Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP)

– Version 1.0 –

Herausgeber: Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“
E-Mail: info@tcdp.de; www.tcdp.de
Im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi)
Stand: September 2016

Inhalt

I. Gegenstand und Ziele des TCDP

Das Trusted Cloud-Datenschutzprofil („TCDP“) ist ein Prüfstandard für die Datenschutz-Zertifizierung von Cloud-Diensten.

1. Adressaten und Funktion des TCDP

Die Datenschutz-Zertifizierung ermöglicht es Anbietern von IT-Diensten, die Vereinbarkeit ihrer IT-Dienste mit datenschutzrechtlichen Anforderungen nachzuweisen. Nutzer von IT-Diensten können auf die Datenschutzkonformität zertifizierter Dienste vertrauen. Das Anwendungsgebiet der Datenschutz-Zertifizierung nach dem TCDP ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (Auftragsdatenverarbeitung). Hier muss sich der Nutzer des Dienstes als Auftraggeber gemäß § 11 BDSG von der Einhaltung der gesetzlichen Anforderungen durch den Auftragnehmer überzeugen. Diese Überzeugung wird wesentlich erleichtert, wenn der Anbieter des IT-Dienstes als Auftragnehmer ein Zertifikat vorweist, das die Erfüllung der gesetzlichen Anforderungen durch den jeweiligen IT-Dienst bestätigt. Für die Nutzung von Cloud-Diensten, die oft 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.

Das TCDP beschreibt datenschutzrechtliche Anforderungen auf der Seite des Auftragnehmers (Cloud-Anbieter). Die datenschutzrechtlichen Anforderungen an den Auftraggeber (Cloud-Nutzer) sind nicht Gegenstand des TCDP.

2. TCDP und gesetzliche Regelung der Datenschutz-Zertifizierung

Das TCDP steht im Zusammenhang mit dem Ziel einer gesetzlich geregelten Datenschutz-Zertifizierung. Grundlage des TCDP ist das Konzept zur Datenschutz-Zertifizierung von Cloud-Diensten, das die Arbeitsgruppe „Rechtsrahmen des Cloud Computing“[1] im Rahmen der Begleitforschung des Programms „Trusted Cloud“ erarbeitet hat.[2] Im Pilotprojekt „Datenschutz-Zertifizierung“ wurden weitere Grundlagen für eine datenschutzrechtliche Zertifizierungen erarbeitet. Das TCDP eignet sich für die modulare Zertifizierung, wie sie im Papier „Modulare Zertifizierung von Cloud-Diensten“ dargestellt ist,[3] und eine Zertifizierung nach den Grundsätzen, die das Papier „Eckpunkte eines Zertifizierungsverfahrens für Cloud-Dienste“[4] des Pilotprojekts „Datenschutz-Zertifizierung für Cloud-Dienste“ beschreibt.

Das TCDP bezieht sich auf das Bundesdatenschutzgesetz (BDSG). Es setzt die gesetzlichen Anforderungen des BDSG an die Auftragsdatenverarbeitung um und konkretisiert diese zu prüffähigen Normen. Es baut auf dem ISO/IEC-Standard 27018[5] auf, der die international anerkannten ISO/IEC-Standards 27001[6] und 27002[7] um cloud- und insbesondere datenschutzspezifische Anforderungen erweitert, und bezieht darüber hinaus den Standard ISO/IEC 27017[8] ein.

Das TCDP bezieht die Normen von ISO/IEC 27018, ISO/IEC 27017 und ISO/IEC 27002 durch Verweisung ein, soweit die ISO/IEC-Normen geeignet sind, die gesetzlichen Anforderungen des BDSG zu konkretisieren. Das TCDP modifiziert und ergänzt die ISO/IEC-Normen, soweit es erforderlich ist, um die gesetzlichen Anforderungen des BDSG zu erfüllen. Maßstab und Leitbild des TCDP sind damit die gesetzlichen Anforderungen des BDSG an die Auftragsdatenverarbeitung.

3. Entstehung und Verwendung des TCDP

Das TCDP wurde vom Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ des Bundesministeriums für Wirtschaft und Energie entwickelt. Im Pilotprojekt, das in einer ersten Phase von November 2013 bis April 2015 und in einer zweiten Phase von September 2015 bis September 2016 durchgeführt wurde, wirkten Datenschutz-Aufsichtsbehörden, Unternehmen als Cloud-Anbieter, Rechtsanwaltsgesellschaften, Wirtschaftsprüfungsgesellschaften sowie Prüfunternehmen, Unternehmensverbände, die Stiftung Datenschutz, der DIN e.V. sowie Wissenschaftler mit. Das Bundesministerium des Innern sowie das Bundesamt für Sicherheit der Informationstechnik, in der ersten Phase auch die EU-Kommission, hatten einen Beobachterstatus inne.[9]

Das TCDP wurde im April 2015 als „Betaversion“ TCDP 0.9 veröffentlicht. Es wurde seit September 2015 durch Pilot-Zertifizierungen getestet und weiterentwickelt. Das TCDP wird als Vollversion 1.0 im September 2016 veröffentlicht.

Die ordnungsgemäße Prüfung und Zertifizierung nach TCDP soll durch die vom Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ erarbeitete „Verfahrensordnung für TCDP-Zertifizierungen“ sichergestellt werden. Die Verfahrensordnung wird gemeinsam mit dem TCDP 1.0 im September 2016 veröffentlicht. Zertifikate nach TCDP sollen nur nach Maßgabe dieser Verfahrensordnung erteilt werden. Das Prüfzeichen für TCDP-Zertifikate darf nur unter Beachtung der Verfahrensordnung geführt werden.

Die Verwaltung und Weiterentwicklung des TCDP als Prüfstandard für Cloud-Dienste auf der Grundlage des BDSG sowie der Verfahrensordnung für TCDP-Zertifizierungen wurde auf die Stiftung Datenschutz übertragen. Der Verwalter unterhält auch eine Informationsstelle zur TCPD-Zertifizierung.

4. Datenschutz-Grundverordnung und europäische Datenschutz-Zertifizierung

Das TCDP ist eingebettet in das Ziel einer europäischen Datenschutz-Zertifizierung auf gesetzlicher Grundlage. Das TCDP soll die Entwicklung der europäischen Datenschutz-Zertifizierung fördern, indem es Grundlagen entwickelt, die für die Ausgestaltung der Datenschutz-Zertifizierung genutzt werden können. Die Datenschutz-Grundverordnung (DSGVO) enthält zentrale Grundlagen eines gesetzlichen Rahmens für Datenschutz-Zertifizierungen. Das Pilotprojekt spricht sich mit Nachdruck für die Entwicklung einer dem Konzept des TCDP entsprechenden Zertifizierung auf der Grundlage der DSGVO aus. Zertifizierungen nach TCDP sollen nach Entwicklung eines entsprechenden Prüfstandards und Zertifizierungsverfahrens in Zertifikate nach einem DSGVO-Standard für Cloud-Dienste übergehen, wie es die Verfahrensordnung für Zertifizierungen nach TCDP vorsieht.

II. Aufbau und Benutzung des TCDP

1. Die Textkategorien des TCDP

Das TCDP unterscheidet, ähnlich wie die ISO/IEC 27000-Reihe und andere Standards, zwischen „Anforderungen“ und „Umsetzungshinweisen“ und enthält zusätzlich „Erläuterungen“.

Die Anforderungen bezeichnen die normativen Voraussetzungen, die zu erfüllen sind, um ein Zertifikat auf der Grundlage des TCDP zu erhalten. Sie sind also die Prüfanforderungen. Soweit TCDP-Anforderungen Maßnahmen (controls) von ISO/IEC 27018, ISO/IEC 27017

oder ISO/IEC 27002 als „maßgeblich“ bezeichnen, werden jene Maßnahmen (controls) zu Anforderungen des TCDP, müssen also erfüllt sein.

Da das BDSG durchgehend verpflichtende Anforderungen stellt, sind auch die Normen des TCDP regelmäßig als verpflichtende Anforderungen formuliert. Da ISO/IEC 27018 und ISO/IEC 27002 aber hauptsächlich nicht-bindende Anforderungen formulieren („should“), muss bei Verweisungen des TCDP auf ISO/IEC-Normen eine Veränderung zu verpflichtenden Anforderungen erfolgen. Insoweit verwendet das TCDP zwei unterschiedliche Vorgehensweisen. Teilweise verweisen TCDP-Normen auf ISO/IEC-Normen und stellen klar, dass diese als verbindliche Anforderungen maßgeblich sind, also als „shall“, nicht als „should“ zu lesen sind. Teilweise enthält das TCDP eine eigene Formulierung der jeweiligen Anforderung und verweist in eckigen Klammern auf die inhaltlich korrespondierenden ISO/IEC-Maßnahmen (controls). In einigen Fällen ist auch die Übereinstimmung der ISO/IEC-Norm mit den Anforderungen des BDSG fraglich oder anhand des Wortlauts nicht offensichtlich. Durch die eigenständige Fassung der Anforderung und den Verweis auf ISO/IEC-Normen als Klammerzusatz wird klargestellt, dass bei etwaigen Abweichungen die am BDSG orientierte Anforderung des TCDP maßgeblich ist.

Die Umsetzungshinweise sollen Leitlinie und Hilfestellung für das Verständnis und die Umsetzung der Anforderungen geben, sind selbst aber keine „normativen“ Anforderungen.

Die Umsetzungshinweise zu den einzelnen TCDP-Normen sind grundsätzlich an den Schutzklassen nach Maßgabe des TCDP-Schutzklassenkonzepts[10] ausgerichtet. Fehlt in einer TCDP-Norm eine solche Einteilung nach Schutzklassen, bedeutet dies, dass die Umsetzungshinweise gleichermaßen für alle Schutzklassen gelten.

Die Umsetzungshinweise beziehen, soweit zweckmäßig, die Umsetzungsempfehlungen der ISO-Normen durch Verweis ein. Insoweit gilt dasselbe wie bei den Anforderungen.

Die „Erläuterungen“ sollen das Verständnis der Anforderungen und ihrer Herleitung aus dem Gesetz erleichtern.

2. Verwendung und Zitierweise der ISO/IEC-Standards

Die Anwendung des TCDP setzt wegen der Verweise auf ISO/IEC 27018 und auf ISO/IEC 27002 sowie auf ISO/IEC 27017 die Kenntnis dieser Standards voraus. Eine vorangegangene Zertifizierung nach ISO/IEC 27001 ist keine Voraussetzung des TCDP. Aufgrund der Verwendung der Systematik und Begrifflichkeit der ISO/IEC 27000-Reihe im TCDP wird eine Zertifizierung nach TCDP erheblich erleichtert, wenn eine derartige Zertifizierung bereits vorhanden ist.

Die ISO/IEC-Standards werden in der aktuellen Fassung (ISO/IEC 27018:2014; ISO/IEC 27002:2013; ISO/IEC 27017:2015) zitiert. Zur besseren Lesbarkeit des TCDP werden im Text die Standards kurz als „ISO/IEC 27018“, „ISO/IEC 27002“ sowie “ISO/IEC 27017“ bezeichnet.

