Verfahrensordnung für Zertifizierungen nach dem Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP)

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

Präambel 4

1. Kapitel: Anwendungsbereich 5
§ 1.1 Anwendungsbereich 5
§ 1.2 Gegenstand der Prüfung und Zertifizierung 5
§ 1.3 Verhältnis zu DIN EN ISO/IEC 17065 5

2. Kapitel: Zertifizierungsstelle und Prüfstelle 5
§ 2.1 Zertifizierungsstelle 5
§ 2.2 Zertifizierer 6
§ 2.3 Prüfstelle 6
§ 2.4 Prüfer 7
§ 2.5 Akkreditierung 7
§ 2.6 Verhältnis zwischen Zertifizierungsstelle und Prüfstelle 8
§ 2.7 Unabhängigkeit und Unparteilichkeit. Gefahr eines Interessenkonflikts 8
§ 2.8 Entgelte 9

3. Kapitel: Das Prüfverfahren 9
§ 3.1 Vertragliche Grundlage 9
§ 3.2 Mitwirkungspflichten des Cloud-Anbieters 10
§ 3.3 Ablauf der Prüfung 10
§ 3.4 Anerkennung von Zertifikaten 11
§ 3.5 Bewertung und Prüfbericht 11
§ 3.6 Zwischenprüfung 12

4. Kapitel: Das Zertifizierungsverfahren 13
§ 4.1 Vertragliche Grundlage 13
§ 4.2 Voraussetzungen der Zertifizierung 13
§ 4.3 Bewertung der Prüfung 14
§ 4.4 Anerkennung von TCDP-Zertifikaten 14
§ 4.5 Anerkennung anderer Zertifikate 14
§ 4.6 Entscheidung der Zertifizierungsstelle 15
§ 4.7 Nachbesserung 15
§ 4.8 Widerspruch 15
§ 4.9 Änderungszertifizierung 16

5. Kapitel: Das Zertifikat 16
§ 5.1 Erteilung und Inhalt des Zertifikats 16
§ 5.2 Veröffentlichung des Zertifikats 17
§ 5.3 Gültigkeitsdauer. Erneute Zertifizierung 17
§ 5.4 Überwachung 17
§ 5.5 Prüfzeichen 17
§ 5.6 Einschränkung, Aussetzung oder Widerruf des Zertifikats 18
§ 5.7 Änderung des Cloud-Dienstes 19

6. Kapitel: Schlussbestimmungen 19
§ 6.1 Fortgeltung der Zertifikate nach einem DSGVO-Standard 19
§ 6.2 Änderungen 19

Anlage 1) Zertifikatsmuster 20

Anlage 2) Muster des Prüfzeichens 22

Präambel

Die Zertifizierung nach dem Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP) steht für alle Cloud-Dienste im Anwendungsbereich des Bundesdatenschutzgesetzes (BDSG) zur Verfügung. TCDP ist ein Datenschutz-Prüfstandard für Cloud-Dienste, der im Rahmen des Pilotprojekts „Datenschutz-Zertifizierung für Cloud-Dienste“ (i.F. Pilotprojekt) im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) erarbeitet wurde.

Die Zertifizierung nach TCDP soll es in- und ausländischen Anbietern von Cloud-Diensten sowie deren Unterauftragnehmern ermöglichen, die Einhaltung des BDSG nachzuweisen. Nutzer von Cloud-Diensten sollen auf die Zertifizierung vertrauen können.

Das Zertifizierungsverfahren nach TCDP ist bisher nicht ausdrücklich gesetzlich geregelt. Ein Zertifikat nach TCDP darf nur nach Maßgabe der nachfolgenden Verfahrensordnung erteilt werden.

1. Kapitel: Anwendungsbereich

§ 1.1 Anwendungsbereich

(1) Die Verfahrensordnung gilt für Prüfungen und Zertifizierungen von Cloud-Diensten nach TCDP.

(2) Die Zertifizierung nach TCDP steht allen Cloud-Diensten offen, die dem BDSG unterliegen oder durch vertragliche Bindung an den Cloud-Nutzer oder Auftragnehmer auf die Einhaltung des BDSG verpflichtet sind.

