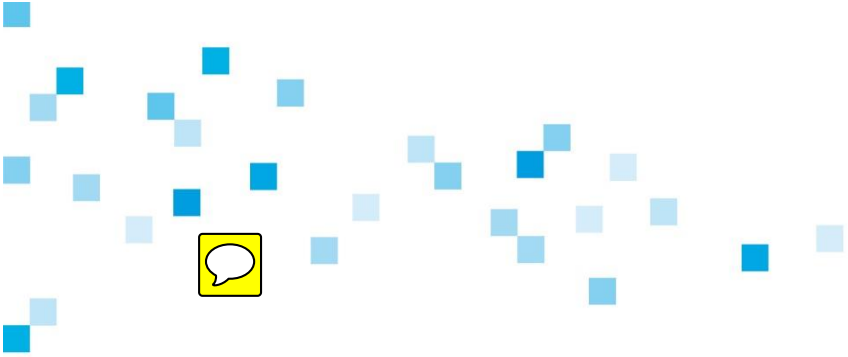

Trusted Cloud

Kompetenzzentrum Trusted Cloud 13. April 2015

Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP) – Version 0.9

Gliederung

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. Diese Eckpunkte der Datenschutz-Zertifizierung, die zur Abgrenzung von anderen Formen der Zertifizierung auch als „Compliance-Zertifizierung“ bezeichnet wird, sollten gesetzlich geregelt sein.

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“[i] im Rahmen der Begleitforschung des Programms „Trusted Cloud“ erarbeitet hat.[ii] 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 sind,[iii] und eine Zertifizierung nach den Grundsätzen, die das Papier „Eckpunkte eines Zertifizierungsverfahrens für Cloud-Dienste“ [iv] des Pilotprojekts „Datenschutz-Zertifizierung für Cloud-Dienste“ beschreibt.

Das TCDP setzt die gesetzlichen Anforderungen des BDSG an die Auftragsdatenverarbeitung um und konkretisiert diese zu prüffähigen Normen. Es baut auf dem ISO/IEC-Standard 27018[v] auf, der die international anerkannten ISO/IEC-Standards 27001[vi] und 27002[vii] um Cloud- und insbesondere datenschutzspezifische Anforderungen erweitert.

Das TCDP bezieht die Normen von ISO/IEC 27018 und ISO/IEC 27002 durch Verweisung ein, soweit die ISO-Normen geeignet sind, die gesetzlichen Anforderungen des BDSG zu konkretisieren. Das TCPD modifiziert und ergänzt die ISO-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 Kompetenzzentrums Trusted Cloud im Auftrag des Bundesministeriums für Wirtschaft und Energie entwickelt. Es steht derzeit als „Betaversion" zur Verfügung und wird als TCDP – v.0.9 zitiert. Es wird ab Sommer 2015 im Auftrag des BMWi in einem Projekt zur praktischen Umsetzung der Datenschutz-Zertifizierung durch Pilot-Zertifizierungen getestet und weiterentwickelt. Das TCDP soll im ersten Halbjahr 2016 als Endversion zur Verfügung stehen.

Das TCDP ist ein Prüfstandard, der zur Verwendung für jedermann freigegeben ist. Insbesondere können Zertifikate auf der Grundlage des TCDP erteilt werden. Das TCDP geht dabei von einer Zertifizierung nach den Grundsätzen aus, die im Papier „Eckpunkte eines Zertifizierungsverfahrens für Cloud-Dienste" beschrieben sind. Voraussetzung ist in jedem Fall, dass das TCDP unverändert und vollständig verwendet wird. Die Verwaltung und Weiterentwicklung des TCDP behält sich der Herausgeber vor.

Das TCDP wurde im Rahmen des Technologieprogramms „Trusted Cloud" entwickelt und setzt den Fokus auf die Datenschutz-Zertifizierung für Cloud-Dienste. Die Normen können jedoch, da sie die allgemeinen gesetzlichen Anforderungen an die Auftragsdatenverarbeitung umsetzen, für jede Art von Auftragsdatenverarbeitung verwendet werden.

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. Das TCDP, das derzeit das Bundesdatenschutzgesetz umsetzt, kann nach Erlass der europäischen Datenschutz-Grundverordnung an diese angepasst werden.

II. Aufbau und Benutzung des TCDP

1. Die Textkategorien des TCDP

Das TCDP unterscheidet, ähnlich wie ISO/IEC 27018 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 Controls von ISO/IEC 27018 oder ISO/IEC 27002 als „maßgeblich“ bezeichnen, werden jene Controls zu Anforderungen des TCDP, müssen also erfüllt sein. Soweit ein ISO/IEC-Control nicht verpflichtend formuliert ist (engl. „should“ oder dt. „soll“), ist dies zunächst auch im Rahmen des TCDP als nicht verpflichtende Anforderung zu verstehen.

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-verpflichtende Anforderungen (Controls) formulieren („should“), muss bei Verweisungen des TCDP auf ISO/IEC-Controls eine Veränderung zu verpflichtenden Anforderungen erfolgen. Insoweit verwendet das TCDP zwei unterschiedliche Vorgehensweisen. Teilweise verweisen TCDP-Normen auf ISO/IEC-Controls 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-Controls. In einigen Fällen ist auch die Übereinstimmung der ISO/IEC-Control mit den Anforderungen des BDSG fraglich oder anhand des Wortlauts nicht offensichtlich. Durch die eigenständige Fassung der Anforderung und den Verweis auf ISO/IEC-Controls 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[viii] ausgerichtet. Fehlt in einer TCDP-Norm eine solche Einteilung nach Schutzklassen, bedeutet dies, dass die Umsetzungshinweise gleichermaßen für alle Schutzklassen gelten. Soweit die Umsetzungshinweise nach Schutzklassen differenzieren, beziehen die Umsetzungshinweise der jeweiligen Schutzklasse die Umsetzungshinweise der niedrigeren Schutzklasse(n) sein, soweit diese nicht widersprechend sind.