ISO/IEC 27018 sowie ISO/IEC 27017 bauen auf ISO/IEC 27001 und ISO/IEC 27002 auf und verweisen häufig auf Maßnahmen (controls) und Umsetzungshinweise (implementation guidance) von ISO/IEC 27002, ohne eigenständige Sachaussagen zu treffen. Das TCDP verweist in diesen Fällen ausschließlich auf die Maßnahmen (controls) und Umsetzungshinweise (implementation guidance) von ISO/IEC 27002. Soweit ISO/IEC 27018 und ISO/IEC 27017 ergänzende Aussagen enthalten, verweist das TCDP auch auf ISO/IEC 27018 und ISO/IEC 27017.

III. Schutzklassen

1. Das Schutzklassenkonzept

Das TCDP beruht auf dem Schutzklassenkonzept, das im Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ entwickelt und im Arbeitspapier „Schutzklassen in der Datenschutz-Zertifizierung“ vom April 2015[11] erstmals beschrieben wurde. Das Schutzklassenkonzept wird in aktualisierter Form als TCDP-Schutzklassenkonzept 1.0 im September 2016 veröffentlicht.[12]

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

Die Schutzbedarfsklassen definieren den Schutzbedarf für Datenverarbeitungsvorgänge anhand genereller Merkmale. Dieser ergibt sich aus der Art der Daten und der Umstände 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.

In der TCDP-Zertifizierung weist das Zertifikat die Schutz(anforderungs)klasse aus, die der zertifizierte Cloud-Dienst erfüllt.

2. Verantwortlichkeiten von Cloud-Nutzer und Cloud-Anbieter

Die Unterscheidung von Schutzbedarfsklassen und Schutzanforderungsklassen korrespondiert mit den Rollen und Verantwortlichkeiten von Cloud-Nutzer und Cloud-Anbieter in der Auftragsdatenverarbeitung.

Der Cloud-Anbieter ist dafür verantwortlich, seinen Dienst einer Schutzanforderungsklasse zuzuordnen und sicherzustellen, dass sein Dienst die Anforderungen der Schutzanforderungsklasse stets erfüllt.

Die Zertifizierungsstelle ordnet den Dienst im Rahmen des Zertifizierungsverfahrens auf Grundlage der Prüfung und anhand der konkreten technischen und organisatorischen Maßnahmen einer bestimmten Schutz(anforderungs)klasse zu. Im Zertifikat wird die Eignung des Dienstes für eine konkrete Schutz(anforderungs)klasse zum Ausdruck gebracht.

Der Cloud-Nutzer als verantwortliche Stelle und Auftraggeber hat die Aufgabe, den Schutzbedarf seiner Datenverarbeitung festzulegen. Ihm obliegt es daher, die für seine Datenverarbeitung maßgebliche Schutzanforderungsklasse zu ermitteln und für seine Datenverarbeitung einen Cloud-Dienst auszuwählen, der mindestens die entsprechende Schutzanforderungsklasse erfüllt. Die Ermittlung des Schutzbedarfs eines Datenverarbeitungsvorgangs ist im TCDP-Schutzklassenkonzept im Einzelnen beschrieben.

3. Die Schutzklassen des TCDP

Das TCDP beruht auf der Unterscheidung von drei Schutzklassen (I, II, III), für die jeweils Schutzbedarf (Schutzbedarfsklassen) und Schutzanforderungen (Schutzanforderungsklassen) beschrieben werden.

Darüber hinaus werden zwei weitere Schutzbedarfsklassen definiert, die jedoch eher eine Abgrenzungs- und Hilfsfunktion haben. Durch die Schutzklasse 0 wird das Fehlen eines datenschutzrechtlichen Schutzbedarfs gekennzeichnet. Dies betrifft etwa Daten ohne Personenbezug. Durch die Schutzklasse III+ wird ein Schutzbedarf gekennzeichnet, der nicht in einer Schutzklasse beschrieben werden kann und damit einer Zertifizierung nicht zugänglich ist. Dies betrifft etwa Datenverarbeitungsvorgänge mit sehr hohem Schutzbedarf und sehr individuellen Umständen. Da nach den Schutzklassen 0 und III+ nicht zertifiziert werden kann, werden insoweit keine Schutzanforderungsklassen formuliert.

a) Schutzbedarfsklassen

Schutzbedarfsklasse 0
Datenverarbeitungsvorgänge (d.h. die im Cloud-Dienst nachgefragte Dienstleitung), die keine oder keine schutzbedürftigen Aussagen über persönliche Verhältnisse natürlicher Personen enthalten, erzeugen, unterstützen oder solche ermöglichen.

Schutzbedarfsklasse 1

Datenverarbeitungsvorgänge, die durch die einbezogenen Daten und die konkrete Erhebung, Verarbeitung oder Nutzung dieser Daten Aussagen über die persönlichen Verhältnisse einer natürlichen Person (Betroffener) enthalten, erzeugen, unterstützen oder solche ermöglichen. Die unbefugte Verarbeitung oder Nutzung dieser Daten führt nach der Erfahrung meist nicht zu einem konkreten Nachteil für den Betroffenen (Beeinträchtigung der Rechtsgüter), oder dieser kann vom Betroffenen leicht verhindert oder abgestellt werden.

Schutzbedarfsklasse 2
Datenverarbeitungsvorgänge, die aufgrund der verwendeten Daten oder der konkreten Erhebung, Verarbeitung oder Nutzung dieser Daten eine Aussagekraft über die Persönlichkeit oder die Lebensumstände des Betroffenen haben, unterstützen oder zu einer solchen führen können oder sonst für die Verhältnisse des Betroffenen von Bedeutung sind. Die unbefugte Verarbeitung oder Nutzung dieser Daten kann nach der Erfahrung zu einem konkreten Nachteil für den Betroffenen führen.

Schutzbedarfsklasse 3
Datenverarbeitungsvorgänge, die aufgrund der verwendeten Daten oder der konkreten Erhebung, Verarbeitung oder Nutzung dieser Daten eine erhebliche Aussagekraft über die Persönlichkeit oder die Lebensumstände des Betroffenen haben, unterstützen oder zu einer solchen führen können oder sonst für die Verhältnisse des Betroffenen von erheblicher Bedeutung sind. Die unbefugte Erhebung, Verarbeitung oder Nutzung dieser Daten kann zu schwerwiegenden Nachteilen für den Betroffenen führen.

b) Schutzanforderungsklassen

Schutzanforderungsklasse 1
Der Cloud-Anbieter muss durch risikoangemessene technische und organisatorische Maßnahmen gewährleisten, dass die Daten nicht unbefugt verarbeitet oder genutzt werden.

Die Maßnahmen müssen geeignet sein, um im Regelfall solche Vorgänge aufgrund techni-

scher 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.

Schutzanforderungsklasse 2
Der Cloud-Anbieter muss durch risikoangemessene technische und organisatorische Maßnahmen gewährleisten, dass die Daten nicht unbefugt verarbeitet oder genutzt werden.

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

Schutzanforderungsklasse 3
Der Cloud-Anbieter muss durch risikoangemessene technische und organisatorische Maßnahmen gewährleisten, dass die Daten nicht unbefugt verarbeitet oder genutzt werden.

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.

4. Die Ermittlung der Schutzbedarfsklasse

Die Festlegung des Schutzbedarfs obliegt dem Cloud-Nutzer (siehe oben 2.). Der Schutzbedarf wird in einem dreistufigen Verfahren ermittelt:

- Im 1. Schritt wird der abstrakte Schutzbedarf der zu verarbeitenden Daten nach der Datenart (Beispiele: siehe Schutzklassenkonzept Trusted Cloud Kapitel 3.2). bestimmt.
- Im 2. Schritt ist zu prüfen, ob sich der Schutzbedarf aufgrund der konkreten Verwendung erhöht.
- Im 3. Schritt ist zu prüfen, ob der Schutzbedarf aufgrund konkreter Umstände sinkt.

Im Ergebnis wird der Schutzbedarf der konkreten Datenverarbeitung nach den oben genannten Schutzbedarfsklassen kategorisiert. Eine ausführliche Beschreibung dieses Vorgangs mit Beispielen zu den Datenarten/Verwendungskontext findet sich im Schutzklassenkonzept Trusted Cloud, Kapitel 3.2.

IV. Normentabelle

BDSG	Inhalt der Norm	Kurzbeschreibung	TCDP-Nr.
§ 11	Anforderungen an den Vertrag	Erfüllung der gesetzlichen Anforderungen an den Vertrag	1
§ 11 II 2	Diensteerbringung aufgrund Vertrags	Diensteerbringung nur aufgrund ADV-Vertrags	1.1
§ 11 II 2	Form des Vertrags	Vertrag bedarf der Schriftform	1.2
§ 11 II 2 Nr. 1	Auftragsgegenstand und Dauer	Gegenstand und Dauer des Auftrags sind festzulegen	1.3
§ 11 II 2 Nr. 2	Umfang/Art/Zweck/Kreis der Betroffenen	Umfang/Art/Zweck der Erhebung, Verarbeitung, Nutzung und Kreis Betroffener sind festzulegen	1.4
§ 11 II 2 Nr. 3	Technische und organisatorische Maßnahmen	Die nach § 9 BDSG zu treffenden Maßnahmen sind festzulegen	1.5
§ 11 II 2 Nr. 4	Berichtigung/Löschung/ Sperrung	Vorgaben zur Berichtigung, Löschung und Sperrung von Daten auf Weisung AG sind festzulegen	1.6
§ 11 II 2 Nr. 5	Pflichten des AN	Pflichten des AN, insbesondere Kontrollen sind festzulegen	1.7
§ 11 II 2 Nr. 6	Unterauftragnehmer	Ob der AN Unterauftragnehmer beauftragen darf, ist festzulegen	1.8
§ 11 II 2 Nr. 7	Rechte des AG und Pflichten des AN	Kontrollrechte des AG und Duldungs- und Mitwirkungspflichten des AN sind festzulegen	1.9
§ 11 II 2 Nr. 8	Mitteilung von Verstößen	Welche Verstöße gegen Vorschriften oder vertragliche Festlegungen mitzuteilen sind, ist festzulegen	1.10
§ 11 II 2 Nr. 9	Weisungsbefugnisse des AG	Die Weisungsbefugnisse des AG gegenüber dem AN sind festzulegen	1.11
§ 11 II 2 Nr. 10	Rücknahmepflichten	Die Rückgabe von Datenträgern & Löschung von Daten beim AN sind festzulegen	1.12
§§ 11, 5	Das Verhältnis zwischen Cloud-Anbieter und Cloud-Nutzer	Vom AN zu treffende organisatorische Vorkehrungen zur datenschutzkonformen Erbringung der Leistung	
§ 11 III 1	Weisungsgebundenheit	Keine Erhebung/Verarbeitung/Nutzung von Daten außerhalb der AG-Weisungen	2
§ 11 III 2	Mitteilungspflicht	Hinweispflicht des AN, wenn AG-Weisung gegen BDSG oder andere DS-Vorschriften verstößt	3
§ 11 II 2 Nr. 2	Unterauftragnehmer (materiell)	AN muss ordnungsgemäße Einschaltung von Subunternehmern nachweisen.	4
§ 11 IV	Betrieblicher Datenschutzbeauftragter	Pflichten des AN nach §§ 5, 9, 43 Abs. 1 Nr. 2, 10 und 11, Abs. 2 Nr. 1 bis 3 und Abs. 3 sowie §§ 44, § 4f, 4g und 38 BDSG	5
§ 11	Berichtigung, Sperrung und Löschung von Daten	Das Berichtigen, Sperren und Löschen von Daten ist zu ermöglichen	6