§ 1.2 Gegenstand der Prüfung und Zertifizierung

(1) Gegenstand der Prüfung und Zertifizierung sind Cloud-Dienste. Cloud-Dienste im Sinne dieser Verfahrensordnung sind Cloud-Dienste im Sinne der Definition des National Institute of Standards and Technology (NIST), d.h. Dienste, die sich durch (1.) bedarfsgerechte Abrufmechanismen für den Nutzer (on-demand self-service), (2.) Netzwerkzugriff (broad network access), (3.) provider-seitige Ressourcenbündelung (resource pooling), (4.) Elastizität (rapid elasticity) und (5.) Nutzungskontrolle (measured service) auszeichnen und sich als Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) oder Software-as-a-Service (SaaS) klassifizieren lassen, die für einen Nutzer solcher Dienste (Cloud-Nutzer) erbracht werden. Cloud-Dienste im Sinne dieser Verfahrensordnung sind ferner Bestandteile von Cloud-Diensten, die als Datenverarbeitung im Auftrag sowie Dienste, die der Cloud-Anbieter zur Unterstützung von Cloud-Diensten einsetzt und im Rahmen ihrer Tätigkeit Zugriff auf personenbezogene Daten erhalten.

(2) Cloud-Anbieter sind Rechtsträger, die Cloud-Dienste betreiben.

§ 1.3 Verhältnis zu DIN EN ISO/IEC 17065

(1) Diese Verfahrensordnung ist ein Zertifizierungsprogramm im Sinne der DIN EN ISO/IEC 17065.

(2) Cloud-Dienste sind Dienstleistungen im Sinne der DIN EN ISO/IEC 17065.

2. Kapitel: Zertifizierungsstelle und Prüfstelle

§ 2.1 Zertifizierungsstelle

(1) Die Zertifizierung nach TCDP erfolgt durch eine unabhängige und fachlich geeignete Zertifizierungsstelle. Die Zertifizierungsstelle führt ihre Tätigkeit nicht diskriminierend und unparteilich aus.

(2) Die Zertifizierungsstelle kann eine rechtsfähige Organisation oder ein abgegrenzter Teil einer rechtsfähigen Organisation sein.

(3) Die Zertifizierungsstelle muss über die für die Tätigkeit notwendige finanzielle Stabilität und die notwendigen Ressourcen verfügen.

(4) Die Zertifizierungsstelle gewährleistet die Vertraulichkeit der Informationen über die und aus den Zertifizierungsverfahren.

§ 2.2 Zertifizierer

(1) Zertifizierer sind natürliche Personen, die für eine Zertifizierungsstelle die Bewertung der Prüfung durchführen. Die Tätigkeit des Zertifizierers kann durch Zusammenwirken mehrerer natürlicher Personen ausgeübt werden. In diesem Fall reicht es aus, wenn die fachlichen Anforderungen nach Abs. 2 bis 4 durch die betreffenden Personen als Gruppe erfüllt werden. Die persönlichen Anforderungen nach Abs. 6 und 7 müssen durch jede Person erfüllt werden.

(2) Zertifizierer müssen eine hinreichende fachliche Eignung für die von ihnen durchgeführten Bewertungen aufweisen.

(3) Für die Zertifizierungstätigkeit ist ein Hochschulabschluss oder eine gleichwertige Ausbildung erforderlich.

(4) Der Zertifizierer hat in den für die Zertifizierung relevanten Bereichen über hinreichende Kenntnisse zu verfügen. Insbesondere muss der Zertifizierer für die Zertifizierung hinreichende Kenntnisse in folgenden Gebieten aufweisen:

a) datenschutzrechtliche Anforderungen an Cloud-Dienste;
b) technische Grundlagen von Cloud-Diensten;
c) technische Anforderungen an Datensicherheit;
d) ISO/IEC 270xy-Standards;
e) Verfahren und Standards der TCDP-Zertifizierung.

(5) Eine für die Zertifizierung hinreichende Erfahrung setzt eine mindestens vierjährige (Vollzeitäquivalent) Tätigkeit im Bereich der Informationstechnik oder des Datenschutzes und eine mindestens zweijährige (Vollzeitäquivalent) Tätigkeit als Zertifizierer oder eine mindestens vierjährige (Vollzeitäquivalent) Tätigkeit als Prüfer von Produkten und/oder Diensten im Bereich Datenschutz oder Informationssicherheit voraus.