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

Die Umsetzungshinweise sind zur Verringerung der Textmasse teilweise tabellarisch aufgebaut und in Stichpunkten wiedergegeben, insbesondere bei den umfangreichen Hinweisen zu den technischen und organisatorischen Maßnahmen im dritten Abschnitt (TCDP Nr. 21 ff.). Im Rahmen der tabellarischen Darstellung erfolgt auch die Einbeziehung der Umsetzungsempfehlungen der ISO-Normen tabellarisch. Die Einbeziehung wird durch Fettdruck der jeweiligen ISO-Umsetzungsempfehlungen kenntlich gemacht.

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

2. Verwendung und Zitierweise des ISO-Standards

Die Anwendung des TCDP setzt wegen der Verweise auf ISO/IEC 27018 und auf ISO/IEC 27002 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 2700x-Familie 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) zitiert, die in den Referenzen genannt ist. Zur besseren Lesbarkeit des TCDP werden im Text die Standards kurz als „ISO/IEC 27018" bzw. „ISO/IEC 27002" zitiert.

ISO/IEC 27018 baut auf ISO/IEC 27001 und ISO/IEC 27002 auf und verweist häufig auf Controls von ISO/IEC 27002. Das TCDP verweist in diesen Fällen, soweit möglich,[1] sowohl auf die verweisende Control von ISO/IEC 27018 als auch auf die maßgebliche Control von ISO/IEC 27002.

[1] In einigen Fällen ist der Verweis von ISO/IEC 27018 auf ISO/IEC 27002 wegen der unterschiedlichen Systematik weniger präzise als nach TCDP. In diesem Fall wird der Verweis in ISO/IEC 27018 im TCDP nicht genannt. Beispiel: TCDP Nr. 23 (Transport von Daten) verweist auf ISO/IEC 27002 Ziff. 8.2. Der Verweis von ISO/IEC 27018 Ziff. 8 auf ISO7IEC 27002 Ziff. 8 ist wesentlich umfassender und wird daher in TCDP Nr. 23 nicht eigens genannt.

III. Normentabelle

BDSG Norm	Inhalt der Norm	Kurzbeschreibung	TCDP Nummer
§ 11	**Anforderungen an den Vertrag**	**Erfüllung der gesetzlichen Anforderungen an den Vertrag**	1
§ 11 Abs. 2 S. 2	Diensteerbringung aufgrund Vertrags	Diensteerbringung nur aufgrund ADV-Vertrags	1.1
§ 11 Abs. 2 S. 2	Form des Vertrags	Vertrag bedarf der Schriftform	1.2
§ 11 Abs. 2 S. 2 Nr. 1	Auftragsgegenstand u. -dauer	Gegenstand und Dauer des Auftrags sind festzulegen	1.3
§ 11 Abs. 2 S. 2 Nr. 2	Umfang / Art / Zweck / Kreis Betroffener	Umfang/Art/Zweck der Erhebung, Verarbeitung, Nutzung und Kreis Betroffener sind festzulegen	1.4
§ 11 Abs. 2 S. 2 Nr. 3	Technische und organisatorische Maßnahmen	Die nach § 9 BDSG zu treffenden Maßnahmen sind festzulegen	1.5
§ 11 Abs. 2 S. 2 Nr. 4	Berichtigung/Löschung/Sperrung	Vorgaben zur Berichtigung, Löschung und Sperrung von Daten auf Weisung AG sind festzulegen	1.6
§ 11 Abs. 2 S. 2 Nr. 5	Pflichten des AN	Pflichten des AN insbesondere Kontrollen sind festzulegen	1.7
§ 11 Abs. 2 S. 2 Nr. 6	Unterauftragnehmer	Ob der AN Unterauftragnehmer beauftragen darf, ist festzulegen	1.8
§ 11 Abs. 2 S. 2 Nr. 7	Rechte des AG u. Pflichten des AN	Kontrollrechte des AG u. Duldungs- und Mitwirkungspflichten des AN sind festzulegen	1.9
§ 11 Abs. 2 S. 2 Nr. 8	Mitteilung von Verstößen	Welche Verstöße gegen Vorschriften oder vertragliche Festlegungen mitzuteilen sind, ist festzulegen	1.10
§ 11 Abs. 2 S. 2 Nr. 9	Weisungsbefugnisse des AG	Die Weisungsbefugnisse des AG gegenüber dem AN sind festzulegen	1.11
§ 11 Abs. 2 S. 2 Nr. 10	Rückgabepflichten	Die Rückgabe von Datenträgern und 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 Abs. 3 S. 1	Weisungsgebundenheit	Keine Erhebung / Verarbeitung / Nutzung von Daten außerhalb der AG-Weisungen	2

