und Vertragsbeziehungen;
- Kontext zu einem Vertragspartner (z.B. Gegenstand einer vereinbarten Leistung);
- Verarbeitungen nicht veränderbarer Personendaten, die lebenslang als Anker für Profilbildungen dienen können wie genetische Daten i.S.v. Art. 4 Nr. 13 DSGVO oder biometrische Daten i.S.v. Art. 4 Nr. 14 DSGVO;
- Daten über die rassische und ethnische Herkunft;
- Daten über politische Meinungen;
- religiöse oder weltanschauliche Überzeugungen;
- Gewerkschaftsangehörigkeit;
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person;
- Verarbeitungen eindeutig identifizierender, hoch verknüpfbarer Daten wie Krankenversichertennummern oder Steuernummern;
- Daten, die mögliche Auswirkungen auf das Ansehen/die Reputation der betroffenen Person haben;
- Daten über den geschützten inneren Lebensbereich der betroffenen Person (z.B. Tagebücher);
- Gesundheitsdaten i.S.v. Art. 4 Nr. 15 DSGVO;
- Grad der Behinderung;
- Verarbeitung von Daten mit inhärenter Intransparenz für die betroffene Person (Schätzwerte beim Scoring, Anwendung von Algorithmen);
- Einkommen;
- Sozialleistungen;
- Steuern;
- Ordnungswidrigkeiten;
- Daten über Mietverhältnisse;

- Patientenverwaltungsdaten (mit Ausnahme von besonders sensiblen Diagnosedaten und dergleichen);
- Arbeitszeitdaten;
- Mitgliederverzeichnisse;
- Melderegister;
- Zeugnisse und Prüfungsergebnisse;
- Versicherungsdaten;
- Personalverwaltungsdaten aus Beschäftigungsverhältnissen (mit Ausnahme von dienstlichen Beurteilungen und beruflicher Laufbahn);
- Verkehrsordnungswidrigkeiten;
- einfache Bewertungen eher geringer Bedeutung (z.B. Ja/Nein-Entscheidung bei Einstufung im Mobilfunkvertrag etc.);
- Zugangsdaten zu einem Dienst;
- Kommunikationsinhalte einer Person (z.B. E-Mail-Inhaltsdaten, Brief, Telefonat);
- (genauer) Aufenthaltsort einer Person;
- Finanzdaten einer Person (z.B. Kontostand, Kreditkartennummer, einzelne Zahlung);
- Kreditauskünfte;
- Verkehrsdaten der Telekommunikation.

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

Datenarten mit sehr hohem Schutzbedarf (Schutzbedarfsklasse 3)

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

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

Nicht abschließende Beispiele für Daten mit sehr hohem Schutzbedarf:

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

b) Schutzanforderungsklassen

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

Schutzanforderungsklasse 1

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

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

Schutzanforderungsklasse 2

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

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

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

Schutzanforderungsklasse 3

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

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

3. Nichtanwendbarkeit von Kriterien

Im Rahmen des Zertifizierungsverfahrens stellt der Cloud-Anbieter der Zertifizierungsstelle ausreichende Informationen zur Beurteilung, Abgrenzung und abschließenden Festlegung des Zertifizierungsgegenstands zur Verfügung. Dies schließt insbesondere die Dokumentation von Verantwortlichkeiten und – insofern anwendbar – die Einbindung von Subauftragsverarbeitern in die zu zertifizierenden Datenverarbeitungsvorgänge ein. In der Regel werden nicht alle Kriterien des AUDITOR-Kriterienkatalogs für jeden Zertifizierungsgegenstand anwendbar sein.

Das AUDITOR-Konformitätsbewertungsprogramm regelt, wie eine akkreditierte Zertifizierungsstelle die Nichtanwendbarkeit von Kriterien feststellt. Es verlangt, dass nicht anwendbare Kriterien dokumentiert werden und für jedes Kriterium eine detaillierte Begründung (d.h. warum es auf den spezifischen Zertifizierungsgegenstand nicht anwendbar ist) ebenfalls dokumentiert wird. Die Zertifizierungsstelle muss sicherstellen, dass sich die Beurteilung der Nichtanwendbarkeit auf die Besonderheiten eines bestimmten Zertifizierungsgegenstands (d.h. den zu zertifizierenden Cloud-Dienst und seine Verarbeitungsprozesse) bezieht und dass dieselbe Entscheidung über die Nichtanwendbarkeit für vergleichbare Zertifizierungsprozesse und Umstände getroffen wird, um die Möglichkeit der Willkür zu verhindern. Insbesondere sollte eine freie oder willkürliche Auswahl von Kriterien und die Feststellung der Nichtanwendbarkeit verhindert werden. Wenn die Zertifizierungsstelle Zweifel an der Nichtanwendbarkeit eines Kriteriums hat, versucht die Zertifizierungsstelle, die Unklarheiten zu beseitigen. Zu diesem Zweck können weitere Unterlagen und Erklärungen vom Cloud-Anbieter angefordert werden oder es können von der Zertifizierungsstelle Bestimmungsmethoden angewendet werden. Erteilt die Zertifizierungsstelle dem Cloud-Anbieter die Zertifizierung, stellt sie u.a. einen öffentlichen zusammenfassenden Bericht über das Ergebnis der Zertifizierung zur Verfügung. Der öffentliche zusammenfassende Bericht dokumentiert die Verwendung des Zertifizierungsgegenstands im Anwendungsbereich und die Anwendungsfälle in einer transparenten und nachvollziehbaren Weise, so dass der Einzelne in angemessener Zeit nachvollziehen kann, was bei der Nutzung des Zertifizierungsgegenstands im Sinne des Datenschutzrechts gewährleistet ist.

Nichtanwendbar sind Kriterien insbesondere dann, wenn der Cloud-Anbieter diese nicht erfüllen kann, weil sie außerhalb seines Verantwortungsbereichs liegen. So wird der Cloud-Anbieter beispielsweise nach Kriterium Nr. 6.2

zur Unterstützung des Cloud-Nutzers bei der Auskunftserteilung verpflichtet. Das Kriterium ist jedoch auf die Datenverarbeitungsvorgänge des Cloud-Anbieters nicht anwendbar und der Cloud-Anbieter somit von der Auskunftserteilung entbunden, wenn der Verantwortungsbereich für die betreffenden Daten beim Cloud-Nutzer liegt und dieser über Anwendungen und Dateien bestimmt (bspw. im Falle eines Infrastructure-as-a-Service-Dienstes). Das gleiche gilt, wenn nicht der Cloud-Anbieter, sondern Subauftragsverarbeiter für den Zugang zu Datenverarbeitungssystemen nach Nr. 2.3 verantwortlich sind. In diesem Fall ist Kriterium Nr. 2.3 auf den Cloud-Anbieter nicht anwendbar. Der Cloud-Anbieter muss sich jedoch davon überzeugen, dass die Subauftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten (siehe Nr. 10.4) und somit ihrerseits das Kriterium Nr. 2.3 erfüllen.

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

C. Kriterien für die Auftragsverarbeitung

Kapitel I: Rechtsverbindliche Vereinbarung zur Auftragsverarbeitung

Erläuterung

Der Cloud-Anbieter muss sicherstellen, dass die Leistungen gegenüber dem Cloud-Nutzer aufgrund einer rechtsverbindlichen Vereinbarung[17] erbracht werden, die die gesetzlichen Anforderungen der Datenschutz-Grundverordnung an die Auftragsverarbeitung erfüllt. Die gesetzlichen Anforderungen an diese Vereinbarung werden durch die nachfolgenden Kriterien der Nummern 1.1 bis 1.8 konkretisiert.

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

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

Kriterium

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

(2) Die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung ist schriftlich oder in einem elektronischen Format[18] abzufassen.

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

Erläuterung

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

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

Kriterium

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

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

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

Kriterium

[17] Art. 28 Abs. 3 UAbs. 1 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 UAbs. 1 Satz 1 DSGVO als Rechtsgrundlage für die Auftragsverarbeitung dienen.

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

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

Nr. 1.4– Festlegung von Weisungsbefugnissen (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h, UAbs. 2 DSGVO)

Kriterium

(1) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung sieht vor, dass die personenbezogenen Daten nur auf dokumentierte Weisung des Cloud-Nutzers – auch in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation – verarbeitet werden, sofern der Cloud-Anbieter nicht durch Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet ist.

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

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

(4) Wird eine rechtsverbindliche Vereinbarung zur Auftragsverarbeitung im Rahmen standardisierter Massengeschäfte auf der Basis von allgemeinen Geschäftsbedingungen geschlossen, hat der Cloud-Anbieter – bevor die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung geschlossen wird – 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.

(5) In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung verpflichtet sich der Cloud-Anbieter zur Information des Cloud-Nutzers, wenn er der Ansicht ist, dass eine Weisung des Cloud-Nutzers gegen datenschutzrechtliche Vorschriften verstößt.

Erläuterung

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

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

Nach Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a DSGVO kann die Weisungsbefolgung den Cloud-Anbieter jedoch nicht von der Gesetzestreue entbinden, sodass der Cloud-Anbieter nicht weisungsgedeckte Verarbeitungen durchführen darf, wenn er durch Unionsrecht oder mitgliedstaatliches Recht hierzu verpflichtet wird. Mit dieser Regelung soll Interessenkonflikten auf Seiten des Cloud-Anbieters vorgebeugt werden.

Nr. 1.5– Ort der Datenverarbeitung (indirekt Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h DSGVO)

Kriterium

(1) In der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung wird festgelegt, ob sich der Ort der Datenverarbeitung innerhalb der EU oder des EWR oder in einem Drittland befindet.[19]

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

[19] Dazu gehört auch der Ort, der von durch weiteren Auftragsverarbeitern (Subauftragsverarbeiter) durchgeführten Verarbeitungstätigkeiten, wenn der Cloud-Anbieter einen anderen Auftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten im Auftrag des für die Verarbeitung Verantwortlichen beauftragt.

(3) In der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung wird festgelegt, dass in den Fällen, in denen sich während ihres Geltungszeitraums der Ort der Verarbeitung ändert, der Cloud-Anbieter diese Änderung dem Cloud-Nutzer unverzüglich mitteilt.

(4) Die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung muss vorsehen, dass der Cloud-Nutzer effektiv einer Änderung hinsichtlich der Orte der Verarbeitung widersprechen kann, wenn diese substantielle Auswirkungen[20] auf die zuvor durchgeführten Beurteilungen haben.

Erläuterung

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

Nicht immer verhindert die ausschließliche Datenverarbeitung in der EU oder im EWR, dass personenbezogene Daten automatisch dem Zugriff staatlicher Stellen von Drittländern entzogen werden. Beispielsweise können durch den Cloud-Act auch Cloud-Anbieter mit Sitz in der EU, die zu einem US-Mutterkonzern gehören und die personenbezogene Daten ausschließlich in der EU oder im EWR verarbeiten, verpflichtet werden, diese in der EU oder im EWR gespeicherten personenbezogenen Daten gegenüber den staatlichen US-Stellen offenzulegen.

Ähnliche Regelungen kann es auch in anderen nationalen Gesetzen von Drittländern geben. Die Auswahl solcher Cloud-Anbieter ist nicht per se verboten, jedoch müssen Cloud-Nutzer und Cloud-Anbieter Lösungen finden, um die personenbezogenen Daten effektiv vor dem Zugang der staatlichen Stellen des betreffenden Drittlands zu schützen. Eine Möglichkeit ist z.B. die Einschaltung eines Treuhänders, der ausschließlich europäischem Recht unterliegt und der ausschließlichen Zugriff auf die ausgelagerten Daten des Cloud-Nutzers hat. Durch die Treuhandvereinbarung sind die personenbezogenen Daten weder im Besitz noch unter der Kontrolle des Cloud-Anbieters und könnten daher nicht an die staatlichen US-Stellen herausgegeben werden. Für einige Cloud-Dienste kann auch die Verschlüsselung eine Lösung sein. S. hierzu die Use Cases in Nr. 11.1 und die weiteren Ausführungen dort.

Nr. 1.6– Verpflichtung zur Vertraulichkeit (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b und h DSGVO)

Kriterium

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

Erläuterung

Die Verpflichtung zur Vertraulichkeit und die Belehrung zur Verschwiegenheit fördern das Gewährleistungsziel der Vertraulichkeit (SDM C1.4).

Dass die Vertraulichkeitspflicht der zur Datenverarbeitung befugten Personen über das Ende ihres Beschäftigungsverhältnisses hinaus fort gilt, geht nicht explizit aus dem Wortlaut des Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b DSGVO hervor. Nach dem Sinn und Zweck der Norm muss diese Vertraulichkeitspflicht jedoch über das Ende des Beschäftigungsverhältnisses fortgelten, da ansonsten kein angemessener Schutz von personenbezogenen Daten gewährleistet werden kann.

Nr. 1.7– Technisch-organisatorische Maßnahmen, Unterbeauftragung und Unterstützung (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. c, h i.V.m. Kap. III und Art. 32 bis 36 DSGVO)

Kriterium

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

(2) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung enthält die Angabe, ob der Cloud-Anbieter eine Pseudonymisierung, Anonymisierung oder Verschlüsselung (Nr. 2.7, Nr. 2.8 und Nr. 2.9) der zu verarbeitenden personenbezogenen Daten vornimmt. Die Angabe sollte klarstellen, ob diese Mechanismen auch gegenüber den Mitarbeitern des Cloud-Anbieters wirksam sind, die Zugang zu personenbezogenen Daten haben können.

[20] Eine substantielle Auswirkung auf die zuvor durchgeführten Bewertungen liegt vor, wenn der neue Ort der Verarbeitung eine Datenübermittlung außerhalb der EU/des EWR nach sich ziehen würde.

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

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

(5) Die Verfahren und TOM zur Unterstützung des Cloud-Nutzers bei der Erfüllung der Betroffenenrechte gemäß Nr. 6, bei der Durchführung einer Datenschutz-Folgenabschätzung gemäß Nr. 7 und zur Erfüllung der Meldepflicht bei Datenschutzverletzungen nach Nr. 8.2 werden in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt.[21]

Nr. 1.8– Rückgabe von Datenträgern und Löschung von Daten; Nachweis der Einhaltung der Vorschriften und Ermöglichung von und Mitwirkung an Audits (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. g und h DSGVO)

Kriterium

(1) Die Pflichten des Cloud-Anbieters zur Rückgabe aller Datenträger[22] (die personenbezogene Daten enthalten), Rückführung von allen personenbezogenen Daten und irreversiblen Löschung von personenbezogenen Daten nach Ende der Auftragsverarbeitung sind in einer rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festzulegen.

(2) Die Pflichten des Cloud-Anbieters, alle Informationen zur Verfügung zu stellen, die für den Nachweis der Einhaltung der in Art. 28 DSGVO erforderlich sind und die Audits, einschließlich Inspektionen, durch den für die Verarbeitung Verantwortlichen oder einen von ihm beauftragten Prüfer zulassen, müssen in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt sein.

Erläuterung

Ist der Cloud-Anbieter auch nach Ende der Auftragsverarbeitung aufgrund gesetzlicher Pflichten aus nationalem Mitgliedstaaten- oder Unionsrecht zur Speicherung oder Aufbewahrung von Daten verpflichtet, sind diese nicht zu löschen. Eine rechtliche Verpflichtung hierzu, die aus einem Drittstaat herrührt, ist dafür nicht hinreichend.

Jeder Cloud-Anbieter ist verpflichtet es dem Verantwortlichen zu ermöglichen, nachzuweisen, dass seine ausgewählten Auftragsverarbeiter die Verpflichtungen des Art. 28 DSGVO einhalten entweder durch das Zurverfügungstellen der relevanten Informationen oder dadurch, dass er Audits bezüglich seiner Dienste oder Vor-Ort-Inspektionen zulässt. Nur so kann der Verantwortliche sicherstellen, dass die Verarbeitung unter Einhaltung der DSGVO erfolgt. Die Verpflichtung des Anbieters ist eine aktive, d.h. er darf nicht nur „ermöglichen“ sondern muss es auch „zulassen“. Zu den damit verbundenen Audits können allgemeine Inspektionen, Audits des Managementsystems, technische Prüfungen und Zertifizierungen gehören.

[21] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

[22] ISO/IEC 2382:2015, Informationstechnik - Vokabular, 2121321, "Datenträger": Material, in oder auf dem Daten aufgezeichnet werden können und von dem Daten abgerufen werden können.