(6) Zertifizierer müssen auf Grund ihrer persönlichen Eigenschaften, ihres Verhaltens und ihrer Fähigkeiten die erforderliche Zuverlässigkeit aufweisen, um ihre Aufgaben ordnungsgemäß zu erfüllen.

(7) Zertifizierer müssen unabhängig im Sinne des § 2.7 Abs. 3 sein. Sie führen ihre Tätigkeit nicht diskriminierend und unparteilich aus.

(8) Die Zertifizierungsstelle stellt sicher, dass die von ihr eingesetzten Zertifizierer die Anforderungen nach Abs. 2 bis 7 erfüllen.

§ 2.3 Prüfstelle

(1) Mit der Prüfung eines Cloud-Dienstes zur Erteilung eines TCDP-Zertifikats können unabhängige und fachlich geeignete Prüfer oder Prüfstellen beauftragt werden. Soweit ein Prüfer beauftragt wird, gelten für ihn die Vorschriften über Prüfstellen entsprechend.

(2) Eine Prüfstelle ist ein Rechtsträger oder ein Teil einer rechtsfähigen Organisation, die Prüfer zur Durchführung von Prüfungen nach dieser Verfahrensordnung einsetzt.

(3) Die Prüfstelle führt ihre Tätigkeit nichtdiskriminierend und unparteilich nach Maßgabe von § 2.7 Abs. 1 und 2 aus und verfügt über die für die Prüfung erforderlichen Ressourcen.

(4) Die Prüfstelle gewährleistet die Vertraulichkeit der Informationen über die und aus den Prüfverfahren.

(5) Die Prüfstelle kann zur Durchführung der Prüfung bei ihr beschäftigte oder externe Prüfer heranziehen.

(6) Die Prüfstelle hat eine angemessene Haftpflichtversicherung abzuschließen und aufrechtzuerhalten.

§ 2.4 Prüfer

(1) Prüfer sind natürliche Personen, die aufgrund eines Auftrags des Cloud-Anbieters oder für eine Prüfstelle Prüfungen nach dieser Verfahrensordnung durchführen.

(2) Sie müssen eine hinreichende fachliche Eignung für die von ihnen durchgeführten Prüfungen aufweisen. Dies setzt eine hinreichende Ausbildung und Erfahrung voraus.

(3) Für die Prüfungstätigkeit ist ein Hochschulabschluss oder eine gleichwertige Ausbildung in den für die Prüfung relevanten Bereichen erforderlich. Dabei ist hinsichtlich der rechtlichen TCDP-Anforderungen eine rechtliche Ausbildung, hinsichtlich der technischen TCDP-Anforderungen eine technische Ausbildung erforderlich.

(4) Insbesondere müssen die Prüfer hinreichende Kenntnisse in folgenden Gebieten aufweisen:

a) datenschutzrechtliche Anforderungen an Cloud-Dienste;
b) technische Grundlagen von Cloud-Diensten;
c) technische Anforderungen an Datensicherheit;
d) ISO/IEC 270xy-Standards;
e) Verfahren und Standards der TCDP-Zertifizierung.

Hinsichtlich der Buchstaben (a) bis (d) ist es ausreichend, dass die eingesetzten rechtlichen Prüfer über Grundkenntnisse zu (b), (c) und (d) verfügen und die eingesetzten technischen Prüfer über Grundkenntnisse zu (a).

(5) Eine für die Prüfung hinreichende Erfahrung setzt eine mindestens vierjährige (Vollzeitäquivalent) Tätigkeit im Bereich der Informationstechnik oder des Datenschutzes und eine mindestens zweijährige (Vollzeitäquivalent) Tätigkeit im Bereich der Prüfung von IT-Produkten und IT-Verfahren im Bereich Datenschutz oder im Bereich Informationssicherheit voraus. Die Tätigkeit als Datenschutz- oder IT-Sicherheitsbeauftragter oder Berater auf den vorgenannten Gebieten ist keine Tätigkeit im Sinne von Satz 1.

(6) Prüfer müssen ferner die erforderliche persönliche Eignung und Zuverlässigkeit zur Durchführung der Prüfung aufweisen.

(7) Prüfer müssen unabhängig im Sinne des § 2.7 Abs. 3 sein und ihre Tätigkeit nicht diskriminierend und unparteilich durchführen. Sie dürfen einen Dienst nicht prü-fen, wenn die Gefahr eines Interessenkonflikts i.S. des Art. 2.7 Abs. 4 besteht.