BDSG	Inhalt der Norm	Kurzbeschreibung	TCDP-Nr.
§ 11	Mitteilungspflicht	Verstöße gegen gesetzliche oder vertragliche Vorschriften sind mitzuteilen	7
§ 11 II 2	Kontrollrechte AG/Duldungs- und Mitwirkungspflichten AN	AN muss Prozesse für Kundenaudits vorhalten	9
§ 11 II 2 Nr. 10	Rückgabepflichten	AN muss Rückgabeprozesse nachweisen	10
§ 5	Datengeheimnis	AN muss Mitarbeiter auf Datengeheimnis verpflichten	11
§ 9 i.V.m. Anlage	Technisch-Organisatorsiche Sicherheit des Cloud-Dienstes		
S. 2 Nr. 1 Anlage zu § 9	Zutrittskontrolle	Verwehrung des Zutritts Unbefugter zu DV-Anlagen	22
S. 2 Nr. 2 Anlage zu § 9	Zugangskontrolle	Verhinderung des Zugangs Unbefugter zu DV-Systemen	23
S. 2 Nr. 3 Anlage zu § 9	Zugriffskontrolle	Gewährleistung, dass Berechtigte nur auf eigenen Datenbereich Zugriff haben	23
S. 2 Nr. 4 Anlage zu § 9	Weitergabekontrolle	Schutz der Daten während Transport, Speicherung und Übermittlung gegen Zugriff Unbefugter	24
S. 2 Nr. 5 Anlage zu § 9	Eingabekontrolle	Gewährleistung, dass Nutzer, die personenbezogene Daten eingeben, verändern oder entfernen, nachträglich ermittelbar sind	25
S. 2 Nr. 6 Anlage zu § 9	Auftragskontrolle	Gewährleistung, dass personenbezogene Daten nur im Rahmen der AG-Weisungen verarbeitet werden können	26
S. 2 Nr. 7 Anlage zu § 9	Verfügbarkeitskontrolle	Gewährleistung, dass personenbezogene Daten nicht zufällig zerstört werden oder verloren gehen	31
S. 2 Nr. 8 Anlage zu § 9	Getrennte Verarbeitung	Gewährleistung, dass erhobene Daten entsprechend des jeweiligen Zwecks getrennt verarbeitet werden können	27
§ 9	Kryptographie	Anforderungen an Einsatz kryptographischer Verfahren	28

V. Anforderungen und Umsetzungsempfehlungen

1. Vertragliche Regelung der Auftragsdatenverarbeitung

TCDP Nr. 1 – Vertragliche Grundlage

Erläuterung
Der Cloud-Anbieter wirkt darauf hin, dass er seine Leistung dem Cloud-Nutzer aufgrund eines Vertrags (Cloud-Vertrag) erbringt, der die gesetzlichen Anforderungen des BDSG an die Auftragsdatenverarbeitung erfüllt. Dieses Ziel soll durch die nachfolgenden Anforderungen gesichert werden.

Die Ziffern 1.3 bis 1.12 des TCDP können dadurch erfüllt werden, dass der Cloud-Anbieter einen Vertrag anbietet, der die genannten Anforderungen erfüllt, und durch organisatorische Vorkehrungen gewährleistet, dass der Cloud-Dienst nur auf der Grundlage eines entsprechenden Cloud-Vertrags erbracht wird. Bei der Erstellung eines solchen Vertrages können Musterverträge hilfreich sein.

TCDP Nr. 1.1 – Diensteerbringung aufgrund eines Vertrags

Anforderung
Der Cloud-Anbieter stellt durch geeignete organisatorische Vorkehrungen sicher, dass der Cloud-Dienst erst erbracht wird, nachdem mit dem Cloud-Nutzer ein Vertrag geschlossen wurde, der die Anforderungen des TCDP Nr. 1 erfüllt.

TCDP Nr. 1.2 – Form des Vertrags

Anforderung
Der Cloud-Anbieter bietet den Abschluss eines schriftlichen Vertrags über Auftragsdatenverarbeitung an.

Umsetzungshinweis
Die Bereitschaft, einen schriftlichen Vertrag zu schließen, kann etwa durch einen Vertragsentwurf (Vertragsformular) und ein Verfahren, wonach der Vertrag in Schriftform abgeschlossen wird, nachgewiesen werden.

TCDP Nr. 1.3 – Gegenstand und Dauer des Auftrags

Anforderung
Der Gegenstand und die Dauer des Auftrags werden im Cloud-Vertrag festgelegt.

Umsetzungshinweis
Im Vertrag sollte entweder eine konkrete Zeitspanne benannt oder klargestellt werden, dass der Vertrag auf unbestimmte Zeit geschlossen werden soll. Bei auf unbestimmte Zeit ge-

schlossenen Verträgen sollen Angaben zur Kündigung, insbesondere zur Kündigungsfrist, aufgenommen werden.

Der Cloud-Anbieter kann dies dadurch gewährleisten, dass ein Vertragsentwurf (Vertragsformular) mit diesen Angaben vorgehalten wird und ein Verfahren implementiert ist, wonach der Vertrag mit diesen Angaben geschlossen wird.

TCDP Nr. 1.4 – Art und Zweck der Datenverarbeitung

Anforderung
Der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen werden im Cloud-Vertrag festgelegt.

Umsetzungshinweis
Diese Einzelangaben müssen zwar nicht jeden konkreten Einzelfall abdecken, sollten jedoch so präzise sein, dass die im Rahmen der Auftragsdatenverarbeitung zulässige Datenverwendung im Einzelnen nachvollzogen werden kann.

Die Festlegung kann je nach Art des Cloud-Dienstes auf unterschiedliche Art erfolgen. Insbesondere bei Standard-SaaS-Diensten, bei denen sich Art und Zweck der Datenverarbeitung schon aus dem Zweck des Programms ergibt, kann die Festlegung schon durch einen Verweis auf die Beschreibung des Programms in der Dokumentation erfolgen. Bei komplexeren oder weniger festgelegten Diensten (z.B. PaaS) ist regelmäßig eine Abstimmung mit dem Cloud-Nutzer erforderlich. Diese kann etwa durch ein elektronisches Formular gestaltet sein, in das der Cloud-Nutzer die erforderlichen Angaben einträgt.

TCDP Nr. 1.5 – Technische und organisatorische Maßnahmen; Ort der Datenverarbeitung

Anforderung

(1) Die nach TCDP Nr. 22-28 zu treffenden technischen und organisatorischen Maßnahmen werden im Cloud-Vertrag festgelegt.

(2) Der Cloud-Anbieter trifft eine Aussage zu der von ihm gewährleisteten Schutzklasse.

(3) Im Cloud-Vertrag wird festgelegt, in welchen Staaten Daten des Cloud-Nutzers verarbeitet, insbesondere gespeichert werden.

Umsetzungshinweis
Die Festlegung kann in einer Anlage zum Vertrag erfolgen. Angaben zur Umsetzung der TCDP Nr. 22 bis 28 (§ 9 BDSG und der Anlage) können an Sicherheitszielen ausgerichtet werden, während die konkreten Maßnahmen der Zielerreichung dem Cloud-Anbieter überlassen werden können. Die Festlegung sollte in Form eines Sicherheitskonzepts (TCDP Nr. 21) erfolgen und dem Vertrag als Anlage beigefügt werden.

Für den Cloud-Nutzer ist es, entsprechend dem Trusted Cloud-Schutzklassenkonzept, wichtig zu wissen, welcher Schutzanforderungsklasse der Cloud-Dienst entspricht. Es empfiehlt

sich daher, in den Cloud-Vertrag die Gewährleistung einer bestimmten Schutzklasse gemäß dem Trusted Cloud-Schutzklassenkonzept explizit aufzunehmen.

TCDP Nr. 1.6 – Berichtigung, Löschung und Sperrung von Daten

Anforderung
Die Verfahren zur Berichtigung, Löschung und Sperrung von Daten (TCDP Nr. 6) werden im Cloud-Vertrag festgelegt.

Umsetzungshinweis
Es empfiehlt sich, Löschfristen und Löschverfahren konkret zu benennen.

TCDP Nr. 1.7 – Pflichten des Cloud-Anbieters

Anforderung
Im Cloud-Vertrag werden die datenschutzrechtlichen Pflichten des Cloud-Anbieters nach § 11 Abs. 4 BDSG als vertragliche Pflichten des Cloud-Anbieters gegenüber dem Cloud-Nutzer festgelegt.

Erläuterung
Gemäß § 11 Abs. 2 S. 2 Nr. 5 BDSG ist erforderlich, dass im Cloud-Vertrag eindeutig klargestellt wird, welchen der dort genannten gesetzlichen Anforderungen der Cloud-Anbieter als Auftragnehmer unterliegt.

Umsetzungshinweis
Es reicht aus, wenn im Cloud-Vertrag die für den Cloud-Anbieter maßgeblichen gesetzlichen Bestimmungen genannt werden. Zweckmäßig und üblich ist es, diese nicht nur mit ihrem Paragraphen, sondern auch inhaltlich zu beschreiben oder im Wortlaut wiederzugeben.

TCDP Nr. 1.8 – Unterauftragnehmer

Anforderung

(1) Im Cloud-Vertrag wird die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen festgelegt.

(2) Der Cloud-Anbieter verpflichtet sich im Cloud-Vertrag gegenüber dem Cloud-Nutzer, bei Beauftragung von Unterauftragnehmern die in TCDP Nr. 4 geregelten Anforderungen einzuhalten.

Erläuterung
Unterauftragnehmer dürfen nur mit Zustimmung des Cloud-Nutzers eingesetzt werden. Erforderlich ist eine allgemeine Zustimmung zum Einsatz von Unterauftragnehmern. Eine spezifische Zustimmung zum Einsatz eines konkreten Unterauftragnehmers ist nicht erforderlich. Der Cloud-Anbieter muss dem Cloud-Nutzer jedoch die Identität aller Unterauftragnehmer mitteilen (Nr. 4.2).

TCDP Nr. 1.9 – Kontrollrechte des Cloud-Nutzers

Anforderung
Die Kontrollrechte des Cloud-Nutzers (TCDP Nr. 9) und die entsprechenden Duldungs- und Mitwirkungspflichten des Cloud-Anbieters werden im Cloud-Vertrag festgelegt.

TCDP Nr. 1.10 – Mitteilung bei Verstößen und Herausgabeverlangen

Anforderung

(1) Im Cloud-Vertrag wird festgelegt, welche Verstöße des Cloud-Anbieters oder der bei ihm beschäftigten Personen (vgl. TCDP Nr. 7) gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen mitzuteilen sind.

(2) Im Cloud-Vertrag wird festgelegt, dass der Cloud-Anbieter dem Cloud-Nutzer unverzüglich Mitteilung von etwaigen Datenherausgabeverlangen macht, soweit die Mitteilung zulässig ist (vgl. TCDP Nr. 8).