Kapitel II: Rechte und Pflichten des Cloud-Anbieters

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

Nr. 2.1 – Datensicherheitskonzept (Art. 24, 25, 28, 32, 35 i.V.m. Art. 5 Abs. 1 lit. f und Abs. 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter führt eine Risikoanalyse nach dem Stand der Technik in Bezug auf die Datensicherheit durch und unterhält ein Datensicherheitskonzept[23] entsprechend seiner Schutzklasse, das den spezifischen Risiken seiner Datenverarbeitungsvorgänge, die sich insbesondere durch Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von und unbefugten Zugang zu personenbezogenen Daten ergeben können, angemessen ist. Im Rahmen der Risikobeurteilung muss der Cloud-Anbieter insbesondere die für Kriterium Nr.2 spezifischen Risikoszenarien berücksichtigen und entsprechende TOM umsetzen.

(2) Der Cloud-Anbieter unterhält eine Beschreibung aller Datenkategorien, für die er eine Verarbeitung durch seinem Cloud-Dienst anbieten kann.

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

(4) Im Datensicherheitskonzept stellt der Cloud-Anbieter dar, welche TOM er umgesetzt hat, um die bestehenden Datensicherheitsrisiken abzustellen oder einzudämmen. Der Cloud-Anbieter schildert auch die Abwägungen, die er vorgenommen hat, um zu diesen Maßnahmen zu gelangen.

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

(6) Das Datensicherheitskonzept ist in regelmäßigen Abständen (d.h. mindestens jährlich und nach jeder erheblichen Veränderung) auf Aktualität und Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren. Falls das Datensicherheitskonzept aktualisiert werden muss, muss der Cloud-Anbieter den Cloud-Nutzer vor Umsetzung des Updates informieren.

(7) Das Datensicherheitskonzept beschreibt, welche Datenverarbeitungsvorgänge vom Cloud-Anbieter selbst durchgeführt werden und welche Datenverarbeitungsvorgänge von Subauftragsverarbeitern durchgeführt werden.

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

(9) Soweit das Datensicherheitskonzept Sicherheitsmaßnahmen des Cloud-Nutzers verlangt, sind diese dem Cloud-Nutzer vor dem Beginn der Datenverarbeitung oder vor Änderungen an diesen schriftlich oder in einem elektronischen Format mitzuteilen.

Erläuterung

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

[23] Ein Datensicherheitskonzept dokumentiert u.a. Schutzprinzipien, identifizierte Risiken und festgelegte TOMs zum Schutz der verarbeiteten Daten. In englischen Sprachfassungen ist auch der Begriff „data security program“ geläufig.

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

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter stellt durch risikoangemessene TOM sicher, dass Räume und Anlagen gegen Schädigung durch höhere Gewalt[24] gesichert werden und Unbefugten der Zutritt zu Räumen und Datenverarbeitungsanlagen verwehrt wird, um unbefugte Kenntnisnahmen personenbezogener Daten und Einwirkungsmöglichkeiten auf die Datenverarbeitungsanlagen auszuschließen.

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

(3) Die Maßnahmen sind geeignet, um den Zutritt Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen Dritter auszuschließen. Der Cloud-Anbieter muss mindestens eine Reihe von Sicherheitsanforderungen für jede Sicherheitszone umsetzen und dokumentieren.

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

(5) Jeder befugte Zutritt wird protokolliert.

Schutzklasse 2 und 3

(6) Die Kriterien von Schutzklasse 1 sind erfüllt.

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

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

Erläuterung

Dieses Kriterium konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und 5 Abs. 1 lit. f DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Verfügbarkeit, Integrität, Vertraulichkeit (SDM C1.2 – C1.4) von personenbezogenen Daten und Diensten auf Dauer zu gewährleisten. Soweit der Cloud-Anbieter für den Sicherheitsbereich und die Zutrittskontrolle zu Räumen und Datenverarbeitungsanlagen verantwortlich ist, benötigt er ein Berechtigungskonzept für den Zutritt zu Datenverarbeitungsanlagen. Die Zutrittskontrolle gewährleistet den Zutrittsschutz nicht nur im Normalbetrieb, sondern auch im Zusammenhang mit höherer Gewalt.

[24] Nach einer auf verschiedenen Gebieten des Unionsrechts entwickelten ständigen Rechtsprechung sind unter „höherer Gewalt“ ungewöhnliche und unvorhersehbare Ereignisse zu verstehen, auf die derjenige, der sich darauf beruft, keinen Einfluss hat und deren Folgen trotz Anwendung der gebotenen Sorgfalt nicht hätten vermieden werden können, vgl. ECLI:EU:C:2017:39, Rn. 53.

Nr. 2.3 – Zugangskontrolle[25]
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

Schutzklasse 1

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

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

(3) Der Cloud-Anbieter überprüft den Zugang von Befugten über das Internet durch eine Zwei-Faktor- Authentifizierung. Der Zugang über das Internet wird über Transportverschlüsselung nach dem Stand der Technik umgesetzt.

Die Maßnahmen zur Zugangskontrolle sind so ausgestaltet um im Regelfall den Zugang zu Datenverarbeitungssystemen durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen. Die Maßnahmen müssen sicherstellen, dass durch die Dokumentation und Umsetzung von Verfahren zur Vergabe, Aktualisierung und Aufhebung von Zugriffsrechten ein unbefugter Zugang zu Datenverarbeitungssystemen verhindert wird.

Schutzklasse 2

(4) Die Kriterien von Schutzklasse 1 sind erfüllt.

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

Schutzklasse 3

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

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

Erläuterungen

Das Kriterium der Zugangskontrolle konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele der Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen. Soweit der Cloud-Anbieter für den Zugang zu Datenverarbeitungssystemen verantwortlich ist, benötigt er ein Berechtigungskonzept für den Zugang zu Datenverarbeitungssystemen.

Nr. 2.4– Zugriffskontrolle[26]
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

Schutzklasse 1

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

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

[25] Der Zugang bezieht sich auf jede Form der Annäherung an Datenverarbeitungssysteme. Im Gegensatz dazu bezieht sich der Zugriff auf jede Form der tatsächlichen Nutzung von Datenverarbeitungssystemen.
[26] Der Zugriff bezieht sich auf jede Form der tatsächlichen Nutzung von Datenverarbeitungssystemen. Im Gegensatz dazu bezieht sich der Zugang auf jede Form der Annäherung an Datenverarbeitungssysteme.

(3) Der Cloud-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zugriff auf personenbezogene Daten in regelmäßigen Abständen (mindestens jährlich oder bei wesentlichen Veränderungen) auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

(4) Der Cloud-Anbieter kontrolliert (d.h. überwacht und bewertet) und protokolliert alle Zugriffe auf personenbezogene Daten.

(5) Die Maßnahmen sind geeignet, um im Regelfall den Zugriff auf personenbezogene Daten durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen Die Maßnahmen müssen sicherstellen, dass vorsätzliche Eingriffe in der Regel verhindert werden.

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

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

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

Schutzklasse 2

(9) Die Kriterien von Schutzklasse 1 sind erfüllt.

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

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

Schutzklasse 3

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

(13) Unbefugte Zugriffe auf Daten sind bezogen auf die Ergebnisse der Risikoanalyse ausgeschlossen. Dies schließt regelmäßig manipulationssichere technische Maßnahmen zur Prävention und aktiven Erkennung von Angriffen ein. Jeder unbefugte Zugriff und entsprechende Versuche sind nachträglich feststellbar.

Erläuterungen

Das Kriterium der Zugriffskontrolle konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen. Dies setzt ein Berechtigungskonzept für den Zugriff auf personenbezogenen Daten voraus.

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

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

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter setzt bei Datenübertragungsvorgängen eine Transportverschlüsselung nach dem Stand der Technik ein oder fordert dies durch entsprechende Konfiguration von Schnittstellen. Er muss zudem die offiziellen Normen oder die dem Stand der Technik entsprechenden Spezifikationen dokumentieren, die er zur Festlegung seiner TOM in Bezug auf Transportverschlüsselung nutzt. Die eingesetzte Transportverschlüsselung muss gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

(2) Die Maßnahmen sind geeignet, im Regelfall Angriffe Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen. Die Maßnahmen sind ferner geeignet, die

fahrlässige Weitergabe von Daten an Unbefugte durch den Cloud-Anbieter und seine Mitarbeiter auszuschließen. Schutzmaßnahmen verhindern vorsätzliche Eingriffe. Bei verschlüsselter Übertragung sind die Schlüssel gemäß offizieller Normen oder des Standes der Technik sicher aufzubewahren und der Zugriff zum Schlüssel muss kontrolliert werden (Nr. 2.4).

(3) Der Cloud-Anbieter protokolliert automatisiert die Metadaten[27] aller Datenübertragungsvorgänge, einschließlich der Empfänger, auch solche vom und an den Cloud-Nutzer oder an Subauftragsverarbeiter. Nr. 2.6 (1) findet entsprechende Anwendung.

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

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

Schutzklasse 2

(6) Die Kriterien von Schutzklasse 1 sind erfüllt.

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

Schutzklasse 3

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

(9) Der Cloud-Anbieter schließt unbefugtes Lesen, Kopieren, Verändern oder Entfernen von aus. Er ergreift regelmäßig Maßnahmen zur aktiven Erkennung und Abwehr von Angriffen und stellt jedes unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten und auch jeden entsprechenden Versuch nachträglich fest.

Erläuterungen

Das Kriterium der Übertragungs- und Transportkontrolle konkretisiert die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen und personenbezogene Daten gegen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugten Zugang oder unbefugte Offenlegung während der elektronischen Übertragung, des Transports oder der Speicherung auf Datenträgern zu schützen.

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

Kriterium

Schutzklasse 1

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

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

[27] Metadaten beziehen sich auf Informationen, die andere Daten beschreiben. Sie liefern Kontext, Attribute und Details zu einem bestimmten Datensatz und helfen dabei, diesen zu organisieren, zu verstehen und zu verwalten. Einfacher ausgedrückt: Metadaten sind Daten über Daten.

(3) Der Cloud-Anbieter muss Verfahren zur Analyse und Überprüfung von Protokollen einrichten, um Anomalien und Vorfälle effektiv erkennen und in der Folge einen Alarm auslösen zu können. Er muss derartige Ereignisse bei der Prüfung der Risikoanalyse miteinbeziehen (Nr. 2.1 [6]).

Schutzklasse 2

(4) Die Kriterien von Schutzklasse 1 sind erfüllt.

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

Schutzklasse 3

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

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

Erläuterung

Das Kriterium der Nachvollziehbarkeit konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen und personenbezogene Daten gegen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugten Zugang oder unbefugte Offenlegung zu schützen. Hierzu muss nachträglich überprüft und festgestellt werden können, ob, wann und von wem und mit welchen inhaltlichen Auswirkungen personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, um gegebenenfalls Zugriffsrechte für die Zukunft anders zu gestalten. Zur sicheren Aufbewahrung der Protokolldaten gehört auch, dass die Auswertbarkeit der Protokolldaten sichergestellt ist.

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

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

Kriterium

Schutzklasse 1

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

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

Schutzklasse 2 und 3

(3) Die Kriterien von Schutzklasse 1 sind erfüllt.

(4) Soweit mit dem Cloud-Nutzer vereinbart (Nr. 1.7), stellt der Cloud-Anbieter sicher, dass die Daten pseudonymisiert verarbeitet werden. Entsprechend der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung pseudonymisiert der Cloud-Nutzer die personenbezogenen Daten selbst oder der Cloud-Anbieter führt die Pseudonymisierung auf Weisung des Cloud-Nutzers durch.

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

(6) Ist die Pseudonymisierung der Daten auf Weisung des Cloud-Nutzers nicht gegenüber allen Mitarbeitern des Cloud-Anbieters wirksam, ist der Kreis der privilegierten Mitarbeiter auf das unbedingt Erforderliche zu begrenzen.

(7) Der Cloud-Anbieter gewährleistet, dass er die technische Entwicklung im Bereich der Pseudonymisierungsverfahren laufend verfolgt (mindestens jährlich) und seine Verfahren dem Stand der Technik[28] entsprechen.

Erläuterung

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

Die Pseudonymisierung wird neben der Verschlüsselung in Art. 32 Abs. 1 lit. a DSGVO explizit als einzusetzende Sicherheitsmaßnahme benannt. Sie trägt dazu bei, das Gewährleistungsziel der Nichtverkettung (SDM C1.5) zu fördern. Da durch Pseudonymisierung Dritte selbst bei einem unbefugten Zugriff auf den Cloud-Dienst keine Kenntnis von den personenbezogenen Daten erlangen können oder der Personenbezug zumindest erheblich erschwert wird, mindert die Pseudonymisierung die Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen.

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

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter stellt durch implementierte TOMs[29] sicher, dass Anonymisierung[30] (d.h. eine Re-Identifizierung personenbezogener Daten in einem anonymisierten Datensatz) nicht rückgängig gemacht werden kann.

Schutzklasse 2 und 3

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

(3) Wird die Anonymisierung vom Cloud-Anbieter durchgeführt, so gewährleistet er, dass er die technische Entwicklung im Bereich der Anonymisierungsverfahren laufend verfolgt und seine Verfahren dem Stand der Technik[31] entsprechen.

[28] Der Stand der Technik umfasst das, was derzeit als beste Praktiken, Technologien, Methoden und Strategien zum Schutz von Informationssystemen allgemein anerkannt ist. Der Stand der Technik bedeutet nicht notwendigerweise die technologisch fortschrittlichste Lösung, sondern umfasst robuste Technologien und Prozesse sowie qualifiziertes Personal, um wirksam gegen die sich fortentwickelnden Datenschutzbedrohungen zu schützen.
[29] Technische Schutzmaßnahmen können die Verhinderung von automatischer Datenaggregation, -synthese usw. umfassen, die zur Aufhebung der Anonymisierung führen könnten, sowie die Verwaltung der Zugriffsrechte der autorisierten Mitarbeiter, um böswilliges Verhalten zu verhindern. Organisatorische Schutzmaßnahmen stellen u. a. sicher, dass Mitarbeiter kein Verhalten an den Tag legen, das auf die Aufhebung der Anonymisierung abzielt, wie z. B. das Ausfragen von Cloud-Nutzern über ihre Anonymisierungspraktiken, um potenzielle Schwachstellen oder Schwachpunkte der angewandten Anonymisierungstechniken auszunutzen.
[30] TOMs in Bezug auf die Anonymisierung müssen daher offiziellen Normen oder dem Stand der Technik entsprechen.
[31] Der Stand der Technik umfasst das, was derzeit als beste Praktiken, Technologien, Methoden und Strategien zum Schutz von Informationssystemen allgemein anerkannt ist. Der Stand der Technik bedeutet nicht notwendigerweise die technologisch fortschrittlichste Lösung, sondern umfasst robuste Technologien und Prozesse sowie qualifiziertes Personal, um wirksam gegen die sich fortentwickelnden Datenschutzbedrohungen zu schützen.

Erläuterung

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

Die Anonymisierung ist neben dem Verzicht der Datenerhebung die wirksamste Maßnahme zur Datenvermeidung und Datenminimierung. Sie trägt dazu bei, das Gewährleistungsziel der Datenminimierung (SDM C1.1) zu fördern.

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

Kriterium

Schutzklasse 1

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

(2) Sofern der Cloud-Anbieter Verfahren zur Verschlüsselung anbietet, muss er die Kriterien der Schutzklasse 2 erfüllen.

Schutzklasse 2

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

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

(5) Der Cloud-Anbieter verfolgt laufend die technische Entwicklung im Bereich der Verschlüsselung. Die von ihm getroffenen Maßnahmen, insbesondere ein sicheres Schlüsselmanagement, entsprechen dem Stand der Technik[33].

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

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

Schutzklasse 3

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

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

(10) Der Cloud-Anbieter stellt sicher, dass seine unterstützenden Maßnahmen in Form von Dokumentationen und Hilfsmaßnahmen zur Durchführung von Verschlüsselung dem Stand der Technik[34] entsprechen.

Erläuterung

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

---

[32] Gespeicherte Daten umfassen auch die Backups gespeicherter Daten.

[33] Der Stand der Technik umfasst das, was derzeit als beste Praktiken, Technologien, Methoden und Strategien zum Schutz von Informationssystemen allgemein anerkannt ist. Der Stand der Technik bedeutet nicht notwendigerweise die technologisch fortschrittlichste Lösung, sondern umfasst robuste Technologien und Prozesse sowie qualifiziertes Personal, um wirksam gegen die sich fortentwickelnden Datenschutzbedrohungen zu schützen.