§ 2.5 Akkreditierung

(1) Zertifizierungsstelle und Prüfstelle haben die Erfüllung der Anforderungen dieser Verfahrensordnung, insbesondere ihre fachliche Eignung, durch eine Akkreditierung nachzuweisen.

(2) Zertifizierungsstellen bedürfen der Akkreditierung der Deutschen Akkreditierungsstelle GmbH (DAkkS) für Zertifizierungen nach dieser Verfahrensordnung.

(3) Solange bei der DAkkS kein spezifisches Akkreditierungsverfahren für Zertifizierungsstellen nach TCDP vorliegt, gelten folgende Akkreditierungen als Akkreditierung für Zertifi-

zierungsstellen im Sinne dieser Verfahrensordnung:

a) Akkreditierung bei der DAkkS nach ISO/IEC 17065 für den Bereich IT-Sicherheit (ISO/IEC 15408, ETSI EN 319 401);
b) Akkreditierung bei der DAkkS nach ISO/IEC 17021 für Informationssicherheits-Managementsysteme nach ISO/IEC 27001.

(4) Die Zertifizierungsstelle darf Zertifizierungen nach dieser Verfahrensordnung nur durchführen, soweit eine gültige Akkreditierung vorliegt.

(5) Prüfstellen bedürfen der Akkreditierung der DAkkS für Prüfungen nach dieser Verfahrensordnung.

(6) Solange bei der DAkkS kein spezifisches Akkreditierungsverfahren für Prüfstellen nach TCDP vorliegt, gelten folgende Akkreditierungen als Akkreditierung für Prüfstellen im Sinne dieser Verfahrensordnung:

a) Akkreditierung bei der DAkkS nach ISO/IEC 17025 für den Bereich IT-Sicherheit (ISO/IEC 15408);
b) Anerkennung als sachverständige Stelle nach § 9 Abs. 3 BSIG;
c) Anerkennung als Prüfstelle oder Sachverständiger für das Datenschutz-Gütesiegel beim ULD Kiel;
d) Zulassung als Experte für Erstellung von Gutachten im Zertifizierungsverfahren der European Privacy Seal GmbH (EuroPriSe).

(7) Die fachliche Eignung der Prüfstelle und der Zertifizierungsstelle besteht nur im zeitlichen und sachlichen Geltungsbereich der Akkreditierung. Der zeitliche Geltungsbereich der Akkreditierung der Prüfstelle und der Zertifizierungsstelle muss den Abschluss des Prüf- und Zertifizierungsverfahrens umfassen.

§ 2.6 Verhältnis zwischen Zertifizierungsstelle und Prüfstelle

(1) Die Zertifizierungsstelle und die Prüfstelle können zur selben Organisation gehören. In diesem Fall dürfen Prüfer und Zertifizierer nicht in einem disziplinarischen Verhältnis zueinanderstehen.

(2) Die Zertifizierungsstelle kann ein Verfahren der Zulassung von Prüfstellen festlegen. In diesem Fall muss die Zulassung nach transparenten, nicht diskriminierenden, objektiven Maßstäben erfolgen. Die Zertifizierungsstelle hat eine Liste der von ihr zugelassenen Prüfstellen zu führen und ständig öffentlich zugänglich zu machen.

(3) Soweit die Zertifizierungsstelle ein Zulassungsverfahren nach Abs. 2 durchführt, kann sie festlegen, dass sie Zertifizierungsaufträge nur annimmt, wenn die Prüfung durch eine von ihr zugelassene Prüfstelle durchgeführt wird.

§ 2.7 Unabhängigkeit und Unparteilichkeit. Gefahr eines Interessenkonflikts

(1) Zertifizierungsstellen und Prüfstellen, Zertifizierer und Prüfer sind unabhängig, wenn sie frei von äußerer und interner Einflussnahme, insbesondere finanzieller Art, sind.

(2) Zertifizierungsstellen, Prüfstellen, Zertifizierer und Prüfer sind unparteilich, wenn sie ihre Zertifizierungs- und Prüftätigkeiten objektiv nach Maßgabe dieser Verfahrensordnung durchführen und sich von keinen sachfremden, insbesondere wirtschaftlichen oder persönlichen, Interessen leiten lassen.

