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

Für jedes Kriterium werden *„Umsetzungshinweise“* als exemplarische Leitlinien und Hilfestellungen für das Verständnis und die Umsetzung der Kriterien gegeben, die jedoch keinen verpflichtenden Charakter haben. Auch sind Umsetzungshinweise nicht abschließend, sondern beschreiben zentrale Umsetzungen für die Kriterien. Die Umsetzungshinweise orientieren sich dabei, wo es angemessen ist, an bestehenden Industriestandards, Normen und Best-Practices. So wird bspw. insbesondere bei den Kriterien unter Nr. 2 zur Gewährleistung der Datensicherheit auf die ISO/IEC 27002 und das BSI C5 verwiesen und es werden entsprechende Textabschnitte zitiert.[17] Zudem finden sich zu jedem Kriterium *„Nachweise“*, die eine Antwort auf die Frage liefern, wie das Vorliegen der Kriterien im konkreten Zertifizierungsverfahren erwiesen werden kann. Sie stellen analog zu den Umsetzungshinweisen exemplarische Leitlinien und informative Hilfestellungen dar, die Cloud-Anbieter, Zertifizierungsstellen, Prüfer und weitere Interessierte bei der Beurteilung der Einhaltung von Kriterien unterstützen sollen. Dabei wird bspw. die Vorlage von Dokumentationen zur Prüfung durch die Zertifizierungsstelle vorgeschlagen, oder die Durchführung einer Vor-Ort-Auditierung durch die Zertifizierungsstelle als Nachweis zur Umsetzung von dokumentierten Maßnahmen vorausgesetzt. Es besteht keine Verpflichtung, den Nachweis anhand der in diesem Dokument genannten zu erbringen. Das akkreditierte AUDITOR-Konformitätsbewertungsprogramm legt fest, wie jedes Kriterium im Rahmen der Zertifizierung zu überprüfen ist.

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

2. Schutzklassen

Anforderungen an TOM des Cloud-Dienstes werden nach Schutzklassen differenziert. Dabei orientiert sich der AUDITOR-Kriterienkatalog an dem TCDP-Schutzklassenkonzept. 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

[17] Es wird darauf hingewiesen, dass der Leser dieses Dokuments überprüfen sollte, ob aktualisierte Versionen der Industriestandards, Normen und Best-Practices existieren.

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 und Umsetzungsempfehlungen für die Auftragsverarbeitung

Kapitel I: Rechtsverbindliche Vereinbarung zur Auftragsverarbeitung

Erläuterung

Der Cloud-Anbieter muss sicherstellen, dass die Leistungen gegenüber dem Cloud-Nutzer aufgrund einer rechtsverbindlichen Vereinbarung[18] 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[19] 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.

Umsetzungshinweis

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

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

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

Nachweis

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

[18] 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.

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

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

Nr. 1.2 – Gegenstand und Dauer der Verarbeitung (Art. 28 Abs. 3 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.

Umsetzungshinweis

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

Auf die Umsetzungshinweise zur transparenten Systembeschreibung im BSI C5, und Abschnitt 3.4.4 und BC-01 bis BC-06 wird hingewiesen.

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

Nachweis

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

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

Kriterium

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

Umsetzungshinweis

Es ist zulässig, dass der Cloud-Anbieter eine allgemeine Beschreibung der Art, des Umfangs und der Zwecke der Datenverarbeitung bereitstellt. Dennoch sollten die Informationen in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung auf die spezifische Verarbeitung zugeschnitten sein, z. B. durch Angabe vordefinierter Datenarten, Kategorien betroffener Personen oder typischer Funktionen zur Erreichung bestimmter Datenverarbeitungszwecke. Die Beschreibung sollte so präzise sein, dass die Cloud-Nutzer eine fundierte Entscheidung über die Nutzung des Cloud-Dienstes treffen können. Dem Cloud-Nutzer ist zu ermöglichen, dass er die für seinen speziellen Fall relevanten Informationen eingeben kann.

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

Auf die Umsetzungshinweise im SDM-Baustein 41 „Planen und Spezifizieren“ und -Baustein 42 „Dokumentieren“ wird hingewiesen.

Nachweis

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

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.

Umsetzungshinweis

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

In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung des Cloud-Anbieters sollten die technisch ausführbaren Dienstleistungen und Weisungsbefugnisse des Cloud-Nutzers aufgeführt werden. Die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung sollte die Rechte des Cloud-Nutzers zur Weisung des Cloud-Anbieters beschreiben, inklusive der Rechte zur Änderung, Anpassung und dem Zurücknehmen von Weisungen. Die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung sollte nicht die Rechte des Cloud-Nutzers, Weisungen zu erteilen, beschränken, um die DSGVO-konforme Verarbeitung gewährleisten zu können. Cloud-Nutzer können ihre Weisungen händisch oder mit automatisierten Verfahren und Funktionen (bspw. durch API-Aufrufe oder Softwarebefehle oder dem Anklicken von Cloud-Dienst-Funktionen) erteilen. Anhand einer (im Massengeschäft einseitig vorgegebenen) Dienstbeschreibung des Cloud-Anbieters sollen die potentiellen Cloud-Nutzer eine Auskunft für ihre Auswahl nach Art. 28 Abs. 1 DSGVO erhalten.

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

lit. c DSGVO oder genehmigte Zertifizierungsverfahren nach Art. 46 Abs. 2 lit. f i.V.m. Art. 42 DSGVO. Darüber hinaus sollten zusätzliche Maßnahmen festgelegt werden, wenn ein angemessenes Schutzniveau nicht allein durch die Instrumente nach Art. 46 Abs. 2 und 3 DSGVO erreicht werden kann (s. hierzu auch Nr. 11.1).

Auf die Umsetzungshinweise zur transparenten Systembeschreibung im BSI C5 Anf. UP-01, Abschnitt 3.4.4 und PSS-01 wird hingewiesen.

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

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

Nachweis

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

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.[20]

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

(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[21] 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.

[20] 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.
[21] 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.

Umsetzungshinweise

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

Auf die Umsetzungshinweise des BSI C5 BC-01 und PSS-12 wird hingewiesen.

Nachweis

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

Nr. 1.6 – Verpflichtung zur Vertraulichkeit (Art. 28 Abs. 3 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.

Umsetzungshinweis

Auf die Umsetzungshinweise des BSI C5 HR-05 und HR-06 wird hingewiesen.

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

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er entsprechende Dokumentationen vorlegt (bspw. Vertragsmuster, -vorlagen oder -instanzen), in denen ersichtlich wird, dass er sich verpflichtet, Personen, die zur Verarbeitung von personenbezogenen Daten befugt sind, vor Aufnahme der datenverarbeitenden Tätigkeit zur Vertraulichkeit zu verpflichten, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen. Durch eine testweise Dienstnutzung (insb. Einsicht, ob Inhalte bei der Registrierung für die Dienstnutzung angezeigt werden) kann er nachweisen, dass er ein Verfahren implementiert hat, wonach die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung mit diesen Festlegungen geschlossen wird.

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.

(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.[22]

Umsetzungshinweis

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

Die Vorgaben des Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. d DSGVO sollten in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung präzisiert werden, so dass ihre Einhaltung für den Cloud-Nutzer leicht überprüfbar ist.

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

Da dem Cloud-Nutzer bei Änderungen in der Unterbeauftragung ein Einspruchsrecht zusteht (Nr. 10.3), sollten in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung die Voraussetzungen und Folgen eines Einspruchs geregelt werden, bspw. ob der Cloud-Nutzer bei Einspruch die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung aufkündigen darf. Das Recht des Cloud-Nutzers, hinsichtlich von Änderungen in Subauftragsverarbeitungen Einspruch erheben zu können, darf nicht entwertet werden.

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

Auf die Umsetzungshinweise des BSI C5 BC-02 bis BC-05 wird hingewiesen.

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

Nachweis

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

Nr. 1.8 – Rückgabe von Datenträgern und Löschung von Daten; 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[23] (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.

[22] 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.

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

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.

Umsetzungshinweis

„Der Vertrag muss Einzelheiten darüber enthalten, wie oft und auf welche Weise der Informationsfluss zwischen dem Auftragsverarbeiter und dem Verantwortlichen stattfinden sollte, damit der Verantwortliche umfassend über die Einzelheiten der Verarbeitung informiert ist, die für den Nachweis der Einhaltung der in Artikel 28 DSGVO festgelegten Pflichten relevant sind. So können beispielsweise die maßgeblichen Teile des Verzeichnisses von Verarbeitungstätigkeiten des Auftragsverarbeiters an den Verantwortlichen weitergegeben werden. Der Auftragsverarbeiter sollte alle Informationen darüber bereitstellen, wie die Verarbeitungstätigkeit im Auftrag des Verantwortlichen durchgeführt wird. Diese Informationen sollten folgende Angaben umfassen: Funktionsweise der verwendeten Systeme, Sicherheitsmaßnahmen, Gewährleistung der Speicher-/ Aufbewahrungspflichten, Speicherort der Daten, Datenübermittlungen, Personen, die Zugriff auf die Daten haben, Empfänger der Daten, eingesetzte Unterauftragsverarbeiter usw."[24]

Der Nachweis der Rückgabe von Datenträgern und der Löschung von Daten kann auch durch Verweis auf entsprechende Grundsätze des Cloud-Anbieters erfolgen. Der Cloud-Nutzer sollte zwischen den Ausführungsmodalitäten wählen können.

Hinsichtlich des Nachweises der Einhaltung der Vorschriften und der Ermöglichung von und des Zulassens von Audits wird auf die Umsetzungsleitlinien im EU Cloud CoC Abschnitt 5.5.3 "Ansatz für Kundenaudits" hingewiesen.

Nachweis

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

Der Cloud-Anbieter kann den Nachweis der Einhaltung des Zuverfügungstellens der erforderlichen Informationen dadurch erbringen, indem er geeignete Unterlagen vorlegt, aus denen hervorgeht, dass er aktiv Maßnahmen zur Bereitstellung von Informationen ergreift und Audits durch den für die Verarbeitung Verantwortlichen oder andere von ihm beauftragte Auditoren zulässt und dazu beiträgt. Durch eine Testnutzung kann der Cloud-Anbieter den Nachweis erbringen, dass die relevanten Informationen auf Anfrage verfügbar sind.

[24] EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO, V. 2.1., § 143.

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[25] 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.

Umsetzungshinweis

Das Datensicherheitskonzept soll die sich aus den spezifischen Umständen des Cloud-Dienstes, seiner Datenverarbeitungsvorgänge und Räumlichkeiten ergebenden Risiken abdecken und zu jedem Risiko eine oder gegebe-

[25] 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.

nenfalls mehrere Richtlinien und Schutzmaßnahmen beinhalten sowie Ressourcen, Verantwortlichkeiten und Priorisierungen für den Umgang mit Datensicherheitsrisiken spezifizieren. Mitarbeiter des Cloud-Anbieters sollten über diese Richtlinien und Schutzmaßnahmen zur Datensicherheit fortlaufend informiert werden. Alle identifizierten Restrisiken des Cloud-Dienstes, die nicht vollständig behandelt werden können, sollten von der Geschäftsleitung des Cloud-Anbieters zur Kenntnis genommen werden. Der Risikobewertungsansatz und die Risikobewertungsmethodik des Cloud-Anbieters sollten dokumentiert werden.

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

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

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

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

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

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

Das Datensicherheitskonzept sollte unter Berücksichtigung neu auftretender Sicherheitsherausforderungen kontinuierlich (mindestens jährlich oder bei Veränderungen) aktualisiert und verbessert werden. Dabei sollten Risikobewertungen, das mögliche Schadensausmaß und die identifizierten akzeptablen Risiken regelmäßig unter Berücksichtigung des technischen und organisatorischen Wandels, erkannten Bedrohungen, der Auswirkung der implementierten Schutzmaßnahmen und externen Ereignisse überprüft werden. Zudem sollten angemessene und für den Cloud-Anbieter relevante Kontakte zu Behörden und Interessenverbänden hergestellt werden, um stets über aktuelle Risiken, Bedrohungslagen und mögliche Gegenmaßnahmen informiert zu sein.

Auf die Umsetzungshinweise im BSI C5 Anf. OIS-02, OIS-03, OIS-05, OIS-06, OIS-07,OPS-010, SP-01, SP-02, SP-03, OPS-18, SIM-01 und HR-04 wird hingewiesen.

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

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

Auf die Umsetzungshinweise im SDM, Abschnitt D3, wird hingewiesen.

Nachweis

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

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

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

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

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

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter stellt durch risikoangemessene TOM sicher, dass Räume und Anlagen gegen Schädigung durch höhere Gewalt[26] 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.

Umsetzungshinweis

Schutzklasse 1

Um sicherzustellen, dass Unbefugte keinen Zutritt zu Räumen und Datenverarbeitungsanlagen erhalten, sollte der Zutritt ins Rechenzentrum über Videoüberwachungssysteme, Bewegungssensoren, Alarmsysteme und von geschultem Sicherheitspersonal fortlaufend überwacht werden. Der Zutritt zu Bereichen, in denen personenbezogene Daten verarbeitet werden, sollte mit einem geeigneten Zwei-Faktor-Authentifizierungsmechanismus gesichert sein, bspw. bestehend aus einer Zutrittskarte und einer geheimen PIN (s. ISO/IEC 27002 Ziff. 11.1.2). Zutrittsrechte sollten regelmäßig (mindestens jährlich und nach jeder wesentlichen Veränderung) überprüft und aktualisiert sowie, sofern erforderlich, wieder entzogen werden. Zur Protokollierung der Zutritte sollte ein physisches Protokollbuch oder ein elektronischer Prüfpfad existieren, der sicher aufbewahrt und überwacht wird (s. ISO/IEC 27002 Ziff. 11.1.2). An- und Abmeldung von Besuchern sollten mit Datum und Uhrzeit vermerkt werden

Einrichtungen sollten durch bauliche, technische und organisatorische Maßnahmen vor Feuer, Wasser, Erdbeben, Explosionen, zivilen Unruhen und anderen Formen natürlicher und von Menschen verursachter Bedrohungen geschützt werden (s. BSI C5 Anf. PS-05). Dazu zählen unter anderem Brandfrüherkennungs- und Löschanlagen, die Durchführung von regelmäßigen Brandschutzübungen und Brandschutzbegehungen, um die Einhaltung der Brandschutzmaßnahmen zu prüfen, die Einbettung von Sensoren zum Überwachen von

[26] 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.

Temperatur und Luftfeuchtigkeit und die Ausstattung aller Gebäude mit Blitzschutzeinrichtungen. Es kann eine fachliche Beratung in Anspruch genommen werden, um mögliche Schäden zu verhindern (s. ISO/IEC 27002 Ziff. 11.1.4).