[34] Der Stand der Technik umfasst das, was derzeit als beste Praktiken, Technologien, Methoden und Strategien zum Schutz von Informationssystemen allgemein anerkannt ist. Der Stand der Technik bedeutet nicht notwendigerweise die technologisch fortschrittlichste Lösung, sondern umfasst robuste Technologien und Prozesse sowie qualifiziertes Personal, um wirksam gegen die sich fortentwickelnden Datenschutzbedrohungen zu schützen.

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

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

Die Verschlüsselung wird neben der Pseudonymisierung in Art. 32 Abs. 1 lit. a DSGVO explizit als eine einzusetzende Sicherheitsmaßnahme benannt. Zweck der Verschlüsselung ist es, die Gewährleistungsziele der Vertraulichkeit und Integrität (SDM C1.4 und C1.3) sicherzustellen. Die Schwelle, ab der zu verschlüsseln ist, ist niedrig, sodass personenbezogene Daten bereits bei niedrigem Risiko verschlüsselt werden sollten, soweit dies möglich ist.

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

Kriterium

Schutzklasse 1

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

(2) Der Cloud-Anbieter verhindert Verletzungen der Datentrennung, die durch technische oder organisatorische Fehler, einschließlich Bedienfehlern, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen des Cloud-Nutzers oder verursacht werden.

Schutzklasse 2

(3) Die Kriterien von Schutzklasse 1 sind erfüllt.

(4) Der Cloud-Anbieter muss Schutz vor bekannten Angriffsszenarien gegen das Trennungsgebot anbieten. Der Cloud-Anbieter kann vorsätzliche Verstöße gegen das Trennungsgebot im Regelfall (nachträglich) feststellen.

Schutzklasse 3

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

(6) Der Cloud-Anbieter schließt eine Verletzung der Datentrennung aus. Der Cloud-Anbieter erkennt vorsätzliche Verstöße gegen die getrennte Verarbeitung.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Verfügbarkeit, Integrität, Vertraulichkeit und Nichtverkettung (SDM C1.2 – C1.5) und zielt damit auch auf die Sicherstellung des Zweckbindungsgrundsatzes aus Art. 5 Abs. 1 lit. b DSGVO. Eine sichere Mandantentrennung schützt die Daten vor unbefugtem Zugang, Veränderungen und Vernichtung und verhindert eine unerwünschte Verkettung der Daten.

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

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

Kriterium

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

Wiederherstellbarkeitsklasse 1

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

Wiederherstellbarkeitsklasse 2

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

Wiederherstellbarkeitsklasse 3

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

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

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Verfügbarkeit (SDM C1.2). Gemäß Art. 32 Abs. 1 lit. c DSGVO muss die Wiederherstellung „rasch“ erfolgen. Was als „rasch“ gilt, hängt auch von der Schwere des Zwischenfalls und der Bedeutung der Systeme und Daten ab. Z.B. sind an die Wiederherstellbarkeit des Dienstes und der Daten im Krankenhaus strengere Anforderungen zu stellen als an die im Datenarchiv.

Da die Verfügbarkeit von Diensten und personenbezogenen Daten nicht notwendigerweise mit ihrer Schutzbedürftigkeit nach dem Schutzklassenkonzept zusammenfallen muss, sondern auf der Seite des Cloud-Nutzers auch das Erfordernis bestehen kann, dass personenbezogene Daten der Schutzklasse 1 nach einem physischen oder technischen Zwischenfall sehr schnell wiederhergestellt sein müssen, wird bei diesem Kriterium nicht nach den Schutzklassen unterschieden.

Stattdessen wird die Möglichkeit der Wiederherstellung in den Wiederherstellbarkeitsklassen 1, 2 und 3 ausgedrückt. Für eine Differenzierung spricht auch, dass es bei der Wiederherstellung nach einem physischen oder technischen Zwischenfall nicht wie bei den anderen Kriterien der Nummer 2 um den Normalbetrieb geht, sondern um physische oder technische Störfälle.

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

Nr. 3 – Sicherstellung der Weisungsbefolgung (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h; 29; 32 Abs. 4 DSGVO)

Kriterium

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

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

(3) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf Grundlage dokumentierter Weisung des Verantwortlichen, auch in Bezug auf die Datenübermittlung an ein Drittland oder eine internationale Organisation, sofern er nicht durch ein ihn betreffendes Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet ist; in diesem Fall soll der Auftragsverarbeiter den Verantwortlichen hinsichtlich dieser rechtlichen Verpflichtung vor der Datenverarbeitung informieren, sofern das jeweilige Recht die Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(4) Im Rahmen von standardisierten Massengeschäften gewährleistet der Cloud-Anbieter die Einhaltung einer konkreten und nachvollziehbaren Dienstbeschreibung zu den von ihm technisch ausführbaren Dienstleistungen, damit der Cloud-Nutzer auf diese Weise den Cloud-Anbieter durch seine konkrete Auswahl der Dienste für die Auftragsverarbeitung anweisen kann. Zudem ermöglicht er dem Cloud-Nutzer, Weisungen mittels Softwarebefehlen (oder andere Mittel) zu erteilen, die automatisiert ausgeführt und dokumentiert werden.

Nr. 4– Hinweispflicht des Cloud-Anbieters

Nr. 4.1 – Weisungen entgegen datenschutzrechtlicher Vorschriften (Art. 28 Abs. 3 UAbs. 2 lit. h i.V.m Art. 29 DSGVO)

Kriterium

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

Erläuterung

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

Nr. 4.2 – Änderungen des Datenverarbeitungsortes (indirekt Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h DSGVO)

Kriterium

Der Cloud-Anbieter informiert den Cloud-Nutzer immer unverzüglich und in der Regel im Voraus in allen Fällen, in denen sich während des Geltungszeitraums der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung der Ort der Datenverarbeitung gegenüber dem in der rechtsverbindlichen Vereinbarung zur Auftragsvereinbarung festgelegten (Nr. 1.5) ändern wird.

.

Nr. 5 – Sicherstellung der Vertraulichkeit beim Personal (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b und h DSGVO)

Kriterium

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

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

Erläuterung

Die Verpflichtung zur Vertraulichkeit und die Belehrung zur Verschwiegenheit fördern das Gewährleistungsziel der Vertraulichkeit (SDM C1.4) (s. auch Nr. 1.6).

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

Nr. 6 – Unterstützung des Cloud-Nutzers bei der Wahrung der Betroffenenrechte[35]

Erläuterung

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

Wenn die betroffene Person ihre Rechte nach Art. 15 bis 22 DSGVO elektronisch ausübt, sollten die Informationen über die auf den Antrag hin ergriffenen Maßnahmen des Cloud-Nutzers gemäß Art. 12 Abs. 3 Satz 4 DSGVO ebenfalls, nach Möglichkeit, elektronisch bereitgestellt werden, außer die betroffene Person hat einen anderen Informationsweg gewünscht. Es ist jedoch zu beachten, dass Art. 22 DSGVO bei der AUDITOR-Zertifizierung in Kapitel C nicht betrachtet wird.

Nr. 6.1 – Informationserteilung[36] (Art. 13 oder 14 i.V.m. Art. 12 Abs. 1 und Art. 5 Abs. 1 lit. a DSGVO)

Kriterium

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

(2) Der Cloud-Anbieter dokumentiert die vom Cloud-Nutzer erhaltenen Weisungen zur Umsetzung der Informationspflicht des Cloud-Nutzers oder wenn er ihn dabei unterstützt.

Erläuterung

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

Der Cloud-Anbieter hat den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

Nr. 6.2 – Auskunftserteilung[37] (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 15 DSGVO)

Kriterium

[35] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

[36] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

[37] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

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

(2) Der Cloud-Anbieter dokumentiert die vom Cloud-Nutzer erhaltenen Weisungen zur Umsetzung der Auskunftserteilungspflicht des Cloud-Nutzers oder wenn er ihn dabei unterstützt.

Erläuterung

Der Cloud-Nutzer ist nach Art. 15 DSGVO verpflichtet, der betroffenen Person auf Antrag Auskunft über eine Datenverarbeitung und ihre Umstände zu erteilen. Der Cloud-Anbieter hat den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

Nr. 6.3– Berichtigung und Vervollständigung[38] (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 16 DSGVO)

Kriterium

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

(2) Der Cloud-Anbieter dokumentiert die vom Cloud-Nutzer erhaltenen Weisungen zur Umsetzung der Berichtigungs- und Vervollständigungspflicht des Cloud-Nutzers oder wenn er ihn dabei unterstützt.

Erläuterung

Der Cloud-Nutzer ist nach Art. 16 DSGVO verpflichtet, auf Antrag unrichtige personenbezogene Daten zu berichtigen und unvollständige personenbezogene Daten zu vervollständigen. Der Cloud-Anbieter ist verpflichtet, den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Die Berichtigung gemäß Art. 16 DSGVO fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

Nr. 6.4– Löschung (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 17 Abs. 1 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass der Cloud-Nutzer die Möglichkeit hat, die Löschung personenbezogener Daten selbst vorzunehmen oder durch den Cloud-Anbieter vornehmen zu lassen, sodass die personenbezogenen Daten irreversibel gelöscht sind und aus ihnen keine Informationen über die betroffene Person gewonnen werden können. Der Cloud-Anbieter stellt sicher, dass die Löschung unwiderruflich erfolgt, indem er Maßnahmen nach dem Stand der Technik erfolgt.

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

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

(4) Der Cloud-Anbieter dokumentiert die vom Cloud-Nutzer erhaltenen Weisungen zur Umsetzung der Verpflichtung in Bezug auf das Rechts auf Löschung oder wenn er ihn dabei unterstützt.

Erläuterung

Der Cloud-Nutzer ist nach Art. 17 Abs. 1 DSGVO verpflichtet, personenbezogene Daten zu löschen. Der Cloud-Anbieter ist verpflichtet, den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert die Gewährleistungsziele der Intervenierbarkeit und Nichtverkettung (SDM C1.7 und C1.5).

Nr. 6.5– Einschränkung der Verarbeitung[39] (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 18 Abs. 1 DSGVO)

Kriterium

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

(2) Der Cloud-Anbieter dokumentiert die vom Cloud-Nutzer erhaltenen Weisungen zur Umsetzung des Rechts auf Einschränkung der Verarbeitung oder wenn er ihn dabei unterstützt.

[38] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

[39] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

Erläuterung

Der Cloud-Nutzer ist nach Art. 18 Abs. 1 DSGVO verpflichtet, die Verarbeitung personenbezogener Daten unter bestimmten Voraussetzungen einzuschränken. Der Cloud-Anbieter ist verpflichtet, den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

Nr. 6.6 – Mitteilungspflicht bei Berichtung, Löschung oder Einschränkung der Verarbeitung[40] (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 19 DSGVO)

Kriterium

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

(2) Der Cloud-Anbieter dokumentiert die vom Cloud-Nutzer erhaltenen Weisungen zur Umsetzung der Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung oder wenn er ihn dabei unterstützt.

Erläuterung

Der Cloud-Nutzer ist nach Art. 19 DSGVO verpflichtet, Empfängern, denen er personenbezogene Daten offengelegt hat, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitzuteilen und die betroffene Person auf Verlangen über die Empfänger zu unterrichten. Soweit der Cloud-Anbieter an der Offenlegung beteiligt war, ist er verpflichtet, den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

Nr. 6.7 – Datenübertragung[41] (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 20 Abs. 1 und 2 DSGVO)

Kriterium

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

(2) Der Cloud-Anbieter dokumentiert die vom Cloud-Nutzer erhaltenen Weisungen zur Umsetzung des Rechts auf Datenübertragbarkeit oder wenn er ihn dabei unterstützt.

Erläuterung

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

Der Cloud-Anbieter ist verpflichtet, den Cloud-Nutzer durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

Nr. 6.8– Widerspruch[42] (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 21 Abs. 1 und Art. 32 Abs. 1 lit. b DSGVO)

Kriterium

[40] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

[41] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

[42] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

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

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

(3) Der Cloud-Anbieter dokumentiert die vom Cloud-Nutzer erhaltenen Weisungen zur Umsetzung des Widerspruchrechts oder wenn er ihn dabei unterstützt.

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. Daher muss der Cloud-Anbieter dem Cloud-Nutzer alle für ihn verfügbaren Informationen bereitstellen, damit der Cloud-Nutzer die Beurteilung treffen kann. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

Nr. 6.9 – Generelle Informationspflicht und Informationspflicht bei Untätigkeit oder verzögerter Antragsbearbeitung[43]
(Art. 12 Abs. 3 und 4, Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 15 bis 21 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch TOM sicher, dass der Cloud-Nutzer die Möglichkeit hat, die betroffene Person über die auf Antrag gemäß den Art. 15 bis 21 DSGVO ergriffenen Maßnahmen unverzüglich, spätestens innerhalb eines Monats nach Antragseingang, zu informieren. Die Information kann alternativ durch den Cloud-Anbieter vorgenommen werden.

(2) Der Cloud-Anbieter stellt durch TOM sicher, dass der Cloud-Nutzer die Möglichkeit hat, die betroffene Person zu informieren, falls er ihren Antrag nach Art. 15 bis 21 DSGVO nicht rechtzeitig, spätestens innerhalb eines Monats beantwortet. Die Information bezieht sich auf die Fristverlängerung und die Gründe hierfür. Die Information kann alternativ durch den Cloud-Anbieter vorgenommen werden.

(3) Der Cloud-Anbieter stellt durch TOM sicher, dass der Cloud-Nutzer die Möglichkeit hat, die betroffene Person, spätestens innerhalb eines Monats darüber zu informieren, falls er keine Maßnahmen ergreift, um einen Antrag nach Art. 15 bis 21 DSGVO zu beantworten. Die Information der betroffenen Person bezieht sich auf die Gründe der Untätigkeit des Cloud-Nutzers und die Möglichkeit bei der Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen. Die Information kann alternativ durch den Cloud-Anbieter vorgenommen werden.

Erläuterung

Nach Art. 12 Abs. 3 Satz 1 DSGVO hat der Cloud-Nutzer der betroffenen Person die erforderlichen Informationen über die auf Antrag nach Art. 15 bis 22 DSGVO ergriffenen Maßnahmen unverzüglich, spätestens innerhalb eines Monats nach Eingang des Antrags mitzuteilen. Art. 22 DSGVO wird jedoch bei der AUDITOR-Zertifizierung in Kapitel C nicht betrachtet. Der Cloud-Nutzer muss daher bei jedem Antrag einer betroffenen Person nach Art. 15 bis 21 DSGVO Stellung zur beantragten Maßnahme nehmen. Stützt sich der Cloud-Nutzer bei der Beantwortung von Anträgen auf eine (nationale) Ausnahme von der Erfüllung von Betroffenenrechten, hat er der betroffenen Person daher auch angemessen darzulegen, aus welchen Gründen er ihren Antrag teilweise oder vollständig ablehnt.

Aufgrund von Komplexität oder der Anzahl von Anträgen kann die Monatsfrist aus Art. 12 Abs. 3 Satz 1 DSGVO um zwei Monate verlängert werden. In diesem Fall muss der Cloud-Nutzer die betroffene Person über die Fristverlängerung und die Gründe dafür gemäß Art. 12 Abs. 3 Satz 3 DSGVO informieren. Der Cloud-Anbieter muss den Cloud Nutzer hierbei unterstützen. Bei elektronischer Antragstellung sollte die Unterrichtung ebenfalls elektronisch erfolgen, wenn die betroffene Person nichts anderes verlangt.

Art. 12 Abs. 4 DSGVO verpflichtet den Cloud-Nutzer, spätestens innerhalb eines Monats, zur Information der betroffenen Person über die Gründe, weshalb er trotz eines Antrags nach Art. 15 bis 21 DSGVO nicht tätig wird, um dem Antrag zu entsprechen. Gründe einem Antrag nicht zu entsprechen, sind z.B. unbegründete oder exzessive Anträge nach Art. 12 Abs. 5 Satz 2 lit. b DSGVO. Weiterhin ist die betroffene Person nach Art. 12 Abs. 4 DSGVO

[43] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

über ihre Möglichkeit, eine Beschwerde bei der Aufsichtsbehörde gemäß Art. 77 DSGVO oder gerichtlichen Rechtsbehelf gemäß Art. 79 DSGVO einzulegen, zu unterrichten.