Umsetzungshinweis
Im Cloud-Vertrag muss als Mindesterfordernis die Verpflichtung zur unverzüglichen Mitteilung von Datenschutzverstößen sowie von Datenherausgabeverlangen enthalten sein. Es empfiehlt sich, im Vertrag auch festzulegen, in welcher Form und auf welchem Kommunikationsweg die Mitteilung erfolgen muss.

TCDP Nr. 1.11 – Weisungsbefugnisse des Cloud-Nutzers

Anforderung
Im Cloud-Vertrag wird der Umfang der Weisungsbefugnisse, die sich der Cloud-Nutzer gegenüber dem Cloud-Anbieter vorbehält (TCDP Nr. 2), festgelegt.

Umsetzungshinweis
Dem Cloud-Nutzer muss das Recht zur Einzelweisung vorbehalten sein. Es empfiehlt sich, im Vertrag vorzusehen, dass die Einzelweisung in Textform erfolgen und durch den Cloud-Anbieter bestätigt werden muss. Es sollte aus dem Vertrag genau hervorgehen, welche Personen zur Erteilung von Einzelweisungen befugt sind. Die zu Einzelweisungen befugten Personen können ausdrücklich im Cloud-Vertrag benannt werden.

TCDP Nr. 1.12 – Rückgabe und Löschung von Daten

Anforderung
Im Cloud-Vertrag werden die Pflichten des Cloud-Anbieters zur Rückgabe und Löschung von Daten (TCDP Nr. 10) festgelegt.

Umsetzungshinweis

Im Cloud-Vertrag sollten zumindest die in TCDP Nr. 10 genannten Pflichten festgelegt werden. Eine detaillierte Regelung ist empfehlenswert. Diese kann auch durch Verweis auf entsprechende Grundsätze des Cloud-Anbieters erfolgen.

2. Das Verhältnis zwischen Cloud-Anbieter und Cloud-Nutzer

TCDP Nr. 2 – Weisungsgebundenheit des Cloud-Anbieters

Anforderung
Der Cloud-Anbieter stellt durch geeignete Maßnahmen sicher, dass er bei der Ausführung des Dienstes verpflichtet ist, die Daten nur im Rahmen der Weisungen des Cloud-Nutzers zu erheben, zu verarbeiten und zu nutzen.

Erläuterung
Die Weisungsgebundenheit des Cloud-Anbieters ist im Gesetz an drei Stellen erfasst (§ 11 Abs. 2 S. 2 Nr. 9, Abs. 3 S. 1, Anlage zu § 9 Nr. 4 BDSG). Daher nennt das TCDP die Weisungsgebundenheit zur Klarstellung ebenfalls an drei Stellen: TCDP Nr. 2 stellt klar, dass der Cloud-Anbieter sich zur Weisungsbefolgung verpflichten muss, TCDP Nr. 1.11 nennt dies als notwendigen Bestandteil des Cloud-Vertrags, TCDP Nr. 26 verpflichtet den Cloud-Anbieter, die Weisungsbefolgung durch technische und organisatorische Maßnahmen abzusichern.

Umsetzungshinweis
Der Cloud-Anbieter sollte durch ein organisatorisches Verfahren sicherstellen, dass er sich im Vertrag gegenüber dem Cloud-Nutzer verpflichtet, die Auftragsdatenverarbeitung ausschließlich im Rahmen der Weisungen des Cloud-Nutzers vorzunehmen. Dies kann durch ein entsprechendes Vertragsformular (vgl. TCDP Nr. 1.11) geschehen. Zudem sollte beim Cloud-Anbieter eine technische oder organisatorische Maßnahme vorhanden sein, wonach kein Cloud-Dienst ausgeführt wird, ohne dass diese Bindung vorliegt.

Die Weisungen umfassen die Festlegung der Datenverarbeitung durch den Cloud-Anbieter. Diese kann durch eine Vereinbarung über die Funktionalitäten des Cloud-Dienstes geschehen. Diese Vereinbarung kann im Cloud-Vertrag, etwa durch Verweis auf die Dokumentation der Funktionalitäten, getroffen werden (vgl. TCDP Nr. 1.11).

Dem Cloud-Nutzer muss darüber hinaus das Recht zur Einzelweisung vorbehalten werden (vgl. TCDP Nr. 1.11).

TCDP Nr. 3 – Remonstrationspflicht

Anforderung
Der Cloud-Anbieter stellt durch geeignete Maßnahmen sicher, dass er den Cloud-Nutzer unverzüglich darauf hinweist, wenn er der Ansicht ist, dass eine Weisung des Cloud-Nutzers gegen datenschutzrechtliche Vorschriften verstößt, und dessen Entscheidung vor der Ausführung der Weisung abwartet.

Erläuterung
Nach den Grundsätzen der Auftragsdatenverarbeitung liegt die Verantwortung für die Datenschutzkonformität der Verarbeitung beim Cloud-Nutzer, der gegenüber dem Cloud-Anbieter deshalb auch ein Weisungsrecht hat. Gleichwohl darf der Cloud-Anbieter eine Weisung, deren Rechtmäßigkeit er bezweifelt, nicht unbesehen ausführen. § 11 Abs. 3 S. 2 BDSG

legt ihm für diese Fälle vielmehr eine Remonstrationspflicht auf. Er muss 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
Der Cloud-Anbieter kann ein Verfahren vorsehen und dokumentieren, wonach Weisungen, hinsichtlich deren datenschutzrechtlicher Zulässigkeit Anlass zu Zweifel besteht, dem Cloud-Nutzer vor Ausführung zur Entscheidung vorgelegt werden können. Es empfiehlt sich, eine ausdrückliche Entscheidung des Cloud-Nutzers in Textform vorzusehen. Dies sollte ggf. im Cloud-Vertrag geregelt werden.

TCDP Nr. 4 – Unterauftragnehmer

Erläuterung
Cloud-Dienste werden vom Cloud-Anbieter regelmäßig durch Einschaltung von Subunternehmern erbracht, die als Unterauftragnehmer in die Auftragsdatenverarbeitung integriert werden. Da auch die Subunternehmer ihrerseits häufig auf Subunternehmer zugreifen, ergeben sich oft mehrstufige Unterauftragsverhältnisse.

Die Einschaltung von Unterauftragnehmern und Unter-Unterauftragnehmern ist grundsätzlich zulässig. Allerdings hat der Cloud-Anbieter als Auftragnehmer dafür Sorge zu tragen, dass die Anforderungen an die Auftragsdatenverarbeitung von allen Unterauftragnehmern auf allen Stufen eingehalten werden.

TCDP Nr. 4.1 – Grundlage der Einschaltung von Unterauftragnehmern

Anforderung
Der Cloud-Anbieter stellt sicher, dass ein Cloud-Dienst unter Einbeziehung von Unterauftragnehmern für einen Cloud-Nutzer nur erbracht wird, wenn und soweit der Cloud-Nutzer dieser zugestimmt hat.

Umsetzungshinweis
Der Cloud-Anbieter kann, wenn er Unterauftragnehmer einsetzt, diese Anforderungen durch ein Verfahren erfüllen, wonach der Dienst für den Cloud-Nutzer erst erbracht wird, wenn – i.d.R. durch Abschluss des Cloud-Vertrags unter Einbeziehung einer entsprechenden Bestimmung (vgl. TCDP Nr. 1.8) – das Vorliegen des Einverständnisses überprüft wurde.

TCDP Nr. 4.2 – Information des Cloud-Nutzers

Anforderung

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

(2) Der Cloud-Anbieter informiert den Cloud-Nutzer über die Identität aller Unter-Unterauftragnehmer (einschließlich ladungsfähiger Anschrift), die von den von ihm beauftragten

Unterauftragnehmern eingeschaltet werden. Dies gilt für alle Stufen der Unter-Unterbeauftragung.

(3) Der Cloud-Anbieter informiert den Cloud-Nutzer über alle Änderungen in der Identität von Unterauftragnehmern oder Unter-Unterauftragnehmern, insbesondere über neu hinzukommende Unterauftragnehmer oder Unter-Unterauftragnehmer.

Umsetzungshinweis
Die Information kann elektronisch bereitgestellt werden, etwa durch einen Link auf einen (geschützten) Bereich der Website, in dem die Informationen enthalten sind. Die Information über Änderungen kann etwa per E-Mail oder in anderer Weise elektronisch erfolgen.

TCDP Nr. 4.3 – Vertragliche Grundlage der Unterbeauftragung

Anforderung

(1) Der Cloud-Anbieter stellt sicher, dass seine Unterauftragnehmer nicht ohne wirksamen Unterauftragsdatenverarbeitungsvertrag tätig werden.

(2) Der Cloud-Anbieter verpflichtet seine Unterauftragnehmer sicherzustellen, dass ihre Unter-Unterauftragnehmer nicht ohne wirksamen Unterauftragsdatenverarbeitungsvertrag tätig werden und auf ihre Unter-Unterauftragnehmer dieselbe Verpflichtung übertragen.

Umsetzungshinweis
Der Cloud-Anbieter kann die Anforderung nach Abs. 1 durch ein Verfahren erfüllen, wonach die Einbindung des Unterauftragnehmers in die Dienstleistung erst erfolgt, wenn das Vorliegen des Unterauftragsdatenverarbeitungsvertrags zwischen Cloud-Anbieter und Unterauftragnehmer überprüft wurde.

Die Anforderung nach Abs. 2 kann etwa dadurch erfüllt werden, dass diese Verpflichtung in den Unterauftragsdatenverarbeitungsvertrag aufgenommen wird.

TCDP Nr. 4.4 – Auswahl und Kontrolle der Unterauftragnehmer

Anforderung

(1) Der Cloud-Anbieter stellt sicher, dass nur solche Unterauftragnehmer einbezogen werden, die die Gewähr für die Einhaltung der datenschutzrechtlichen Anforderungen an die von ihnen zu erbringende Leistung bieten.

(2) Der Cloud-Anbieter überzeugt sich davon, dass seine Unterauftragnehmer die datenschutzrechtlichen Anforderungen an die von ihnen zu erbringende Leistung erfüllen.

(3) Die Anforderungen nach Abs. 1 und Abs. 2 gelten entsprechend für Unterauftragnehmer auf allen Stufen hinsichtlich der von ihnen eingesetzten Unter-Unterauftragnehmer.

Umsetzungshinweis
Die Anforderungen nach Abs. 1 und Abs. 2 können dadurch erfüllt werden, dass sich der Cloud-Anbieter durch Einsichtnahme in ein (gültiges) Zertifikat davon überzeugt, dass der Unterauftragnehmer die Anforderungen (noch) erfüllt.

Soweit der Cloud-Anbieter nicht auf Zertifikate seiner Unterauftragnehmer vertrauen kann, ist er verpflichtet, sich selbst von der Einhaltung der datenschutzrechtlichen Anforderungen durch die Unterauftragnehmer zu überzeugen. Insoweit sind die Umsetzungshinweise (implementation guidance) von ISO/IEC 27017 Ziff. 15.1.2, 15.1.3 und ISO/IEC 27002 Ziff. 15 im Sinne unverbindlicher Hinweise anwendbar.