Schutzklasse 2 und 3

Es gelten die Umsetzungshinweise für Schutzklasse 1.

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

Physische Zutrittssteuerungen sollten insbesondere vor bösartigen Angriffen oder Unfällen konzipiert und angewendet werden, und gleichzeitig an die technischen und wirtschaftlichen Bedingungen des Cloud-Anbieters angepasst werden, die im Datensicherheitskonzept dargelegt sind. Die Gebäudestruktur des Standorts sollte stabil gebaut sein, und alle Außentüren sollten ausreichend mit Hilfe von Kontrollmechanismen (bspw. Schranken, Alarmvorrichtungen, Verriegelungen) vor unbefugtem Zutritt geschützt sein (s. ISO/IEC 27002 Ziff. 11.1.1). Bei den äußeren Türen und Fenstern sollten einbruchhemmendes Material (bspw. nach DIN EN 1627 Widerstandsklasse RC 2) und entsprechende Schließvorrichtungen verbaut sein (s. BSI C5 Anf. PS-03). Alle Außentüren und alle zugänglichen Fenster sollten mit Einbruchmeldeanlagen überwacht werden.

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

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

Auf die Umsetzungshinweise im BSI C5 Anf. OIS-04, PS-01, PS -03, PS-04, PS-06, PS-07 wird hingewiesen.

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

Nachweis

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

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

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

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

Nr. 2.3 – Zugangskontrolle[27] (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.

Umsetzungshinweis

Schutzklasse 1

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

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

[27] 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.

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

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

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

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

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

Der Zugang sollte ausreichend überwacht und geschützt werden, um Angriffe zu erkennen. Dazu sollten u.a. Viren-Schutz- und Reparaturprogramme eingesetzt werden, die eine signatur- und verhaltensbasierte Erkennung und Entfernung von Schadprogrammen ermöglichen (s. BSI C5 OPS-04, OPS-05).

Die Zuteilung geheimer Authentifizierungsinformationen (z. B. Passwörter, Zertifikate, Sicherheitstoken) an Mitarbeiter des Cloud-Anbieters oder den Cloud-Nutzer sollte, soweit diese organisatorischen oder technischen Verfahren des Cloud-Anbieters unterliegt, in einem geordneten Verfahren erfolgen, das die Vertraulichkeit der Informationen sicherstellt (s. BSI C5 Anf. IDM-07 und IDM-09). Soweit die Authentifizierungsinformationen initial vergeben werden, sollten diese nur temporär, höchstens aber 14 Tage lang gültig sein. Benutzer sollten ferner gezwungen werden, diese bei der ersten Verwendung zu ändern. Es sollten interaktive Systeme zur Verwaltung von Kennwörtern genutzt werden sowie starke Kennwörter gemäß dem Stand der Technik (s. ISO/IEC 27002 Ziff. 9.4.3).

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

Die Zugangsberechtigung für netzübergreifende Zugriffe sollte auf einer Sicherheitsbewertung auf Grundlage von Kundenanforderungen basieren (s. BSI C5 Anf. COS-04). Administrative Berechtigungen sollten mindestens halbjährlich überprüft werden (s. BSI C5 Anf. IDM-05).

Auf die Umsetzungshinweise im BSI C5 Anf. OIS-04, OPS-04, OPS-05, OPS-18 bis OPS-23, IDM-01 bis IDM-09, COS-04, COS-05 und SIM-01 bis SIM-05 wird hingewiesen.

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

Schutzklasse 3

Es gelten die Umsetzungshinweise für Schutzklasse 1 und 2.

Der Zugang sollte ausreichend überwacht und geschützt werden, um Angriffe zu erkennen. Dazu sollten u.a. Schwachstellen-Scanner und Intrusion-Detection- and Prevention-Systeme eingesetzt und jährliche Penetrationstests durchgeführt werden, um Schwachstellen zu identifizieren und zu beheben. Systemkomponenten, welche für die Erbringung des Cloud-Dienstes verwendet werden, sollten gemäß allgemein etablierter und akzeptierter Industriestandards gehärtet werden (s. BSI C5 OPS-23).

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

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

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

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

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

Nachweis

Der Cloud-Anbieter legt als Nachweis die Dokumentation zur Zugangskontrolle vor, darunter bspw. Dokumentation der TOM im Datensicherheitskonzept, Berechtigungskonzepte, Verfahrensanweisungen, Richtlinien/Konzepte zu Kennwörtern, Dokumentation zu Authentifizierungs- und Verschlüsselungskonzepten bei dem Zugriff (berechtigter Mitarbeiter) und zu Zugangsberechtigungen. Aus der Dokumentation muss ersichtlich werden, dass das Zugangskonzept und die Berechtigungen aktuell sind und fortlaufend aktualisiert werden (bspw. durch Zeitstempel, Versionierungshistorie oder Protokolle der Aktualisierung).

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

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

Nr. 2.4 – Zugriffskontrolle[28] (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.

(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.

[28] 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.

(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.

Umsetzungshinweis

Schutzklasse 1

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

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

Es sollten angemessene Sicherheitsmaßnamen gegen interne und externe Angriffe implementiert werden, um einen unbefugten Zugriff zu verhindern. Hierzu zählen beispielsweise sämtliche Standardmaßnahmen für den Schutz des Cloud-Hosts, d. h. Host Firewalls, Network-Intrusion-Detection-Systeme, Applikationsschutz, Antivirus und regelmäßige Integritätsüberprüfungen wichtiger Systemdateien. Alle Zugriffe auf personenbezogene Daten sollten protokolliert werden.

Vergabe und Änderung von Zugriffsberechtigungen für Benutzer mit administrativen oder weitreichenden Berechtigungen unter Verantwortung des Cloud-Anbieters sollten gemäß dokumentierten Zugriffsrichtlinien erfolgen (s. BSI C5 IDM-01, IDM-06 und PSS-08). Die Zuweisung sollte personalisiert und nach dem für die Aufgabenwahrnehmung notwendigen Maß erfolgen („Need-to-know-Prinzip“). Organisatorische und/oder technische Maßnahmen sollten sicherstellen, dass durch die Vergabe dieser Berechtigungen keine ungewollten, kritischen Kombinationen entstehen, die gegen das Prinzip der Funktionstrennung verstoßen (z. B. Zuweisen von Berechtigungen zur Administration der Datenbank wie auch des Betriebssystems). Soweit dies in ausgewählten Fällen nicht möglich ist, sollten angemessene, kompensierende Kontrollen eingerichtet werden, um einen Missbrauch dieser Berechtigungen zu identifizieren (z. B. Protokollierung und Überwachung durch eine SIEM-Lösung).

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

Es wird auf die Umsetzungshinweise im SDM-Baustein 43 „Protokollieren“ und -Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“ hingewiesen.

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

Sicherheitsparameter auf Netzwerk, Betriebssystem- (Host und Gast), Datenbank- und Anwendungsebene (soweit für den Cloud-Dienst relevant) sollten angemessen konfiguriert werden, um unautorisierte Zugriffe zu verhindern (s. BSI C5 Anf. IDM-01, IDM-06, PSS-05, PSS-06, PSS-07 und PSS-09). Der Cloud-Dienst sollte ununterbrochen auf Angriffe und Sicherheitsvorfälle überwacht werden, um verdächtige Aktivitäten (z.B. Extraktion großer Datenmengen mehrerer Mandanten), Angriffe und Sicherheitsvorfälle rechtzeitig erkennen und angemessene und zeitnahe Reaktionen einleiten zu können.

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

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

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

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

Richtlinien und Anweisungen mit TOM für die ordnungsgemäße Verwendung mobiler Endgeräte im Verantwortungsbereich des Cloud-Anbieters, die Zugriffe auf IT-Systeme zur Entwicklung und zum Betrieb des Cloud-Dienstes ermöglichen, sollten dokumentiert, kommuniziert und bereitgestellt werden (s. auch BSI C5 OPS-04).

Auf die Umsetzungshinweise im BSI C5 Anf. OIS-04, OPS-04, OPS-05, OPS-10, OPS-18 bis OPS-23, IDM-01 bis IDM-09 und COS-01, COS-04, COS-04, COS-05, und SIM-01 bis SIM-05 wird hingewiesen.

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

Schutzklasse 3

Es gelten die Umsetzungshinweise für Schutzklasse 1 und 2.

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

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

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

Nachweis

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

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

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

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

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

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

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter setzt bei Datenübertragungsvorgängen eine Transportverschlüsselung nach dem Stand der Technik 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[29] 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.

Umsetzungshinweis

Schutzklasse 1

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

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

Auf die Umsetzungshinweise im BSI C5 CRY-01, CRY-02, COS-01, COS-02, COS-06 und COS-08 wird hingewiesen.

Auf die Umsetzungshinweise im SDM-Baustein 43 „Protokollieren“ wird hingewiesen.

[29] 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.

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

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

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

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

Schutzklasse 3

Es gelten die Umsetzungshinweise für Schutzklasse 1 und 2.

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

Nachweis

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

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

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

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

Kriterium

Schutzklasse 1

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

(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.

Umsetzungshinweis

Schutzklasse 1

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

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

Die erstellten Protokolle sollten auf zentralen Protokollierungsservern aufbewahrt werden, wo sie vor unautorisierten Zugriffen und Veränderungen geschützt sind (s. BSI C5 OPS-14). Protokolldaten sollten unverzüglich gelöscht werden, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind.

Auf die Umsetzungshinweise im SDM-Baustein 43 „Protokollieren“ wird hingewiesen.

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

Zwischen den zentralen Protokollierungsservern und den protokollierten (virtuellen) Servern sollte eine Authentisierung erfolgen, um die Integrität und Authentizität der übertragenen und gespeicherten Informationen zu schützen (s. BSI C5 OPS-14). Die Übertragung sollte nach einer dem Stand der Technik entsprechenden Verschlüsselung oder über ein eigenes Administrationsnetz (Out-of-Band-Management) erfolgen.

Der Zugriff und die Verwaltung der Protokollierungs- und Überwachungsfunktionalitäten sollten auf ausgewählte und autorisierte Mitarbeiter des Cloud-Anbieters beschränkt werden. Änderungen der Protokollierungen und Überwachungen sollten vorab durch unabhängige und autorisierte Mitarbeiter überprüft und freigegeben werden (s. BSI C5 OPS-16).

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

Auf die Umsetzungshinweise im BSI C5 OPS-10 und OPS-11 sowie OPS-12 wird hingewiesen.

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

Schutzklasse 3

Es gelten die Umsetzungshinweise für Schutzklasse 1 und 2.

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

Die Verfügbarkeit der Protokollierungs- und Überwachungssoftware sollte unabhängig überwacht werden (s. BSI C5 OPS-17). Bei einem Ausfall der Protokollierungs- und Überwachungssoftware sollten die verantwortlichen Mitarbeiter umgehend informiert werden. Die Protokollierungs- und Überwachungssoftware sollte redundant vorhanden sein, um auch bei Ausfällen die Protokollierung und Überwachung durchführen zu können.

Die erstellten Protokolle erlauben eine eindeutige Identifizierung von Benutzerzugriffen auf Tenant-Ebene, um (forensische) Analysen im Falle eines Sicherheitsvorfalls zu unterstützen (s. BSI C5 OPS-15).

Auf die Umsetzungshinweise im BSI C5 OPS-14 bis OPS-17 wird hingewiesen.

Nachweis

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

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

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

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

Kriterium

Schutzklasse 1

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

(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[30] entsprechen (wie in den Umsetzungshinweisen beschrieben).

Erläuterung

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

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

Umsetzungshinweis

Schutzklasse 1

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

Um eine weisungsgetreue De-Pseudonymisierung durchführen zu können, sollten mit dem Cloud-Nutzer dokumentierte Fälle von gewünschten Aufdeckungen definiert werden. Der Vorgang der De-Pseudonymisierung sollte protokolliert werden. Aus dem Protokoll sollte hervorgehen, wer die De-Pseudonymisierung durchgeführt hat. In ihm sollten jedoch keine Angaben enthalten sein, die Rückschlüsse auf die dem Pseudonym zugrunde liegenden Identitätsdaten erlauben.

Schutzklasse 2 und 3

Es gelten die Umsetzungshinweise für Schutzklasse 1.

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

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

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

[30] 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.

Nachweis

Für Schutzklasse 1 legt der Cloud-Anbieter Dokumentationen über den Prozess der Datenverarbeitung, insbesondere im Hinblick auf pseudonymisierte Daten vor. Durch eine testweise Dienstnutzung mit pseudonymisierten Daten kann nachgewiesen werden, dass Verarbeitungen unter Wahrung der Pseudonymität durchgeführt werden. Erfordert die Art des Auftrags mit dem Cloud-Nutzer die De-Pseudonymisierung der Daten, legt ein Cloud-Anbieter die rechtsverbindliche Vereinbarung mit dem Cloud-Nutzer oder andere Dokumente zur Weisungserteilung des Cloud-Nutzers vor.

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

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

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

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

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter stellt durch implementierte TOMs[31] sicher, dass Anonymisierung[32] (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[33] entsprechen.

[31] 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.

[32] TOMs in Bezug auf die Anonymisierung müssen daher offiziellen Normen oder dem Stand der Technik entsprechen.

[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.

Erläuterung

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

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

Umsetzungshinweis

Schutzklasse 1

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

Schutzklasse 2 und 3

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

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

Nachweis

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

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

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

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

Nr. 2.9 – Verschlüsselung gespeicherter Daten[34] (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.

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

(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[35] (wie in den Umsetzungshinweisen beschrieben).

(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[36] (wie in den Umsetzungshinweisen beschrieben) entsprechen.

Erläuterung

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

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

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

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

Umsetzungshinweis

Schutzklasse 1

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

Schutzklasse 2

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

Soweit der Cloud-Anbieter Daten verschlüsselt, sollte die Schlüsselerzeugung in einer sicheren Umgebung und unter Einsatz geeigneter Schlüsselgeneratoren erfolgen. Kryptografische Schlüssel sollten möglichst nur einem Einsatzzweck dienen und generell nie in klarer Form, sondern grundsätzlich verschlüsselt im System gespeichert werden. Die Speicherung sollte stets redundant gesichert und wiederherstellbar sein, um einen

[35] 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.

[36] 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.

Verlust eines Schlüssels auszuschließen. Schlüsselwechsel sollten regelmäßig durchgeführt werden. Der Zugang zum Schlüsselverwaltungssystem sollte eine separate Authentisierung erfordern. Cloud-Administratoren sollten keinen Zugriff auf Nutzerschlüssel haben.