Nr. 7– Unterstützung bei der Datenschutz-Folgenabschätzung[44] (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f i.V.m. Art. 35 und 36 DSGVO)

Kriterium

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

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

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

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

Erläuterung

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

Die deutschen Aufsichtsbehörden haben gemäß Art. 35 Abs. 4 DSGVO eine Liste von Verarbeitungsvorgängen veröffentlicht, für die neben den Fällen des Art. 35 Abs. 3 DSGVO eine Datenschutz-Folgenabschätzung vom Cloud-Nutzer zwingend durchgeführt werden muss (DSFA-Liste Verarbeitungsvorgänge). Auf diese wird hiermit verwiesen.

Kapitel III: Datenschutz-Managementsystem des Cloud-Anbieters

Erläuterung

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

Nr. 8 – Datenschutz-Managementsystem

Nr. 8.1 – Benennung, Stellung und Aufgaben eines Datenschutzbeauftragten (Art. 37 bis 39 DSGVO, § 38 Abs. 1; Abs. 2 i.V.m. § 6 Abs. 5 Satz 2 BDSG)

Kriterium

(1) Der Cloud-Anbieter muss einen Datenschutzbeauftragten (DSB) benennen, wo die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen.

(2) Der Cloud-Anbieter muss einen DSB benennen, wo die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.

(3) Der Cloud-Anbieter muss einen DSB benennen, soweit er in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt.

[44] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

(4) Der Cloud-Anbieter muss einen DSB benennen, wenn er Datenverarbeitungen vornimmt, die einer Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO unterliegen, unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen.

(5) Der Cloud-Anbieter muss einen DSB benennen, wenn er personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet, unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen.

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

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

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

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

(10) 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.

(11) Der Cloud-Anbieter stellt sicher, dass der DSB seinen Aufgaben nach Art. 39 Abs. 1 DSGVO im angemessenen Umfang nachkommen kann, einschließlich der Unterrichtung und Beratung, der Überwachung der Einhaltung der Vorschriften sowie der Zusammenarbeit mit der Aufsichtsbehörde und der Funktion als Kontaktstelle für diese.

(12) Der Cloud-Anbieter stellt sicher, dass der DSB bei der Erfüllung seiner Aufgaben über das Ende seines Rechtsverhältnisses mit dem Cloud-Anbieter hinaus an die Wahrung der Geheimhaltung oder Vertraulichkeit gebunden ist. Dies umfasst insbesondere die Pflicht des DSB zur Verschwiegenheit über die Identität der betroffenen Person sowie über die Umstände, die Rückschlüsse auf die betroffene Person zulassen, soweit er nicht davon durch die betroffene Person befreit wird.

(13) Der Cloud-Anbieter veröffentlicht die Kontaktdaten des DSB und teilt diese Daten der Aufsichtsbehörde mit.

(14) Der Cloud-Anbieter stellt sicher, dass andere Aufgaben oder Pflichten des DSB zu keinem Interessenkonflikt mit seiner Tätigkeit als DSB führen.

Erläuterung

Sofern Cloud-Anbieter die Pflicht haben, einen DSB zu benennen, müssen sie ihn sorgfältig auswählen, ausstatten, schützen und ihm in der Betriebsorganisation einen gebührenden Platz zuweisen. Art. 38 Abs. 5 DSGVO erklärt, dass der DSB bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder Vertraulichkeit gebunden ist. Die Norm ist so auszulegen, dass diese Pflicht für den DSB auch über das Ende seines Rechtsverhältnisses mit dem Cloud-Anbieter hinaus fort gilt.

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

Nach § 38 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) sind der Verantwortliche und der Auftragsverarbeiter verpflichtet, einen DSB zu benennen, wenn bei ihnen ständig in der Regel mindestens 20 Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Sie benennen auch einen DSB, unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen, wenn der Verantwortliche oder der Auftragsverarbeiter eine Verarbeitung vornimmt, die einer Datenschutz-Folgenabschätzung gemäß Artikel 35 der Verordnung (EU) 2016/679 unterliegt, oder wenn sie personenbezogene Daten zum Zwecke der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung gewerblich verarbeiten.

Nr. 8.2– Meldung von Datenschutzverletzungen[45]

[45] Dieses Kriterium würde nicht für den Cloud-Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

(Art. 33 Abs. 2 und Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f DSGVO)

Kriterium

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

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

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

Erläuterung

Der Cloud-Anbieter ist nach Art. 33 Abs. 2 DSGVO zur unverzüglichen Meldung von Datenschutzverstößen an den Cloud-Nutzer verpflichtet, damit dieser seiner Meldepflicht gegenüber der Aufsichtsbehörde aus Art. 33 Abs. 1 DSGVO und seiner Unterrichtungspflicht gegenüber den betroffenen Personen aus Art. 34 Abs. 1 DSGVO nachkommen kann. Diese Pflicht bezieht sich auch auf Verstöße von Subauftragnehmern in der gesamten Subauftragsverarbeiterkette. Das Kriterium fördert das Gewährleistungsziel der Integrität und Transparenz (SDM C1.3 und C1.6).

Nr. 8.3– Führen eines Verarbeitungsverzeichnisses (Art. 30 Abs. 2 bis 5 DSGVO)

Kriterium

(1) Der Cloud-Anbieter führt ein Verarbeitungsverzeichnis, wenn er 250 oder mehr Personen beschäftigt.

(2) Der Cloud-Anbieter führt ein Verarbeitungsverzeichnis, wenn die Verarbeitung, die er vornimmt, wahrscheinlich zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt.

(3) Der Cloud-Anbieter führt ein Verarbeitungsverzeichnis, wenn die Verarbeitung nicht nur gelegentlich erfolgt.

(4) Der Cloud-Anbieter führt ein Verarbeitungsverzeichnis, wenn die Verarbeitung besondere Kategorien von Daten im Sinne von Artikel 9 Absatz 1 DSGVO oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten im Sinne von Artikel 10 DSGVO umfasst.

(5) Ist der Cloud-Anbieter zur Führung eines Verarbeitungsverzeichnisses verpflichtet, führt er in diesem alle Kategorien von Verarbeitungen auf, die er im Auftrag von Cloud-Nutzern vornimmt. Das Verzeichnis enthält die in Art. 30 Abs. 2 lit. a bis d DSGVO aufgelisteten Inhalte.

(6) Der Cloud-Anbieter verfügt über Prozesse zur Aktualisierung des Verarbeitungsverzeichnisses, wenn neue Kategorien von Verarbeitungen, die er im Auftrag des Cloud-Nutzers vornimmt, eingeführt werden oder wegfallen, sich die Angaben nach Art. 30 Abs. 2 lit. a bis d DSGVO bei aufgeführten Kategorien von Verarbeitungen oder bei bestehenden Cloud-Nutzern, in deren Auftrag Verarbeitungen durchgeführt werden, ändern und Cloud-Nutzer, in deren Auftrag Verarbeitungen durchgeführt werden, hinzukommen oder wegfallen.

(7) Um das Verarbeitungsverzeichnis aktualisieren zu können, verfügt der Cloud-Anbieter über Prozesse zur Zusammenarbeit zwischen den an den Verarbeitungen beteiligten Fachabteilungen, den Cloud-Nutzern, in deren Auftrag Verarbeitungen durchgeführt werden sowie deren Vertretern und ggf. den DSB der Cloud-Nutzer und regelt hierfür die internen Zuständigkeiten.

(8) Das Verarbeitungsverzeichnis ist schriftlich oder in einem elektronischen Format zu führen und die Aufbewahrungs- oder Speicherorte sind bekannt.

(9) Das Verarbeitungsverzeichnis ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen. Der Cloud-Anbieter verfügt über Prozesse zur Entgegennahme, Bearbeitung und Beantwortung von Anfragen von Aufsichtsbehörden und regelt hierfür die internen Zuständigkeiten.

(10) Ist der Cloud-Anbieter zur Benennung eines Vertreters und zur Führung eines Verarbeitungsverzeichnisses verpflichtet, stellt er sicher, dass auch der Vertreter ein Verarbeitungsverzeichnis führt und die Kriterien nach Abs. 1 bis 5 einhält.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Transparenz (SDM C1.6).

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

Nach Art. 30 Abs. 2 DSGVO hat auch der Vertreter des Cloud-Anbieters ein Verarbeitungsverzeichnis zu führen, wenn ein solcher benannt ist (s. Nr. 11.2).

Nr. 8.4 – Rückgabe von Datenträgern und Löschung von Daten; Nachweis der Einhaltung und Ermöglichung von sowie Mitwirkung an Audits (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. g und h DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch geeignete Maßnahmen sicher, dass die Rückgabe überlassener Datenträger (die personenbezogene Daten enthalten), die Rückführung von personenbezogenen Daten und die Löschung der beim Cloud-Anbieter gespeicherten personenbezogenen Daten nach Abschluss der Auftragsverarbeitung oder nach Weisung des Cloud-Nutzers erfolgen, sofern nicht nach nationalem oder Unionsrecht eine Verpflichtung zur Datenspeicherung besteht. Dieses Kriterium würde nicht für den Cloud-

Nutzer gelten, der unter die Haushaltsausnahme fällt. Der Cloud-Anbieter als Auftragsverarbeiter ist gut beraten, das Kriterium als vorhanden und potenziell zu erfüllen zu betrachten, um auf solche Veränderungen in der Rolle eines Cloud-Nutzers, der zum für die Verarbeitung Verantwortlichen wird, reagieren zu können.

(2) Der Cloud-Anbieter stellt durch geeignete Maßnahmen sicher, dass er in der Lage ist, alle Informationen, die für den Nachweis der Einhaltung der in Art. 28 DSGVO enthaltenen Verpflichtungen erbringen zu können und dass er Audits, einschließlich Inspektionen, durch den Verantwortlichen oder einen anderen von diesem beauftragten Prüfer zulässt und dazu beiträgt.

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

Kriterium

(1) Der Cloud-Anbieter überprüft die Umsetzung aller in diesem Katalog geprüften Kriterien regelmäßig (mindestens jährlich und nach jeder wesentlichen Veränderung) in einem internen Revisionsverfahren. Hierfür legt der Cloud-Anbieter Kontrollverfahren und Zuständigkeiten fest und handelt bei Befunden aus Audits mit präventiven und korrektiven Maßnahmen

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

Erläuterungen

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

Nr. 8.6– Auswahl und Einsatz geeigneter Personen (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e und f DSGVO)

Kriterium

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

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

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

Erläuterungen

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

Kapitel IV: Datenschutz durch Systemgestaltung

Nr. 9 – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

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

Kriterium

(1) Der Cloud-Anbieter führt eine Risikoanalyse für alle Verarbeitungstätigkeiten des angebotenen Dienstes durch und verfügt im Rahmen seines angebotenen Dienstes über TOM zur praktikablen und zielführenden Umsetzung der Grundsätze des Art. 5 DSGVO (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckfestlegung und Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Systemdatenschutz und Verantwortlichkeit).

(2) Der Cloud-Anbieter unterhält Prozesse um darstellen zu können, dass personenbezogene Daten auf transparente Weise in Bezug auf die betroffenen Personen verarbeitet werden (Prinzip der Transparenz). Er muss zudem Prozesse etablieren, welche die aktive Überwachung seiner Einhaltung des Stand der Technik auf allen Ebenen der konzeptionellen Zielsetzung seiner Dienste[46], ihrer Architektur und ihrer Systemgestaltung sicherstellen.

(3) Der Cloud-Anbieter stellt sicher, dass zu jedem Zeitpunkt durch seine Systemgestaltung in den angebotenen Anwendungen und durch die Konzeption der Dienstleistung die Nachvollziehbarkeit (unter Beachtung der Datenminimierung, s. Nr. 2.6 [1]) und Transparenz der Datenverarbeitungen, auch in den verlängerten Leistungsketten durch etwaige Subauftragsverhältnisse, gewährleistet ist.

Erläuterung

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

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

Kriterium

(1) Der Cloud-Anbieter stellt durch seine Voreinstellungen im jeweiligen Dienst sicher, dass nur personenbezogene Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck erforderlich sind im Hinblick auf die Menge der erhobenen personenbezogenen Daten, der Umfang ihrer Verarbeitung und die Dauer ihrer Speicherung und auch der Zugang zu den personenbezogenen Daten auf das Maß beschränkt wird[47], das erforderlich ist, um den Verarbeitungszweck des Cloud-Nutzers zu erfüllen.

(2) Der Cloud-Anbieter stellt durch Voreinstellungen sicher, dass personenbezogene Daten nicht ohne Eingreifen der betroffenen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden und hierbei keine unangemessenen Risiken[48] für die betroffenen Personen durch eine zu umfassende Zugänglichmachung[49] von personenbezogenen Daten entstehen.

Erläuterung

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

Kapitel V: Subauftragsverarbeitung

Erläuterung

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

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

[46] Konzeptionelle Zielsetzungen sind solche, die auf das jeweilige Modell der angebotenen Dienste abzielen, d. h. das Angebot von Software-, Plattform- oder Infrastrukturdiensten usw.
[47] In Bezug auf Letzteres muss der Cloud-Anbieter sicherstellen, dass Personen, die unter seiner Aufsicht handeln, nur auf einer Need-To-Know-Basis auf personenbezogenen Daten zugreifen können, d.h. wenn sie diese kennen müssen.
[48] Unangemessene Risiken ergeben sich aus der Nichtberücksichtigung des Stands der Technik, der Kosten der Umsetzung und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Risiken unterschiedlicher Wahrscheinlichkeit und Schwere für die Rechte und Freiheiten natürlicher Personen, die von der Verarbeitung ausgehen.
[49] Eine „zu umfassende Zugänglichmachung“ liegt vor, wenn ein technischer oder persönlicher Zugriff einen Einblick in mehr Informationen zulässt als für den jeweiligen Zweck der Verarbeitung erforderlich.

Nr. 10 – Subauftragsverhältnisse

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

Kriterium

(1) Der Cloud-Anbieter verfügt über einen definierten Prozess, der sicherstellt, dass ein Cloud-Dienst unter Einbeziehung von Subauftragsverarbeitern nur dann erbracht wird, wenn und soweit der Cloud-Nutzer seine vorherige gesonderte oder allgemeine Genehmigung in die Subauftragsverarbeitung erteilt hat. Die Genehmigung muss schriftlich oder im elektronischen Format erfolgen. Im Falle einer allgemeinen schriftlichen Genehmigung muss der Cloud-Anbieter den Cloud-Nutzer über jede beabsichtigte Veränderung in Bezug auf die Ergänzung oder den Ersatz eines Auftragsverarbeiters informieren und auf diese Weise dem Cloud-Nutzer die Möglichkeit geben, derartigen Veränderungen zu widersprechen.

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

(3) Der Cloud-Anbieter stellt sicher, dass alle von ihm beauftragten Subauftragsverarbeiter, die durch den Cloud-Anbieter im Rahmen seiner Risikobewertung oder aufgrund der Zertifizierungskriterien definierten TOM umsetzen. Der Cloud-Anbieter muss zudem sicherstellen, dass dieselben Verpflichtungen zwischen ihm und den Subauftragsverarbeitern, wie sie in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung oder in einem anderen Rechtsinstrument niedergelegt sind, jedem Glied der Kette der Subauftragsverarbeiter auferlegt sind.

Erläuterung

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

Da das Widerspruchsrecht gegen Änderungen in der Subauftragsverarbeitung in der Praxis nicht entwertet werden darf, müssen die vertraglichen Verpflichtungen aus der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung, die die Voraussetzungen und Folgen eines Widerspruchs gegenüber Subauftragsverarbeitern regeln, bei den vertraglichen Verpflichtungen mit den jeweiligen Subauftragsverarbeitern auf allen Ebenen der Auftragsverarbeitung berücksichtigt werden.

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

Kriterium

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

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

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

Kriterium

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

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

Erläuterung

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

Siehe auch zu den Kriterien Nr. 1.5 und Nr. 4.2.

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

Kriterium

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

(2) Der Cloud-Anbieter überzeugt sich davon, dass alle eingesetzten Subauftragsverarbeiter die in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung niedergelegten datenschutzrechtlichen Verpflichtungen an die von ihnen zu erbringende Leistung erfüllen.

.

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

Kriterium

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

(2) Der Cloud-Anbieter stellt sicher, dass seine Unterstützungsfunktionen und seine Verpflichtungen als der Hauptauftragsverarbeiter im vereinbarten Umfang erfüllt werden, auch wenn (mehrere) Subauftragsverarbeiter beauftragt sind.