BDSG Norm	Inhalt der Norm	Kurzbeschreibung	TCDP Nummer
§ 11 Abs. 3 S. 2	Mitteilungspflicht	Hinweispflicht des AN, wenn AG-Weisung gegen BDSG oder andere DS-Vorschriften verstößt	3
§ 11 Abs. 2 S. 2 Nr. 6	Unterauftragnehmer (materiell)	AN muss ordnungsgemäße Einschaltung von Subunternehmern nachweisen	4
§ 11 Abs. 4	Betrieblicher Datenschutzbeauftragter und gesetzliche Anforderungen	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	5
§ 11 Abs. 2 S.2 Nr. 4	Berichtigung, Sperrung und Löschung von Daten	Das Berichtigen, Sperren und Löschen von Daten ist zu ermöglichen	6
§ 11 Abs. 2 S. 2 Nr. 8	Mitteilungspflicht	Verstöße gegen gesetzliche oder vertragliche Vorschriften sind mitzuteilen	7
§ 11 Abs. 2 S. 2	Kontrollrechte AG / Duldungs- und Mitwirkungspflichten AN	AN muss Prozesse für Kundenaudits vorhalten	8
§ 11 Abs. 2 S. 2 Nr. 10	Rückgabepflichten	AN muss Rückgabeprozesse nachweisen	9
§ 5	Datengeheimnis	AN muss Mitarbeiter auf Datengeheimnis verpflichten	10
§ 9 i.V.m. Anlage	**Technisch-organisatorische Sicherheit des Cloud-Dienstes**	**Gewährleistung der Sicherheit der Datenverarbeitung**	
S. 2 Nr. 1 Anlage zu § 9	Zutrittskontrolle	Verwehrung des Zutritts Unbefugter zu DV-Anlagen	21
S. 2 Nr. 2 Anlage zu § 9	Zugangskontrolle	Verhinderung des Zugangs Unbefugter zu DV-Systemen	22
S. 2 Nr. 3 Anlage zu § 9	Zugriffskontrolle	Gewährleistung, dass Berechtigte nur auf eigenen Datenbereich Zugriff haben	22
S. 2 Nr. 4 Anlage zu § 9	Weitergabekontrolle	Schutz der Daten während Transport, Speicherung und Übermittlung gegen Zugriff Unbefugter	23
S. 2 Nr. 5 Anlage zu § 9	Eingabekontrolle	Gewährleistung, dass Nutzer die personenbezogene Daten eingeben, verändern oder entfernen nachträglich ermittelbar sind	24

BDSG Norm	Inhalt der Norm	Kurzbeschreibung	TCDP Nummer
S. 2 Nr. 6 Anlage zu § 9	Auftragskontrolle	Gewährleistung, dass personenbezogene Daten nur im Rahmen der AG-Weisungen verarbeitet werden können	25
S. 2 Nr. 7 Anlage zu § 9	Verfügbarkeitskontrolle	Gewährleistung, dass personenbezogene Daten nicht zufällig zerstört werden oder verloren gehen	26
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

IV. Anforderungen und Umsetzungsempfehlungen

1. Vertragliche Regelung der Auftragsdatenverarbeitung

TCDP Nr. 1 – Vertragliche Grundlage

Der Cloud-Anbieter muss darauf hinwirken, dass er seine Leistung dem Cloud-Nutzer aufgrund eines Vertrags 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. 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 geschlossenen 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 Daten 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

Anforderung
1. Die nach TCDP Nr. 21 – 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.

Umsetzungshinweis
Die Festlegung kann in einer Anlage zum Vertrag erfolgen. Angaben zur Umsetzung der TCDP Nr. 21 – 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 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 auf den Cloud-Anbieter nach § 11 Abs. 4 BDSG anwendbaren datenschutzrechtlichen Normen genannt.

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, müssen aber nicht im Vertrag konkret bezeichnet werden.

TCDP Nr. 1.9 – Kontrollrechte des Cloud-Nutzers

Anforderung
Die Kontrollrechte des Cloud-Nutzers (TCDP Nr. 8) und die entsprechenden Duldungs- und Mitwirkungspflichten des Cloud-Anbieters werden im Cloud-Vertrag festgelegt.

TCDP Nr. 1.10 – Mitteilung bei Verstößen

Anforderung
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.

Umsetzungshinweis
Im Cloud-Vertrag muss als Mindesterfordernis die Verpflichtung zur unverzüglichen Mitteilung von Datenschutzverstößen 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, 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. 9) festgelegt.

Umsetzungshinweis

Im Cloud-Vertrag sollten zumindest die in TCDP Nr. 9 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, 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. 25 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 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, mittels dessen Mitarbeiter des Cloud-Anbieters Weisungen, die zu einer Verarbeitung führen, die von den für den jeweiligen Dienst üblichen oder erwartbaren Verarbeitung abweichen, oder auf sonstige Weise Anlass zu Zweifeln geben, überprüft und bei fortbestehenden Zweifeln 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
1. 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 Computing-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, insb. 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 Unter-Auftragsdatenverarbeitungsvertrag tätig werden.
2. Der Cloud-Anbieter verpflichtet seine Unterauftragnehmer, sicherzustellen dass ihre Unter-Unterauftragnehmer nicht ohne wirksamen Unter-Auftragsdatenverarbeitungsvertrag 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 Unter-Auftragsdatenverarbeitungsvertrags zwischen Cloud-Anbieter und Unterauftragnehmer überprüft wurde.

Die Anforderung nach Abs. 2 kann etwa dadurch erfüllt werden, dass diese Verpflichtung in den Unter-Auftragsdatenverarbeitungsvertrag 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.

Umsetzungshinweis

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

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 Unter-Auftragnehmern und dessen Unter-Unterauftragnehmern 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 umsetzen, 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 Unter-Auftragsdatenverarbeitungsvertrag 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 – Betrieblicher 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 §§ 43, 44 BDSG sind als Ordnungswidrigkeit- bzw. Straftatbestände nicht zertifizierungsrelevant, ebenso § 38 BDSG (Aufsichtsbehörde) bzw. §§ 24-26 BDSG (Bundesbeauftragter für Datenschutz und Informationsfreiheit) bzw. die entsprechenden Vorschriften der Landesdatenschutzgesetze. 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. 10 umgesetzt.