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

Auf die Technischen Reports BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ in der jeweils aktuellen Fassung wird hingewiesen.

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

Schutzklasse 3

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

Nachweis

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

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

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

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

Kriterium

Schutzklasse 1

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

(2) 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.

Umsetzungshinweis

Schutzklasse 1

Daten sollten auf gemeinsam genutzten virtuellen und physischen Ressourcen (Speichernetz, Arbeitsspeicher) gemäß einem dokumentierten Konzept sicher und strikt separiert werden (s. BSI C5 OPS-24). Eine technische Trennung der gespeicherten und verarbeiteten Daten der Cloud-Nutzer in gemeinsam genutzten Ressourcen kann durch Firewalls, Zugriffslisten, Tagging (Auszeichnung des Datenbestandes), VLANs, Virtualisierung und Maßnahmen im Speichernetz (z. B. LUN Masking) erreicht werden.

Auf die Umsetzungshinweise des BSI C5 OPS-24 und COS-06 wird hingewiesen.

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

Auf die Umsetzungshinweise im SDM-Baustein 50 „Trennen“ wird hingewiesen.

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

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

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

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

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

Bei IaaS/PaaS ist die sichere Trennung durch physisch getrennte Netze oder durch stark verschlüsselte VLANs sichergestellt (s. BSI C5 Anf. COS-06).

Schutzklasse 3

Es gelten die Umsetzungshinweise für Schutzklasse 1 und 2.

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

Nachweis

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

der TOM, Verfahrensanweisungen, Richtlinien, Ergebnisprotokolle interner/externer Audits, Risikoanalysen und Produktbeschreibungen als Nachweis vorlegen.

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

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

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

Kriterium

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

Wiederherstellbarkeitsklasse 1

Der Cloud-Anbieter sichert seinen Dienst gegen zu erwartende, naheliegende Ereignisse so zuverlässig ab 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.

Umsetzungshinweis

Wiederherstellbarkeitsklasse 1

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

Es sollten regelmäßig Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß einem Datensicherungskonzept angefertigt werden. Hierin sollten auch Aufbewahrungs- und Schutzanforderungen festgelegt werden. Die Wiederherstellbarkeit der Sicherheitskopien sollte regelmäßig überprüft werden.

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

Auf die Umsetzungshinweise im BSI C5 OPS-01 bis OPS-03, OPS-06 bis OPS-10 wird hingewiesen.

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

Auf die Umsetzungshinweise im SDM-Baustein 11 „Aufbewahren“ wird hingewiesen.

Wiederherstellbarkeitsklasse 2

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

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

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

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

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

Wiederherstellbarkeitsklasse 3

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

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

Nachweis

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

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

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

Nr. 3 – Sicherstellung der Weisungsbefolgung (Art. 28 Abs. 3 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.

Umsetzungshinweis

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

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

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

Der Cloud-Anbieter sollte durch TOM sicherstellen, dass er den Cloud-Nutzer über die rechtlichen Anforderungen einer nicht weisungsgedeckten Verarbeitung zur Erfüllung von Pflichten aus dem Unionsrecht oder aus mitgliedstaatlichem Recht vor deren Durchführung informiert. Auf diese Weise wird sichergestellt, dass auch diese Verarbeitung dem Cloud-Nutzer transparent gemacht wird, sodass er ggf. betroffene Personen informieren kann. Ausnahmen von der Informationspflicht bestehen nach Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a DSGVO nur, sofern das betreffende Recht eine solche Mitteilung im wichtigen öffentlichen Interesse verbietet. Beispiele hierfür sind Übermittlungen des Cloud-Anbieters an Ermittlungsbehörden in Strafsachen, Steuerangelegenheiten oder staatsschutz- und geheimdienstrelevante Sachverhalte.

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

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

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

Nachweis

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

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

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

Der Cloud-Anbieter legt als Nachweis erfolgte Mitteilungen an den Cloud-Nutzer über rechtliche Anforderungen zu nicht weisungsgedeckten Verarbeitungen zur Erfüllung rechtlicher Pflichten aus dem Unionsrecht oder dem mitgliedstaatlichen Recht vor, soweit er über solche verfügt. Als Nachweis können auch Dokumentationen dienen, darunter bspw. Dokumentation der TOM oder Verfahrensanweisungen, z.B., wie mit Anfragen von Ermittlungsbehörden umzugehen ist, die eine Herausgabe von Daten zum Inhalt haben oder wie der Cloud-Nutzer über diese rechtlichen Anforderungen zu informieren ist.

Nr. 4 – Hinweispflicht des Cloud-Anbieters

Nr. 4.1 – Weisungen entgegen datenschutzrechtlicher Vorschriften (Art. 28 Abs. 3 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.

Umsetzungshinweis

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

Bei Massengeschäften, in denen der Cloud-Nutzer durch die Auswahl des Cloud-Dienstes aufgrund einer Dienstbeschreibung des Cloud-Anbieters die Weisung erteilt, sollte der Cloud-Anbieter TOM vorsehen, die den Cloud-Nutzer darauf hinweisen, wenn er den Dienst datenschutzwidrig entgegen der Dienstbeschreibung nutzt. Dazu zählt beispielsweise ein Informationstext, der den Cloud-Nutzer warnt, wenn die vom Cloud-Anbieter zur Verfügung gestellten Datensicherungsmaßnahmen wie Verschlüsselung und Pseudonymisierung nicht genutzt werden.

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

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

Nachweis

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

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

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

Nr. 4.2 – Änderungen des Datenverarbeitungsortes (indirekt Art. 28 Abs. 3 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.

Umsetzungshinweis

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

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

Nachweis

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

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

Nr. 5 – Sicherstellung der Vertraulichkeit beim Personal (Art. 28 Abs. 3 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.

Umsetzungshinweis

Den Mitarbeitern des Cloud-Anbieters sollte der Cloud-Anbieter eine Ausfertigung des Verpflichtungstextes mitsamt den Hinweisen auf mögliche Folgen von Verschwiegenheitspflichtverletzungen aushändigen. Er sollte die Belehrung in angemessenen Abständen wiederholen, etwa im Zusammenhang mit Schulungen oder insbesondere bei

Änderung der Zugriffs- und Verarbeitungskompetenz des jeweiligen Mitarbeiters. Außerdem sollte der Cloud-Anbieter die betroffenen Personen zu Fragen des Datenschutzes und der Datensicherheit in Bezug auf ihre Tätigkeit regelmäßig sensibilisieren.

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

Auf die Umsetzungshinweise im BSI C5 HR-05 und HR-06 wird hingewiesen.

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

Nachweis

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

Im Rahmen eines Audits kann die Einhaltung dieser Vorgaben in allen Prozesskonstellationen durch Interviews mit Mitarbeitern nachgewiesen werden (bspw. Befragung, ob Mitarbeiter zur Vertraulichkeit verpflichtet wurden und ihnen bekannt ist, welche Vertraulichkeitspflichten damit einhergehen). Auch kann eine Beobachtung bei einer testweisen Änderung von Verarbeitungsbefugnissen durchgeführt werden, um die Anpassungen von Verpflichtungserklärungen zu simulieren.

Nr. 6 – Unterstützung des Cloud-Nutzers bei der Wahrung der Betroffenenrechte[37]

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[38] (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

[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.

[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.

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

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

Umsetzungshinweis

Soweit personenbezogene Daten betroffen sind, auf die nur der Cloud-Anbieter Zugriff gewähren kann (z.B. Server-Logs), sollte für den Cloud-Nutzer eine organisatorische Kontaktstelle vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung dieser veranlassen kann. Mit Hilfe eines Ticketsystems können die Weisungen des Cloud-Nutzers dokumentiert werden.

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

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

Nachweis

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

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

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

Nr. 6.2 – Auskunftserteilung[39] (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 15 DSGVO)

Kriterium

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

(2) Der Cloud-Anbieter dokumentiert 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).

[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.

Umsetzungshinweis

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

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

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

Nachweis

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

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

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

Nr. 6.3 – Berichtigung und Vervollständigung[40] (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).

Umsetzungshinweis

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

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

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

Auf die Umsetzungshinweise im SDM-Baustein 61 „Berichtigen“ wird hingewiesen.

[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.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er dokumentiert, welche Maßnahmen er ergriffen hat, um dem Cloud-Nutzer die Berichtigung und Vervollständigung von Daten zu ermöglichen oder diese durch den Cloud-Anbieter vornehmen zu lassen (z.B. Dokumentation der relevanten Mechanismen und Meldewege, Dienstbeschreibungen). Auch können anhand von Prozessdokumentationen und Protokollen die tatsächlich durchgeführten Berichtigungen und Vervollständigungen nachgewiesen werden.

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

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

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).

Umsetzungshinweis

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

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

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

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

Da die Löschung von Daten in Backup- und Ausfallsicherungssystemen im Vergleich zur Löschung im aktiven Datenbestand aufwändiger ist, können Kopien und Daten aus Sicherungssystemen auch zu späteren Zeitpunkten als im aktiven Datenbestand gelöscht werden, z.B. im Zuge der Überschreibung oder Vernichtung der betroffenen Datenträger. Regelhaft sollte die Löschung in den Sicherungsdateien spätestens ein Jahr nach der Löschung im aktiven Datenbestand erfolgen, wobei regelmäßig kürzere Fristen angestrebt werden sollten. Die Löschung in Backup- und Ausfallsicherungssystemen sollte alle Vorgängerversionen der Daten, temporäre Daten, Metadaten und Dateifragmente umfassen. Der Cloud-Anbieter kann auch TOMs verwenden, um selektive Löschungen durchzuführen, bei denen Backups zumindest teilweise gelöscht werden, um die Daten so schnell wie möglich zu löschen.

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

Auf die Umsetzungshinweise im SDM-Baustein 60 „Löschen und Vernichten“ wird hingewiesen.

Nachweis

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

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

Nr. 6.5 – Einschränkung der Verarbeitung[41] (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.

Erläuterung

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

Umsetzungshinweis

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

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

Auf die Umsetzungshinweise im SDM-Baustein 62 „Einschränken der Verarbeitung“ wird hingewiesen.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er dokumentiert, welche Maßnahmen er ergriffen hat, um dem Cloud-Nutzer die Einschränkung der Verarbeitung von Daten zu ermöglichen oder dies durch den Cloud-Anbieter vornehmen zu lassen. Er kann Protokolle zu getätigten Weisungen und darauffolgenden Einschränkungen vorlegen.

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

[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.

Nr. 6.6 – Mitteilungspflicht bei Berichtung, Löschung oder Einschränkung der Verarbeitung[42] (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).

Umsetzungshinweis

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

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

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er dokumentiert, welche Maßnahmen er ergriffen hat, um es dem Cloud-Nutzer zu ermöglichen, Empfängern, denen er personenbezogene Daten offengelegt hat, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitzuteilen und die betroffene Person auf Verlangen über die Empfänger zu unterrichten oder dies durch den Cloud-Anbieter vornehmen zu lassen (z.B. Dokumentation der relevanten Mechanismen und Meldewege, Dienstbeschreibungen). Er kann Protokolle zu getätigten Weisungen und darauffolgenden Mitteilungen vorlegen.

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

Nr. 6.7 – Datenübertragung[43] (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.

[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.

[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.

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).

Umsetzungshinweis

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

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

Auf die Umsetzungshinweise im BSI C5 Anf. PI-01 bis PI-02 und COS-08 wird hingewiesen.

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

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

Auf die Umsetzungshinweise im SDM-Baustein 11 „Aufbewahren“ wird hingewiesen.

Nachweis

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

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

Nr. 6.8 – Widerspruch[44] (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

(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

[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.

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).

Umsetzungshinweis

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

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

Nachweis

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

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

Nr. 6.9 – Generelle Informationspflicht und Informationspflicht bei Untätigkeit oder verzögerter Antragsbearbeitung[45]
(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.

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

Umsetzungshinweis

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

Werden Weisungen zur Umsetzung der Informationspflicht automatisiert ausgeführt (z.B. mittels Softwarebefehlen durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeileneingabe), sollten auch entsprechende Felder implementiert sein, in denen der Cloud-Nutzer Informationen über die ergriffenen Maßnahmen, die Fristverlängerung und die Gründe hierfür bzw. die Gründe seiner Untätigkeit und die Möglichkeit bei der Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen, angeben kann. Diese Nutzerinteraktionen sollten automatisiert protokolliert werden, um nachzuweisen, dass der Cloud-Anbieter weisungsgebunden handelt.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er Dokumentationen zu Maßnahmen vorlegt, die er ergriffen hat, um dem Cloud-Nutzer die Informationserteilung gegenüber einer betroffenen Person zu ermöglichen oder die Information durch den Cloud-Anbieter mitteilen zu lassen (z.B. Mechanismen und Meldewege, oder Dienstbeschreibungen).

Anhand von Prozessdokumentationen und Protokollen kann nachgewiesen werden, ob die tatsächlich durchgeführten Informationserteilungen an die betroffenen Personen durchgeführt wurden und vollständig sind.

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

Nr. 7 – Unterstützung bei der Datenschutz-Folgenabschätzung[46] (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

[46] 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.

Cloud-Nutzer zwingend durchgeführt werden muss (DSFA-Liste Verarbeitungsvorgänge). Auf diese wird hiermit verwiesen.

Umsetzungshinweis

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

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

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

Auf die Umsetzungshinweise im SDM-Baustein 41 „Planen und Spezifizieren“ wird hingewiesen.

Nachweis

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

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

Kapitel III: Datenschutz-Managementsystem des Cloud-Anbieters

Erläuterung

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

Nr. 8 – Datenschutz-Managementsystem

Nr. 8.1 – Benennung, Stellung und Aufgaben eines Datenschutzbeauftragten (Art. 37 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.

(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.

Umsetzungshinweis

Der Cloud-Anbieter sollte dokumentieren, ob ein DSB benannt werden muss, einschließlich der gemäß den Absätzen 1 bis 5 bewerteten Bedingungen und der Bewertungsergebnisse für jede Bedingung.

Der Cloud-Anbieter sollte eine schriftliche Dokumentation der für den jeweiligen Cloud-Dienst eingesetzten Systeme, Verfahren und Prozesse (Software, Hardware, beteiligte Organisationseinheiten, Rollen und Dienstleister) und eine möglichst exakte Beschreibung der Gesamtheit der getroffenen TOM führen (z.B. in einem Datensicherheitskonzept) und dem DSB sowie (auf Anfrage) der Aufsichtsbehörde zugänglich machen. Der Cloud-Anbieter sollte TOM treffen, um sicherzustellen, dass der DSB bereits in einem frühen Stadium des Cloud-Entwicklungsprozesses konsultiert wird, der zu Änderungen bei der Datenverarbeitung führen kann. Zur Einbeziehung des DSB kann beispielsweise ein Ticketsystem verwendet werden.