Kapitel VI: Datenverarbeitung außerhalb der EU und des EWR

Nr. 11 – Datenübermittlung[50]

Nr. 11.1 – Geeignete Garantien für die Datenübermittlung; Maßnahmen zum Schutz vor der Offenlegung gegenüber staatlichen Stellen von Drittländern (Art. 45, 46 und Art. 48 DSGVO)

Kriterium

(1) Der Cloud-Anbieter kann personenbezogene Daten in Drittländer oder an internationale Organisationen übermitteln, sofern er überprüft hat, dass 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 und der Cloud-Anbieter regelmäßig (mindestens jährlich) prüft, ob der Angemessenheitsbeschluss fort gilt und die in Frage stehende Übermittlung über den benannten Beschluss erfasst wird.

(2) Alternativ kann die Datenübermittlung stattfinden, wenn der Cloud-Anbieter nach Überprüfung von Rechtslage und Praxis im Drittland sicherstellt, dass die in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegten geeigneten Garantien im Sinne des Art. 46 Abs. 2 oder 3 DSGVO verwendet werden und diese geeigneten Garantien ein angemessenes Datenschutzniveau sicherstellen, das dem der Datenschutz-Grundverordnung gleichwertig ist.

(3) Reichen nach Überprüfung von Rechtslage und Praxis im Drittland die in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung[51] festgelegten geeigneten Garantien im Sinne des Art. 46 Abs. 2 oder 3 DSGVO nicht aus, um ein angemessenes Datenschutzniveau sicherzustellen, das dem der Datenschutz-Grundverordnung gleichwertig ist, ergreift der Cloud-Anbieter zusätzliche Maßnahmen, um dieses angemessene Datenschutzniveau sicherzustellen. Andernfalls darf keine Datenübermittlung stattfinden. Der Cloud-Anbieter muss dafür sorgen, dass der Cloud-Nutzer die durchgeführte Bewertung erhält, in Bezug auf das Recht und Praxis des Drittlandes, um überprüfen zu können, ob die vom Auftragsverarbeiter getroffenen zusätzlichen Maßnahmen tatsächlich ein angemessenes Schutzniveau für die in das Drittland übermittelten personenbezogenen Daten gewährleisten.

(4) Der Cloud-Anbieter überwacht fortlaufend die Angemessenheit des Datenschutzniveaus und stellt sicher, dass Datenübermittlungen umgehend ausgesetzt oder beendet werden, wenn im Fall des Abs. 2 oder 3 der Empfänger die Pflichten, die er nach den geeigneten Garantien des Art. 46 Abs. 2 oder 3 DSGVO eingegangen ist, verletzt hat oder ihre Erfüllung unmöglich ist und im Fall von Abs. 3 die zusätzlichen Maßnahmen nicht mehr eingehalten werden können oder unwirksam sind.[52]

(5) Cloud-Anbieter, die personenbezogene Daten verarbeiten und nicht nur dem Recht der Datenschutz-Grundverordnung unterliegen, sondern zugleich dem Recht eines Drittlands, das sie zu einer Offenlegung dieser personenbezogenen Daten gegenüber staatlichen Stellen des Drittlands verpflichtet, ergreifen zusätzliche Maßnahmen, um die personenbezogenen Daten vor einer Offenlegung an staatliche Stellen des Drittlands wirksam zu schützen. Der Cloud-Anbieter stellt sicher, dass personenbezogene Daten staatlichen Stellen von Drittländern nur offengelegt werden, wenn die Offenlegung auf eine in Kraft befindliche internationale Übereinkunft zwischen dem ersuchenden Drittland und der Union oder Deutschland gestützt ist. Der Cloud-Anbieter muss den Cloud-Nutzer über diese rechtliche Verpflichtung vor einer Offenlegung informieren, sofern die Information nicht aus anerkannten wichtigen Gründen des öffentlichen Interesses im EU- oder deutschem Recht verboten ist.

(6) Wenn der Cloud-Anbieter Daten an einen außerhalb der EU oder des EWR ansässigen Auftragsverarbeiter übermittelt (im Sinne von Art. 44 DSGVO), muss er die in Kapitel V der DSGVO festgelegten Verpflichtungen in vollem Umfang erfüllen.

Erläuterung

[50] Die Übermittlung bezieht sich auf die Bewegung personenbezogener Daten, wenn diese aus der EU/dem EWR in ein Land oder mehrere Länder außerhalb der EU/des EWR übermittelt werden sowie auch die Fälle, in denen Daten durch Fernzugriff zugänglich gemacht oder dem Datenimporteur mitgeteilt werden. Siehe EDSA-Leitlinien 05/2021 zum Zusammenspiel zwischen Art. 3 und Kapitel V der Datenschutz-Grundverordnung.

[51] Es versteht sich von selbst, dass der Auftragsverarbeiter bei Datenübermittlungen weiterhin an die Weisungen des Verantwortlichen gebunden ist, wie sie in der rechtsverbindlichen Vereinbarung zur Auftragsdatenverarbeitung festgelegt sind, siehe Kriterium Nr. 1.4(1).

[52] Es versteht sich von selbst, dass der Auftragsverarbeiter bei Datenübermittlungen weiterhin an die Weisungen des Verantwortlichen gebunden ist, wie sie in der rechtsverbindlichen Vereinbarung zur Auftragsdatenverarbeitung festgelegt sind, siehe Kriterium Nr. 1.4(1).

Übermittlungen personenbezogener Daten von betroffenen Personen in Drittländer sind nur unter den in Art. 44 ff. DSGVO genannten Voraussetzungen zulässig. Das Gleiche gilt für die Übermittlung personenbezogener Daten an eine internationale Organisation, für die kein angemessenes Datenschutzniveau anerkannt ist. Es ist wichtig, dass der Auftragsverarbeiter gemäß den Anweisungen des Verantwortlichen handelt.

Beinhaltet die Auftragsverarbeitung die weisungsgebundene Datenübermittlung an Drittländer oder an internationale Organisationen, verpflichtet Art. 44 DSGVO zusätzlich zur Einhaltung der Bedingungen von Kapitel V DSGVO. Es sollte beachtet werden, dass die Regelung des Art. 49 DSGVO keine Erlaubnistatbestände für die systematische und regelmäßige Datenübermittlung zwischen Exporteur und Importeur[53] enthält, wie sie im Cloud Computing üblich ist. Systematische und regelmäßige Datenübermittlungen zwischen Exporteur und Importeur müssen daher auf Angemessenheitsbeschlüsse nach Art. 45 Abs. 3 DSGVO oder geeignete Garantien nach Art. 46 Abs. 2 oder 3 DSGVO gestützt werden, die zwischen dem Cloud-Anbieter und dem Cloud-Nutzer nach Nr. 1.4 festgelegt worden sind. Datenübermittlungen auf Grundlage von Art. 49 DSGVO dürfen allenfalls in sehr restriktiven Ausnahmefällen erfolgen, die jedoch nicht von diesem Kriterienkatalog erfasst sind.

Art. 46 Abs. 2 und 3 DSGVO nennt verschiedene Übermittlungsinstrumente, die geeignete Garantien zur Sicherstellung eines angemessenen Datenschutzniveaus im Drittland darstellen können und die für alle Drittländer einheitlich angewendet werden können. Wegen der besonderen rechtlichen und/oder praktischen Gegebenheiten in einem Drittland, in das personenbezogene Daten übermittelt werden sollen, kann es allerdings erforderlich sein, dass der Cloud-Anbieter diese Übermittlungsinstrumente um zusätzliche organisatorische, technische und/oder vertragliche Maßnahmen ergänzen muss, um ein angemessenes Datenschutzniveau sicherzustellen, das im Wesentlichen dem der Datenschutz-Grundverordnung entspricht.

Es ist zu beachten, dass die Verwendung der EU-Standardertragsklauseln vom Juni 2021 (EU-SVK) allein kein angemessenes Datenschutzniveau gewährleitet. Vielmehr muss der Cloud-Anbieter auch bei diesem Übermittlungsinstrument, ggf. mit dem Empfänger gemeinsam, prüfen, ob Rechtslage und Praxis des Drittlands die Effektivität der EU-SVK beeinträchtigen. Diese Prüfung ist auch bei der Verwendung der anderen geeigneten Garantien nach Art. 46 Abs. 2 und 3 DSGVO durchzuführen. Liegt eine Beeinträchtigung vor, darf die Datenübermittlung nicht stattfinden oder es müssen zusätzliche Maßnahmen ergriffen werden, um die identifizierten Lücken zu schließen und ein angemessenes Datenschutzniveau im Drittland sicherzustellen.

Dem Recht eines Drittlands, das zu einer Offenlegung von personenbezogenen Daten an staatliche Stellen des jeweiligen Drittlands verpflichtet, können Cloud-Anbieter unterliegen, wenn sie Daten ganz oder teilweise im jeweiligen Drittland verarbeiten, aber auch wenn sie, z.B. als europäisches Tochterunternehmen eines Mutterkonzerns aus einem Drittland, personenbezogene Daten ausschließlich auf Servern in der EU oder im EWR verarbeiten. Auch in diesem Fall kann der Cloud-Anbieter nach dem Recht von Drittländern verpflichtet sein, personenbezogene Daten, die sich auf Servern in der EU oder im EWR befinden, gegenüber staatlichen Stellen des betreffenden Drittlands offenzulegen, wenn er durch gerichtliches Urteil oder Entscheidungen von Verwaltungsbehörden dazu verpflichtet wird. Dies ist z.B. für europäische Tochterunternehmen von US-Mutterkonzernen im Rahmen des CLOUD Acts der Fall. Solche rechtlichen Offenlegungspflichten nach dem Recht von Drittländern stehen in Konflikt mit Art. 48 DSGVO. Dieser verpflichtet Verantwortliche und Auftragsverarbeiter dazu, jeglichen Urteilen von Gerichten von Drittländern und jeglichen Entscheidungen von Verwaltungsbehörden von Drittländern, mit denen eine Offenlegung personenbezogener Daten verlangt wird, nur Folge zu leisten, wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind.

Der für die Verarbeitung Verantwortliche muss die Möglichkeit haben, die durchgeführte Bewertung in Bezug auf das Recht und die Praxis des Drittlandes zu erhalten, um zu überprüfen, ob die vom Auftragsverarbeiter getroffenen zusätzlichen Maßnahmen tatsächlich ein angemessenes Schutzniveau für die in das Drittland übermittelten personenbezogenen Daten gewährleisten.

Es versteht sich von selbst, dass weiterhin die rechtsverbindliche Vereinbarung zur Auftragsdatenverarbeitung eingehalten werden muss im Hinblick auf Datenübermittlungen, siehe Kriterium Nr. 1.4(1).

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

Kriterium

(1) Cloud-Anbieter ohne Niederlassung in der EU oder im EWR, für die dennoch gemäß Art. 3 Abs. 2 DSGVO die Datenschutz-Grundverordnung gilt, benennen schriftlich einen Vertreter in der EU oder im EWR. Der

[53] Datenexporteur ist/sind die natürliche(n) oder juristische(n) Person(en), Behörde(n), Agentur(en) oder sonstige(n) Stelle(n) ("Stelle(n)"), die die personenbezogenen Daten in ein Drittland übermittelt/übermitteln. Die Stelle(n) in einem Drittland, die die personenbezogenen Daten vom Datenexporteur direkt oder indirekt über eine andere Stelle erhält/erhalten, ist/sind der Datenimporteur, siehe: Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates.

Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen sich die betroffenen Personen befinden, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird.

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

D. Kriterien für Verarbeitung als Verantwortlicher

Kapitel VII: Der Cloud-Anbieter als Verantwortlicher

Erläuterung

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

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

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

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

Kriterium

(1) Der Cloud-Anbieter stellt bei der Verarbeitung von personenbezogenen Daten, die für die Durchführung des Auftrags über die Erbringung des Cloud-Dienstes oder zur Erfüllung rechtlicher Verpflichtungen erforderlich sind, der betroffenen Person alle Informationen zur Verfügung, die diese benötigt, um die Rechtmäßigkeit der Verarbeitung überprüfen zu können (Grundsatz der Transparenz und Rechtmäßigkeit). Der Cloud-Anbieter darf die Daten der betroffenen Person nur nach Treu und Glauben verarbeiten (Grundsatz von Treu und Glauben[54]).

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

(3) Der Cloud-Anbieter legt einen Prozess fest und verfügt über TOM, die gewährleisten, dass nur personenbezogene Daten verarbeitet werden, soweit diese zur Erreichung der festgelegten Verarbeitungszwecke

[54] "Treu und Glauben [Fairness]" kann als eine Art Auffangklausel gesehen werden, "um eine unzulässige Datenverarbeitung auch in Ermangelung einer entsprechenden Regelung als rechtswidrig qualifizieren zu können". Dieser Rechtsbegriff ist bereits im deutschen Zivilrecht belegt und bezieht sich dort auf "Treu und Glauben" und das Element des Vertrauens in die Pflichterfüllung durch den Verpflichteten aufgrund einer berechtigten Erwartung. In Bezug auf die Verarbeitung personenbezogener Daten kann die Verarbeitung als unlauter verstanden werden, wenn sie das Vertrauen missbraucht. Gerechtfertigtes Vertrauen kann explizit durch Vereinbarungen oder früheres Verhalten oder implizit durch die berechtigte Erwartung der Einhaltung von Verkehrs-, Handels- oder Berufsregeln begründet werden. Vertrauensmissbrauch liegt auch vor, wenn eine Einwilligung verlangt wird, obwohl die Datenverarbeitung gesetzlich erlaubt ist. Der Grundsatz der Fairness ist z.B. "bei der Abwägung der widerstreitenden Interessen zwischen dem Verantwortlichen und der betroffenen Person gemäß Art. 6 Abs.1 UAbs. 1 lit. f, bei der Bestimmung der Freiwilligkeit der Einwilligung und des Koppelungsverbots nach Art. 7 Abs. 4 und bei der Festlegung von Verhaltensregeln nach Art. 40 Abs. 2." zu berücksichtigen, vgl. Simitis/Hornung/Spiecker gen. Döhmann, 2019, Art. 5, Rn. 47.

erforderlich (d.h. angemessen, erheblich und auf das notwenige Maß beschränkt) sind (Grundsatz der Datenminimierung).

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

(5) Der Cloud-Anbieter legt einen Prozess fest und stellt durch TOM sicher, dass bei der Datenverarbeitung der Personenbezug nur solange hergestellt wird, wie dies für die Erreichung der festgelegten Zwecke zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes oder zur Erfüllung rechtlicher Verpflichtungen unverzichtbar ist und löscht nicht erforderliche Daten frühestmöglich. Dazu legt er Kriterien fest, nach denen ein Personenbezug ermittelt, für den konkreten Verarbeitungszweck erhalten und für die geeignete Speicherung im erforderlichen Maß (Umfang und Dauer) vorgehalten wird (Grundsatz der Speicherbegrenzung).

Erläuterung

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

Angemessen sind personenbezogene Daten, wenn sie aus objektiver Perspektive für den jeweiligen Zweck hinsichtlich Funktion, Inhalt und Umfang sachgerecht sind. Erheblich sind personenbezogene Daten, wenn sie für die Erfüllung des jeweiligen Zwecks einen Unterschied bewirken und somit einen entscheidenden Beitrag zur jeweiligen Zweckerreichung leisten. Auf das notwendige Maß beschränkt sind personenbezogene Daten, wenn der jeweilige Zweck der Verarbeitung ohne diese Daten nicht erreicht werden kann.

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

Kriterium

(1) Der Cloud-Anbieter verarbeitet personenbezogene Daten und führt Verarbeitungsvorgänge nur durch, die für die Erfüllung eines Vertrags zur Datenverarbeitung im Auftrag des Cloud-Nutzers[55] oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage des Cloud-Nutzers erfolgen, erforderlich sind. In Bezug auf Letzteres darf der Cloud-Anbieter nur Daten des Cloud-Nutzers verarbeiten, die es ihm ermöglichen, ein Angebot auf der Grundlage der geografischen, technischen und individuellen Bedürfnisse des Cloud-Nutzers zu erstellen, bevor er eine rechtsverbindliche Vereinbarung zur Auftragsdatenverarbeitung abschließt. Der Cloud-Anbieter dokumentiert Strukturen und Abläufen, die zu einem Vertragsschluss oder zu einem vorvertraglichen Verhältnis führen.