(3) Zertifizierungsstellen und Prüfstellen stellen die Unabhängigkeit und Unparteilichkeit

der Zertifizierer und Prüfer durch geeignete organisatorische Maßnahmen sicher. Sie verpflichten die Zertifizierer und Prüfer vertraglich zur Wahrung der Unabhängigkeit. Bei der Erfüllung der Anforderungen von Satz 1 und Satz 2 ist insbesondere folgenden Grundsätzen Rechnung zu tragen:

a) Jede Art von Einflussnahme durch andere Personen oder Organisationen auf die Prüfungen und deren Ergebnisse ist ausgeschlossen.
b) Das Einkommen der Zertifizierer und Prüfer ist nicht von den Bewertungs- oder Prüfergebnissen und der Anzahl der durchgeführten Bewertungen oder Prüfungen abhängig.
c) Zertifizierungs- und Prüfungstätigkeiten dürfen nicht mit anderen Aufgaben vermengt werden, die nach ihrer Art oder Intensität zu einem Interessenkonflikt führen und damit einen negativen Einfluss auf die Qualität der Zertifizierungs- oder Prüfungstätigkeit haben können.
d) Weder die eingesetzten Zertifizierer und Prüfer noch andere Mitarbeiter, die direkt oder indirekt mit der Zertifizierungs- oder Prüfungstätigkeit zu tun haben, dürfen im Zeitpunkt der Zertifizierung oder Prüfung Beziehungen zum Cloud-Anbieter unterhalten, die über den Prüfungsauftrag hinausgehen.
e) Die Zertifizierer und Prüfer dürfen keine Beratung oder sonstige Tätigkeit, welche die Unabhängigkeit gefährden könnte, für den Cloud-Anbieter innerhalb der letzten zwei Jahre vor der Zertifizierung oder Prüfung übernommen haben und eine solche auch nicht zwei Jahre nach der Zertifizierung übernehmen.

(4) Zertifizierungsstellen, Zertifizierer, Prüfstellen und Prüfer dürfen bei Gefahr eines Interessenkonflikts nicht tätig werden. Diese besteht insbesondere, soweit Zertifizierungsstellen, Zertifizierer, Prüfstellen und Prüfer innerhalb der letzten zwei Jahre vor oder während des Prüf- oder Zertifizierungsverfahrens Cloud-Dienste oder Bestandteile von Cloud-Diensten konzeptionieren, implementieren oder anbieten oder Anbieter von Cloud-Diensten oder Bestandteilen von Cloud-Diensten beraten oder die künftige Vornahme einer solchen Tätigkeit mit einem Anbieter von Cloud-Diensten vereinbaren.

§ 2.8 Entgelte

Zertifizierungsstelle und Prüfstelle können für ihre Tätigkeit angemessene Entgelte verlangen. Die Entgelte sind im Vertrag mit dem Cloud-Anbieter festzulegen.

3. Kapitel: Das Prüfverfahren

§ 3.1 Vertragliche Grundlage

(1) Das Prüfverfahren beruht auf einem Vertrag zwischen dem Cloud-Anbieter und der Prüfstelle.

(2) Im Vertrag sind mindestens festzulegen:

a) der Prüfgegenstand mit Angabe aller für den Betrieb des Cloud-Dienstes relevanten Standorte;
b) die TCDP-Anforderungen in der maßgeblichen Fassung;
c) diese Verfahrensordnung als für Prüfung und Zertifizierung maßgebliche Verfahrensregelung;
d) der Prüfungsauftrag (Umfang der Prüfung, Ort der Prüfung, geplante Prüfdauer, Prüfbericht) einschließlich der Angabe der vom Cloud-Anbieter beantragten Schutz-

anforderungsklasse;
e) die Zertifizierungsstelle, welche die Zertifizierung durchführen soll;
f) die Mitwirkungspflichten des Cloud-Anbieters.

Bei der Beschreibung des Prüfgegenstandes ist insbesondere anzugeben, welche Bestandteile der Cloud-Dienst umfasst.

§ 3.2 Mitwirkungspflichten des Cloud-Anbieters

(1) Der Cloud-Anbieter nimmt die für die ordnungsgemäße Prüfung und Zertifizierung erforderlichen bzw. ggf. vertraglich zugesagten Mitwirkungshandlungen auf eigene Kosten vor.