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 Cloud-Anbieter vorgenommen wird, um die Erfüllung der Anforderungen bezüglich der Zuverlässigkeit (insb. im Hinblick auf mögliche Interessenkonflikte) und das Vorliegen der erforderlichen 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.

Umsetzungshinweis

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

Schutzklasse	Umsetzungsempfehlungen
I, II, III	- Dokumentation der für den jeweiligen Cloud-Dienst eingesetzten Systeme, Verfahren und Prozesse (Software, Hardware, beteiligte Organisationseinheiten, Rollen und Dienstleister). - Exakte Beschreibung der Gesamtheit der getroffenen technischen und organisatorischen Maßnahmen (z.B. in einem Datenschutzkonzept). - Wirksame Bestellung eines Datenschutzbeauftragten (DSB): o 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, o Schriftliche, beiderseitig unterzeichnete Bestellurkunde, o Nachweis erforderlicher Weisungsfreiheit des DSB. Soweit ein externer DSB bestellt wird, ist ggfs. auch der Nachweis der Weisungsfreiheit gegenüber seinem Arbeitgeber erforderlich, o 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, o unmittelbare organisatorische Unterstellung des Datenschutzbeauftragten dem Leiter des Cloud Anbieters. - Angemessene Einbindung des DSB und des Beauftragten für IT-/Informationssicherheit in die Organisation des Cloud-Anbieters. - Dem Schutzbedarf und der Anzahl der Auftraggeber angemessene Zeitressource für den DSB (ggf. Unterstützung durch die Datenschutz-Koordinatoren). - Jährliche Planung und Zuweisung von Budgets für die Tätigkeiten des DSB (z.B. für den Zugriff auf externen Sachverstand, Weiterbildung). - Regelmäßige, z.B. vierteljährlich stattfindende interne Audits und Berichterstattung durch den DSB.

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, 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

Der Cloud-Anbieter sollte ein Verfahren vorsehen und dokumentieren, im Rahmen dessen die Berichtigung, Löschung und Sperrung von Daten sowie die Unterstützung des Auftraggebers bei der Auskunftserteilung geregelt wird. Der Cloud-Anbieter kann die Anforderung z.B. dadurch erfüllen, dass er dem Cloud-Nutzer die für die Auskunftserteilung relevanten Daten auf Anforderung bereitstellt und dem Cloud-Nutzer die Berichtigung, Löschung und Sperrung im Rahmen der Selbstverwaltung ermöglicht.

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.

Umsetzungshinweis

Schutzklasse	**Umsetzungsempfehlungen**
I	- **ISO/IEC 27018 Ziff. A.9.1** - Festlegung der Verantwortlichkeiten und Zuständigkeiten für die Prüfung der Mitteilungspflicht. - Kontaktstelle mit angemessener Erreichbarkeit. - Beschreibung und Implementierung des Verfahrens zur Meldung von Vorfällen und für die Mitteilung von Datenschutz- und Sicherheitsverstößen an den Auftraggeber. - Dokumentation von gemeldeten Verstößen und an den Auftraggeber erfolgten Mitteilungen.
II, III	- Beschreibung und Implementierung des Verfahrens zur Mitteilung von Datenschutzvorfällen an den Auftraggeber zur Umsetzung der Verpflichtung gemäß § 42a BDSG.

TCDP Nr. 8 – 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. 9 – 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 nach Beendigung des Auftrags geregelt wird. Der Cloud-Anbieter kann die Anforderung auch dadurch erfüllen, dass er dem Cloud-Nutzer die Löschung der Daten im Rahmen der Selbstverwaltung ermöglicht.

TCDP Nr. 10 – Datengeheimnis

Anforderung

Die Controls von ISO/IEC 27018 Ziff. A.10.1. und 7.2.2 und ISO/IEC 27002 Ziff. 7.2.1 und 7.2.2 sind im Sinne verbindlicher Anforderungen maßgeblich.

Umsetzungshinweis

Schutzklasse	Umsetzungsempfehlungen
I, II, III	- **ISO/IEC 27018 Ziff. A.10.1** - **ISO/IEC 27002 Ziff. 7.1.2** - **ISO/IEC 27002 Ziff. 7.2.2** **Anmerkungen** Die Verpflichtung auf das Datengeheimnis muss nicht notwendigerweise formeller Bestandteil des Arbeitsvertrags oder als Zusatz dazu gestaltet sein. Belehrung und Verpflichtung sind nicht schon bei Begründung des Beschäftigungsverhältnisses zwingend, sondern müssen erst bei Aufnahme der datenverarbeitenden Tätigkeit erfolgen.

3. Technische und organisatorische Maßnahmen

TCDP Nr. 21 – Sicherheitsbereich und Zutrittskontrolle

Anforderung

Die Controls von ISO/IEC 27018 Ziff. 11.1 und ISO/IEC 27002 Ziff. 11.1 sind im Sinne verbindlicher Anforderungen maßgeblich.