Ist der DSB bei einem anderen Unternehmen beschäftigt (externer DSB des Cloud-Anbieters) oder gleichzeitig DSB anderer Unternehmen, gilt seine Weisungsfreiheit auch gegenüber seinem Arbeitgeber und seinen anderen Auftraggebern. Die Anforderung der Abwesenheit von Interessenskonflikten ist primär eine Benennungsvoraussetzung und in sekundärer Hinsicht eine Organisationspflicht des Cloud-Anbieters. Der Cloud-Anbieter weist dem DSB keine zusätzlichen Aufgaben zu, die ihn in einen Interessenskonflikt bringen könnten. Interessenskonflikte sind im

Rahmen folgender Tätigkeiten anzunehmen: Tätigkeiten, im Rahmen derer der DSB sich selbst kontrollieren müsste, z.B. Stellung als Geschäftsführer, IT- oder Personalabteilungsleiter, wirtschaftliche Interessen des DSB am Unternehmenserfolg oder zu große Nähe zur benennenden Stelle.

Die Geheimhaltungs- oder Vertraulichkeitspflicht des DSB umfasst alle diesbezüglich relevanten Informationen. Dies sollte auch aus der Benennungsurkunde hervorgehen. Auch gegenüber der ihn benennenden Stelle ist der DSB zur umfassenden Verschwiegenheit verpflichtet. Das Kriterium fördert das Gewährleistungsziel der Vertraulichkeit (SDM C1.4).

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

Nachweis

Der Cloud-Anbieter kann den Nachweis dadurch erbringen, indem er einen DSB benennt und die Kontaktdaten des DSB der zuständigen Aufsichtsbehörde meldet sowie ihn auf seiner Webseite als Ansprechpartner der Öffentlichkeit vorstellt. Auch interne Dokumente wie z.B. die Vorlage der Stellenbeschreibung des DSB oder von Benennungsurkunden, Fachkundenachweisen (bspw. Zeugnissen, Schulungsnachweisen), Aufgaben- und Verfahrensbeschreibungen, Richtlinien, oder Organigrammen, die die Einordnung des DSB beschreiben, können geeignete Nachweise sein. Gleiches gilt für die Bereitstellung von Protokollen über die Mitarbeiterinformation zur Rolle des DSB; für Gesprächsprotokolle mit dem DSB zur Überprüfung der Anforderungserfüllung und für Tätigkeitsberichte.

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

Zur Beurteilung der Geheimhaltungs- oder Vertraulichkeitspflicht kann der Cloud-Anbieter die entsprechende unterzeichnete Benennungsurkunde des DSB mit den geforderten Inhalten vorlegen.

Mit den regelmäßig durchzuführenden internen Audits des DSB kann der Nachweis über seine Tätigkeiten, seine Unabhängigkeit sowie seine Einbindung und Wirksamkeit im Organisationsgefüge des Cloud-Anbieters nachgewiesen werden. Hierzu sollten entsprechende Auditprotokolle zur Prüfung vorgelegt werden. Mittels Protokollen und sonstigen Dokumenten sowie einer Befragung des Managements kann nachgewiesen werden, ob der DSB der obersten Managementebene direkt berichtet. Eine Befragung des DSB zu seinen Aufgaben ist geeignet um nachzuweisen, dass er keinem Interessenkonflikt unterliegt. Zusätzlich können Dokumente vorgelegt werden, die Auskunft über die geleisteten Arbeitsstunden des DSB geben.

Nr. 8.2 – Meldung von Datenschutzverletzungen[47] (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).

[47] 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.

Umsetzungshinweis

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

Auf die Umsetzungshinweise in der Guideline 9/2022 betreffend die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß DSGVO wird hingewiesen.

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

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

Nachweis

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

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

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

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

Umsetzungshinweis

Der Cloud-Anbieter sollte seine Ausarbeitung darüber dokumentieren, ob ein Verzeichnis der Verarbeitungstätigkeiten geführt werden muss, einschließlich der gemäß den Absätzen 1 bis 4 bewerteten Bedingungen und der Bewertungsergebnisse für jede Bedingung.

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

Das Verarbeitungsverzeichnis kann für alle Dokumentationspflichten als Nachweis oder Nachweisbekräftigung herangezogen werden. Dieses Verzeichnis ist jedoch nicht öffentlich und richtet sich nicht an betroffene Personen, sondern ist ausschließlich nach innen und auf das Verhältnis zur Aufsichtsbehörde gerichtet.

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

Auf die Umsetzungshinweise im SDM-Baustein 41 „Planen und Spezifizieren“ und Baustein 42 „Dokumentieren“ wird hingewiesen.

Nachweis

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

Der Cloud-Anbieter legt Prozessdokumentationen zur Aktualisierung der Verarbeitungsverzeichnisse und zur Zusammenarbeit der an der Erstellung der Verarbeitungsverzeichnisse beteiligten Akteure vor. Ebenso sind Prozessdokumentationen zur Entgegennahme, Bearbeitung und Beantwortung von Anfragen von Aufsichtsbehörden zu Verarbeitungsverzeichnissen vorzulegen. Zum Nachweis über geregelte Zuständigkeiten können Organigramme, Aufgabenverteilungspläne oder sonstige Dokumente vorgelegt werden. Weiterhin können im Rahmen eines Audits Befragungen von Mitarbeitern durchgeführt werden, um nachzuweisen, dass die festgelegten Prozesse im Unternehmen bekannt sind und gelebt werden. Die aktuellen und vollständigen Verarbeitungsverzeichnisse des Vertreters kann der Cloud-Anbieter ebenfalls durch ihre Vorlage nachweisen.

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.

Umsetzungshinweis

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

Da die Löschung von Daten in Backup- und Ausfallsicherungssystemen im Vergleich zur Löschung im aktiven Datenbestand aufwändiger ist, können Kopien und Daten aus Sicherungssystemen auch zu späteren Zeitpunkten als im aktiven Datenbestand gelöscht werden, z.B. im Zuge der Überschreibung oder Vernichtung der betroffenen Datenträger. Regelhaft sollte die Löschung in den Sicherungsdateien spätestens ein Jahr nach der Löschung im aktiven Datenbestand erfolgen, wobei regelmäßig kürzere Fristen angestrebt werden sollten. Die Löschung in Backup- und Ausfallsicherungssystemen sollte alle Vorgängerversionen der Daten, temporäre Daten, Metadaten und Dateifragmente umfassen. Der Cloud-Anbieter kann auch TOMs verwenden, um selektive Löschungen durchzuführen, bei denen Backups zumindest teilweise gelöscht werden, um die Daten so schnell wie möglich zu löschen.

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

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

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

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

Auf die Umsetzungshinweise im BSI C5 Anf. AM-04, AM-05 und PI-03 wird hingewiesen.

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

Auf die Umsetzungshinweise im SDM-Baustein 11 „Aufbewahren“ und -Baustein 60 „Löschen und Vernichten“ wird hingewiesen.

Hinsichtlich des Nachweises der Einhaltung der Vorschriften und der Ermöglichung von und der Mitwirkung an Audits wird auf die Umsetzungsleitlinien im EU Cloud CoC Abschnitt 5.5 "Recht auf Audit" verwiesen.

Nachweis

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

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

Der Cloud-Anbieter legt geeignete Dokumentationen vor die belegen, dass der Cloud-Anbieter aktiv Maßnahmen ergreift, um die für Artikel 28 DSGVO erforderlichen Informationen zur Verfügung zu stellen und Audits durch den Verantwortlichen oder andere von ihm beauftragte Auditoren 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.

Umsetzungshinweis

Der Cloud-Anbieter sollte vor allem die internen Audits des DSB zu Datenschutzfragen heranziehen. Des Weiteren wird auf die Umsetzungshinweise zur regelmäßigen Überprüfung durch die oberste Leitung beim Cloud-Anbieter nach ISO/IEC 27002 Ziff. 18.1 und 18.2. hingewiesen.

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

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

Auf die Umsetzungshinweise im BSI C5 DEV-01 bis DEV-10 in Hinblick auf die Einbettung des Revisionsprozesses in das Change-Management sowie Anf. COM-01 bis COM-4 wird hingewiesen.

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

Nachweis

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

Nr. 8.6 – Auswahl und Einsatz geeigneter Personen (Art. 28 Abs. 3 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.

Umsetzungshinweis

Um die fachliche Kompetenz der Mitarbeiter zu erhalten, sollte der Cloud-Anbieter regelmäßige Mitarbeiterschulungen (ca. 1 Mal pro Jahr) zu datenschutzrechtlichen und datensicherheitstechnischen Themen durchführen – auch zur konkreten Technik des Cloud-Dienstes. Die Schulung von Mitarbeitern obliegt dem DSB.

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

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

Nachweis

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

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

Kapitel IV: Datenschutz durch Systemgestaltung

Nr. 9 – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

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

Kriterium

(1) Der Cloud-Anbieter 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[48], 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.

[48] Konzeptionelle Zielsetzungen sind solche, die auf das jeweilige Modell der angebotenen Dienste abzielen, d. h. das Angebot von Software-, Plattform- oder Infrastrukturdiensten usw.

Umsetzungshinweis

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

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

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

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

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

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

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

Auf die Umsetzungshinweise im SDM-Baustein 41 „Planen und Spezifizieren“, -Baustein 42 „Dokumentieren“ und -Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“ wird hingewiesen.

Nachweis

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

Der Cloud-Anbieter kann Dokumente vorlegen, aus denen hervorgeht, mit welchen Risiken er sich auseinandergesetzt hat und welche Gestaltungsprinzipien und -maßnahmen er vorgesehen hat, um die identifizierten Risiken zu minimieren und die Datenschutzgrundsätze umzusetzen. Die Dokumentationen sollten auch die Erwägungen enthalten, die den Cloud-Anbieter bei der Wahl der TOM i geleitet haben. Relevante Dokumentationen umfassen Dienstbeschreibungen, das Datensicherheitskonzept mit den TOM, Rollen- und Berechtigungskonzepte, Prozessbeschreibungen, Verfahrensanweisungen, Richtlinien, Musterverträge für Subauftragsverarbeiter, Ergebnisprotokolle von internen Audits und Subauftragsverarbeiterkontrollen, Risikoanalysen, Dokumentationen des Information Security Management Systems, Incident-Response-Management Dokumentationen und Datenschutz-Folgenabschätzungen.

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

Darüber hinaus kann eine Entwicklungs- und Designprüfung durchgeführt werden, um nachzuweisen, dass die datenschutzrechtlichen Anforderungen bereits bei der Entwicklung des Systems berücksichtigt werden. Hierzu kann der Cloud-Anbieter Dokumente über eingesetzte Entwicklungsmethoden und -verfahren (insb. Abnahmekriterien und Anforderungslisten) vorlegen. Eine Prüfung von Testsystemen und -umgebungen (bspw. auf Angemes-

senheit und Sicherheit) kann bei Bedarf durchgeführt werden. Bei der Designprüfung können unter anderem Dokumentationen zur gewählten Architektur, Datenbankdiagramme, Datenflussdiagramme, Designentscheidungen, aber auch die Konfiguration und Einstellung des Cloud-Dienstes zur Erbringung des Datenverarbeitungsvorgangs vorgelegt werden.

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

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

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

Kriterium

(1) Der Cloud-Anbieter stellt durch seine Voreinstellungen im jeweiligen Dienst sicher, dass nur personenbezogene Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck erforderlich sind 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[49], 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[50] für die betroffenen Personen durch eine zu umfassende Zugänglichmachung[51] von personenbezogenen Daten entstehen.

Erläuterung

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

Umsetzungshinweis

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

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

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

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

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

---

[49] 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.

[50] 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.

[51] 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.

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

Auf die Umsetzungshinweise im SDM-Baustein 41 „Planen und Spezifizieren“, -Baustein 42 „Dokumentieren“ und -Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“ wird hingewiesen.

Nachweis

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

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

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

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

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

Kapitel V: Subauftragsverarbeitung

Erläuterung

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

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

Nr. 10 – Subauftragsverhältnisse

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

Kriterium

(1) Der Cloud-Anbieter 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.

Umsetzungshinweis

Nach Art. 28 Abs. 2 Satz 1 DSGVO bedarf es für die Einbindung von Subauftragsverarbeitern der Genehmigung des Cloud-Nutzers. Die Genehmigung kann gesondert oder allgemein erteilt werden. Die gesonderte Genehmigung bietet sich für solche Fälle an, in denen absehbar ist, dass Subauftragsverarbeiter nur ausnahmsweise eingesetzt werden sollen und keine Änderungen zu erwarten sind. Die allgemeine Genehmigung sollte genutzt werden, wenn bereits bei Abschluss der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung klar ist, dass zahlreiche Subauftragsverarbeiter eingesetzt werden sollen und der Cloud-Nutzer damit einverstanden ist.

Bei standardisierten Massengeschäften sollten die Cloud-Nutzer bei Änderungen in den Subauftragsverarbeitungen automatisiert und proaktiv („Push"-Nachricht), z.B. über eine automatisch generierte E-Mail, informiert werden. In den AGB von Cloud-Anbietern im Massengeschäft kann z.B. auch vorab eine Generalzustimmung für etwaige Änderungen in der Subauftragsverarbeitung, die vorbehalten werden, eingeholt werden. Da im Massengeschäft ein Einspruch (i.S.d. Art. 28 Abs. 2 Satz 2 Hs. 2 DSGVO) von einem einzelnen Cloud-Nutzer die Beauftragung eines weiteren oder anderen Auftragsverarbeiters durch den Cloud-Anbieter nicht verhindern wird, sollten in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung (Nr. 1.7) die Voraussetzungen und Folgen eines Einspruchs geregelt werden, bspw. ob der Cloud-Nutzer bei Einspruch die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung aufkündigen darf.

Auf die Umsetzungshinweise im BSI C5 OIS-03, SSO-01 bis SSO-05 wird hingewiesen.

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

Nachweis

Der Cloud-Anbieter kann den Nachweis über die rechtskonforme weitere Datenverarbeitung dadurch erbringen, dass er die erteilte Zustimmung der Cloud-Nutzer vorlegt. Die gesondert erteilte Genehmigung enthält die Identitäten der genehmigten Subauftragsverarbeiter, ihre Anschriften sowie die Beschreibungen der Verarbeitungen, die sie durchführen sollen und eine Abgrenzung der Zuständigkeiten zwischen dem Cloud-Anbieter und dem/den Subauftragsverarbeiter(n) sowie zwischen verschiedenen Subauftragsverarbeitern.