(2) Der Cloud-Anbieter ist insbesondere verpflichtet, der Prüfstelle eine hinreichende Dokumentation zum Prüfgegenstand zur Verfügung zu stellen oder Einsicht zu gewähren. Gegenstand der Dokumentation sind neben einer Beschreibung des Cloud-Dienstes insbesondere die technischen und organisatorischen Maßnahmen des Cloud-Anbieters i.S. des § 9 BDSG.

(3) Der Cloud-Anbieter versichert gegenüber der Prüfstelle, dass die in der Dokumentation genannten Maßnahmen vollständig umgesetzt sind.

(4) Soweit der Cloud-Anbieter die Anerkennung von Zertifikaten für Bestandteile seines Cloud-Dienstes anstrebt, hat er den Anerkennungswunsch vor Beginn der Prüfung unter genauer Bezeichnung des anzuerkennenden Zertifikats und des Bestandteils seines Cloud-Dienstes, für den die Anerkennung gewünscht wird, mitzuteilen und die für die Beurteilung der Anerkennung relevanten Dokumente vorzulegen.

§ 3.3 Ablauf der Prüfung

(1) Die Prüfung erfolgt auf Grundlage der im Auftrag klar abgegrenzten Beschreibung des Prüfgegenstandes und umfasst mindestens eine Prüfung der vom Cloud-Anbieter zur Verfügung gestellten Dokumentation (Abs. 3), Befragung (Abs. 4) sowie eine Vor-Ort-Prüfung (Abs. 5). Soweit erforderlich, sind technische Tests (Abs. 6) durchzuführen.

(2) Gegenstand der Prüfung ist auch das Zusammenwirken des Cloud-Dienstes oder Bestandteils mit anderen Bestandteilen oder Diensten.

(3) Mit der Dokumentenprüfung überprüft der Prüfer die Einhaltung der Anforderungen des TCDP anhand der Angaben in der Dokumentation des Cloud-Anbieters.

(4) Die Befragung von Mitarbeitern des Cloud-Anbieters oder anderen Personen, die mit der Erbringung des Prüfgegenstandes befasst sind, kann zur Sachverhaltsermittlung einzelner Aspekte und zur Überprüfung der Richtigkeit der Dokumentation eingesetzt werden. Sie soll insbesondere zur Überprüfung bei vom Prüfer als kritisch erkannten Aspekten eingesetzt werden. Befragungen können schriftlich oder persönlich durchgeführt werden. Sie sollen jedenfalls hinsichtlich zentraler Aspekte als mündliche Befragung durchgeführt werden. Soweit eine persönliche Befragung unverhältnismäßig wäre, kann sie in Form von Videokonferenzen durchgeführt werden.

(5) Die Vor-Ort-Prüfung umfasst mindestens die Inaugenscheinnahme der Verfahren und technischen Einrichtungen in den Räumlichkeiten des Cloud-Anbieters bzw. seiner Unterauftragnehmer.

(6) Soweit für die vom Cloud-Anbieter angestrebte Schutzanforderungsklasse erforderlich, werden entsprechende sicherheitstechnische Tests durchgeführt.

(7) Die Prüfung erstreckt sich auf alle Anforderungen des TCDP einschließlich der vom TCDP in Bezug genommen Maßnahmen (controls) von ISO/IEC-Standards.

(8) Die Prüfung umfasst in Bezug auf die Anforderungen des TCDP einschließlich der durch das TCDP in Bezug genommenen Maßnahmen (controls) von ISO/IEC-Standards eine Überprüfung der tatsächlichen Einhaltung der organisatorischen und technischen Maßnahmen.

(9) Die Prüfung erfolgt stichprobenartig. Dabei ist in Bezug auf eine Anforderung (z.B. sichere Passwörter) eine Stichprobe an Aktivitäten (activities) zur Erfüllung einer Anforderung (z.B. Passwortlänge) zu untersuchen. In Bezug auf die Umsetzung einzelner Aktivitäten ist eine Stichprobe an Elementen (z.B. einzelne Passwörter) zu untersuchen.

(10) Die Stichprobe ist so zu wählen, dass die Untersuchung der ausgewählten Aktivitäten (activities) bzw. Elemente einen Rückschluss auf die Erfüllung der Anforderung zulässt.