Umsetzungshinweis

Schutzklasse	Umsetzungsempfehlungen
I	- **ISO/IEC 27002 Ziff. 11.1.1 a)** - **ISO/IEC 27002 Ziff. 11.1.1 b)** - **ISO/IEC 27002 Ziff. 11.1.1 c)**
II	- **ISO/IEC 27002 Ziff. 11.1.1 d)** - Keine Fenster im IT- und **Technik**-Bereich.
III	- **ISO/IEC 27002 Ziff. 11.1.1 e)** - **ISO/IEC 27002 Ziff. 11.1.1 f)** - **ISO/IEC 27002 Ziff. 11.1.1 g)** - Einteilung des Rechenzentrums in Sicherheitszonen mit gesonderten Zutrittsregelungen. - Sicherheitszonen sind im Zwiebelschalenprinzip aufgebaut (jede Sicherheitszone wird von der jeweils vorhergehenden voll umschlossen). - Der Zutritt in eine Sicherheitszone und zu IT- und Technik-Bereichen des Rechenzentrums ist durch ein geeignetes Zutrittskontrollsystem gezielt eingeschränkt, wird mittels Zutrittskontrollanlage gesteuert und auf Verschluss überwacht. - Die IT- und Technik Bereiche sind durch ein Einbruchmeldesystem gesichert. Zusätzlich sind alle Öffnungen wie z.B. Schächte, Kriechgänge oder Lüftungsöffnungen zu den jeweiligen Sicherheitszonen durch ein Einbruchmeldesystem überwacht. IT- Bereiche sind durch geeignete Bewegungsmelder überwacht. - Der Zutritt in alle Räume des Rechenzentrums ist Video-überwacht, durch Zutrittskontrollanlagen gesichert und der Zutritt wird registriert. - Die äußere Begrenzung des Rechenzentrums wird vollständig und kontinuierlich per Video-überwacht. - Die Sicherheitszentrale ist ständig (7x24h) durch dediziertes und geschultes Sicherheitspersonal besetzt. - Rundgänge des Sicherheitspersonals erfolgen in unregelmäßigen Abständen und werden registriert. - Erkennung und Registrierung von einzelnen Personen und von mitgeführten Gegenständen. - Gesonderte Sicherung der HW (Server, Netzelemente, etc.). - Es existieren keine Fenster im Rechenzentrum (eine Ausnahme bildet der Empfang). - Es dürfen nur registrierte Datenverarbeitungsgeräte und Datenträger in das Rechenzentrum mitgenommen werden.

TCDP Nr. 22 – Logischer Zugang zu Datenverarbeitungsanlagen und Zugriff auf Daten

Erläuterung

Die in Anlage zu § 9 BDSG Nrn. 2 und 3 genannten Anforderungen der Zugangs- und Zugriffskontrolle sind in der Praxis kaum zu trennen und werden etwa auch in ISO-Standards zusammengefasst. Diesem Ansatz folgt auch das TCDP.

Anforderung

1. Die Controls von ISO/IEC 27018 Ziff. 9, 12.4 und ISO/IEC 27002 Ziff. 9 und 12.4, 13.1.1 sind im Sinne verbindlicher Anforderungen maßgeblich.

2. Die Anforderungen nach Absatz 1 gelten auch für Sicherungskopien.

Umsetzungshinweis

Zur Umsetzung sind geeignete Maßnahmen auszuwählen und in angemessener Art zu implementieren. Zu beachten ist, dass bestimmte administrative Tätigkeiten zur Zugriffsverwaltung bei der Nutzung von Cloud-Diensten auf den Nutzer übergehen können (vgl. ISO/IEC 27018 Ziff. 9.2).

Schutzklasse	**Umsetzungsempfehlungen**
I	- **ISO/IEC 27018 Ziff. 12.4** - **ISO/IEC 27002 Ziff. 9.1.1** - **ISO/IEC 27002 Ziff. 9.1.2** - **ISO/IEC 27002 Ziff. 9.2.1 a-b)** - **ISO/IEC 27002 Ziff. 9.2.2 a)** - **ISO/IEC 27002 Ziff. 9.2.3 a-c)** - **ISO/IEC 27002 Ziff. 9.2.4 a-b)** - **ISO/IEC 27002 Ziff. 9.2.5** - **ISO/IEC 27002 Ziff. 9.3.1** - **ISO/IEC 27002 Ziff. 9.4.1** - **ISO/IEC 27002 Ziff. 9.4.2 i-l)** - **ISO/IEC 27002 Ziff. 9.4.3** - **ISO/IEC 27002 Ziff. 9.4.4 a-d)** - **ISO/IEC 27002 Ziff. 9.4.5** - **ISO/IEC 27002 Ziff. 12.1.4 a-b)** - Rechte- und Rollenkonzept (vgl. auch ISO/IEC 27002 9.1.1). - automatisches Abschalten der Arbeitsplatzcomputer (log-off) oder Funktionsbegrenzung (funktionell/zeitlich). - enge Begrenzung der befugten Benutzer. - Anwenden von Methoden zur Trennung von Datentypen (z.B. Trennung von Nutzer- und Betriebsdaten, personenbezogenen und nicht-personenbezogenen Daten). - regelmäßige Auswertung der Protokolle.