Weiterhin können Verträge zu den weiteren Auftragsverarbeitungen (Sub-Cloud-Verträge) mitsamt der für die Konformitätsprüfung erforderlichen Angaben (Dauer, Art und Zweck, Ort der weiteren Verarbeitung, Angaben über den weiteren Auftragsverarbeiter und dessen Dienstbeschreibung) vorgelegt werden.

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

Kriterium

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

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

Umsetzungshinweis

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

Nachweis

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

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

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

Kriterium

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

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

Erläuterung

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

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

Umsetzungshinweis

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

Zur Darstellung der involvierten Subauftragsverarbeiter eignen sich Informationsportale innerhalb oder außerhalb des angebotenen Cloud-Dienstes und ebenfalls für das proaktive Informieren („Push"-Nachricht) der Cloud-Nutzer hinsichtlich Veränderungen in der Subauftragsverarbeitung. Diese sollten fortlaufend gepflegt und aktualisiert werden.

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

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er Dokumente (wie konkrete rechtsverbindliche Subauftragsvereinbarungen oder Muster solcher Vereinbarungen) vorlegt, die den Cloud-Nutzer in Kenntnis darüber setzen wie er bei beabsichtigten Änderungen von Subauftragsverarbeitern informiert wird (z.B. per E-Mail oder in Informationsportalen). Zudem sollte der Cloud-Anbieter Dokumentationen darüber vorlegen, wie Einsprüche von

Cloud-Nutzer entgegengenommen und bearbeitet werden. Weitere relevante Nachweisdokumente können bspw. Dokumentationen der Einwilligungen von Cloud-Nutzern sowie solche über die Ausübung des Widerspruchsrechts sein. Protokolle über mitgeteilte Änderungen der Einbindung von Subauftragsverarbeitern oder bearbeitete Einsprüche sollten vom Cloud-Anbieter, sofern angefallen, vorgelegt werden.

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

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

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

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass nur solche Subauftragsverarbeiter in die Auftragsverarbeitung einbezogen werden, die die Gewähr für die Einhaltung der 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.

Umsetzungshinweis

Soweit der Cloud-Anbieter nicht auf Zertifikate seiner Subauftragsverarbeiter vertrauen kann, sollte er sich selbst von der Einhaltung der datenschutzrechtlichen Anforderungen durch die Subauftragsverarbeiter überzeugen.

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

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

Nachweis

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

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

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

Umsetzungshinweis

Der Cloud-Anbieter sollte wegen des gesteigerten Risikos bei weiteren Auftragsverarbeitungen interne Dokumentationen führen und die Verarbeitungsprozesse protokollieren. Dies dient auch der Selbstkontrolle des Cloud-Anbieters bei der Pflichtenerfüllung auf den weiteren Auftragsstufen. Abhängig von den jeweiligen ausgelagerten Verarbeitungsprozessen sollten in der rechtsverbindlichen Vereinbarung mit dem Subauftragsverarbeiter die entsprechenden Unterstützungsfunktionen festgehalten werden. Insbesondere sollten Kontaktstellen und die jeweiligen Verantwortlichkeiten bei Subauftragsverarbeitern protokolliert und fortlaufend aktualisiert werden. Es sollten Prozesse, Meldewege und Verfahrensrichtlinien definiert und dokumentiert werden.

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

Nachweis

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

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

Falls vorhanden, sollten die vom Cloud-Anbieter zur automatischen Überwachung der Datenverarbeitung durch Subauftragsverarbeiter verwendeten TOM geprüft werden (z. B. SIEM-Systeme oder von Subauftragsverarbeitern angebotene APIs).

Kapitel VI: Datenverarbeitung außerhalb der EU und des EWR

Nr. 11 – Datenübermittlung[52]

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[53] 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

[52] 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.

[53] 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).

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.[54]

(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

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[55] 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.

[54] 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).

[55] 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.

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).

Umsetzungshinweis

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

Der Europäische Datenschutzausschuss hat in seinen „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Datenschutzniveaus für personenbezogene Daten“ einen sechsschritten Fahrplan veröffentlicht, der angibt, wie der Cloud-Anbieter vorgehen sollte, um festzustellen, ob die Instrumente nach Art. 46 Abs. 2 oder 3 DSGVO hinreichend sind, um ein angemessenes Datenschutzniveau für die Datenübermittlung in das betreffende Drittland sicherzustellen, oder ob zusätzliche Maßnahmen ergriffen werden müssen, um ein angemessenes Datenschutzniveau sicherzustellen. Es wird daher insbesondere auf diesen sechsschrittigen Fahrplan in den Empfehlungen 01/2020 als Umsetzungshinweis verwiesen.

Besonderes Augenmerk sollte auf den 3. und 4. Schritt des Fahrplans gelegt werden: Im 3. Schritt des Fahrplans ist zu prüfen, ob Rechtslage und Rechtspraxis im Drittland, die Wirksamkeit der angemessenen Garantien nach Art. 46 Abs. 2 oder 3 DSGVO bei der konkreten Datenübermittlung beeinträchtigen und falls dies der Fall sein sollte, sollte im 4. Schritt des Fahrplans geprüft werden, ob zusätzliche Maßnahmen effektiv ergriffen werden können, um ein angemessenes Datenschutzniveau sicherzustellen. Im Rahmen der Prüfung des 3. Schritts sollten zunächst die Rechtsvorschriften des betreffenden Drittlands beleuchtet werden.

Folgende Rechtsvorschriften, die gesetzliche Befugnisse für staatliche Stellen auf Zugang zu personenbezogenen Daten implizit oder explizit regeln, können für die Bewertung von Rechtslage und Rechtspraxis in folgenden Ländern berücksichtigt werden, wobei diese Aufzählung sowohl in Bezug auf die Länder als auch die Rechtsvorschriften exemplarisch und nicht abschließend ist:[56]

1. USA: Foreign Intelligence Surveillance Act (FISA), Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Executive Order 12333 (United States intelligence activities).

   Cloud-Anbieter mit Sitz in den USA unterliegen dem US-amerikanischen FISA, der es staatlichen US-Stellen in Sec. 702 FISA gestattet, auf durch US-Unternehmen („electronic communication service providers“) verarbeitete Daten von Nicht-US Bürgern, die in den USA gespeichert sind, Zugriff zu nehmen. Für diese Rechtsnorm hat der EuGH festgestellt, dass die Zugangsbefugnisse auf personenbezogene Daten nicht auf das in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maß beschränkt sind, sodass die Verwendung von geeigneten Garantien nach Art. 46 Abs. 2 oder 3 DSGVO für eine Datenübermittlung allein nicht zu einem gleichwertigen Schutzniveau in den USA führt.

   Auch der CLOUD Act ermöglicht es staatlichen US-Stellen, von US-Unternehmen den Zugang auf Daten von Nicht-US-Bürgern zu erzwingen, wenn die Unternehmen in der Lage sind, diesen Zugang zu ermöglichen, auch wenn diese auf europäischen Servern liegen. Dies ist bei einem Cloud-Anbieter der Fall, wenn dieser ein europäisches Tochterunternehmen eines US-Mutterkonzerns ist. Diese Zugriffsrechte gehen über das Maß hinaus, das in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist. Schließlich hat das dem CLOUD Act unterliegende Unternehmen bei personenbezogenen Daten von Europäern kaum effektive Möglichkeiten, die Anordnung der staatlichen US-Stelle gerichtlich überprüfen zu lassen, da diese Möglichkeit nur gegeben ist, wenn der Empfänger durch die Offenlegung zur Verletzung von Gesetzen qualifizierter ausländischer Regierungen verleitet würde. Weder Deutschland noch die EU haben ein Exekutiv-

[56] Die ausgewählten Beispiele entsprechen dem Rechtstand von September 2021 und werden nicht aktualisiert.

Abkommen mit den USA abgeschlossen, das sie zu einer solchen qualifizierten ausländischen Regierung machen würde. Ein unabhängiger Aufsichtsmechanismus als Säule der wesentlichen europäischen Garantien liegt somit nicht vor, sodass kein gleichwertiges Datenschutzniveau angenommen werden kann. Zudem steht eine solche Offenlegung in Widerspruch zu Art. 48 DSGVO, da zwischen Deutschland/der EU und den USA kein Rechtshilfeabkommen besteht und personenbezogene Daten daher nicht an die staatlichen US-Stellen gegeben werden dürfen.

Die Executive Order 12333 zielt auf die geheimdienstliche Informationsausstattung des Präsidenten, des National Security Council und des Homeland Security Council. Eine effektive Beschränkung der Maßnahmen zur Informationsgewinnung ausschließlich auf US-Bürger ist hierin nicht vorgesehen. Auch diese Regelung verhindert ein gleichwertiges Datenschutzniveau.

2. Russland: Förderales Gesetz über die Auslandsaufklärung vom 10.1.1996 Nr. 5-FZ (Федеральный закон от 10.1.1996 г. N 5-ФЗ „О внешней разведке“), Föderales Gesetz „über den Bundessicherheitsdienst“ vom 3.4.1995 Nr. 40-FZ (Федеральный закон „о федеральной службе безопасност“ от 3.4.1995 г. N 40-ФЗ), Föderales Gesetz „über operative Suchaktivitäten“ vom 12.8.1995 Nr. 144-FZ (Федеральный закон "Об оперативно-розыскной деятельности" от 12.8.1995 г. N 144-ФЗ), Förderales Gesetz „über Kommunikation“ vom 7.7.2003 Nr. 126-FZ (Федеральный закон "О связи" от 7.7.2003 г. N 126-ФЗ). Diese Regelungen ermöglichen staatlichen Stellen, Unternehmen aus Russland für nachrichtendienstliche Zwecke in Anspruch zu nehmen und sie zu zwingen, personenbezogene Daten preiszugeben.

3. China: National Intelligence Law of the People’s Republic of China vom 27.6.2017, Cryptography Law of the People’s Republic of China vom 26.10.2019, Counterterrorism Law of the People's Republic of China (Order No. 36) vom 27.12.2015. Diese Regelungen ermöglichen staatlichen Stellen, Unternehmen aus China für nachrichtendienstliche Zwecke in Anspruch zu nehmen und sie zu zwingen, personenbezogene Daten preiszugeben.

Rechtsvorschriften sollten jedoch nicht als einzige Quelle genutzt werden, da sie formal ein gleichwertiges Datenschutzniveau suggerieren können, welches in der Rechtspraxis jedoch nicht gewährleistet wird. Neben den Rechtsvorschriften selbst, sollten daher, sofern für das betreffende Drittland vorhanden, auch folgende Quellen berücksichtigt werden:

- die Rechtsprechung des EuGH wie z.B. das Schrems II-Urteil für die USA oder die Rechtsprechung des EGMR wie z.B. das Faktenblatt zur Massenüberwachung (factsheet – mass surveillance);
- Angemessenheitsbeschlüsse für das Drittland, wenn die Datenübermittlung auf einem anderen Übermittlungsinstrument beruht;
- Resolutionen und Berichte zwischenstaatlicher Organisationen wie beispielsweise des Europarats oder regionaler Organisationen wie z.B. die Länderberichte der Interamerikanischen Kommission für Menschenrechte oder Organisationen der Vereinten Nationen wie z.B. des Menschenrechtsrats oder der Menschenrechtskommission der Vereinten Nationen;
- Berichte und Analysen von zuständigen Regulierungsnetzwerken wie z.B. der Global Privacy Assembly (GPA);
- Nationale Rechtsprechung oder Entscheidungen unabhängiger Justiz- oder Verwaltungsbehörden, die für Datenschutz und den Schutz der Privatsphäre in Drittländern zuständig sind;
- Berichte unabhängiger Kontrollorgane oder parlamentarischer Gremien;
- Berichte über praktische Erfahrungen mit früheren Fällen von Offenlegungsersuchen von staatlichen Stellen oder dem Ausbleiben solcher Ersuchen von Einrichtungen, die in der gleichen Branche wie der Empfänger tätig sind;
- „Warrant Canary“-Erklärungen[57] anderer Unternehmen, die Daten in der gleichen Branche wie der Empfänger arbeiten;
- Berichte, die von Handelskammern, Wirtschafts-, Berufs- und Handelsverbänden, staatlichen diplomatischen Vertretungen, Handels- und Investitionsagenturen des Exporteurs oder anderen Drittländern, die in das Drittland, in das die Datenübermittlung erfolgen soll, exportieren, erstellt oder in Auftrag gegeben wurden;
- Berichte von akademischen Einrichtungen und Organisationen der Zivilgesellschaft (z.B. NGOs).

[57] Dabei handelt es sich um kryptografisch signierte Mitteilungen, mit denen der Datenübermittler informiert wird, dass dem Datenempfänger bis zu einem bestimmten Zeitpunkt (Datum und Uhrzeit) kein Ersuchen um Offenlegung personenbezogener Daten o. Ä. zugegangen ist. Wenn eine solche Erklärung dann ausbleibt, ist das für den Datenübermittler ein Hinweis darauf, dass dem Datenempfänger ein solches Ersuchen zugegangen sein könnte.

Die praktischen Erfahrungen des Empfängers dürfen in die Gesamtbewertung über das Datenschutzniveau des Drittlands einfließen, sie darf sich jedoch nicht ausschließlich darauf stützen. Die praktischen Erfahrungen sollten nach Möglichkeit untermauert werden, z.B. durch Erfahrungsberichte anderer Unternehmen, die in der gleichen Branche arbeiten oder z.B. durch investigative Artikel namhafter Zeitungen oder wissenschaftliche Aufsätze in Fachzeitschriften, die sich mit den spezifischen Rechtsvorschriften und der tatsächlichen Rechtspraxis befassen. Hat der Empfänger bisher keine Offenlegungsersuchen erhalten, sollte daraus nicht der Schluss gezogen werden, dass diese auch für die Zukunft ausgeschlossen sind. Alle herangezogenen Quellen zur Beurteilung von Rechtslage und Rechtspraxis müssen sorgfältig dokumentiert werden. Rechtsvorschriften sind mit vollständigem Namen der Rechtsvorschrift und den einschlägigen Paragrafen zu dokumentieren. In die Bewertung einbezogene Berichte, Urteile etc. müssen ebenfalls klar benannt werden. Insofern empfiehlt sich ein aktuell zu haltendes Fundstellenmanagement.