TCDP Nr. 4.5 – Weisungen des Cloud-Nutzers

Anforderung

(1) Der Cloud-Anbieter stellt sicher, dass die Weisungen des Cloud-Nutzers an die Unterauftragnehmer weitergegeben werden.

(2) Der Cloud-Anbieter verpflichtet seine Unterauftragnehmer sicherzustellen, dass die vom Cloud-Nutzer stammenden Weisungen eingehalten werden, und dass sie dieselbe Verpflichtung auf ihre Unter-Unterauftragnehmer übertragen.

(3) Der Cloud-Anbieter vergewissert sich, dass die Weisungen des Cloud-Nutzers von Unterauftragnehmern und deren Unter-Unterauftragnehmern auf allen Stufen befolgt werden.

Erläuterung

Der Cloud-Anbieter hat, wenn die Weisungen des Cloud-Nutzers entlang der „Kette“ der (Unter-)Auftragnehmer weitergegeben werden, eine organisatorische Gesamtverantwortung für die Befolgung der Weisungen des Cloud-Nutzers.

Umsetzungshinweis

Der Cloud-Anbieter kann die Anforderung nach Abs. 1 durch Etablierung eines Verfahrens durchführen, wonach die Weisungen des Cloud-Nutzers an die Unterauftragnehmer weiterzugeben sind, etwa technisch, durch automatische Weiterleitung oder, bei manueller Bearbeitung von Weisungen, durch ein organisatorisches Verfahren.

Die Anforderung nach Abs. 2 kann etwa dadurch erfüllt werden, dass diese Verpflichtung in den Unterauftragsdatenverarbeitungsvertrag aufgenommen wird. Der Cloud-Anbieter kann die Anforderung nach Abs. 3 etwa dadurch erfüllen, dass er sich durch geeignete Maßnahmen (Einsichtnahme in Zertifizierungen oder eigene Überprüfungen) davon überzeugt, dass die Weitergabe und Befolgung der Weisungen erfolgt.

TCDP Nr. 5 – Datenschutzbeauftragter und gesetzliche Anforderungen

Anforderung

Der Cloud-Anbieter trägt Sorge dafür, dass die Erfüllung der datenschutzrechtlichen Anforderungen nach §§ 4f, 4g BDSG bzw. § 18 BDSG bzw. den Landesdatenschutzgesetzen durch geeignete Maßnahmen gewährleistet wird.

Erläuterung

§ 11 Abs. 4 BDSG unterwirft den Cloud-Anbieter als Auftragnehmer bestimmten gesetzlichen Anforderungen. Die dort genannten §§ 9 und 11 BDSG werden durch die übrigen

Anforderungen des TCDP umgesetzt. Die Vorschriften zum Datenschutzbeauftragen (§§ 4f, 4g BDSG) bzw. zur Compliance (§ 18 BDSG bzw. Landesdatenschutzgesetze) werden in TCDP Nr. 5, die Vorschriften zum Datengeheimnis (§ 5 BDSG) in TCDP Nr. 11 umgesetzt. § 38 BDSG (Aufsichtsbehörde) bzw. §§ 24-26 BDSG (Bundesbeauftragter für Datenschutz und Informationsfreiheit) bzw. die entsprechenden Vorschriften der Landesdatenschutzgesetze sind nur in Bezug auf die Bezugnahme im Vertrag zertifizierungsrelevant und werden insoweit durch TCDP Nr. 1.7 umgesetzt. Die §§ 43, 44 BDSG sind als Ordnungswidrigkeits- bzw. Straftatbestände nicht zertifizierungsrelevant.

Ist der Cloud-Anbieter zur Bestellung eines Beauftragten für den Datenschutz verpflichtet, so hat er die Anforderungen an eine wirksame Bestellung umzusetzen, indem er für die Erfüllung der Vorgaben an die Weisungsfreiheit, die Zuverlässigkeit und die erforderliche Fachkunde des Datenschutzbeauftragten sorgt. Dies setzt voraus, dass eine vorherige Prüfung der Eignung des zu bestellenden Datenschutzbeauftragten durch den bestellenden Cloud-Anbieter vorgenommen wird, um die Anforderungen bezüglich der Zuverlässigkeit (insbesondere im Hinblick auf mögliche Interessenkonflikte) und das Vorliegen erforderlicher Fachkunde des zu bestellenden Datenschutzbeauftragten, bezogen auf den konkreten Bedarf des bestellenden Cloud-Anbieters, zu bestätigen. Dabei ist auch die Mitwirkung des zu bestellenden Datenschutzbeauftragten (Eigenprüfung der Voraussetzungen, Mitteilungen über fachliche Eignung, Interessenkonflikte etc.) erforderlich.

Ist der Datenschutzbeauftragte bei einem anderen Unternehmen beschäftigt (also externer Datenschutzbeauftragter des Cloud-Anbieters) oder gleichzeitig Datenschutzbeauftragter anderer Unternehmen, gilt seine Weisungsfreiheit auch gegenüber seinem Arbeitgeber bzw. seinen anderen Auftraggebern.

Umsetzungshinweis
Der Cloud-Anbieter hat durch organisatorische Vorkehrungen im Sinne der Einrichtung einer Datenschutzorganisation sicherzustellen, dass der Datenschutzbeauftragte seine Aufgaben weisungsfrei und gesetzestreu wahrnehmen kann.

Der Cloud-Anbieter hat eine schriftliche Dokumentation der für den jeweiligen Cloud-Dienst eingesetzten Systeme, Verfahren und Prozesse (Software, Hardware, beteiligte Organisationseinheiten, Rollen und Dienstleister) und eine exakte Beschreibung der Gesamtheit der getroffenen technischen und organisatorischen Maßnahmen zu führen (z.B. in einem Datenschutzkonzept) und dem Datenschutzbeauftragten sowie (auf Anfrage) der Aufsichtsbehörde zugänglich zu machen.

Zur wirksamen Bestellung eines Datenschutzbeauftragten (DSB) gehören:
- eine Dokumentation der Eignungsprüfung durch den DSB und den Cloud-Anbieter, insbesondere hinsichtlich seiner Fachkunde und Zuverlässigkeit, bezogen auf Art und Umfang der Datenverarbeitung und mögliche Interessenkonflikte;
- eine schriftliche, beiderseitig unterzeichnete Bestellungsurkunde;
- ein Nachweis erforderlicher Weisungsfreiheit des DSB (soweit ein externer DSB bestellt wird, ist ggf. auch der Nachweis der Weisungsfreiheit gegenüber seinem Arbeitgeber erforderlich);
- ein Nachweis, dass der DSB über die für seine Aufgabenerfüllung erforderlichen Ressourcen verfügt und fern von Interessenkonflikten ist, im Fall von externen DSB Offenlegung der betreuten verantwortlichen Stellen und der hierfür notwendigen Zeitressourcen (die Zeitressourcen des DSB müssen dem Schutzbedarf und der Anzahl der Auftraggeber angemessen sein [ggf. Unterstützung durch Datenschutz-

Koordinatoren]; es sollte eine jährliche Planung und Zuweisung von Budgets für die Tätigkeiten des DSB geben [z.B. für den Zugriff auf externen Sachverstand und für die Aufrechterhaltung der Fachkunde des DSB]);
- eine unmittelbare organisatorische Unterstellung des DSB unter die Geschäftsleitung des Cloud-Anbieters.

Der DSB und der Beauftragte für IT-/Informationssicherheit sind in die Organisation des Cloud-Anbieters angemessen einzubinden. Sie haben in angemessener Weise zu kooperieren (gegenseitige Information und Unterstützung).

Der DSB hat regelmäßige, z.B. vierteljährlich stattfindende interne Audits durchzuführen und darüber der Leitung des Cloud-Anbieters Bericht zu erstatten.

TCDP Nr. 6 – Berichtigung, Löschung, Sperrung von Daten

Anforderung
Der Cloud-Anbieter stellt durch geeignete Maßnahmen sicher, dass der Cloud-Nutzer die Möglichkeit hat, die Berichtigung, Sperrung und Löschung personenbezogener Daten selbst vorzunehmen oder durch den Cloud-Anbieter vornehmen zu lassen [ISO/IEC 27018 Ziff. A.1.1.].

Erläuterung
Aus § 11 Abs. 2 S. 2 Nr. 4 BDSG ergibt sich, dass der Auftraggeber die Möglichkeit haben muss, personenbezogene Daten zu berichtigen, zu löschen oder zu sperren oder diese Maßnahmen jedenfalls zu veranlassen, damit er seinen Pflichten aus § 35 BDSG nachkommen kann. Diese Anforderung ist in der Sache wohl in ISO/IEC 27018 Ziff. A.1.1. enthalten, auch wenn etwa die Sperrung nicht ausdrücklich genannt wird.

Umsetzungshinweis
Es ist ein Verfahren zur Unterstützung des Auftraggebers bei der Umsetzung von Betroffenenrechten auf Berichtigung, Sperrung, Löschung und Auskunftserteilung zu errichten und zu dokumentieren. Dabei sind Zuständigkeiten festzulegen.

Soweit dem Cloud-Nutzer eine Umsetzung der Betroffenenrechte nicht selbst möglich ist, ist eine Kontaktstelle für den Cloud-Nutzer vorzuhalten, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann.

Es ist sicherzustellen, dass Vorfälle (Anfragen auf Umsetzung von Betroffenenrechten) dokumentiert werden.

TCDP Nr. 7 – Mitteilungspflicht bei Datenschutzverstößen

Anforderung
Der Cloud-Anbieter stellt durch geeignete Maßnahmen sicher, dass Verstöße gegen gesetzliche oder vertragliche Datenschutzanforderungen dem Cloud-Nutzer unverzüglich mitgeteilt werden, sofern nicht eine unrechtmäßige Übermittlung, Kenntniserlangung oder Veränderung personenbezogener Daten ausgeschlossen werden kann.

Erläuterung
TCDP Nr. 7 entspricht der Sache nach weitgehend ISO/IEC 27018 Ziff. A.9.1., geht aber, entsprechend der gesetzlichen Vorgabe, insoweit darüber hinaus, als Verstöße auch dann mitzuteilen sind, wenn eine unrechtmäßige Übermittlung, Kenntniserlangung oder Veränderung personenbezogener Daten zwar nicht festgestellt wird, aber auch nicht ausgeschlossen werden kann. Die Mitteilungspflicht bezieht sich auch auf Verstöße von Unterauftragnehmern und Unter-Unterauftragnehmern in der gesamten „Kette“ von Unterbeauftragungen.

Umsetzungshinweis
Um eine unverzügliche Mitteilung zu ermöglichen, ist im Regelfall festzulegen, wer zuständig ist und festzustellen, ob ein mitteilungspflichtiger Verstoß vorliegt und wer die Mitteilung an den Cloud-Nutzer vornimmt. Die zuständigen Stellen müssen für Mitarbeiter und Unterauftragnehmer in einer Weise erreichbar sein, dass Mitteilungen über (etwaige) Verstöße zeitnah entgegengenommen und bearbeitet werden können.