II	- **ISO/IEC 27002 Ziff. 6.1.2** - **ISO/IEC 27002 Ziff. 9.2.1 c), d)** - ISO/IEC 27002 Ziff. 9.2.1 e) mit der Einschränkung, dass die Nutzer, die in Eigenverwaltung (self-service) durch den Administrator des Cloud-Nutzers registriert und de-registriert werden, zentral nicht sichtbar sein können. - **ISO/IEC 27002 Ziff. 9.2.1 f-h)** - ISO/IEC 27018 Ziff. 9.2.1 kann beispielsweise durch eine Anzeige des letzten Logins adressiert werden, damit der Nutzer erkennen kann ob die Registrierungsdaten kompromittiert wurden. Auch sollte eine Möglichkeit der Vergabe eines neuen Nutzernamens und Passworts vorhanden sein. - **ISO/IEC 27002 Ziff. 9.2.2 b-h)** - **ISO/IEC 27002 Ziff. 9.2.3 e-f)** - **ISO/IEC 27002 Ziff. 9.2.4 c-e)** - **ISO/IEC 27002 Ziff. 9.4.2 a-e)** - **ISO/IEC 27002 Ziff. 9.4.3** - **ISO/IEC 27002 Ziff. 9.4.4 e-i)** - **ISO/IEC 27002 Ziff. 12.1.4 c-g)** - ISO/IEC 27018 Ziff. 12.3 (letzter Absatz: Policy for erasure of PII contained in the backup). - **ISO/IEC 27018 Ziff. 12.4.2** - **ISO/IEC 27018 Ziff. A.4.1** - **ISO/IEC 27002 Ziff. 13.1.1** - ISO/IEC 27018 Ziff. A.9.3: Die Nichtwiederherstellbarkeit der durch den Cloud-Nutzer gelöschten Daten sollte mindestens ein mit DIN 66399 Stufe 2 vergleichbares Maß aufweisen. - Implementierung von Schutzmaßnahmen für Metadaten (keine Beschränkung auf den Schutz von Inhaltsdaten). - Sanktionen bei fehlerhaften Zugangsversuchen (Zeitsperren, Ungültigkeit der Chipkarte u.ä.). - Verschlüsselung und digitale Signaturen.
III	- **ISO/IEC 27002 Ziff. 9.4.5** - ISO/IEC 27002 Ziff. 9.2.3 d) Wird ein Zugriffsgeheimnis (Registrierungs-Link, Einladungs-Link etc.), auf einem unsicheren Kanal übertragen, sollte ein zweiter Faktor auf einem davon unabhängigen Kanal notwendig sein. - Zu ISO/IEC 27002 Ziff. 9.2.4: Auf Server oder Netzelemente, auf denen Daten der Cloud-Nutzer unverschlüsselter Form verarbeitet werden darf kein Zugriffsprivileg vergeben werden. Auf Server oder Netzelemente, auf denen keine Daten der Cloud-Nutzer oder Daten der Cloud-Nutzer in verschlüsselter Form verarbeitet werden, sollte ein Zugriffsprivileg nur anlassbezogen, d.h. beispielsweise für eine definierte und dokumentierte Wartungsaufgabe erteilt werden. - **ISO/IEC 27002 Ziff. 9.4.2 f-h)** - Zu ISO/IEC 27002 Ziff. 9.4.4: Technologien sollten zum Einsatz kommen, die sicherstellen, dass der Zugriff auf Server oder Netzelemente, die besonders privilegiert sind , d.h. Zugriff auf Daten der Cloud-Nutzer ermöglichen, über die üblichen organisatorischen

	Maßnahmen hinausgehende Mechanismen zur Gewaltenteilung entsprechend dem Stand der Technik beinhalten. - Zu ISO/IEC 27018 Ziff. 12.4.2: Entsprechend dem Stand der Technik können diese Umsetzungsempfehlungen für organisatorische Maßnahmen auch durch technische Maßnahmen zum Log- bzw. Metadatenschutz ersetzt werden. - ISO/IEC 27002 Ziff. 6.1.2: Gewaltenteilung sollte entsprechend dem Stand der Technik erzwungen werden. Insbesondere gilt: „Care should be taken that no single person can access, modify or use assets without authorization or detection“. - ISO/IEC 27002 Ziff. 12.3.1f: Die Verschlüsselung der Daten im Backup sollte so gestaltet sein, dass der Auftragnehmer keinen Zugriff auf Leseschlüssel hat. Die Wiederherstellung der Lesbarkeit der personenbezogenen Daten soll nur mit Schlüsseln beim Cloud-Nutzer möglich sein. - ISO/IEC 27018 Ziff. 12.4.2 Die unter dieser Ziffer empfohlene Maßnahme, die Log-Informationen regelmäßig zu löschen, sollte in dieser Schutzklasse automatisch erfolgen. - ISO/IEC 27018 Ziff. A.5.1: In dieser Schutzklasse sollten Daten im Auftrag verarbeitet werden können, die einem Beschlagnahmeschutz unterliegen. Daher sollte eine Herausgabe von personenbezogenen Daten entsprechend dem Stand der Technik durch technische Maßnahmen so weit wie möglich unterbunden sein. - ISO/IEC 27018 Ziff. A.9.3: Die Nichtwiederherstellbarkeit der durch den Cloud-Nutzer gelöschten Daten sollte ein mindestens mit DIN 66399 Stufe 3 vergleichbares Maß aufweisen. - abhörsichere Geräte und Leitungen. - strahlungsarme Monitore. - Signaturverfahren zur Identifizierung eines Benutzers. - gesonderte Sicherung der HW (Server, Netzelemente etc.) / Festlegung von Sicherungsbereichen. - Anwesenheitsaufzeichnungen.

TCDP Nr. 23 – 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 nachvollzogen werden kann, an welchen Empfängerkreis eine Übermittlung personenbezogener Daten vorgesehen ist. Außerdem muss eine Protokollierung der Übermittlungsvorgänge vorgesehen sein [ISO/IEC 27018 Ziff. 10, A.10.4, 10.5, 10.6, 10.9; ISO/IEC 27002 Ziff. 8.3, 10, 12.4.1, 12.4.2, 12.4.3, 13].

Erläuterung

Die genannten Normen von ISO/IEC 27018 und ISO/IEC 27002 entsprechen inhaltlich jedenfalls im Wesentlichen den gesetzlichen Anforderungen an die Weitergabekontrolle (§ 9 S. 1 BDSG i.V.m. Anlage Nr. 4). TCDP ergänzt die ISO-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-Standards nicht ausdrücklich angesprochen werden.