Bei der Beurteilung von Rechtslage und Rechtspraxis im Drittland ist es wichtig zu prüfen, ob die konkrete Datenübermittlung in den Anwendungsbereich von Gesetzen fällt, die staatlichen Stellen des Drittlandes Befugnisse zum Zugang auf personenbezogene Daten einräumen, die über das hinausgehen, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt. Für diese Bewertung können die „wesentlichen europäischen Garantien“ der „Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen“ als Bewertungsmaßstab herangezogen werden.

Die nachfolgenden Ausführungen zu den wesentlichen europäischen Garantien stellen eine verkürzte Zusammenfassung der „Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen“ dar, um dem Cloud-Anbieter eine erste Orientierung für die Bewertung der Rechtsvorschriften und Rechtspraxis im Drittland zu geben. Die vier wesentlichen europäischen Garantien sollten als Hauptvoraussetzungen verstanden werden, die nicht unabhängig voneinander, sondern in ihrer Gesamtheit geprüft werden sollten, wenn es darum geht, zu beurteilen, ob Zugangsmaßnahmen auf personenbezogene Daten von staatlichen Stellen von Drittländern auf das in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maß beschränkt sind oder nicht. Für weitere Hinweise für die Bewertung wird auf die Empfehlungen 2/2020 verwiesen.

Die vier wesentlichen europäischen Garantien sind:

1. **Klare, präzise und zugängliche Vorschriften für die Datenverarbeitung**
   Gesetzliche Vorschriften für den Zugang von staatlichen Stellen zu personenbezogenen Daten müssen klare, präzise und öffentlich zugängliche Regeln für die Anwendung der betreffenden Zugangsmaßnahmen und Mindestanforderungen an diese vorsehen. Dies beinhaltet auch, dass die Rechtsvorschrift regeln muss, unter welchen Umständen und Bedingungen eine Zugangsmaßnahme durch die staatliche Stelle angewendet werden darf und in welchem Umfang die Rechte auf Schutz der Privatsphäre und den Schutz personenbezogener Daten der betroffenen Person eingeschränkt werden dürfen. Zudem muss die gesetzliche Vorschrift Folgendes definieren: Personengruppen, die von Zugangsmaßnahmen betroffenen sein können, zeitliche Begrenzungen der Zugangsmaßnahmen, Verfahren für die Auswertung, Verwendung und Speicherung der gewonnenen Daten und zu treffende Vorsichtsmaßnahmen für die Übermittlung der Daten an andere Parteien. Weiterhin muss die gesetzliche Vorschrift rechtsverbindlich sein und den betroffenen Personen Rechte gegenüber der staatlichen Stelle verleihen, die sie gerichtlich geltend machen und durchsetzen können. Liegen keine öffentlich zugänglichen Vorschriften vor, die den Zugang von staatlichen Stellen auf personenbezogene Daten regeln oder werden den betroffenen Personen keine Rechte gegenüber der Behörde eingeräumt, kann kein gleichwertiges Schutzniveau für das Drittland angenommen werden.

2. **Nachweis der Erforderlichkeit und Angemessenheit im Hinblick auf die verfolgten legitimen Ziele**

   Nach Art. 52 Abs. 1 Satz 1 GRCh muss jede Einschränkung der in der Charta anerkannten Rechte den Wesensgehalt dieser Rechte achten, weshalb Einschränkungen durch Zugangsmaßnahmen nur vorgenommen werden dürfen, wenn sie unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich sind und sie in der EU anerkannten Zielsetzungen des Gemeinwohls dienen oder dem Schutz von Rechten und Freiheiten anderer entsprechen. Um zu beurteilen, ob eine Einschränkung verhältnismäßig ist, kommt es zum einen auf die Schwere des Eingriffs an, der mit der Einschränkung verbunden ist, und zum anderen, ob die mit der Einschränkung verfolgte Zielsetzung des Gemeinwohls der Schwere des Eingriffs angemessen ist. So ist z.B. ein Zugang durch staatliche Stellen auf den Standort eines Mobiltelefons einer betroffenen Person in Echtzeit ein schwerer Eingriff, weil er der staatlichen Stelle ermöglicht, jederzeit die Bewegungen der betroffenen Person zu verfolgen. Er könnte aber angemessen sein, wenn er etwa auf die Verhinderung unmittelbar bevorstehender, schwerwiegender Terrorismusakte oder auf die Suche nach Verletzten oder Vermissten abzielt. Die Einschränkung eines Rechts muss auf das absolut Notwendige beschränkt sein, was voraussetzt, dass für die Zugangsmaßnahmen durch gesetzliche Vorschriften präzise geregelt sein muss, wann, unter welchen Umständen und Voraussetzungen die Zugangsmaßnahmen eingesetzt werden dürfen und welche Mindesterfordernisse die staatliche Stelle hierbei einhalten muss. Gesetzliche Vorschriften, die Eingriffe i.S.v. Zugangsmaßnahmen auf personenbezogene Daten durch staatliche Stellen erlauben, ohne hierfür Einschränkungen vorzusehen, genügen den Anforderungen an ein gleichwertiges Datenschutzniveau nicht, da jede gesetzliche Vorschrift für einen Eingriff den Umfang der Einschränkung der jeweiligen Rechte definieren muss. Weiterhin ist der Grundsatz der Erforderlichkeit nicht eingehalten, wenn gesetzliche Vorschriften für Zugangsmaßnahmen den Wesensgehalt von Rechten missachten. Dies ist z.B. für Art. 7 GRCh der Fall, wenn staatliche Stellen durch gesetzliche Vorschriften befugt

sind, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, ohne dass der Eingriff beschränkt wird, die mit dem Eingriff verfolgten Ziele benannt sind und objektive Kriterien für den Einsatz der Zugangsmaßnahme definiert werden.

3. Unabhängiger Aufsichtsmechanismus

Weiterhin muss im Drittland für jeden Eingriff in die Rechte auf Schutz der Privatsphäre und den Schutz personenbezogener Daten eine wirksame, unabhängige und unparteiische Aufsicht durch einen Richter oder eine andere unabhängige Stelle etabliert sein. Der Aufsichtsmechanismus muss einerseits sicherstellen, dass manche Zugangsmaßnahmen durch staatliche Stellen von der vorherigen Genehmigung eines Richters oder einer unabhängigen Stelle abhängig gemacht werden und diese Genehmigung oder Ablehnung bindend ist. Andererseits muss der Aufsichtsmechanismus über alle Befugnisse verfügen, um Kontrollen wirksam durchführen und etwaiges missbräuchliches Handeln durch staatliche Stellen feststellen zu können. Dies erfordert etwa Zugang zu sämtlichen relevanten Schriftstücken u.a. auch zu Verschlusssachen. Die Unabhängigkeit des Aufsichtsmechanismus setzt zudem voraus, dass er über eine hinreichende Unabhängigkeit von der Exekutive verfügt. Ebenso wichtig ist aber auch, dass die Tätigkeit der die Aufsicht ausübenden Stelle selbst einer öffentlichen Kontrolle unterliegt, d.h. dass auch ihr Ergebnis entsprechend unabhängig und unparteiisch überprüfbar ist.

4. Wirksame Rechtsbehelfe

Nach Art. 47 Abs. 1 GRCh hat jede Person, die der Ansicht ist, dass ihre durch EU-Recht garantierten Rechte oder Freiheiten verletzt worden sind, das Recht, bei einem Gericht einen wirksamen Rechtsbehelf einzulegen. Dies erfordert etwa bei Eingriffen, die im Verborgenen in die Rechte auf Schutz der Privatsphäre und den Schutz personenbezogener Daten stattfinden, auch die nachträgliche Benachrichtigung der betroffenen Person hierüber. Eine gleichwertige Garantie muss auch im Drittland gegeben sein, was bedeutet, dass die betroffene Person im Drittland die Möglichkeit haben muss, Rechtsbehelfe vor einem unabhängigen und unparteiischen Gericht oder Organ einzulegen, um Zugang zu den sie betreffenden personenbezogenen Daten oder ihre Berichtigung oder Löschung zu erwirken. Das Gericht oder Organ muss insbesondere gegenüber der Exekutive unabhängig sein und ermächtigt sein, verbindliche Entscheidungen gegen die betreffenden staatlichen Stellen zu treffen.

Führt die Beurteilung von Rechtslage und Rechtspraxis im Drittland zum Ergebnis, dass die Instrumente aus Art. 46 Abs. 2 und 3 DSGVO nicht ausreichend sind, um ein angemessenes Datenschutzniveau sicherzustellen, darf die Datenübermittlung nicht ohne zusätzliche Maßnahmen stattfinden.

Gemäß Artikel 28 Abs. 3 lit. a DSGVO muss der für die Verarbeitung Verantwortliche von dem Auftragsverarbeiter die Beurteilung erhalten, die er im Hinblick auf die Rechtsvorschriften und Praxis des Drittlandes vorgenommen hat, um zu prüfen, ob die von dem Auftragsverarbeiter getroffenen zusätzlichen Maßnahmen tatsächlich ein angemessenes Schutzniveau hinsichtlich der in das Drittland übermittelten personenbezogenen Daten gewährleisten. Es versteht sich von selbst, dass der Auftragsverarbeiter bei Datenübermittlungen nach wie vor an die Weisungen des für die Verarbeitung Verantwortlichen gebunden ist, wie sie in der rechtsverbindlichen Auftragsdatenverarbeitungsvereinbarung festgelegt sind (siehe Kriterium Nr. 1.4(1)), weshalb eine Übermittlung nur auf Weisung des für die Verarbeitung Verantwortlichen erfolgen kann.

Soll die Datenübermittlung dennoch stattfinden, sollte der Cloud-Anbieter, ggf. mit dem Empfänger zusammen im 4. Schritt des Fahrplans prüfen, ob durch zusätzliche Maßnahmen ein angemessenes Datenschutzniveau im Drittland sichergestellt werden kann. Grundsätzlich können zusätzliche Maßnahmen vertraglicher, organisatorischer oder technischer Art sein. Um ein gleichwertiges Schutzniveau im Drittland zu erreichen, kann eine Kombination mehrerer Maßnahmen sinnvoll sein.

Sinnvoll ist z.B. eine vertragliche Zusicherung durch den Empfänger, dass er nicht absichtlich Hintertüren, sonstige technischen Möglichkeiten oder Geschäftsprozesse etabliert hat, die staatlichen Stellen Zugang zum Cloud-Dienst und zu personenbezogenen Daten verschaffen oder diesen erleichtern und dass er nach dem nationalen Recht des Drittlands auch nicht verpflichtet ist, Hintertüren im Cloud-Dienst zu etablieren, staatlichen Stellen Zugang zum Cloud-Dienst oder zu personenbezogenen Daten zu verschaffen und Verschlüsselungsschlüssel zu besitzen oder herauszugeben. Sinnvoll ist es auch, den Empfänger zu verpflichten, den Exporteur umgehend zu informieren, wenn Änderungen im nationalen Recht oder in der Rechtspraxis dazu führen, dass die genannten Zusicherungen nicht mehr eingehalten werden können, sodass der Exporteur den Vertrag kurzfristig kündigen und die Datenübermittlung beenden kann. Zu beachten ist jedoch, dass solche Zusicherungen des Empfängers nach dem nationalen Recht des Drittlands untersagt sein können.

Unterliegt ein Empfänger nationalen Gesetzen wie FISA, CLOUD Act oder ähnlichen Gesetzen anderer Drittländer, werden vertragliche und organisatorische Maßnahmen allein i.d.R. nicht ausreichen, um einen Zugang auf personenbezogene Daten durch staatliche Stellen des Drittlands zu verhindern, sodass technische Maßnahmen ergriffen werden sollten.

Die folgenden drei Use Cases sollen eine Hilfestellung bieten, wann zusätzliche technische Maßnahmen zu einem gleichwertigen Datenschutzniveau beitragen können und wann nicht:

1. Use Case: Datenspeicherung im Cloud-Dienst z.B. für Backup-Zwecke, bei der der Empfänger keinen Zugriff auf die personenbezogenen Daten im Klartext benötigt. Die Verschlüsselung vor der Datenübermittlung stellt eine wirksame zusätzliche technische Maßnahme dar, wenn

   a. eine starke Verschlüsselung gewählt wird und die Identität des Empfängers geprüft wird;

   b. der Verschlüsselungsalgorithmus und seine Parametrisierung (z.B. Schlüssellänge, Betriebsart) dem Stand der Technik entsprechen und – unter Berücksichtigung der zur Verfügung stehenden Ressourcen und technischen Möglichkeiten (z. B. Rechenleistung für Brute-Force-Angriffe) – Robustheit gegen die von den Behörden im Drittland durchgeführte Kryptoanalyse bieten;

   c. die Verschlüsselungsstärke den Zeitraum berücksichtigt, für den die Vertraulichkeit der verschlüsselten personenbezogenen Daten sicherzustellen ist;

   d. der Verschlüsselungsalgorithmus fehlerfrei durch ordnungsgemäß gepflegte Software implementiert ist, deren Konformität mit der Spezifikation des ausgewählten Algorithmus bestätigt wurde;

   e. die Schlüssel beim Exporteur zuverlässig verwaltet (erzeugt, angewandt, gespeichert, falls relevant, mit der Identität des vorgesehenen Empfängers verknüpft sowie widerrufen) werden und

   f. die Kontrolle über die Schlüssel allein beim Exporteur oder bei anderen mit dieser Aufgabe betrauten Stellen im EWR oder in einem Drittland mit Angemessenheitsbeschluss liegt.

   Die Anf. CRY-01, CRY-03 und CRY-04 des BSI C5 enthalten Richtlinien zur Nutzung von Verschlüsselungsverfahren und zur sicheren Schlüsselverwaltung, die bei der Umsetzung der verwendeten Verschlüsselung befolgt werden sollten. Auch ISO/IEC 11770-2 enthält weitere Informationen zur Schlüsselverwaltung. Weiterhin bieten die Technischen Reporte des BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“; BSI TR-02102-3 „Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPSec) und Internet Key Exchange (IKEv2)“; und BSI TR-02102-4 „Kryptographische Verfahren: Verwendung von Secure Shell (SSH)“ weitere hilfreiche Hinweise für die Verschlüsselung, sodass auf diese hingewiesen wird.

   Zum Stand der Technik bei Verschlüsselungsverfahren und anderen TOM kann auch die „Handreichung zum Stand der Technik“ von TeleTrust in der aktuellen Fassung verwiesen werden.