Zur Erfüllung von TCDP Nr. 7 ist regelmäßig ein System zum Management von Informationssicherheitsvorfällen erforderlich. Dabei sind Sicherheitsvorfälle auf etwaige Datenschutzverstöße zu überprüfen. Die Umsetzungshinweise (implementation guidance) von ISO/IEC 27018 Ziff. 16.1.1; ISO/IEC 27017 Ziff. 16.1.1, 16.1.2 und ISO/IEC 27002 Ziff. 16.1.1, 16.1.2 sind im Sinne unverbindlicher Hinweise anwendbar.

Die Organisation der Mitteilung durch den Cloud-Anbieter ist so zu wählen, dass der Cloud-Nutzer etwaigen Informationspflichten nach § 42a BDSG oder anderen Gesetzen nachkommen kann.

TCDP Nr. 8 – Mitteilungs- und Dokumentationspflicht bei Datenherausgabeverlangen

Anforderung

(1) Der Cloud-Anbieter teilt dem Cloud-Nutzer etwaige Verlangen auf Herausgabe von Daten, die für den Cloud-Anbieter rechtlich verbindlich sind, unverzüglich mit, soweit die Mitteilung rechtlich zulässig ist.

(2) Die Maßnahmen (controls) von ISO/IEC 27018 Ziff. A.5.2. sind im Sinne verbindlicher Anforderungen maßgeblich.

Umsetzungshinweis
Der Cloud-Anbieter kann ein Verfahren vorsehen und dies dokumentieren, wonach bei entsprechenden Anforderungen auf Datenherausgabe, etwa von Strafverfolgungsbehörden, die Zulässigkeit einer Mitteilung an den Cloud-Nutzer unverzüglich geprüft wird und, soweit diese zulässig ist, der Cloud-Nutzer unverzüglich informiert wird.

Die Umsetzungshinweise (implementation guidance) von ISO/IEC 27018 Ziff. A.5.2 sind im Sinne unverbindlicher Hinweise anwendbar.

TCDP Nr. 9 – Unterstützung der Kontrollen durch den Cloud-Nutzer

Anforderung
Der Cloud-Anbieter stellt durch geeignete Maßnahmen sicher, dass der Cloud-Nutzer sich von der Erfüllung der technischen und organisatorischen Anforderungen nach § 9 BDSG überzeugen und die im Cloud-Vertrag festgelegten Kontrollrechte (vgl. TCDP Nr. 1.9) wahrnehmen kann.

Erläuterung
Der Cloud-Nutzer ist nach § 11 BDSG gesetzlich verpflichtet, sich von der Erfüllung der technischen und organisatorischen Anforderungen durch den Cloud-Anbieter zu überzeugen. Zwar kann diese Anforderung durch Einsichtnahme in die Zertifizierung grundsätzlich erfüllt werden. Jedoch wird angenommen, dass dem Cloud-Nutzer, dessen ungeachtet, das Recht zur Überprüfung zustehen muss.

Umsetzungshinweis
Der Cloud-Anbieter kann ein Verfahren vorsehen und dies dokumentieren, durch das Anfragen des Cloud-Nutzers bearbeitet und die erforderliche Mitwirkung des Cloud-Anbieters gesichert ist. Dabei sollte vorgesehen werden, dem Cloud-Nutzer Informationen über die technischen und organisatorischen Maßnahmen zur Verfügung zu stellen, Fragen zu beantworten und eine Kontrolle vor Ort zu ermöglichen.

TCDP Nr. 10 – Rückgabe und Löschung von Daten

Anforderung
Der Cloud-Anbieter stellt durch geeignete Maßnahmen sicher, dass die Rückgabe überlassener Datenträger und die Löschung der beim Cloud-Anbieter gespeicherten Daten nach Beendigung des Auftrags nach Weisung des Cloud-Nutzers erfolgen [ISO/IEC 27018 Ziff. A.9.3].

Umsetzungshinweis
Der Cloud-Anbieter kann ein Verfahren vorsehen und dokumentieren, im Rahmen dessen die Herausgabe der Datenträger und die Löschung der Daten nach Beendigung des Auftrags geregelt werden. Der Cloud-Anbieter kann die Anforderung auch dadurch erfüllen, dass er dem Cloud-Nutzer die Löschung der Daten im Rahmen der Selbstverwaltung ermöglicht. Die Umsetzungshinweise (implementation guidance) von ISO/IEC 27018 Ziff. A.9.3 sind im Sinne unverbindlicher Hinweise anwendbar.

TCDP Nr. 11 – Datengeheimnis

Anforderung

Die Personen, die für den Cloud-Anbieter oder seine Unterauftragnehmer oder Unter-Unterauftragnehmer jedweder Stufe im Rahmen der Verarbeitung von Daten des Cloud-Nutzers tätig werden, sind vor Aufnahme ihrer Datenverarbeitungstätigkeit auf das Datengeheimnis nach § 5 BDSG oder nach anderen Gesetzen zu verpflichten. Die Vornahme der Verpflichtung ist zu dokumentieren. Ein organisatorisches Verfahren zur Vornahme der Verpflichtung ist einzurichten und zu dokumentieren.

Erläuterung

Die Verpflichtung auf das Datengeheimnis muss nicht notwendigerweise formeller Bestandteil des Arbeitsvertrags oder als Zusatz dazu gestaltet sein. Belehrung und Verpflichtung müssen vor Aufnahme der datenverarbeitenden Tätigkeit erfolgen.

Bei Beschäftigten von öffentlichen Stellen, die bereits gesetzlich auf das Datengeheimnis verpflichtet sind, ist eine Verpflichtung nicht erforderlich. Erforderlich ist jedoch eine Belehrung über das Datengeheimnis und seine Geltungsdauer.

Umsetzungshinweis

Mit der Verpflichtung bzw. Belehrung sollte eine Sensibilisierung der betroffenen Personen zu Fragen des Datenschutzes und der Datensicherheit in Bezug auf ihre Tätigkeit einhergehen. Den Personen sollte eine Ausfertigung des Verpflichtungstextes mitsamt relevanten Auszügen aus dem anwendbaren Datenschutzgesetz ausgehändigt werden (z.B. Wiedergabe der §§ 5, 43, 44 BDSG). Die Belehrung ist in angemessenen Abständen zu wiederholen, etwa im Zusammenhang mit Schulungen.

Die Dokumentation der Verpflichtung muss zumindest die Angabe enthalten, wer wann in welcher Weise und mit welchem Inhalt auf das Datengeheimnis verpflichtet bzw. darüber belehrt worden ist. Empfehlenswert ist es, eine von der Person unterzeichnete Ausfertigung der Verpflichtungserklärung aufzubewahren.

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

3. Technische und organisatorische Maßnahmen

TCDP Nr. 21 – Schutzkonzept

Anforderung
Der Cloud-Anbieter verfügt über ein risikoangemessenes Schutzkonzept hinsichtlich der für seinen Dienst und seine Datenverarbeitungsanlagen spezifischen Risiken. Das Schutzkonzept stellt auch die vom Cloud-Nutzer einzuhaltenden Sicherheitsheitsmaßnahmen fest. Es muss schriftlich dokumentiert sein und regelmäßig überprüft und aktualisiert werden. Soweit das Schutzkonzept Sicherheitsmaßnahmen des Cloud-Nutzers verlangt, sind diese dem Cloud-Nutzer in Textform mitzuteilen.

Erläuterung
Technische und organisatorische Schutzmaßnahmen müssen nach dem gesetzlichen Maßstab risikoangemessen sein. Die Ermittlung und Bewertung von Risiken und die Ableitung von angemessenen Schutzmaßnahmen liegen bei einer Auftragsdatenverarbeitung in der Regel in der Hand des Auftraggebers. Nach dem TCDP-Schutzklassenkonzept ermittelt der Cloud-Nutzer seinen Schutzbedarf und legt die Schutzbedarfsklasse fest. Dieser Schutzbedarfsklasse entspricht auf Seiten des Cloud-Anbieters die entsprechende Schutzanforderungsklasse. Das Schutzkonzept des Cloud-Nutzers und die von ihm vorgenommene Auswahl der Schutzbedarfsklasse werden im Rahmen von TCDP nicht geprüft.

Auch der Cloud-Anbieter muss über ein Schutzkonzept verfügen, in dem er seine spezifischen Risiken behandelt und dazu angemessene Schutzmaßnahmen festlegt. Solche Risiken können sich z.B. daraus ergeben, dass das Rechenzentrum in einem erdbebengefährdeten Gebiet steht und daher Maßnahmen gegen Erschütterungen zu treffen sind, oder dass über das Nachbargebäude leicht auf das Dach des Rechenzentrums gelangt werden kann und daher Schutzmaßnahmen gegen unbefugten Zutritt vom Dach aus zu treffen sind.

Hier werden nur Vorhandensein und Angemessenheit des Schutzkonzepts geprüft. Die Prüfung der Angemessenheit der einzelnen darin genannten technischen und organisatorischen Sicherheitsmaßnahmen und die Prüfung der Umsetzung dieser Maßnahmen erfolgen in den nachfolgenden Nummern des TCDP.

Umsetzungshinweise
Das Schutzkonzept soll die sich aus den spezifischen Umständen des Cloud-Dienstes, seiner Datenverarbeitungsanlagen und Räumlichkeiten ergebenden Risiken abdecken und zu jedem Risiko eine oder ggf. mehrere Schutzmaßnahmen beinhalten.

Die Umsetzungshinweise (implementation guidance) von ISO/IEC 27018 Ziff. 5.1.1; ISO/IEC 27017 Ziff. 5.1.1, CLD 6.3.1 und ISO/IEC 27002 Ziff. 5.1 sind im Sinne unverbindlicher Hinweise anwendbar.

TCDP Nr. 22 – Sicherheitsbereich und Zutrittskontrolle

Anforderung
Die Maßnahmen (controls) von ISO/IEC 27002 Ziff. 11.1 sind im Sinne verbindlicher Anforderungen maßgeblich.

Erläuterung
Der Schutz gegen Schädigung durch Naturereignisse wird vor allem im Rahmen des Schutzes gegen Datenverlust (Wiederherstellbarkeit) angesprochen. Er ist aber mittelbar auch für den Schutz gegen Zutritt Unbefugter erforderlich.

Umsetzungshinweis
Die Umsetzungshinweise (implementation guidance) von ISO/IEC 27002 Ziff. 11.1 sind im Sinne unverbindlicher Hinweise anwendbar.

Umsetzungshinweise zu den Schutzklassen

Schutzklasse 1
Der Cloud-Anbieter gewährleistet durch risikoangemessene technische und organisatorische Maßnahmen, dass Räume und Anlagen gegen Schädigung durch Naturereignisse gesichert werden und Unbefugte keinen Zutritt zu Räumen und Datenverarbeitungsanlagen erhalten.

Die Maßnahmen müssen geeignet sein, um im Regelfall den Zutritt Unbefugter 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.

Schutzklasse 2
Darüber hinaus gilt: Die Maßnahmen müssen auch geeignet sein, Schädigungen durch fahrlässige Handlungen Befugter im Regelfall auszuschließen. Gegen vorsätzlichen unbefugten Zutritt ist ein Schutz vorzusehen, der zu erwartende Zutrittsversuche hinreichend sicher ausschließt. Dazu gehört insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die ein unbefugter Zutritt im Regelfall (nachträglich) festgestellt werden kann.