Umsetzungshinweis

Schutzklasse	Umsetzungsempfehlungen
I	- **ISO/IEC 27018 Ziff. A.10.4** - **ISO/IEC 27018 Ziff. A.10.5** - **ISO/IEC 27018 Ziff. A.10.6** - **ISO/IEC 27018 Ziff. A.10.9** - **ISO/IEC 27002 Ziff. 8.3** - **ISO/IEC 27002 Ziff. 10.1.1** - **ISO/IEC 27002 Ziff. 10.1.2** - **ISO/IEC 27002 Ziff. 12.4.1** - **ISO/IEC 27002 Ziff. 12.4.2** - **ISO/IEC 27002 Ziff. 12.4.3** - **ISO/IEC 27002 Ziff. 13.1.1 a-b)** - **ISO/IEC 27002 Ziff. 13.1.2 a-c)** - **ISO/IEC 27002 Ziff. 13.1.3** - **ISO/IEC 27002 Ziff. 13.2**
II	- ISO/IEC 27002 Ziff. 10.1.2: Das Schlüsselmanagement sollte so gestaltet sein, dass der Cloud-Anbieter und Betreiber keinen Zugriff zu Schlüsseln hat, die das Lesen von personenbezogenen Daten der Cloud-Nutzer erlauben. - **ISO/IEC 27002 Ziff. 13.1.1 c-g)** - ISO/IEC 27002 Ziff. 13.1.3: Trennung der Netze, die zum Betrieb des Operational Frameworks und zum Betrieb der Anwendungssoftware genutzt werden.

III	-	ISO/IEC 27002 Ziff. 13.2.3: Insbesondere diese Umsetzungsempfehlungen sollten im Kundendienst-Prozess bei der Kommunikation des Cloud-Anbieters mit den Cloud-Nutzern beachtet werden.

TCDP Nr. 24 – Nachvollziehbarkeit der Datenverarbeitung

Anforderung

Die Controls von ISO/IEC 27018 Ziff. 12.4 und ISO/IEC 27002 Ziff. 12.4. sind im Sinne verbindlicher Anforderungen maßgeblich.

Erläuterung

Die Controls von ISO/IEC 27002 Ziff. 12, auf die ISO/IEC 27018 Ziff. 12 verweist, entsprechen inhaltlich den gesetzlichen Anforderungen an die Eingabekontrolle (§ 9 S. 1 i.V.m. Nr. 5 der Anlage zu § 9 S. 1 BDSG) und konkretisieren diese in einem hinreichenden Maße. Beim Cloud-Anbieter hat die Nachvollziehbarkeit jeglicher Datenveränderung besondere Bedeutung. Daher bezeichnet TCDP Nr. 24 die Controls von ISO/IEC 27002 als verbindlich („shall“).

Umsetzungshinweis

Schutzklasse	**Umsetzungsempfehlungen**
I, II, III	- **ISO/IEC 27018 Ziff. 12.4** - **ISO/IEC 27002 Ziff. 12.4**

TCDP Nr. 25 – Auftragskontrolle

Anforderung

Die Controls von ISO/IEC 27018 Ziff. A.5, A.10.11 und A.10.12 sowie A.2.1 sind im Sinne verbindlicher Anforderungen maßgeblich.

Umsetzungshinweis

Bei der Umsetzung ist zu beachten, dass die Auftragskontrolle sowohl die Überwachung der vertraglich vereinbarten als auch der sonstigen beim Cloud-Anbieter umgesetzten technischen und organisatorischen Maßnahmen umfassen muss. Die Anforderungen des Cloud-Nutzers müssen auch in die Verträge des Cloud-Anbieters mit Subunternehmern aufgenommen werden. Es besteht die Möglichkeit, die Geeignetheit der Kontrolle zur auftragsgemäßen Datenverarbeitung durch unabhängige Stellen durchführen zu lassen (vgl. ISO/IEC 27018 Ziff. 18.2.1).

Schutzklasse	**Umsetzungsempfehlungen**
I	- **ISO/IEC 27018 Ziff. A.2.1** - **ISO/IEC 27018 Ziff. A.5.1** - **ISO/IEC 27018 Ziff. A.5.2** **Allgemeine organisatorische Maßnahmen** - Dokumentation der für den jeweiligen Cloud-Dienst eingesetzten Systeme, Verfahren und Prozesse (Software, Hardware, beteiligte Organisationseinheiten, Rollen und Dienstleister). - Exakte Beschreibung der Gesamtheit der getroffenen technischen und organisatorischen Maßnahmen. - Verfahren zur internen Überprüfung der Einhaltung der technischen und organisatorischen Maßnahmen. - Einrichtung (und Dokumentation) eines Verfahrens zur Überprüfung der Einhaltung der Maßnahmen zu: o Bestellung eines Datenschutzbeauftragten (TCDP Nr. 5). o Überprüfung der Einhaltung der Anforderungen an den Einsatz von Unterauftragnehmern nach TCDP Nr. 4. o Überprüfung der Verpflichtung des Personals des Cloud-Anbieters auf das Datengeheimnis nach TCDP Nr. 10.