2. Use Case: Verarbeitung pseudonymisierter Daten durch den Empfänger. Die Pseudonymisierung der Daten durch den Exporteur vor der Datenübermittlung an den Empfänger stellt eine wirksame zusätzliche technische Maßnahme dar, wenn

   a. der Exporteur die personenbezogenen Daten in solcher Weise übermittelt, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen weder einer spezifischen betroffenen Person zugeordnet noch dazu verwendet werden können, die betroffene Person in einer größeren Gruppe zu identifizieren;

   b. die zusätzlichen Informationen allein vom Exporteur vorgehalten werden, und zwar separat in einem Mitgliedstaat oder in einem Drittland, bei einer vom Exporteur betrauten Stelle im EWR oder in einer Rechtsordnung, die ein dem EWR im Wesentlichen gleichwertiges Schutzniveau bietet.

   c. die Offenlegung oder die unerlaubte Verwendung der zusätzlichen Informationen durch geeignete technische und organisatorische Garantien verhindert wird und sichergestellt ist, dass die Kontrolle über den Algorithmus oder den Datenspeicher, der die Re-Identifizierung anhand der zusätzlichen Informationen ermöglicht, allein beim Exporteur liegt, und

   d. der Verantwortliche durch gründliche Analyse der betreffenden Daten, unter Berücksichtigung sämtlicher Informationen, die den staatlichen Stellen im Empfängerland erwartungsgemäß zur Verfügung stehen, festgestellt hat, dass die pseudonymisierten personenbezogenen Daten keiner identifizierten oder identifizierbaren natürlichen Person zugeordnet werden können, selbst wenn sie mit derartigen Informationen abgeglichen werden.

      Weiterhin sollten die Ausführungen in den Randnummern 86 bis 89 der Empfehlungen 01/2020 beachtet werden.

      Hinweise zur rechtssicheren Umsetzung von Pseudonymisierungsverfahren können dem Arbeitspapier „Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen“ von Schwartmann/Weiß entnommen werden, auf das hiermit verwiesen wird.

3. Use Case: Datenübermittlung an einen Cloud-Dienst, der aufgrund der Art der Auftragsverarbeitung Zugang zu unverschlüsselten Daten benötigt: Findet auf den Empfänger das Recht eines Drittlands Anwendung, das staatlichen Stellen Zugang zu personenbezogenen Daten gewährt, das über das Maß hinausgeht, was in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, reichen technische

Maßnahmen wie Transportverschlüsselung während der Übermittlung und die Verschlüsselung von personenbezogenen Daten im Ruhezustand nicht aus, um die Rechte der betroffenen Personen zu schützen. Auch die Kombination der genannten technischen Maßnahmen mit zusätzlichen vertraglichen Maßnahmen wie z.B. die vertraglich zugesicherte Pflicht des Importeurs zugegangene Offenlegungsersuchen von staatlichen Stellen anzufechten und den nationalen Rechtsweg gegen ein Offenlegungsersuchen zu bestreiten oder die vertragliche Pflicht den Exporteur über eingegangene Offenlegungsersuchen vor der Datenübermittlung an die staatliche Stelle zu informieren, reichen nicht aus, um eine Datenübermittlung in das betreffende Drittland zu legitimieren. **Im 3. Use Case sollte die Datenübermittlung daher unterlassen werden**.

Eine nicht abschließende Aufzählung denkbarer zusätzlicher vertraglicher, organisatorischer oder technischer Maßnahmen sowie eine Auflistung weiterer Use Cases ist in Anhang 2 der Empfehlungen 01/2020 enthalten, auf die hiermit verwiesen wird.

Cloud-Anbieter, die auch dem Recht von Drittländern unterliegen, müssen gemäß Art. 48 DSGVO, die Herausgabeverlangen von staatlichen Stellen von Drittländern bezüglich personenbezogener Daten aus der EU und dem EWR ablehnen und auf in Kraft befindliche internationale Übereinkünfte wie z.B. Rechtshilfeabkommen verweisen, soweit diese mit dem betreffenden Drittland bestehen.

Wenn der Cloud-Anbieter personenbezogene Daten verarbeitet und nicht nur dem Recht der Datenschutz-Grundverordnung unterliegt, sondern zugleich dem Recht eines Drittlands, das ihn zu einer Offenlegung dieser personenbezogenen Daten gegenüber staatlichen Stellen des betreffenden Drittlands verpflichtet, sind zum Schutz der europäischen Grundrechte und Grundfreiheiten der betroffenen Personen zusätzliche Maßnahmen zu ergreifen, um die personenbezogenen Daten vor einer Offenlegung gegenüber den staatlichen Stellen des Drittlands zu schützen. **Eine denkbare Lösung ist z.B. ein Treuhandmodell, bei dem die Daten im Besitz und in der Herrschaft eines Unternehmens verbleiben, das ausschließlich europäische, Recht unterliegt**. Hierfür wird auch auf die Erläuterung in Kriterium Nr. 1.5 verwiesen. Bezüglich anderer denkbarer zusätzlicher Maßnahmen, die zum Schutz der europäischen Grundrechte und Grundfreiheiten ergriffen werden müssen, können in manchen Fällen auch die zusätzlichen Maßnahmen aus Anhang 2 der Empfehlungen 01/2020 des Europäischen Datenschutzausschusses hilfreich sein, weshalb auf diesen verwiesen wird. Auch hier sollte beachtet werden, dass zusätzliche vertragliche oder organisatorische Maßnahmen im Regelfall nicht ausreichen werden, um die personenbezogenen Daten vor einer Offenlegung gegenüber staatlichen Stellen von Drittländern zu schützen, sodass sie mit technischen Maßnahmen kombiniert werden sollten.

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er ein Verzeichnis eingesetzter Subauftragsverarbeiter aus Drittländern mit Angemessenheitsbeschluss nach Art. 45 Abs. 3 DSGVO vorlegt.

Liegt kein Angemessenheitsbeschluss vor, können Nachweise durch Dokumente zu den vereinbarten geeigneten Garantien nach Art. 46 Abs. 2 oder 3 DSGVO vorgelegt werden (z.B. Standarddatenschutzklauseln, verbindliche interne Datenschutzvorschriften nach Art. 47 DSGVO).

Zusätzlich müssen in diesem Fall Dokumentationen des Cloud-Anbieters zur Beurteilung von Rechtslage und Praxis im betreffenden Drittland anhand des sechsschrittigen Fahrplans vorgelegt werden. Aus der Dokumentation des 3. Schritts des Fahrplans hat hervorzugehen, welche Quellen der Cloud-Anbieter genutzt hat, um Rechtslage und Praxis im Drittland zu beurteilen. Zunächst muss der Cloud-Anbieter offenlegen, mit welchen konkreten Rechtsvorschriften des Drittlands er sich für die Prüfung von Rechtslage und Rechtspraxis im Drittland auseinandergesetzt hat. Die Dokumentationen des Cloud-Anbieters haben nicht nur die Auseinandersetzung mit Rechtsvorschriften zu enthalten, sondern auch weitere Quellen einzubeziehen, soweit vorhanden, wie z.B. relevante Gerichtsentscheidungen des EuGH, Stellungnahmen und Berichte zwischenstaatlicher Organisationen, nationale Rechtsprechung oder Entscheidungen unabhängiger Justiz- oder Verwaltungsbehörden mit Zuständigkeit für den Schutz der Privatsphäre und den Datenschutz in Drittländern, Berichte von Forschungseinrichtungen und zivilgesellschaftlichen Organisationen etc. In die Dokumentation zur Rechtspraxis im Drittland kann der Cloud-Anbieter auch Statistiken des Empfängers oder seiner Partner zum Zugang staatlicher Stellen auf personenbezogene Daten sowie allgemein zugängliche Quellen wie Artikel namhafter Zeitungen aufnehmen, die sich mit der Anwendung der betreffenden Rechtsvorschriften durch die staatlichen Stellen befassen. Aus den Dokumentationen des Cloud-Anbieters muss hervorgehen, warum er zur Überzeugung gelangt ist, dass das für die Datenübermittlung genutzte Instrument nach Art. 46 Abs. 2 oder 3 DSGVO hinreichend ist, um ein angemessenes Datenschutzniveau sicherzustellen. Wichtig ist auch, dass aus den vorgelegten Dokumentationen hervorgeht, wie im betreffenden Drittland die vier wesentlichen europäischen Garantien eingehalten werden. Daher haben detaillierte Ausführungen zu diesen einzelnen Garantien sowie ihrem Zusammenwirken vorgenommen zu werden. Weiterhin soll im Rahmen eines Audits eine Befragung von Mitarbeitern erfolgen, die mit der Bewertung von Rechtslage und Rechtspraxis im Drittland betraut sind, um herauszufinden, wie Informationen über das Drittland beschafft werden und wie Rechtsvorschriften und Rechtspraxis hinsichtlich der Einhaltung der wesentlichen europäischen Garantien analysiert und bewertet werden.

Sind zusätzliche Maßnahmen nötig, um ein angemessenes Datenschutzniveau im Drittland sicherzustellen, legt der Cloud-Anbieter Dokumentationen über die zusätzlichen Maßnahmen vor, die nach dem 4. Schritt des Fahrplans ergriffen worden sind. Werden z.B. Pseudonymisierung oder Verschlüsselung eingesetzt, legt er Dokumentationen

zu den jeweiligen Verfahren vor, aus denen auch hervorgeht, dass Verfahren nach dem Stand der Technik eingesetzt werden und die Verschlüsselung oder Pseudonymisierung vor der Übermittlung an den Empfänger durchgeführt wird. Weiterhin muss bei der Verschlüsselung nachgewiesen werden, dass die Schlüssel ordnungsgemäß verwaltet werden und beim Exporteur verbleiben. Technische Maßnahmen müssen auch durch technische Tests oder Inspektionen nachgewiesen werden. Zusätzliche vertragliche Maßnahmen müssen durch die Vorlage von entsprechenden Verträgen mit den Empfängern nachgewiesen werden. Werden im Vertrag zusätzliche organisatorische Maßnahmen zugesichert, können diese je nach Art der organisatorischen Maßnahme z.B. durch die Vorlage von erhaltenen Transparenzberichten oder „Warrant Canary"-Erklärungen des Empfängers nachgewiesen werden.

Der Cloud-Anbieter kann weitere Dokumente zu Maßnahmen vorlegen, die genutzt werden, um die Angemessenheit des Datenschutzniveaus im Drittland regelmäßig zu überprüfen, z.B. proaktive Abfragen bei Empfängern nach Rechtsänderungen im betreffenden Drittland, Bearbeitung der regelmäßigen Meldungen, die der Empfänger aufgrund vertraglicher Pflichten zu geänderten Rechtsvorschriften oder Anfragen von staatlichen Stellen an den Cloud-Anbieter macht. Weiterhin sollten Dokumentationen zu Maßnahmen, Verfahren und Zuständigkeiten vorgelegt werden, die vom Cloud-Anbieter ergriffen werden, wenn das Datenschutzniveau im Drittland nicht mehr angemessen ist und die Datenübermittlung daher eingestellt wird. Auch hier kann eine Befragung im Rahmen eines Audits mit den zuständigen Mitarbeitern, z.B. im Hinblick auf die Kenntnis des relevanten Vorgehens in diesem Fall, als Nachweis angebracht werden.

Eine aktuell gültige Zertifizierung nach Art. 42 Abs. 2 DSGVO, die bereits für Datenverarbeitungsvorgänge des zu zertifizierenden Zertifizierungsgegenstands erlangt worden ist, kann ebenfalls als Nachweis dienen. In diesem Fall sind auch die eingegangene Verpflichtungen zur Anwendung der geeigneten Garantien offenzulegen und müssen überprüft werden.

Wenn der Cloud-Anbieter personenbezogene Daten verarbeitet und nicht nur dem Recht der Datenschutz-Grundverordnung unterliegt, sondern zugleich dem Recht eines Drittlands , das ihn zu einer Offenlegung dieser personenbezogenen Daten gegenüber staatlichen Stellen des betreffenden Drittlands verpflichtet, hat er Dokumente über die zusätzlichen Maßnahmen vorzulegen, die er ergriffen hat, um die personenbezogenen Daten vor einer Offenlegung gegenüber den staatlichen Stellen des Drittlands wirksam zu schützen. Verpflichtet sich der Cloud-Anbieter z.B. vertraglich gegenüber dem Cloud-Nutzer dazu, absichtlich keine Hintertüren oder Ähnliches im Cloud-Dienst implementiert zu haben, die es den staatlichen Stellen des Drittlands erlauben, auf die auf die personenbezogenen Daten zuzugreifen, dies auch nicht zu beabsichtigen, und auch nach dem Recht des Drittlands nicht hierzu verpflichtet zu sein, legt er die entsprechenden Klauseln des Vertrags offen. Werden als technische Maßnahmen z.B. Pseudonymisierung oder Verschlüsselung eingesetzt, legt der Cloud-Anbieter Dokumentationen zu den jeweiligen Verfahren vorl, aus denen auch hervorgeht, dass Verfahren nach dem Stand der Technik eingesetzt werden. Technische Maßnahmen sind auch durch technische Tests oder Inspektionen nachzuweisen. Weiterhin sind Dokumentationen zum Vorgehen und zu Zuständigkeiten für den Fall, in dem der Cloud-Anbieter zur Offenlegung von personenbezogenen Daten an staatliche Stellen von Drittländern verpflichtet wird, vorzulegen. Eine Befragung im Rahmen eines Audits mit den zuständigen Mitarbeitern, z.B. im Hinblick auf die Kenntnis des festgelegten Vorgehens, kann als Nachweis dienen.

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

Kriterium

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

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

Umsetzungshinweis

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

Nachweis

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

D. Kriterien und Umsetzungshinweise für Verarbeitung als Verantwortlicher

Kapitel VII: Der Cloud-Anbieter als Verantwortlicher

Erläuterung

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

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

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

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

Kriterium

(1) Der Cloud-Anbieter stellt bei der Verarbeitung von personenbezogenen Daten, die für die Durchführung des Auftrags über die Erbringung des Cloud-Dienstes oder zur Erfüllung rechtlicher Verpflichtungen erforderlich sind, der betroffenen Person alle Informationen zur Verfügung, die diese benötigt, um die Rechtmäßigkeit der Verarbeitung überprüfen zu können (Grundsatz der Transparenz und Rechtmäßigkeit). Der Cloud-Anbieter darf die Daten der betroffenen Person nur nach Treu und Glauben verarbeiten (Grundsatz von Treu und Glauben[58]).

(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

[58] "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.

Umsetzungshinweis

Der Transparenzgrundsatz wird erfüllt, wenn der Cloud-Anbieter seinen Informations- und Auskunftspflichten über die Datenverarbeitung (Nr. 15.1, Nr. 15.3, Nr. 15.3) nachkommt. Außerdem können die Grundsätze der Transparenz und der Datenminimierung durch datenschutzgerechte Systemgestaltung und datenschutzfreundliche Voreinstellungen (Nr. 19.1 und Nr. 19.2) erreicht werden. Der Cloud-Anbieter sollte bei der Datenverarbeitung zur Diensterbringung Überlegungen und Entscheidungen hinsichtlich der hierfür erforderlichen Daten vornehmen und dokumentieren.