(2) Der Cloud-Anbieter verarbeitet personenbezogene Daten und führt Verarbeitungsvorgänge nur durch, die zur Erfüllung einer rechtlichen Verpflichtung nach deutschem oder EU-Recht erforderlich sind, der er unterliegt. Der Cloud-Anbieter dokumentiert die rechtlichen Verpflichtungen, einschließlich der Bedingungen ihres Eintritts, ihres Umfangs und der Umstände ihres Wegfalls.

(3) Der Cloud-Anbieter verarbeitet personenbezogene Daten und führt Verarbeitungsvorgänge durch, die zur Wahrung seiner berechtigten Interessen oder solcher eines Dritten erforderlich sind, es sei denn, diese Interessen werden durch die Interessen oder Grundrechte und -freiheiten des Cloud-Nutzers, die den Schutz personenbezogener Daten erfordern, überwogen. Der Cloud-Anbieter dokumentiert den Prozess der Interessenabwägung, inklusive der Beteiligten, deren Interessen abgewogen werden, der konkreten Interessen, Grundrechte und Grundfreiheiten und der personenbezogenen Daten und Verarbeitungsvorgänge, den einbezogenen Abwägungskriterien und dem Ergebnis der Abwägung und, falls erforderlich, die Ausgleichs- oder zusätzlichen Maßnahmen die vorgesehen werden müssen, um die Auswirkung der Verarbeitung auf betroffene Personen zu begrenzen und auf diese Weise einen Ausgleich zwischen den involvierten Rechten und Interessen zu schaffen.

(4) Der Cloud-Anbieter prüft, bestimmt und dokumentiert die Rechtsgrundlagen für die Verarbeitungsvorgänge nach Abs. 1 bis 3.

[55] Da der Cloud-Nutzer auch eine natürliche Person sein kann, ist es auch möglich, dass er die „betroffene Person“ (wie indirekt über Art. 4 Nr. 1 DSGVO definiert) ist.

(5) Der Cloud-Anbieter verfügt über Anweisungen an Mitarbeiter, anhand derer das Vorhandensein einer ausreichenden Rechtsgrundlage zu prüfen ist und legt entsprechende Zuständigkeiten für Prüfungen fest.

Erläuterung

AUDITOR betrachtet die Datenverarbeitungsvorgänge des Cloud-Anbieters in seiner Rolle als Verantwortlicher nur, soweit diese erforderlich sind, um den Auftrag mit dem Cloud-Nutzer über die Erbringung des Cloud-Dienstes zu erfüllen. Da der Cloud-Nutzer auch eine natürliche Person sein kann, ist es auch möglich, dass er die „betroffene Person“ (wie indirekt über Art. 4 Nr. 1 DSGVO definiert) ist. Die Rechtsgrundlage der Verarbeitung von personenbezogenen Daten des Cloud-Nutzers bildet daher Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO. Die Norm erlaubt die Datenverarbeitung, soweit diese für die Erfüllung eines Vertrags oder für vorvertragliche Maßnahme mit der betroffenen Person erforderlich ist. Der Datenumgang für das Zustandekommen eines Vertrags, für Vertragsänderungen und -beendigungen gehört zur Vertragserfüllung. Auch Daten, die für die Ermöglichung der Inanspruchnahme des Cloud-Dienstes oder die Abrechnung der Nutzung des Cloud-Dienstes erforderlich sind, sind Teil der Vertragserfüllung und fallen somit unter Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO.

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

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

Verarbeitungsvorgänge, die auf derselben Rechtsgrundlage beruhen, können bei der Darstellung, Prüfung und Dokumentation zusammengefasst werden.

Beispiele für Verarbeitungen, die zur Erfüllung des Vertrags mit dem Cloud-Nutzer über die Erbringung des Cloud-Dienstes erforderlich sind, sind zum einen die Behebung von Fehlern oder Fehleranalysen und zum anderen die Erfüllung von Service Level Agreements. In vielen Fällen ist es unerlässlich, den Kontext eines Prozesses zu kennen, um Fehler analysieren zu können. In bestimmten Fällen kann dies auch die Verarbeitung personenbezogener Daten umfassen. Ziel ist es also, einen möglichen Fehler in der Dienstleistung eindeutig zu diagnostizieren und zu beheben. Ebenso kann in der Praxis in einigen Fällen eine direkte Kommunikation mit dem Nutzer erforderlich sein. Um Service Level Agreements in einem konkreten Vertragsverhältnis einzuhalten und Ressourcen bedarfsgerecht zu skalieren, ist es notwendig, das Zugriffsverhalten zu analysieren und daraus Schlüsse für die Ressourcenbereitstellung zu ziehen. In bestimmten Konstellationen können auch personenbezogene Daten in diese Analyse einbezogen werden.

Diese Beispiele sind von Fällen zu unterscheiden, in denen Datenanalysen und möglicherweise Profile auf der Grundlage personenbezogener Daten (möglicherweise sogar über eine große Anzahl von Kunden) erstellt werden, um Nutzerpräferenzen für die Weiterentwicklung der nächsten Generation des Dienstes zu erhalten. Eine solche Verarbeitung kann nicht als notwendig angesehen werden, um den Vertrag mit dem Cloud-Nutzer über die Erbringung des Cloud-Dienstes zu erfüllen.

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

Erläuterungen

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

Nr. 14.1 – Datensicherheitskonzept (Art. 24, 25, 32 i.V.m. Art. 5 Abs. 1 lit. f und Abs. 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter führt eine Risikoanalyse nach dem Stand der Technik in Bezug auf die Datensicherheit durch und verfügt über ein Datensicherheitskonzept entsprechend seiner Schutzklasse, das den spezifischen Risiken seiner Datenverarbeitungsvorgänge zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen, die sich insbesondere durch Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von und unbefugten Zugang zu personenbezogenen Daten ergeben können, angemessen ist.

(2) Der Cloud-Anbieter unterhält eine Beschreibung aller personenbezogenen Daten oder Datenkategorien, die er als Verantwortlicher zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen verarbeitet.

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

(4) 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.

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

(6) Das Datensicherheitskonzept ist in regelmäßigen Abständen (mindestens jährlich und nach jeder wesentlichen Veränderung) auf Aktualität und Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren.

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

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

Erläuterung

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

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

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter sichert Räume und Anlagen gegen Schädigung durch höhere Gewalt[56] und verwehrt Unbefugten den Zutritt zu Räumen und Datenverarbeitungsanlagen, um unbefugte Kenntnisnahmen personenbezogener Daten und Einwirkungsmöglichkeiten auf die Datenverarbeitungsanlagen auszuschließen. Die TOM müssen geeignet sein, um im Regelfall den Zutritt Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen Dritter auszuschließen. Der Cloud-Anbieter muss wenigstens eine Reihe von Sicherheitsanforderungen für jede Sicherheitszone festlegen, dokumentieren und umsetzen.

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

(3) Jeder befugte Zutritt ist zu protokollieren.

Schutzklasse 2 und 3

[56] Nach einer auf verschiedenen Gebieten des Unionsrechts entwickelten ständigen Rechtsprechung sind unter „höherer Gewalt“ ungewöhnliche und unvorhersehbare Ereignisse zu verstehen, auf die derjenige, der sich darauf beruft, keinen Einfluss hat und deren Folgen trotz Anwendung der gebotenen Sorgfalt nicht hätten vermieden werden können, vgl. ECLI:EU:C:2017:39, Rn. 53.

(4) Die Kriterien von Schutzklasse 1 sind erfüllt.

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

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

Erläuterung

Es wird auf die Erläuterungen in Nr. 2.2 verwiesen.

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

Kriterium

Schutzklasse 1

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

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

(3) Der Cloud-Anbieter schützt Zugänge von Befugten über das Internet mit einer Zwei-Faktor-Authentifizierung. Der Zugang über das Internet hat über eine Transportverschlüsselung nach dem Stand der Technik zu erfolgen.

(4) Der Cloud-Anbieter implementiert die Maßnahmen zur Zugangskontrolle derart, um im Regelfall den Zugang zu Datenverarbeitungssystemen durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen.

Schutzklasse 2

(5) Die Kriterien von Schutzklasse 1 sind erfüllt.

(6) Gegen zu erwartenden vorsätzlichen unbefugten Zugang ist ein Schutz vorzusehen, der zu erwartende Zugangsversuche ausschließt. Das umfasst einen hinreichenden Schutz gegen bekannte Angriffsszenarien und stellen einen unbefugten Zugang im Regelfall nachträglich fest.

Schutzklasse 3

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

(8) Der Cloud-Anbieter muss unbefugten Zugang zu Datenverarbeitungssystemen ausschließen. Dies umfasst regelmäßige Maßnahmen zur aktiven Detektion von und Reaktion auf Angriffe. Jeder unbefugte Zugang und Zugangsversuch sind nachträglich feststellbar.

Erläuterungen

Es wird auf die Erläuterungen in Nr. 2.3 verwiesen.

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

Kriterium

Schutzklasse 1

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

(2) Der Cloud-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zugriff auf personenbezogene Daten in regelmäßigen Abständen (mindestens jährlich oder bei wesentlichen Veränderungen) auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

(3) Zugriffe auf personenbezogene Daten sind zu kontrollieren (d.h. zu überwachen und zu bewerten) und müssen protokolliert werden.

(4) Der Cloud-Anbieter implementiert Maßnahmen, die im Regelfall den Zugriff auf personenbezogene Daten durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter ausschließen.

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

Schutzklasse 2

(6) Die Kriterien von Schutzklasse 1 sind erfüllt.

(7) Zu erwartender vorsätzlicher, unbefugter Zugriff muss ausgeschlossen werden. Dies umfasst insbesondere einen angemessenen Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, mit denen ein unbefugter Zugriff in der Regel nachträglich erkannt werden kann.

Schutzklasse 3

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

(9) Unbefugter Datenzugriff muss unter Berücksichtigung der Ergebnisse der Risikoanalyse ausgeschlossen sein. Dazu gehören regelmäßig manipulationssichere technische Maßnahmen zur Verhinderung und aktiven Erkennung von Angriffen. Unbefugte Zugriffe und damit verbundene Versuche können nachträglich erkannt werden.

Erläuterungen

Es wird auf die Erläuterungen in Nr. 2.4 verwiesen.

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

Kriterium

Schutzklasse 1

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

(2) Die Maßnahmen müssen geeignet sein im Regelfall Angriffe Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen. Außerdem müssen die Maßnahmen geeignet sein, die fahrlässige Weitergabe von Daten an Unbefugte durch den Cloud-Anbieter und seine Mitarbeiter zu verhindern. Gegen vorsätzliche Eingriffe ist Schutz vorzusehen, der diese verhindert.

(3) Der Cloud-Anbieter protokolliert automatisiert die Metadaten aller Datenüberübermittlungsvorgänge, einschließlich der Empfänger, auch solche vom und an den Cloud-Nutzer oder an Subauftragsverarbeiter. Nr. 14.6 (1) gilt entsprechend.

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

(5) Der Cloud-Anbieter schützt den Transport von Datenträgern durch TOM, so dass personenbezogene Daten während des Transports von Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Der Cloud-Anbieter führt ein Verzeichnis der Transporte.

Schutzklasse 2

(6) Die Kriterien von Schutzklasse 1 sind erfüllt.

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

Schutzklasse 3

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

(9) Der Cloud-Anbieter verhindert unbefugtes Lesen, Kopieren, Verändern oder Löschen von Daten. Er unternimmt regelmäßig Maßnahmen, um Angriffe aktiv zu erkennen und abzuwehren, und um jedes unbefugte Lesen, Kopieren, Ändern oder Löschen von Daten sowie jeden diesbezüglichen Versuch.

Erläuterungen

Es wird auf die Erläuterungen in Nr. 2.5 verwiesen.

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

Kriterium

Schutzklasse 1

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

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

(3) Der Cloud-Anbieter verhindert vorsätzliche Manipulation durch Gestaltung der Protokollierung der administrativen Aktivitäten und der Nutzer-Aktivitäten dergestalt, dass die Nachvollziehbarkeit von Eingaben, Veränderungen und Löschungen im Regelfall auch bei technischen oder organisatorischen Fehlern, einschließlich Bedienfehlern des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter gewahrt bleibt.

Schutzklasse 2

(4) Die Kriterien von Schutzklasse 1 sind erfüllt.

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

Schutzklasse 3

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

(7) Der Cloud-Anbieter verhindert Manipulationen der Protokollinstanzen und Protokolldateien (Logs). Er unternimmt regelmäßig Maßnahmen, um Manipulationen aktiv zu erkennen und deckt jede Manipulation und, wenn möglich, jeden damit verbundenen Versuch nachträglich auf.

Erläuterung

Es wird auf die Erläuterungen in Nr. 2.6 verwiesen.

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

Kriterium

Schutzklasse 1,2 und 3

(1) Der Cloud-Anbieter stellt sicher, dass Anmeldedaten zur Nutzung des Cloud-Dienstes verschlüsselt gespeichert werden.

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

(3) Der Cloud-Anbieter verfolgt laufend die technische Entwicklung im Bereich der Verschlüsselung. Die Maßnahmen des Cloud-Anbieters, insbesondere die sichere Schlüsselverwaltung, entsprechen dem Stand der Technik[57].

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

(5) Unbefugter Zugang zu Verschlüsselungsschlüsseln ist durch geeignete Maßnahmen zu verhindern.

Erläuterung

Die Verschlüsselung wird neben der Pseudonymisierung in Art. 32 Abs. 1 lit. a DSGVO explizit als eine einzusetzende Sicherheitsmaßnahme benannt. Zweck der Verschlüsselung ist es, die Gewährleistungsziele der Vertraulichkeit und Integrität (SDM C1.4 und C1.3) sicherzustellen. Die Schwelle, ab der zu verschlüsseln ist, ist niedrig, sodass personenbezogene Daten bereits bei niedrigem Risiko verschlüsselt werden sollten, soweit dies möglich ist.

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

Kriterium

Schutzklasse 1

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

(2) Der Cloud-Anbieter verhindert vorsätzliche Verletzungen bezüglich der Datentrennung bei technischen oder organisatorischen Fehlern, einschließlich Bedienfehlern, des Cloud-Anbieters oder seiner Mitarbeiter.

Schutzklasse 2

(3) Die Kriterien von Schutzklasse 1 sind erfüllt.

(4) Der Cloud-Anbieter schließt zu erwartende vorsätzliche Verstöße aus. Dies umfasst Schutz gegen bekannte Angriffsszenarien in Bezug auf das Trennungsprinzip. Zu den dafür erforderlichen TOM gehört im Rahmen der Datenspeicherung die Verschlüsselung mit individuellen Schlüsseln. Er stellt vorsätzliche Verstöße gegen das Trennungsgebot im Regelfall (nachträglich) fest.

[57] Der Stand der Technik umfasst das, was derzeit als beste Praktiken, Technologien, Methoden und Strategien zum Schutz von Informationssystemen allgemein anerkannt ist. Der Stand der Technik bedeutet nicht notwendigerweise die technologisch fortschrittlichste Lösung, sondern umfasst robuste Technologien und Prozesse sowie qualifiziertes Personal, um wirksam gegen die sich fortentwickelnden Datenschutzbedrohungen zu schützen.

Schutzklasse 3

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

(6) Der Cloud-Anbieter schließt Verletzungen der Datentrennung aus. Der Cloud-Anbieter erkennt vorsätzliche Verletzungen der getrennten Verarbeitung.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Verfügbarkeit, Integrität, Vertraulichkeit und Nichtverkettung (SDM C1.2 – C1.5) und zielt damit auch auf die Sicherstellung des Zweckbindungsgrundsatzes aus Art. 5 Abs. 1 lit. b DSGVO ab.

Nr. 15– Wahrung von Betroffenenrechten

Erläuterung

Wenn die betroffene Person ihre Rechte nach Art. 15 bis 22 DSGVO elektronisch ausübt, sollten die Informationen über die auf den Antrag hin ergriffenen Maßnahmen des Cloud-Anbieters gemäß Art. 12 Abs. 3 Satz 4 DSGVO ebenfalls, nach Möglichkeit, elektronisch bereitgestellt werden, außer die betroffene Person hat einen anderen Informationsweg gewünscht. Es ist jedoch zu beachten, dass die Art. 20 bis 22 DSGVO bei der AUDITOR-Zertifizierung in Kapitel D nicht betrachtet werden.