I	**Maßnahmen bezüglich der Umsetzung von Weisungen** - Einführung und Dokumentation eines Verfahrens zur Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können, insbesondere: - Verfahren zur Entgegennahme, Umsetzung und Dokumentation von Einzelweisungen des Auftraggebers. - Prüfung der Identität des Auftraggebers und seiner Mitarbeiter sowie deren Vertretungsbefugnis bei Erteilung von Aufträgen und Weisungen sowie bei Anlieferung und Entgegennahme von Daten und Unterlagen. - Einhaltung der Remonstrationspflicht (TCDP Nr. 3). - Einhaltung der Mitteilungspflicht bei Datenschutzverstößen (TCDP Nr. 7). **Maßnahmen bezüglich der Verarbeitung im Auftrag** - Aussagekräftige Dokumentation des Cloud-Dienstes unter dem Gesichtspunkt der Abgrenzung der datenschutzrechtlichen Verantwortlichkeiten des Auftraggebers und des Auftragnehmers. - Bereitstellung der Angaben für die Verfahrensübersicht gemäß § 4g Abs. 2 BDSG. - Maßnahmen zur Gewährleistung von: o Berichtigung, Sperrung und Löschung von Daten, (TCDP Nr. 6), o Rückgabe von Daten an den Auftraggeber (TCDP Nr.9). o Verfahren zur Löschung von Restdaten während und insbesondere auch bei Beendigung des ADV-Verhältnisses (TDP Nr. 9). o Protokollierung der Datenverarbeitungsvorgänge (lesende und ändernde Zugriffe) in einem dem Schutzbedarf angemessenen Umfang und eine angemessene zeitliche Aufbewahrung dieser Protokolle. o Anlassbezogenen internen Kontrollen.
II	- Verfahren zur Mitteilung von Datenschutzvorfällen an den Auftraggeber zur Unterstützung der Pflichterfüllung gemäß § 42a BDSG. - Verpflichtung zum Abschluss von Versicherungen. - Vereinbarung von Konventionalstrafen für Verstöße gegen Weisungen. - Angemessener Schutz der Integrität der Protokolle. - Protokollierung der Konfigurationsänderungen. - Dokumentation der Änderungsprozesse. - Regelmäßige intern veranlasste Kontrollen des weisungsgemäßen Umgangs mit Daten des Auftraggebers.
III	- Erhöhter Integritätsschutz der Protokolle (z.B. durch Einsatz separater Protokollierungsserver). - Automatisiertes Monitoring von Veränderungen. - Zunehmende Kontrolldichte durch ausgewiesene Experten.

TCDP Nr. 26 – Verfügbarkeit von Daten

Anforderung

Die Controls von ISO/IEC 27018 Ziff. 12.3 sowie ISO/IEC 27002 Ziff. 11.1.4, 11.2.1, 11.2.2, 11.2.4, 12.1., 12.2, 12.3, 12.6 und 12.7 sind im Sinne verbindlicher Anforderungen maßgeblich.

Umsetzungshinweis

Schutzklasse	Umsetzungsempfehlungen
I	- **ISO/IEC 27018 Ziff. 12.3** - **ISO/IEC 27002 Ziff. 12.1.4** - **ISO/IEC 27002 Ziff. 11.2.2** - **ISO/IEC 27002 Ziff. 11.2.4** - **ISO/IEC 27002 Ziff. 12.1.3** - **ISO/IEC 27002 Ziff. 12.1.4** - **ISO/IEC 27002 Ziff. 12.2** - **ISO/IEC 27002 Ziff. 12.3** - **ISO/IEC 27002 Ziff. 12.6** - **ISO/IEC 27002 Ziff. 12.3**
II, III	- **ISO/IEC 27002 Ziff. 11.1.4** - **ISO/IEC 27002 Ziff. 12.1.1** - **ISO/IEC 27002 Ziff. 12.1.2**

TCDP Nr. 27 – Getrennte Verarbeitung

Anforderung

Es sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Umsetzungshinweis

Schutzklasse	**Umsetzungsempfehlungen**
I	- Mandantentrennung durch die „business logic“ der Anwendungssoftware.
II	- Kryptographische Mandantentrennung. - Trennung der verschiedenen Nutzer eines Mandanten in der „business logic“ der Anwendungssoftware.
III	- Kryptographische Trennung verschiedener Arbeitsbereiche desselben Mandanten für Daten die zu unterschiedlichen Zwecken erhoben wurden.

TCDP Nr. 28 – Kryptographie

Anforderung

Soweit der Cloud-Anbieter kryptographische Verfahren einsetzt, sind ISO/IEC 27018 Ziff. 10 und ISO/IEC 27002 Nr. 10 im Sinne verbindlicher Anforderungen maßgeblich.

Umsetzungshinweis

Schutzklasse	**Umsetzungsempfehlungen**
I, II, III	- **ISO/IEC 27018 Ziff. 10** - **ISO/IEC 27002 Ziff. 10**

V. Referenzen

[i] Siehe zur Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ http://www.trusted-cloud.de/560.php.

[ii] Thesenpapier „Datenschutzrechtliche Lösungen für Cloud Computing“, abrufbar unter http://www.trusted-cloud.de/369.php.

[iii] Arbeitspapier „Modulare Zertifizierung von Cloud-Diensten“, abrufbar unter http://www.trusted-cloud.de/369.php.

[iv] Thesenpapier „Eckpunkte eines Zertifizierungsverfahrens für Cloud-Dienste“, abrufbar unter http://www.trusted-cloud.de/369.php.

[v] 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.

[vi] ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.

[vii] ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls.

[viii] Arbeitspapier „Schutzklassen in der Datenschutz-Zertifizierung“, abrufbar unter http://www.trusted-cloud.de/369.php.

Impressum

Herausgeber
Kompetenzzentrum Trusted Cloud
Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“
E-Mail: kompetenzzentrum@trusted-cloud.de
www.trusted-cloud.de

Im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi)

Stand: April 2015