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

Zur Einhaltung der Speicherbegrenzung sollte der Cloud-Anbieter für alle Daten oder Datenkategorien Speicherfristen festlegen, die auf das erforderliche Mindestmaß beschränkt sind. Zudem sollten Fristen bestimmt werden, wann personenbezogene Daten gelöscht werden oder der Personenbezug beseitigt wird. Müssen Daten aufgrund gesetzlicher Vorschriften aufbewahrt werden, sollten sie pseudonym aufbewahrt werden und der Personenbezug erst bei Bedarf wiederhergestellt werden. Auf die Umsetzungshinweise unter Nr. 8.4 zur Datenlöschung wird hingewiesen.

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

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

Auf die Umsetzungshinweise im SDM-Baustein 11 „Aufbewahren“, -Baustein 41 „Planen und Spezifizieren“ und -Baustein 50 „Trennen“ wird hingewiesen.

Nachweis

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

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

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

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

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

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

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

Kriterium

(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[59] 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.

(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.

[59] 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.

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.

Umsetzungshinweis

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

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

Auf die Umsetzungshinweise im SDM-Baustein 41 „Planen und Spezifizieren“ wird hingewiesen.

Nachweis

Der Cloud-Anbieter legt die erteilten Anweisungen an Mitarbeiter vor, anhand derer das Vorhandensein einer ausreichenden Rechtsgrundlage zu prüfen ist und aus denen die Zuständigkeiten für die Prüfungen hervorgehen.

Der Cloud-Anbieter kann im Rahmen der Zertifizierung alle oder eine repräsentative Stichprobe von rechtsverbindlichen Vereinbarungen vorlegen, die er mit den Cloud-Nutzern über die Bereitstellung eines Cloud-Dienstes geschlossen hat. Der Cloud-Anbieter legt im Rahmen der Zertifizierung eine Übersicht vor, aus der hervorgeht, welchen rechtlichen Verpflichtungen er zur Datenverarbeitung unterliegt.

Der Cloud-Anbieter legt die Dokumentation des Prozesses zur Durchführung einer Interessenabwägung vor. Ebenso kann er Dokumentationen bereits erfolgter Interessenabwägungen vorlegen. Ebenso können im Rahmen eines Audits Befragungen mit Mitarbeitern zur Kenntnis des Prozesses der Interessenabwägung durchgeführt werden.

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.

Umsetzungshinweis

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

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

Nachweis

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

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

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter sichert Räume und Anlagen gegen Schädigung durch höhere Gewalt[60] 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

(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.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 2.2 sind anwendbar.

Nachweis

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

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

Kriterium

Schutzklasse 1

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

[60] 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.

(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.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 2.3 sind anwendbar.

Nachweis

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

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

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter stellt durch TOM sicher, dass Berechtigte nur im Rahmen ihrer Berechtigungen auf personenbezogene Daten zugreifen können und schließt unbefugte Einwirkungen auf 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.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 2.4 sind anwendbar.

Nachweis

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

Nr. 14.5 – 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.

Umsetzungshinweis

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

Nachweis

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

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

Kriterium

Schutzklasse 1

(1) Der Cloud-Anbieter protokolliert Eingaben, Veränderungen und Löschungen an Daten, die zur Durchführung des Auftrags über die Erbringung des Cloud-Dienstes und zur Erfüllung rechtlicher Verpflichtungen erforderlich sind, um eine nachträgliche Prüfbarkeit und Nachvollziehbarkeit der Datenverarbeitung sicherzustellen. 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.

Umsetzungshinweis

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

Nachweis

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

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

Kriterium

Schutzklasse 1,2 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[61] (wie in den Umsetzungshinweisen beschrieben).

(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.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 2.9 sind anwendbar.

Nachweis

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

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

Kriterium

Schutzklasse 1

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

(2) 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.

[61] 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.

Umsetzungshinweis

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

Nachweis

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

Nr. 15 – Wahrung von Betroffenenrechten

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).

Umsetzungshinweis

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

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

Auf die Umsetzungshinweise im SDM-Baustein 41 „Planen und Spezifizieren“ wird hingewiesen.

Nachweis

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

pflicht gegenüber anderen betroffenen Personen wie z.B. den Mitarbeitern des Cloud-Nutzers legt der Cloud-Anbieter ebenfalls das Muster seiner Datenschutzerklärung vor, dass er dem Mitarbeiter z.B. über E-Mail bei Erhebung der Daten übermittelt.

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

Kriterium

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

Erläuterung

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

Umsetzungshinweis

Der Cloud-Anbieter sollte die Zuweisung von Verantwortlichkeiten und Meldewege sicherstellen und diese dokumentieren, damit die betroffene Person fristgemäß informiert werden kann. Die Angemessenheit der Frist zur Informationserteilung bemisst sich nach den spezifischen Verarbeitungsumständen. Gemäß Art. 14 Abs. 3 lit a. DSGVO beträgt die Frist längstens einen Monat nach Erlangung der personenbezogenen Daten. Es gelten kürzere Fristen, wenn die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet oder anderen Empfängern offengelegt werden sollen. Im ersten Fall verpflichtet Art. 14 Abs. 3 lit. b DSGVO den Cloud-Anbieter dazu, seiner Informationspflicht spätestens bei der ersten Mitteilung an die betroffene Person nachzukommen. Im zweiten Fall kann gemäß Art. 14 Abs. 3 lit. c DSGVO die Information spätestens zum Zeitpunkt der ersten Offenlegung der Daten an den Empfänger erfolgen.

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

Nachweis

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

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

Kriterium

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

Erläuterung

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

Umsetzungshinweise

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

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

Nachweis

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

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

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

Kriterium

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

Erläuterung

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

Umsetzungshinweise

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

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

Auf die Umsetzungshinweise im SDM-Baustein 61 „Berichtigen“ wird hingewiesen.

Nachweis

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

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

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

Kriterium

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

Umsetzungshinweis

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

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

Die Umsetzungshinweise unter Nr. 6.4 sind anwendbar.

Nachweis

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

Die Möglichkeiten zum Nachweis unter Nr. 6.4 sind anwendbar.

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

Kriterium

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

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

Erläuterung

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

Umsetzungshinweis

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

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

Auf die Umsetzungshinweise im SDM-Baustein 62 „Einschränken der Verarbeitung“ wird hingewiesen.

Nachweis

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

Im Rahmen einer Prüfung können testweise Einschränkungen (inkl. Mitteilung an die betroffene Person) und die Aufhebungen dieser durchgeführt werden. Die Einschränkung kann bspw. durch eine technische Funktion innerhalb

des Cloud-Dienstes oder durch manuelle Anfragen beim Cloud-Dienst-Support erfolgen. Im Rahmen eines Audits kann auch anhand von Befragungen (z.B. zur Kenntnis über Verfahrensschritte etc.) und Beobachtungen nachgewiesen werden, wie Einschränkungen und ihre Aufhebungen durchgeführt werden und wie die betroffene Person benachrichtigt wird.

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

Kriterium

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

Erläuterung

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

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

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

Nachweis

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

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

Nr. 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.

Umsetzungshinweis

Der Cloud-Anbieter sollte möglichst präzise, verständlich und klar formulieren, welche Maßnahmen er ergriffen hat, um dem Antrag der betroffenen Person zu entsprechen oder nicht zu entsprechen. Gerade wenn der Antrag einer betroffenen Person teilweise oder vollständig abgelehnt wurde, sollte eine möglichst detaillierte Begründung hierfür erfolgen, damit die betroffene Person beurteilen kann, ob sie ggf. Maßnahmen gegen den Cloud-Anbieter (z.B. eine Beschwerde bei der Aufsichtsbehörde) ergreifen möchte.

Auch sollte möglichst präzise, verständlich und klar formuliert werden, warum für die Antragsbearbeitung eine längere Frist benötigt wird und diese Frist genau benannt werden. Dasselbe gilt für die Benennung der Gründe bei Untätigkeit.

Nachweis

Anhand von Prozessdokumentationen und Protokollen kann nachgewiesen werden, ob die tatsächlich durchgeführten Informationserteilungen an die betroffenen Personen durchgeführt wurden und vollständig sind.

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[62] 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.

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

(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 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).

Umsetzungshinweis

Der Cloud-Anbieter sollte seine Risikobewertung, ob eine Verletzung des Schutzes personenbezogener Daten als „wahrscheinlich zu einem Risiko für die Rechte und Freiheiten des Cloud-Nutzers führend“ anzusehen ist, dokumentieren, einschließlich der gemäß (3) bewerteten Bedingung und der Bewertungsergebnisse.

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

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

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

Für die Meldung von Datenschutzverletzungen an die Aufsichtsbehörde können die aufsichtsbehördlichen Meldeformulare genutzt werden.

Nachweis

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

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

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

Nr. 17 – Benachrichtigung der betroffenen Person bei Datenschutzverletzungen (Art. 34 Abs. 1 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.

Umsetzungshinweise

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

Nachweis

Der Cloud-Anbieter kann das Datensicherheitskonzept und die darin beschriebenen TOM zur Meldung von Datenschutzverletzungen sowie weitere Dokumentationen als Nachweise vorlegen, darunter bspw. die Prozessdokumentation mit den Verfahrensschritten und Fristen zur Benachrichtigung der betroffenen Personen über Datenschutzverletzungen, Richtlinien, Muster und Vorlagen zur Benachrichtigung der betroffenen Person, Entscheidungsregeln zur Beurteilung von Datenschutzverletzungen, Verfahren zur Risikoanalyse und zu den Faktoren, die bei der Risikoanalyse einbezogen werden, inklusive der Meldewege und der Zuständigkeiten. Ergänzend können im Rahmen eines Audits Befragungen von Mitarbeitern durchgeführt werden, um nachzuweisen, dass das festgelegte Verfahren zur Benachrichtigung betroffener Personen bekannt ist und im Unternehmen gelebt wird.

Sofern vorhanden, kann der Cloud-Anbieter ebenfalls bereits erfolgte Benachrichtigungen über Datenschutzverletzungen an betroffene Personen vorlegen.

Die Benachrichtigung der betroffenen Person über die Datenschutzverletzung darf nur unterbleiben, wenn eine der Bedingungen des Art. 34 Abs. 3 DSGVO vorliegt. Hier sollte der Cloud-Anbieter insbesondere Dokumentationen, z.B. im Datensicherheitskonzept vorlegen, aus denen die TOM hervorgehen, die er ergriffen hat, um zu gewährleisten, dass künftig keine hohen Risiken für die Rechte und Freiheiten der betroffenen Person mehr bestehen. Aus der Dokumentation sollte ebenfalls hervorgehen, welche Risiken durch die Maßnahmen adressiert werden. Die TOM können auch einer Inspektion unterzogen werden. Falls keine individuelle Benachrichtigung der betroffenen Personen erfolgt ist, können Dokumentation der erfolgten öffentlichen Bekanntmachung, z.B. in einer Tageszeitung vorgelegt werden sowie die Darlegung, dass ein unverhältnismäßiger Aufwand bestanden hat.

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.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 8.3 sind anwendbar.

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

Nachweis

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

Nr. 19 – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

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

Kriterium

Der Cloud-Anbieter 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.

Umsetzungshinweise

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

Nachweis

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

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

Kriterium

(1) Der Cloud-Anbieter stellt durch Voreinstellungen sicher, dass er bei der Inbetriebnahme und Nutzung des Cloud-Dienstes nur personenbezogene Daten verarbeitet, die erforderlich sind, um den Cloud-Dienst erbringen zu können 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[63] 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[64] für die betroffene Person durch das Zugänglichmachen in einem zu großen Umfang[65] zu den verfügbaren personenbezogenen Daten entstehen.

Umsetzungshinweise

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

Nachweise

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

[63] 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“).
[64] 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.
[65] 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.

Umsetzungshinweis

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

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

Nachweis

Der Cloud-Anbieter legt die rechtsverbindliche(n) Vereinbarung(en) zur Auftragsverarbeitung mit den entsprechenden Festlegungen vor, die er mit dem/den Auftragsverarbeiter(n) abgeschlossen hat. Für die jeweiligen Subauftragsverarbeiter sollten Dokumente wie das Datensicherheitskonzept mit den TOM oder Zertifikate nachgewiesen werden. Weitere relevante Dokumente können als Nachweis einbezogen werden, darunter der Mustervertrag zur Auftragsverarbeitung mit Subauftragsverarbeitern, Richtlinien und Anweisungen, weitere Garantien der Subauftragsverarbeiter, interne Kontrollbereiche des Cloud-Anbieters über Subauftragsverarbeiterkontrollen, das Datenschutzkonzept oder die Risikoabschätzung bei der Unterbeauftragung.

Nr. 20.2 – Sicherstellung ordnungsgemäßer Auftragsverarbeitung

Kriterium

(1) Der Cloud-Anbieter stellt sicher, dass der Auftragsverarbeiter personenbezogene Daten nur auf seine dokumentierte Weisung hin verarbeitet (Art. 28 Abs. 3 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.

Umsetzungshinweis

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

Nachweis

Der Cloud-Anbieter kann den Nachweis erbringen, indem er Dokumentationen, Prüfungsergebnisse oder ähnliche Nachweise des Auftragsverarbeiters vorlegt, die ihn überzeugt haben anzunehmen, dass der Auftragsverarbeiter allen für ihn geltenden Pflichten nach der Datenschutz-Grundverordnung nachkommt und daher über die geeigneten Garantien nach Art. 28 Abs. 1 DSGVO verfügt. Diese können befolgte Verhaltensregeln, Zertifikate, rechtsverbindliche Vereinbarungen zur Auftragsverarbeitung (insb. im Hinblick auf Weisungen durch den Cloud-Anbieter und Pflichten des Subauftragsverarbeiters), Dienstbeschreibungen, Datensicherheitskonzepte, oder sonstige Dokumente sein. Darüber hinaus kann der Cloud-Anbieter Dokumente über die Auswahl (bspw. Protokolle über Auswahlüberlegungen und -entscheidungen) und die Durchführung von eigenen Kontrollen (bspw. Protokolle der Subauftragsverarbeiterkontrollen) vorlegen.

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

Nr. 21– Datenübermittlung[66]

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[67], 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.

[66] 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.
[67] 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[68] 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.

Umsetzungshinweis

Auf die Umsetzungshinweise in Nr. 11.1 wird verwiesen.

Nachweis

Auf die Nachweise in Nr. 11.1 wird verwiesen.

[68] 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