Schutzklasse 3
Darüber hinaus gilt: Es muss sichergestellt sein, dass unbefugter Zutritt durch fahrlässige und vorsätzliche Handlungen hinreichend sicher ausgeschlossen ist. Dies schließt Schutz gegen Zutrittsversuche durch Täuschung oder Gewalt ein. Jeder Zutritt und jeder Zutrittsversuch müssen festgestellt werden können.

TCDP Nr. 23 – Logischer Zugang zu Datenverarbeitungsanlagen und Zugriff auf Daten

Erläuterung
Die in Nrn. 2 und 3 der Anlage zu § 9 Satz 1 BDSG genannten Anforderungen der Zugangs- und Zugriffskontrolle sind in der Praxis kaum zu trennen und werden etwa auch in ISO/IEC-Standards zusammengefasst. Diesem Ansatz folgt auch das TCDP. Bei Cloud-Diensten bestehen Pflichten in Bezug auf den Zugriff auf Daten sowohl auf Seiten des Cloud-Anbieters als auch auf Seiten des Cloud-Nutzers. TCDP adressiert ausschließlich die Pflichten auf Seiten des Cloud-Anbieters.

Anforderung

(1) Die Maßnahmen (controls) von ISO/IEC 27017 Ziff. CLD.9.5.1, CLD.13.1.4 und ISO/IEC 27002 Ziff. 9, 13.1.1 sind im Sinne verbindlicher Anforderungen maßgeblich.

(2) Die Anforderungen nach Absatz 1 gelten auch für Sicherungskopien sowie für Verbindungs- und Metadaten, soweit diese personenbezogene Daten enthalten.

Umsetzungshinweis

Die Umsetzungshinweis (implementation guidance) von ISO/IEC 27018 Ziff. 9.2, 9.2.1, 9.4.2; ISO/IEC 27017 Ziff. 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.4.1, 9.4.4, 13.1.3, CLD.9.5.1, CLD.13.1.4 und ISO/IEC 27002 Ziff. 6.1.5, 9, 13.1.1 sind im Sinne unverbindlicher Hinweise anwendbar.

Umsetzungshinweis zu den Schutzklassen

Schutzklasse 1

Der Cloud-Anbieter gewährleistet durch risikoangemessene technische und organisatorische Maßnahmen, dass Unbefugte keinen Zugang zu Datenverarbeitungsanlagen erhalten und auf personenbezogene Daten nicht zugreifen können. Die Maßnahmen müssen geeignet sein, um im Regelfall den Zugang zu Datenverarbeitungsanlagen und den Zugriff auf Daten durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert.

Schutzklasse 2

Darüber hinaus gilt: Gegen zu erwartenden vorsätzlichen unbefugten Zugang und Zugriff ist ein Schutz vorzusehen, der zu erwartende Zugangs- und Zugriffsversuche hinreichend sicher ausschließt. Dazu gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die ein unbefugter Zugang oder Zugriff im Regelfall (nachträglich) festgestellt werden kann.

Schutzklasse 3

Darüber hinaus gilt: Es muss sichergestellt sein, dass unbefugter Zugang zu Datenverarbeitungsanlagen und Zugriff auf Daten hinreichend sicher ausgeschlossen ist. Dies schließt regelmäßig Maßnahmen zur aktiven Erkennung von Angriffen ein. Jeder unbefugte Zugang sowie Zugriff und entsprechende Versuche müssen nachträglich festgestellt werden können. Regelmäßig ist der Einsatz eines Identity Access Management Systems oder eines gleichwertigen Systems zur zentralen Dokumentation und Verwaltung der Rollen und Rechte zum Zugang zu Daten erforderlich. Für Zugänge über das Internet ist eine starke Authentifizierung erforderlich, die mindestens zwei Elemente der Kategorien Wissen, Besitz oder Inhärenz verwendet, die insofern voneinander unabhängig sind, als die Überwindung eines Elements die Zuverlässigkeit des anderen nicht in Frage stellt, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten gewährleistet ist.

TCDP Nr. 24 – Übertragung und Speicherung von Daten

Anforderung
Der Cloud-Anbieter trifft Maßnahmen, die geeignet sind zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und durch die nachvollzogen werden kann, an welchen Empfängerkreis eine Übermittlung personenbezogener Daten vorgesehen ist. Außerdem muss eine Protokollierung der Übermittlungsvorgänge vorgesehen sein [ISO/IEC 27018 Ziff. A.10.4, A.10.5, A.10.6, A.10.9 und ISO/IEC 27002 Ziff. 8.3, 10, 12.4.1, 12.4.2, 12.4.3, 13].

Erläuterung
Die genannten Maßnahmen (controls) von ISO/IEC 27018 und ISO/IEC 27002 entsprechen inhaltlich jedenfalls im Wesentlichen den gesetzlichen Anforderungen von Nr. 4 der Anlage zu § 9 Satz 1 BDSG. TCDP ergänzt die ISO/IEC-Standards um Maßnahmen zur Vorabeingrenzung des Empfängerkreises und zur Protokollierung von Übermittlungen an Empfänger, die nicht zugleich Nutzer des Systems sind, da diese Maßnahmen in den ISO/IEC-Standards nicht ausdrücklich angesprochen werden.

Umsetzungshinweis
Die Umsetzungshinweise (implementation guidance) von ISO/IEC 27018 Ziff. 10.1.1, A.10.6, A.10.9; ISO/IEC 27017 Ziff. 13.1.3 und ISO/IEC 27002 Ziff. 8.3, 10, 12.4.1, 12.4.2, 12.4.3, 13 sind im Sinne unverbindlicher Hinweise anwendbar.

Umsetzungshinweis zu den Schutzklassen

Schutzklasse 1
Der Cloud-Anbieter gewährleistet durch risikoangemessene technische und organisatorische Maßnahmen, dass Unbefugte personenbezogene Daten bei der Weitergabe oder Speicherung nicht lesen, kopieren, verändern oder entfernen können.

Die Maßnahmen müssen geeignet sein, um im Regelfall solche Handlungen Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässiger Handlungen des Cloud-Nutzers oder Dritter auszuschließen. Die Maßnahmen müssen ferner geeignet sein, die fahrlässige Weitergabe von Daten an Unbefugte durch den Cloud-Anbieter und seine Mitarbeiter im Regelfall auszuschließen.

Dies betrifft auch den Transport von Datenträgern, auf denen sich Daten des Cloud-Nutzers befinden. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert. Es muss dokumentiert sein, an welche Empfänger eine Übertragung personenbezogener Daten vorgesehen ist. Datenübertragungen, auch solche an den Cloud-Nutzer oder an Unterauftragnehmer, müssen automatisiert protokolliert werden. Transport und Übergabe von Datenträgern sind zu dokumentieren. Diese Maßnahmen müssen sich auch auf die Übertragung von Daten im eigenen Netzwerk des Cloud-Anbieters und seiner Unterauftragnehmer und zwischen diesen beziehen.

Schutzklasse 2
Darüber hinaus gilt: Gegen vorsätzliches unbefugtes Lesen, Kopieren, Verändern oder Entfernen ist ein Schutz vorzusehen, der zu erwartende Versuche hinreichend sicher aus-

schließt. Dazu gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen im Regelfall (nachträglich) festgestellt werden kann. Bei verschlüsselter Speicherung und Übertragung ist durch technische und organisatorische Maßnahmen sicherzustellen, dass der Cloud-Anbieter keinen Zugriff auf die Schlüssel hat, die ihm das Lesen von personenbezogenen Daten ermöglichen.

Schutzklasse 3
Darüber hinaus gilt: Es muss sichergestellt sein, dass unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Daten durch den Cloud-Anbieter, seine Mitarbeiter oder Dritte hinreichend sicher ausgeschlossen ist. Dies schließt regelmäßig Maßnahmen zur aktiven Erkennung und Abwehr von Angriffen ein. Jedes unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten und möglichst auch jeder entsprechende Versuch müssen nachträglich festgestellt werden können.

TCDP Nr. 25 – Nachvollziehbarkeit der Datenverarbeitung

Anforderung

(1) Die Maßnahmen (controls) von ISO/IEC 27002 Ziff. 12.4 sind im Sinne verbindlicher Anforderungen maßgeblich. Bei Protokollierungen sind die Grundsätze der Erforderlichkeit, Zweckbindung und Datensparsamkeit zu beachten.

(2) Der Cloud-Anbieter erstellt ein Protokollierungskonzept, in dem insbesondere Gegenstand und Umfang der Protokollierung, Aufbewahrung, Integritätsschutz und Löschung von Protokollen, die Verwendung der Protokolldaten sowie die Wahrung der Datenschutzziele im Rahmen der Protokollierung dokumentiert sind.

Erläuterung

Da im Rahmen von Protokollierungen regelmäßig personenbezogene Daten anfallen, unterliegt der Umgang mit Protokollierungsdaten seinerseits dem Datenschutzrecht. Zur Verdeutlichung nimmt TCDP Nr. 25 die Pflicht zur Wahrung der datenschutzrechtlichen Grundsätze ausdrücklich auf.

Umsetzungshinweis

Die Umsetzungshinweise (implementation guidance) von ISO/IEC 27018 Ziff. 12.4.1, 12.4.2; ISO/IEC 27017 Ziff. 12.4.1, 12.4.4 und ISO/IEC 27002 Ziff. 12.4 sind im Sinne unverbindlicher Hinweise anwendbar.

Umsetzungshinweis zu den Schutzklassen

Schutzklasse 1
Der Cloud-Anbieter gewährleistet durch risikoangemessene technische und organisatorische Maßnahmen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die Maßnahmen müssen geeignet sein, um Dateneingaben, -veränderungen und -löschungen, die bei der bestimmungsgemäßen Nutzung des Dienstes durch den Cloud-Nutzer so-

wie bei administrativen Maßnahmen des Cloud-Anbieters erfolgen, jederzeit nachvollziehen zu können.

Die dafür eingesetzten Maßnahmen, etwa Protokollierung der administrativen Aktivitäten und der Nutzer-Aktivitäten, müssen so gestaltet sein, dass die Nachvollziehbarkeit von Eingaben, Veränderungen und Löschungen im Regelfall auch bei technischen oder organisatorischen Fehlern, einschließlich Bedienfehlern, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässigen Handlungen des Cloud-Nutzers oder Dritter gewahrt bleibt. Gegen vorsätzliche Manipulationen an den Maßnahmen zur Nachvollziehbarkeit ist ein Mindestschutz vorzusehen, der diese Manipulationen erschwert.

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

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

TCDP Nr. 26 – Auftragskontrolle

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

Erläuterung
Der Cloud-Anbieter darf nach den gesetzlichen Vorgaben Daten nur nach Weisung des Cloud-Nutzers verarbeiten. Die Bindung an die Weisungen ist vertraglich zu vereinbaren (vgl. TCDP Nr. 1.11). Der Cloud-Anbieter muss weiterhin sicherstellen, dass eine Datenverarbeitung nur aufgrund einer solchen Vereinbarung erfolgt (vgl. TCDP Nr. 2). Schließlich muss die Befolgung der Weisungen durch organisatorische und technische Maßnahmen abgesichert werden. Dies ist Gegenstand von TCDP Nr. 26. Weitgehend üblich und zulässig ist es, wenn Weisungen des Cloud-Nutzers in Form von Software-Befehlen erteilt werden, die seitens des Cloud-Anbieters automatisch ausgeführt werden.