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

Kriterium

Der Cloud-Anbieter stellt durch TOM sicher, dass die betroffene Person zum Zeitpunkt der Erhebung ihrer personenbezogenen Daten zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen über die Umstände der Verarbeitung und über ihre Betroffenenrechte verständlich und in klarer und einfacher Sprache informiert wird. Die Information an die betroffene Person umfasst alle in Art. 13 Abs. 1 und 2 DSGVO geforderten Angaben.

Erläuterung

Der Cloud-Anbieter ist nach Art. 13 DSGVO verpflichtet, die betroffene Person über die Umstände der Direkterhebung zu informieren. Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

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

Kriterium

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

Erläuterung

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

Nr. 15.3– Auskunftserteilung (Art. 15 i.V.m. Art. 5 Abs. 1 lit. a 3. Alt. DSGVO)

Kriterium

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

Erläuterung

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

Nr. 15.4– Berichtigung und Vervollständigung (Art. 16 i.V.m. Art. 5 Abs. 1 lit. d DSGVO)

Kriterium

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

Erläuterung

Der Cloud-Anbieter ist nach Art. 16 DSGVO verpflichtet, auf Antrag unrichtige personenbezogene Daten zu berichtigen und unvollständige personenbezogene Daten von betroffenen Personen zu vervollständigen. Die Berichtigung gemäß Art. 16 DSGVO fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

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

Kriterium

(1) Der Cloud-Anbieter stellt durch TOM sicher, dass er personenbezogene Daten, die er zur Erfüllung des Auftrags über die Erbringung des Cloud-Dienstes verarbeitet, auf Antrag der betroffenen Person hin und von sich aus unverzüglich löscht, wenn die Voraussetzungen von Art. 17 Abs. 1 lit. a, d oder e DSGVO vorliegen. Die Löschung hat irreversibel zu erfolgen, sodass keine Informationen über die betroffene Person gewonnen werden können. Der Cloud-Anbieter stellt sicher, dass die Löschung durch die Nutzung von Maßnahmen nach dem Stand der Technik unwiderruflich ist.

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

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

Erläuterung

Das Kriterium fördert die Gewährleistungsziele der Intervenierbarkeit und Nichtverkettung (SDM C1.7 und C1.5). Keine Pflicht zur Löschung besteht insbesondere, wenn der Cloud-Anbieter zur Verarbeitung verpflichtet ist, um eine rechtliche Verpflichtung zu erfüllen (Art. 17 Abs. 3 lit. b DSGVO).

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

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

Nr. 15.6– Einschränkung der Verarbeitung (Art. 18 Abs. 1 und 3 DSGVO)

Kriterium

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

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

Erläuterung

Der Cloud-Anbieter ist nach Art. 18 Abs. 1 DSGVO verpflichtet, die Verarbeitung personenbezogener Daten unter bestimmten Voraussetzungen einzuschränken, sodass Daten nicht weiterverarbeitet oder verändert werden können. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

Nr. 15.7– Mitteilungspflicht bei Berichtung, Löschung oder Einschränkung der Verarbeitung (Art. 19 i.V.m. Art. 5 Abs. 1 lit. a 3. Alt. DSGVO)

Kriterium

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

Erläuterung

Der Cloud-Anbieter ist nach Art. 19 DSGVO verpflichtet, Empfängern, denen er personenbezogene Daten offengelegt hat, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitzuteilen und die betroffene Person auf Verlangen über die Empfänger zu unterrichten. Das Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

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

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

Nr. 15.8 – Generelle Informationspflicht, Informationspflicht bei Untätigkeit oder verzögerter Antragsbearbeitung (Art. 12 Abs. 3 und 4, Art. 15 bis 19 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch TOM sicher, dass er die betroffene Person über die auf Antrag gemäß den Art. 15 bis 19 DSGVO ergriffenen Maßnahmen in Bezug auf die Datenverarbeitung, die er als Verantwortlicher über sie zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen durchführt, unverzüglich, spätestens innerhalb eines Monats nach Antragseingang, informiert.

(2) Der Cloud-Anbieter stellt durch TOM sicher, dass er die betroffene Person informiert, falls er ihren Antrag nach Art. 15 bis 19 DSGVO in Bezug auf die Datenverarbeitung, die er als Verantwortlicher über sie zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen durchführt, nicht unverzüglich, spätestens innerhalb eines Monats beantwortet. Die Information bezieht sich auf die Fristverlängerung und die Gründe hierfür.

(3) Der Cloud-Anbieter stellt durch TOM sicher, dass er die betroffene Person, spätestens innerhalb eines Monats darüber informiert, falls er keine Maßnahmen ergreift, um ihren Antrag nach Art. 15 bis 19 DSGVO in Bezug auf die Datenverarbeitung, die er als Verantwortlicher über sie zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen durchführt, zu beantworten. Die Information der betroffenen Person bezieht sich auf die Gründe der Untätigkeit und die Möglichkeit bei der Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen.

Erläuterung

Nach Art. 12 Abs. 3 Satz 1 DSGVO hat der Cloud-Anbieter der betroffenen Person die erforderlichen Informationen über die auf Antrag nach Art. 15 bis 22 DSGVO ergriffenen Maßnahmen unverzüglich, spätestens innerhalb eines Monats nach Eingang des Antrags mitzuteilen. Die Art. 20 bis 22 DSGVO werden jedoch bei der AUDITOR-Zertifizierung in Kapitel D nicht betrachtet. Der Cloud-Anbieter muss daher bei jedem Antrag einer betroffenen Person nach Art. 15 bis 19 DSGVO Stellung zur beantragten Maßnahme nehmen. Stützt sich der Cloud-Anbieter bei der Beantwortung von Anträgen auf eine (nationale) Ausnahme von den Betroffenenrechten, hat er der betroffenen Person daher auch angemessen darzulegen, aus welchen Gründen er ihren Antrag teilweise oder vollständig ablehnt.

Aufgrund von Komplexität oder der Anzahl von Anträgen kann die Monatsfrist aus Art. 12 Abs. 3 Satz 1 DSGVO um zwei Monate verlängert werden. In diesem Fall muss der Cloud-Anbieter die betroffene Person über die Fristverlängerung und die Gründe dafür gemäß Art. 12 Abs. 3 Satz 3 DSGVO informieren. Bei elektronischer Antragstellung sollte die Unterrichtung ebenfalls elektronisch erfolgen, wenn die betroffene Person nichts anderes verlangt.

Art. 12 Abs. 4 DSGVO verpflichtet den Cloud-Anbieter, spätestens innerhalb eines Monats, zur Information der betroffenen Person über die Gründe, weshalb er trotz eines Antrags nach Art. 15 bis 19 DSGVO nicht tätig wird, um dem Antrag zu entsprechen. Gründe einem Antrag nicht zu entsprechen, sind z.B. unbegründete oder exzessive Anträge nach Art. 12 Abs. 5 Satz 2 lit. b DSGVO. Weiterhin ist die betroffene Person nach Art. 12 Abs. 4 DSGVO über ihre Möglichkeit, eine Beschwerde bei der Aufsichtsbehörde gemäß Art. 77 DSGVO oder gerichtlichen Rechtsbehelf gemäß Art. 79 DSGVO einzulegen, zu unterrichten.

Nr. 16– Meldung von Datenschutzverletzungen (Art. 33 Abs. 1, 3 bis 5 DSGVO)

Kriterium

(1) Der Cloud-Anbieter verfügt über einen Prozess zur Meldung von Datenschutzverletzungen aus der Verarbeitung von Daten, die zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen vorgenommen werden, inklusive der Festlegung von Verfahrensschritten, Fristen und Maßnahmen zur Identifikation, Analyse und Bewertung der Datenschutzverletzung und ihrer Meldung, der Verantwortlichkeiten und der Sensibilisierung der beteiligten Mitarbeiter.

(2) Der Cloud-Anbieter meldet der Aufsichtsbehörde Datenschutzverletzungen[58] aus der Verarbeitung von Daten, die zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen vorgenommen werden, unverzüglich nach Bekanntwerden, sofern sie voraussichtlich zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führen.

(3) Bei der Bewertung der Risiken für die Rechte und Freiheiten des Cloud-Nutzers, muss der Cloud-Anbieter den Typus der Sicherheitsverletzung, die Art, die Sensibilität und das Volumen der personenbezogenen Daten, die leichte Identifizierbarkeit der Personen, die Schwere der Folgen für die Personen, die besonderen Merkmale des Cloud-Nutzers, die besonderen Merkmale des Cloud-Anbieters und die Zahl der betroffenen Personen berücksichtigen.

(4) Der Cloud-Anbieter verfügt über einen Prozess und Maßnahmen zur Identifikation, Analyse und Bewertung des Risikos für die Rechte und Freiheiten der betroffenen Personen.

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

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

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

Erläuterung

Der Cloud-Anbieter ist nach Art. 33 DSGVO zur unverzüglichen Meldung von Datenschutzverstößen an die Aufsichtsbehörde verpflichtet, sofern sie voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen. Der Cloud-Anbieter muss Datenschutzverletzungen dokumentieren, damit die Aufsichtsbehörde überprüfen kann, ob der Cloud-Anbieter allen seinen diesbezüglichen Pflichten nachgekommen ist. Das Kriterium fördert das Gewährleistungsziel der Integrität und Transparenz (SDM C1.3 und C1.6).

Die Verletzung des Schutzes personenbezogener Daten gilt als "wahrscheinlich zu einem Risiko für die Rechte und Freiheiten des Cloud-Nutzers führend", wenn die Risikobewertung zu dem Ergebnis kommt, dass sowohl die Wahrscheinlichkeit als auch die Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person gegeben sind. Da die Datenschutzverletzung bereits stattgefunden hat, d. h. nicht hypothetischer Natur ist, liegt der Schwerpunkt der Bewertung ausschließlich auf dem daraus resultierenden Risiko der Auswirkungen der Verletzung auf die betroffenen Personen. Der Cloud-Anbieter sollte die besonderen Umstände der Datenschutzverletzung berücksichtigen, einschließlich der Schwere der potenziellen Auswirkungen und der Wahrscheinlichkeit des Eintretens, wie es in den "Leitlinien 9/2002 oder Meldung von Datenschutzverletzungen nach der DSGVO" (Version 2.0, angenommen am 28. März 2023) als obligatorisch angesehen wird. Die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) hat Empfehlungen für eine Methodik zur Bewertung des Schweregrads einer

[58] Wenn möglich, spätestens 72 Stunden, nach Kenntniserlangung.

Datenschutzverletzung ausgearbeitet, die bei der Ausarbeitung eines Plans zur Bewältigung von Datenschutzverletzungen nützlich sind (ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity).

Nr. 17 – Benachrichtigung der betroffenen Person bei Datenschutzverletzungen (Art. 34 Abs. 1 bis 3 DSGVO)

Kriterium

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

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

(3) Der Cloud-Anbieter verfügt über ein Verfahren zur Identifikation, Analyse und Bewertung von Datenschutzverletzungen aus der Verarbeitung von Daten zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen, anhand dessen bestimmt wird, wann, von einem voraussichtlich hohen Risiko für die Rechte und Freiheiten von betroffenen Personen ausgegangen werden muss, welche Fristen einzuhalten sind und wer für die Benachrichtigung zuständig ist. Die zuständigen Mitarbeiter sind ausreichend geschult, um Verstöße beurteilen zu können.

(4) Die Benachrichtigung nach Abs. 1 und 2 darf unter Einhaltung der Voraussetzungen des Art. 34 Abs. 3 DSGVO unterbleiben.

(5) Der Cloud-Anbieter dokumentiert die Benachrichtigungen von betroffenen Personen über Datenschutzverletzungen aus der Verarbeitung von Daten zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen sowie die Umstände, Gründe und Maßnahmen, wenn die Benachrichtigung der betroffenen Personen gemäß Abs. 4 unterbleibt.

Erläuterungen

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

Die Benachrichtigung der betroffenen Person nach Art. 34 Abs. 1 DSGVO ist gemäß Art. 34 Abs. 3 DSGVO nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

a. der Verantwortliche hat geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen wurden auf die von der Verletzung betroffenen personenbezogenen Daten angewandt, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;

b. der Verantwortliche hat durch nachfolgende Maßnahmen sichergestellt, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;

c. die Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

Nr. 18– Führen eines Verarbeitungsverzeichnisses (Art. 30 Abs. 1, 3 bis 5 DSGVO)

Kriterium

(1) Ist der Cloud-Anbieter zur Führung eines Verarbeitungsverzeichnisses verpflichtet, bezieht sich dieses auf die Verarbeitungstätigkeiten, die er durchführt, um den Auftrag über die Erbringung des Cloud-Dienstes zu erfüllen und auf Verarbeitungstätigkeiten zur Erfüllung rechtlicher Verpflichtungen. Das Verzeichnis enthält die in Art. 30 Abs. 1 lit. a bis g DSGVO aufgelisteten Inhalte.

(2) Der Cloud-Anbieter verfügt über Prozesse zur Aktualisierung des Verarbeitungsverzeichnisses, wenn Verarbeitungstätigkeiten eingeführt werden oder wegfallen, oder sich die Angaben nach Art. 30 Abs. 1 lit. a bis g DSGVO bei aufgeführten Verarbeitungstätigkeiten ändern.

(3) Zum Zweck der Aktualisierung des Verarbeitungsverzeichnisses verfügt der Cloud-Anbieter über Prozesse zur Zusammenarbeit zwischen den an den Verarbeitungstätigkeiten beteiligten Fachabteilungen, seinem Vertreter sowie ggf. dem DSB und regelt hierfür die internen Zuständigkeiten.

(4) Das Verarbeitungsverzeichnis ist schriftlich oder in einem elektronischen Format zu führen und die Aufbewahrungs- oder Speicherorte sind bekannt.

(5) Das Verarbeitungsverzeichnis ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen. Der Cloud-Anbieter verfügt über Prozesse zur Entgegennahme, Bearbeitung und Beantwortung von Anfragen von Aufsichtsbehörden und regelt hierfür die internen Zuständigkeiten.

(6) Ist der Cloud-Anbieter zur Benennung eines Vertreters und zur Führung eines Verarbeitungsverzeichnisses verpflichtet, stellt er sicher, dass auch der Vertreter ein Verarbeitungsverzeichnis führt und die Kriterien nach Abs. 1 bis 5 einhält.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Transparenz (SDM C1.6).

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

Nach Art. 30 Abs. 2 DSGVO hat auch der Vertreter des Cloud-Anbieters ein Verarbeitungsverzeichnis zu führen, wenn ein solcher benannt ist.

Nr. 19 – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Nr. 19.1 – Datenschutz durch Systemgestaltung (Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 und 2 DSGVO)

Kriterium

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

Erläuterung

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

Nr. 19.2– Datenschutz durch datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 i.V.m. Art. 5 Abs. 1 und 2 DSGVO)

Kriterium

(1) Der Cloud-Anbieter stellt durch Voreinstellungen sicher, dass er bei der Inbetriebnahme und Nutzung des Cloud-Dienstes nur personenbezogene Daten verarbeitet, die erforderlich sind, um den Cloud-Dienst erbringen zu können im Hinblick auf die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung und die Dauer ihrer Speicherung sowie dass der Zugang zu den personenbezogenen Daten auf das erforderliche Maß[59] beschränkt wird.

(2) Der Cloud-Anbieter stellt durch Voreinstellungen sicher, dass personenbezogene Daten nicht ohne Eingreifen der betroffenen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden und dass keine unangemessenen Risiken[60] für die betroffene Person durch das Zugänglichmachen in einem zu großen Umfang[61] zu den verfügbaren personenbezogenen Daten entstehen.

[59] In Bezug auf Letzteres muss der Cloud-Anbieter sicherstellen, dass Personen, die unter seiner Aufsicht handeln, nur dann auf die personenbezogenen Daten zugreifen, wenn sie diese kennen müssen („need to know“).
[60] Unangemessene Risiken ergeben sich aus der Nichtberücksichtigung des Stands der Technik, der Kosten der Umsetzung und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Risiken unterschiedlicher Wahrscheinlichkeit und Schwere für die Rechte und Freiheiten natürlicher Personen, die von der Verarbeitung ausgehen.
[61] Ein „zu großer Umfang“ ist gegeben, wenn ein technischer oder persönlicher Zugang mehr Informationen gewährt, als für den jeweiligen Zweck der Verarbeitung erforderlich sind.

Nr. 20 – Auftragsverarbeitung des Cloud-Anbieters

Erläuterung

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

Nr. 20.1 – Dienstleistung aufgrund einer rechtsverbindlichen Vereinbarung (Art. 28 Abs. 3 UAbs. 1 Satz 2 DSGVO)

Kriterium

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

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

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

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

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

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

(7) Der Cloud-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festgelegt ist, dass personenbezogene Daten nur auf seine dokumentierte Weisung hin vom Auftragsverarbeiter verarbeitet werden, auch in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation, sofern er nicht durch das Recht der Union oder des Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist. Für diesen Fall enthält die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung die Verpflichtung, dass der Auftragsverarbeiter dem Cloud-Anbieter diese rechtlichen Anforderungen vor der Verarbeitung mitzuteilen hat, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(8) Für den Fall, dass die Auftragsverarbeitung weisungsgebundene Übermittlungen personenbezogener Daten an Drittländer oder internationale Organisationen vorsieht, stellt der Cloud-Anbieter sicher, dass die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung die Instrumente nach Art. 45 DSGVO oder Art. 46 Abs. 2 und 3 DSGVO festlegt, die für die Übermittlungen genutzt werden sollen und ggf. auch die weiteren zusätzlich zu ergreifenden Maßnahmen, um ein angemessenes Schutzniveau sicherzustellen.

(9) Der Cloud-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festgelegt ist, dass sich der Auftragsverarbeiter zur Information des Cloud-Anbieters verpflichtet, wenn er der Ansicht ist, dass eine Weisung des Cloud-Anbieters gegen datenschutzrechtliche Vorschriften verstößt.

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

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

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

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

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

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

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

Erläuterung

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

Nr. 20.2– Sicherstellung ordnungsgemäßer Auftragsverarbeitung

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter personenbezogene Daten nur auf seine dokumentierte Weisung hin verarbeitet (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h, 29; 32 Abs. 4 DSGVO).

(2) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter ihn informiert, wenn er der Ansicht ist, dass seine Weisungen gegen datenschutzrechtliche Vorschriften verstoßen (Art. 28 Abs. 3 UAbs.1 Satz 2 lit. h i.V.m. Art. 29 DSGVO).

(3) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter bei der ausgelagerten Verarbeitung Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Systeme, die Belastbarkeit der Systeme sowie die Verfügbarkeit der Daten und den Zugang zu ihnen nach einem physischen oder technischen Zwischenfall gewährleistet. Die implementierten TOM müssen vom Auftragsverarbeiter regelmäßig (mindestens jährlich und nach jeder wesentlichen Änderung) überprüft und gegebenenfalls angepasst werden (Art. 24, 25, 28, 32, 35 i.V.m. Art. 5 Abs. 1 lit. f und Abs. 2 DSGVO).

(4) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter seine Mitarbeiter vor Beginn der Datenverarbeitung zur Vertraulichkeit über das Ende ihres Beschäftigungsverhältnisses hinaus verpflichtet, sofern sie nicht einer gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b und h DSGVO).

(5) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter nur Mitarbeiter mit der Durchführung von Verarbeitungsvorgängen betraut, die die dafür erforderliche Fachkunde aufweisen und die im Datenschutz und der Datensicherheit geschult sind (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e und f DSGVO).

(6) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter den Cloud-Anbieter in jenen Fällen informiert, in denen sich der Datenverarbeitungsort ändert (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h DSGVO).

(7) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter nach Abschluss der Auftragsverarbeitung oder auf Weisung des Cloud-Anbieters überlassene Datenträger zurückgibt, Daten zurückführt und beim ihm gespeicherte Daten irreversibel löscht (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. g und h DSGVO).

(8) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter dem Cloud-Anbieter die Erfüllung der Betroffenenrechte ermöglicht und alle Weisungen zur Umsetzung der Betroffenenrechte dokumentiert (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e und h i.V.m. Kapitel III DSGVO).

(9) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter einen DSB benennt, sofern er hierzu gesetzlich verpflichtet ist (Art. 37-39 DSGVO, § 38 Abs. 1; Abs. 2 i.V.m. § 6 Abs. 5 Satz 2 BDSG).

(10) Der Cloud-Anbieter verpflichtet den Auftragsverarbeiter darauf, ein Verarbeitungsverzeichnis zu führen, wenn er gesetzlich dazu verpflichtet ist (Art. 30 Abs. 2 - 5 DSGVO).

(11) Der Cloud-Anbieter stellt sicher, dass ihm der Auftragsverarbeiter Datenschutzverletzungen und deren Ausmaß unverzüglich meldet (Art. 33 Abs. 2 und Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f).

(12) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter allen Anforderungen aus der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung nach Nr. 20.1 nachkommt und alle Anforderungen nach diesem Kriterium erfüllt (Art. 24 Abs. 1 DSGVO).

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

(14) Sieht die Auftragsverarbeitung die weisungsgebundene Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen vor oder unterliegt der Auftragsverarbeiter dem Recht eines Drittlands, das ihn zur Offenlegung von personenbezogenen Daten an staatliche Stellen des Drittlands verpflichtet, obwohl die Datenverarbeitung ausschließlich in der EU oder im EWR stattfindet, stellt der Cloud-Anbieter sicher, dass der Auftragsverarbeiter das Kriterium Nr. 11.1 aus Kapitel VI einhält (Art. 46 i.V.m. Art. 42 Abs. 1 und 2; Art. 48 DSGVO).

(15) Der Cloud-Anbieter verpflichtet den Auftragsverarbeiter zur Benennung eines Vertreters nach Kriterium Nr. 11.2 aus Kapitel VI, wenn dieser gesetzlich dazu verpflichtet ist (Art. 27 i.V.m. Art. 3 Abs. 2 DSGVO).

Erläuterung

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

Nr. 21– Datenübermittlung[62]

Nr. 21.1 – Geeignete Garantien für die Datenübermittlung; Maßnahmen zum Schutz vor der Offenlegung gegenüber staatlichen Stellen von Drittländern (Art. 45, 46 und Art. 48 DSGVO)

Vorbemerkung

Es ist möglich, dass der Cloud-Anbieter in seiner Rolle als für die Verarbeitung Verantwortlicher Daten des Cloud-Nutzers oder von Personen, die für ihn arbeiten, im Rahmen seines Geschäfts/Unternehmens übermittelt. Dies kann z.B. aus technischen, rechtlichen oder anderen Gründen geschehen. Zum Beispiel könnte ein technisches Update/Support aus dem Ausland seines Server-Lieferanten im laufenden Geschäftsbetrieb dazu führen, dass ein Cloud-Nutzer den Cloud-Dienst nutzt, obwohl die Systeme gerade vom technischen Support bearbeitet werden. Ein anderes Beispiel könnte sein, dass der Cloud-Anbieter als Verantwortlicher für seine Systeme und deren Verarbeitung durch EU- oder mitgliedstaatliches Recht gesetzlich dazu verpflichtet ist. Daher müssen entsprechende Kriterien eingeführt werden, die sicherstellen, dass Übermittlungen in dieser Hinsicht auch dem Regime der Datenschutz-Grundverordnung unterliegen. In dieser Hinsicht ist es der für seine Geschäftslösung und die Verarbeitung Verantwortliche, der personenbezogener Daten verarbeitet. Er übermittelt Daten unter seiner eigenen Verantwortung und gegebenenfalls unter seiner eigenen rechtlichen Verpflichtung.

Kriterium

(1) Der Cloud-Anbieter kann personenbezogene Daten in Drittländer oder an internationale Organisationen übermitteln, sofern er überprüft hat, dass für den Empfängerstaat oder die internationale Organisation, in der der Datenimporteur ansässig ist, ein Beschluss der Europäischen Kommission nach Art. 45 Abs. 3 DSGVO vorliegt, dass dort ein angemessenes Datenschutzniveau gilt und der Cloud-Anbieter regelmäßig (mindestens jährlich) prüft, ob der Angemessenheitsbeschluss fort gilt und die in Frage stehende Übermittlung über den benannten Beschluss erfasst wird.

(2) Alternativ kann die Datenübermittlung stattfinden, wenn der Cloud-Anbieter nach Überprüfung von Rechtslage und Praxis im Drittland sicherstellt, dass geeignete Garantien im Sinne des Art. 46 Abs. 2 oder 3 DSGVO verwendet werden und diese geeigneten Garantien ein angemessenes Datenschutzniveau sicherstellen, das dem der Datenschutz-Grundverordnung gleichwertig ist.

(3) Reichen nach Überprüfung von Rechtslage und Praxis im Drittland die geeigneten Garantien im Sinne des Art. 46 Abs. 2 oder 3 DSGVO nicht aus, um ein angemessenes Datenschutzniveau sicherzustellen, das dem der Datenschutz-Grundverordnung gleichwertig ist, ergreift der Cloud-Anbieter zusätzliche Maßnahmen[63], um dieses angemessene Datenschutzniveau sicherzustellen. Andernfalls darf keine Datenübermittlung stattfinden.

(4) Der Cloud-Anbieter überwacht fortlaufend die Angemessenheit des Datenschutzniveaus und stellt sicher, dass Datenübermittlungen umgehend ausgesetzt oder beendet werden, wenn im Fall des Abs. 2 oder 3 der Empfänger die Pflichten, die er nach den geeigneten Garantien des Art. 46 Abs. 2 oder 3 DSGVO eingegangen ist, verletzt hat oder ihre Erfüllung unmöglich ist und im Fall von Abs. 3 die zusätzlichen Maßnahmen nicht mehr eingehalten werden können oder unwirksam sind.

(5) Cloud-Anbieter, die personenbezogene Daten verarbeiten und nicht nur dem Recht der Datenschutz-Grundverordnung unterliegen, sondern zugleich dem Recht eines Drittlands, das sie zu einer Offenlegung dieser personenbezogenen Daten gegenüber staatlichen Stellen des Drittlands verpflichtet, ergreifen zusätzliche Maßnahmen, um die personenbezogenen Daten vor einer Offenlegung an staatliche Stellen des Drittlands wirksam zu schützen. Der Cloud-Anbieter stellt sicher, dass personenbezogene Daten staatlichen Stellen von Drittländern nur offengelegt werden, wenn die Offenlegung auf eine in Kraft befindliche internationale Übereinkunft zwischen dem ersuchenden Drittland und der Union oder Deutschland gestützt ist.

Erläuterung

Übermittlungen personenbezogener Daten von betroffenen Personen in Drittländer sind nur unter den in Art. 44 ff. DSGVO genannten Voraussetzungen zulässig. Das Gleiche gilt für die Übermittlung personenbezogener Daten an eine internationale Organisation, für die kein angemessenes Datenschutzniveau anerkannt ist.

[62] Die Übermittlung bezieht sich auf die Bewegung personenbezogener Daten, wenn diese aus der EU/dem EWR in ein Land oder mehrere Länder außerhalb der EU/des EWR übermittelt werden.
[63] Z.B. TOMs in Übereinstimmung mit den Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten.

Es sollte beachtet werden, dass die Regelung des Art. 49 DSGVO keine Erlaubnistatbestände für die systematische und regelmäßige Datenübermittlung zwischen Exporteur und Importeur[64] enthält, wie sie im Cloud Computing üblich ist. Systematische und regelmäßige Datenübermittlungen zwischen Exporteur und Importeur müssen daher auf Angemessenheitsbeschlüsse nach Art. 45 Abs. 3 DSGVO oder geeignete Garantien nach Art. 46 Abs. 2 oder 3 DSGVO gestützt werden, die zwischen dem Cloud-Anbieter und dem Cloud-Nutzer nach Nr. 1.4 festgelegt worden sind. Datenübermittlungen auf Grundlage von Art. 49 DSGVO dürfen allenfalls in sehr restriktiven Ausnahmefällen erfolgen, die jedoch nicht von diesem Kriterienkatalog erfasst sind.

Im Übrigen wird auf die Ausführungen in Nr. 11.1 verwiesen.

[64] Datenexporteur ist/sind die natürliche(n) oder juristische(n) Person(en), Behörde(n), Agentur(en) oder sonstige(n) Stelle(n) ("Stelle(n)"), die die personenbezogenen Daten übermittelt/übermitteln. Die Stelle(n) in einem Drittland, die die personenbezogenen Daten vom Datenexporteur direkt oder indirekt über eine andere Stelle erhält/erhalten, ist/sind der Datenimporteur. Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates.

E. Referenzen

Arbeitspapier „Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen“	Schwartmann/Weiß (Hrsg.), Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen, Ein Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2018, https://www.gdd.de/downloads/anforderungen-an-datenschutzkonforme-pseudonymisierung
BSI C5	Cloud Computing Compliance Controls Catalogue (BSI C5), Version 2020, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Cloud-Computing/ComplianceControlsCatalogue/2020/C5_2020.html, Englische Fassung
BSI TR-02102-1	Kryptographische Verfahren: Empfehlungen und Schlüssellängen, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html, Stand 22.02.2019
BSI TR-02102-2	Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2 – Verwendung von Transport Layer Security (TLS), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html, Stand 22.02.2019
BSI TR-02102-3	Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPSec) und Internet Key Exchange (IKEv2), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-3.html, Stand 25.01.2018
BSI TR-02102-4	Kryptographische Verfahren: Verwendung von Secure Shell (SSH), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-4.html, Stand 25.01.2018
DIN EN 1627	Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung. Stand 2011
DIN 66398	Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten. Stand 2016
DIN 66399	Vernichtung von Datenträgern. Stand 2012
EU-SVK	Europäische Kommission, Durchführungsbeschluss vom 4.6.2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der DSGVO, https://ec.europa.eu/info/sites/default/files/1_de_act_part1_v3_1.pdf.
DSFA-Liste Verarbeitungsvorgänge	Datenschutzkonferenz, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, Version 1.1 vom 17.10.2018, https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf.
Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Datenschutzniveaus für personenbezogene Daten	Europäischer Datenschutzausschuss, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Datenschutzniveaus für personenbezogene Daten vom 10. November 2020, https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_de.pdf
Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen“ erfolgen	Europäischer Datenschutzausschuss, Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen vom 10. November 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_de.pdf
Factsheet – mass surveillance	European Court of Human Rights, Factsheet – mass surveillance, May 2021, https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf.
https://gdprhub.eu/Article_2_GDPR#(c)_Processing_by_a_natural_person_in_the_course_of_purely_personal_or_household_activity	Verweis auf NOYB – European Center for Digital Rights. Abgerufen am 05.06.2024.

Guidelines 4/2019	European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, Stand 20.10.2020
Handreichung zum Stand der Technik	Teletrust, IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum „Stand der Technik". Technische und organisatorische Maßnahmen, https://www.teletrust.de/fileadmin/user_upload/2021-02_TeleTrusT-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf, Stand: 2021
ISO/IEC 11770-2	IT Security techniques — Key management — Part 2: Mechanisms using symmetric techniques. Stand 2018
ISO/IEC 19941	Information technology — Cloud computing — Interoperability and portability. Stand 2017
ISO/IEC 21964-1	Information technology — Destruction of data carriers — Part 1: Principles and definitions. Stand 2018
ISO/IEC 24760-1	IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts. Stand 2019
ISO/IEC 24760-2	Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements. Stand 2015
ISO/IEC 24760-3	Information technology — Security techniques — A framework for identity management — Part 3: Practice. Stand 2016
ISO 25237	Health informatics — Pseudonymization. Stand 2017
ISO/IEC 27002	Information technology — Security techniques — Code of practice for information security controls. Stand 2013
ISO/IEC 27018	Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Stand 2019
ISO/IEC 27040	Information technology — Security techniques — Storage security. Stand 2015
ISO/IEC 27701	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. Stand 2019
ISO/IEC 29101	Information technology — Security techniques — Privacy architecture framework. Stand 2018
ISO/IEC 29134	Information technology — Security techniques — Guidelines for privacy impact assessment. Stand 2017
ISO/IEC 29146	Information technology — Security techniques — A framework for access management. Stand 2016
ISO 31000	Risk management – Guidelines. Stand 2018
IEC 31010	Risk management — Risk assessment techniques. Stand 2019
Länderberichte	Inter-American Commission on Human Rights, Country Reports, https://www.oas.org/en/IACHR/jsForm/?File=/en/iachr/reports/country.asp.
SDM	Standard-Datenschutzmodell, Version 2.0, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode.pdf, Stand November 2019
SDM-Bausteine	Maßnahmenkatalog des SDM, https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/, Stand Juni 2024