Umsetzungshinweis
Allgemeine Umsetzungshinweise zu TCDP Nr. 26 werden nicht gegeben. Es gelten die Umsetzungshinweise zu den Schutzklassen.

Umsetzungshinweis zu den Schutzklassen

Schutzklasse 1
Der Cloud-Anbieter gewährleistet durch risikoangemessene technische und organisatorische Maßnahmen, dass die Verarbeitung der Daten des Cloud-Nutzers nur nach Maßgabe von dessen Weisungen erfolgt.

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

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

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

TCDP Nr. 27 – Getrennte Verarbeitung

Anforderung
Der Cloud-Anbieter gewährleistet durch geeignete Maßnahmen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Umsetzungshinweis
Allgemeine Umsetzungshinweise zu TCDP Nr. 27 werden nicht gegeben. Es gelten die Umsetzungshinweise zu den Schutzklassen.

Umsetzungshinweis zu den Schutzklassen

Schutzklasse 1
Der Cloud-Anbieter gewährleistet durch risikoangemessene technische und organisatorische Maßnahmen, dass die Daten des Cloud-Nutzers von den Datenbeständen anderer Cloud-Nutzer und von den anderen Datenbeständen des Cloud-Anbieters getrennt verarbeitet werden und dass der Cloud-Nutzer die Datenverarbeitung nach verschiedenen Verarbeitungszwecken trennen kann. Dazu gehören etwa die anwendungsseitige Trennung verschiedener Mandanten und die Mandantenfähigkeit der Anwendungsprogramme. Die Maßnahmen müssen so gestaltet sein, dass die Datentrennung im Regelfall auch bei technischen oder organisatorischen Fehlern, einschließlich Bedienfehlern, des Cloud-Anbieters oder seiner Mitarbeiter oder fahrlässigen Handlungen des Cloud-Nutzers oder Dritter gewahrt bleibt. Es ist ein Mindestschutz vorzusehen, der vorsätzliche Verstöße gegen das

Trennungsgebot erschwert.

Schutzklasse 2
Darüber hinaus gilt: Gegen zu erwartende vorsätzliche Verstöße ist ein Schutz vorzusehen, der diese hinreichend sicher ausschließt. Dazu gehören im Rahmen von Datenspeicherung die Verschlüsselung mit getrennten Schlüsseln und die Verwendung getrennter Betriebsumgebungen für verschiedene Verarbeitungen oder der Einsatz gleichwertiger Verfahren. Weiterhin sind Maßnahmen zu ergreifen, durch die vorsätzliche Verstöße gegen das Trennungsgebot im Regelfall (nachträglich) festgestellt werden können, beispielsweise durch Protokollierung der Zugriffe.

Schutzklasse 3
Darüber hinaus gilt: Es muss sichergestellt sein, dass eine Verletzung der Datentrennung hinreichend sicher ausgeschlossen ist. Dazu gehören im Rahmen von Datenspeicherung die Verschlüsselung mit getrennten Schlüsseln und die Verwendung getrennter Betriebsumgebungen für verschiedene Verarbeitungen. Es muss zudem ein Verfahren zur Erkennung von Missbräuchen geben.

TCDP Nr. 28 – Kryptographie

Anforderung
Soweit der Cloud-Anbieter kryptographische Verfahren einsetzt, sind die Maßnahmen (controls) von ISO/IEC 27002 Ziff. 10 im Sinne verbindlicher Anforderungen maßgeblich.

Umsetzungshinweis
Die Umsetzungshinweise (implementation guidance) von ISO/IEC 27018 Ziff. 10.1.1 und ISO/IEC 27002 Ziff. 10 sind im Sinne unverbindlicher Hinweise anwendbar.

Umsetzungshinweis zu den Schutzklassen

Schutzklasse 1
Der Cloud-Anbieter gewährleistet, dass die technische Entwicklung im Bereich der Kryptographie verfolgt wird und dass die von ihm getroffenen Maßnahmen den aktuellen technischen Anforderungen (Eignung der Maßnahmen) entsprechen. Dabei ist die angemessene Implementierung der Maßnahmen durch geeignete Tests zu überprüfen und zu dokumentieren.

Schutzklasse 2
Der Cloud-Anbieter gewährleistet, dass die technische Entwicklung im Bereich der Kryptographie laufend verfolgt wird und dass die von ihm getroffenen Maßnahmen den aktuellen technischen Empfehlungen (best practice) entsprechen. Dabei ist die angemessene Implementierung der Maßnahmen durch geeignete Tests zu überprüfen und zu dokumentieren.

Schutzklasse 3
Der Cloud-Anbieter gewährleistet, dass die technische Entwicklung im Bereich der Kryptographie laufend verfolgt wird und dass die von ihm getroffenen Maßnahmen den aktuellen technischen Empfehlungen (best practice) entsprechen. Dabei ist die angemessene Imple-

mentierung der Maßnahmen durch unabhängige, sachkundige Stellen zu überprüfen. Die Prüfung einschließlich des Ergebnisses ist zu dokumentieren.

4. Wiederherstellbarkeit

TCDP Nr. 31 – Schutz gegen zufällige Zerstörung oder Verlust (Wiederherstellbarkeit)

Erläuterung
Die Anforderungen an die Wiederherstellbarkeit von Daten werden nicht durch die Schutzklassen 1 bis 3, sondern durch die separaten Wiederherstellbarkeitsniveaus „normale Wiederherstellbarkeit“, „hohe Wiederherstellbarkeit“ und „sehr hohe Wiederherstellbarkeit“ ausgedrückt.

Der Wiederherstellbarkeitsschutz des TCDP zielt auf die Wiederherstellbarkeit der im Cloud-Dienst verarbeiteten Daten im Falle von ungewollter Zerstörung oder Verlust auf Seiten des Cloud-Anbieters ab. Der Wiederherstellbarkeitsschutz betrifft nicht die Verfügbarkeit des Dienstes, die typischerweise in einem Service Level Agreement (SLA) zwischen Cloud-Anbieter und Cloud-Nutzer geregelt ist.

Anforderung

(1) Der Cloud-Anbieter verfügt über ein Konzept zur Gewährleistung der Wiederherstellbarkeit der Daten und stellt es dem Cloud-Nutzer auf Anfrage zur Verfügung.

(2) Der Cloud-Anbieter macht im Cloud-Vertrag Angaben zur maximalen Datenwiederherstellungszeit.

(3) Der Cloud-Anbieter gewährleistet durch risikoangemessene Maßnahmen, dass die Daten innerhalb der im Cloud-Vertrag angegebenen Zeit wiederhergestellt werden können. Die Maßnahmen (controls) von ISO/IEC 27002 Ziff. 11.1.4, 11.2.1, 11.2.2, 11.2.4, 12.1, 12.2, 12.3, 12.6, 12.7 sind im Sinne verbindlicher Anforderungen maßgeblich.

Umsetzungshinweis
Die Umsetzungshinweise (implementation guidance) von ISO/IEC 27018 Ziff. 12.3.1; ISO/IEC 27017 Ziff. 12.1.3, 12.3.1 und ISO/IEC 27002 Ziff. 11.1.4, 11.2.1, 11.2.2, 11.2.4, 11.2.6, 12.1., 12.2, 12.3, 12.6, 12.7 und 17.2 sind im Sinne unverbindlicher Hinweise anwendbar.

Umsetzungshinweis zu Wiederherstellbarkeitsniveaus

Normale Wiederherstellbarkeit
Es ist ein Schutz zu gewährleisten, der gegen zu erwartende, naheliegende Ereignisse so zuverlässig absichert, dass diese Risiken bei normalem Verlauf nicht zu endgültigem Datenverlust führen.

Hohe Wiederherstellbarkeit
Es ist ein Schutz zu gewährleisten, der gegen seltene Ereignisse so zuverlässig absichert, dass diese Risiken bei normalem Verlauf nicht zu endgültigem Datenverlust führen.

Sehr hohe Wiederherstellbarkeit
Es ist ein Schutz zu gewährleisten, der außergewöhnliche, aber nicht als theoretisch auszuschließende Ereignisse so zuverlässig absichert, dass diese Risiken bei normalem Verlauf nicht zu endgültigem Datenverlust führen.

Als Ereignisse gelten Naturereignisse (z.B. Witterung, Wetterlage, Sturm, Hochwasser), Störungen der Infrastruktur (z.B. Strom, Klimatisierung), Betriebsstörungen, Bedienungsfehler oder fahrlässige oder vorsätzliche Eingriffe.

Erläuterung

„Zu erwarten, naheliegend“ sind Ereignisse, die nicht vorkommen sollen, nach der Lebenserfahrung aber trotz hinreichender Vorsicht nicht ausgeschlossen werden können und „immer wieder einmal“ vorkommen, wie etwa Unfälle im Straßenverkehr.

„Selten“ sind Ereignisse, die nicht vorkommen sollen und nach der Lebenserfahrung bei hinreichender Vorsicht „praktisch nie“ vorkommen, aber gleichwohl in einigen Fällen zu beobachten sind, wie etwa „Jahrhunderthochwasser“.

„Außergewöhnlich, aber nicht als theoretisch auszuschließen“ sind Ereignisse, die nicht vorkommen sollen und nach der Lebenserfahrung nicht auftreten, aber gleichwohl in extrem seltenen Einzelfällen zu beobachten sind, wie etwa „Black Swan“-Ereignisse.

Referenzen

1 Siehe zur AG „Rechtsrahmen des Cloud Computing“ http://www.digitale-technologien.de/DT/Navigation/DE/Foerderprogramme/Trusted_Cloud/Rechtliche_Fragen/rechtliche-fragen.html.

2 Thesenpapier „Datenschutzrechtliche Lösungen für Cloud Computing“, abrufbar unter http://www.tcdp.de/index.php/start.

3 Arbeitspapier „Modulare Zertifizierung von Cloud-Diensten“, abrufbar unter http://www.tcdp.de/index.php/start.

4 Thesenpapier „Eckpunkte eines Zertifizierungsverfahrens für Cloud-Dienste“, abrufbar unter www.tcdp.de.

5 ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

6 ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements.

7 ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls.

8 ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud service.

9 Siehe weitere Informationen zum Pilotprojekt unter http://www.tcdp.de/index.php/pilotprojekt.

10 Arbeitspapier „Schutzklassen in der Datenschutz-Zertifizierung“, abrufbar unter http://www.tcdp.de/index.php/start.

11 Arbeitspapier „Schutzklassen in der Datenschutz-Zertifizierung“, abrufbar unter http://www.tcdp.de/index.php/start.

12 TCDP-Schutzklassenkonzept für die Datenschutz-Zertifizierung von Cloud-Diensten 1.0, September 2016, abrufbar unter http://www.tcdp.de/index.php/start.