§ 3.4 Anerkennung von Zertifikaten

(1) Soweit die Zertifizierungsstelle Zertifikate für Bestandteile von Cloud-Diensten anerkennt, ist eine Prüfung des im Zertifikat benannten Bestandteils des Cloud-Dienstes nicht erforderlich. Erforderlich ist jedoch eine Prüfung des Zusammenwirkens des anerkannten Bestandteils des Cloud-Dienstes mit anderen Bestandteilen, insbesondere der für dieses Zusammenwirken maßgeblichen Schnittstellen.

(2) Wenn der Cloud-Anbieter eine Anerkennung anstrebt, prüft die Prüfstelle unverzüglich, ob und inwieweit eine Anerkennung erfolgen kann.

(3) Die Prüfstelle kann die Zertifizierungsstelle um eine Vorabentscheidung über die Anerkennung von Zertifikaten ersuchen. Dem Ersuchen sind mindestens die Angaben und Dokumente nach § 3.2 Abs. 4 beizufügen.

§ 3.5 Bewertung und Prüfbericht

(1) Die Prüfstelle erstellt auf der Grundlage der Prüfung eine Bewertung der Erfüllung der Anforderungen des TCDP durch den Cloud-Dienst in Bezug auf eine bestimmte Schutzklasse. Dabei ist sowohl eine Bewertung hinsichtlich der Erfüllung der einzelnen Anforderungen des TCDP als auch hinsichtlich der Erfüllung der Anforderungen des TCDP insgesamt, jeweils bezogen auf eine bestimmte Schutzklasse, erforderlich. Soweit einzelne Anforderungen des TCDP für die beantragte Schutzklasse nicht erfüllt sind, können diese durch andere Maßnahmen ausgeglichen werden, wenn dadurch der Cloud-Dienst das Schutzniveau der beantragten Schutzklasse insgesamt erreicht. Soweit die Prüfstelle einen solchen Ausgleich annimmt, ist dies im Rahmen der Begründung des Gesamtergebnisses gesondert zu begründen.

(2) Die Prüfstelle erstellt auf der Grundlage der Prüfung einen Prüfbericht. Der Prüfbericht enthält mindestens folgende Angaben:

a) den Gegenstand der Prüfung;
b) eine Darstellung des zeitlichen Ablaufs und des Umfangs der Prüfung mit Angabe der Standorte und Räumlichkeiten, an bzw. in denen die Prüfung erfolgt ist;
c) eine Kurzbeschreibung der Umsetzung der einzelnen TCDP-Anforderungen;
d) die begründete Bewertung hinsichtlich der Erfüllung oder Nichterfüllung der einzelnen TCDP-Anforderungen für die betreffende Schutzanforderungsklasse;
e) die Maßnahmen, mit der die Prüfstelle die Erfüllung festgestellt hat, insbesondere

Angaben zur Prüfmethode nach § 3.3 Abs. 2 bis 6 und – sofern für das Verständnis erforderlich – eine Begründung für deren Einsatz;

f) die Angabe der anzuerkennenden Zertifikate sowie eine Aussage über die Prüfung des Zusammenwirkens der Dienste;
g) eine Begründung der Gleichwertigkeit anzuerkennender Zertifikate i.S. des § 4.5.
h) das Gesamtergebnis hinsichtlich der Erfüllung oder Nichterfüllung der TCDP-Anforderungen für eine bestimmte Schutzanforderungsklasse;
i) die Begründung des Gesamtergebnisses;
j) eine Aufstellung der geprüften Dokumentation;
k) die Erklärung des Cloud-Anbieters gemäß § 3.2 Abs. 3;
l) eine Aussage über die Erfüllung der einzelnen vom TCDP in Bezug genommenen ISO/IEC-Normen. Diese Aussage kann in tabellarischer Form durch Stichpunkte oder Symbole erfolgen, aus welcher sich die Erfüllung oder Nichterfüllung der jeweiligen ISO/IEC-Norm erschließt. Die Aufzählung kann dem Prüfbericht als Anlage beigefügt werden;
m) die Erklärung des Prüfers, dass er die Anforderungen dieser Verfahrensordnung nach Unabhängigkeit und Unparteilichkeit erfüllt hat und kein Grund für Besorgnis der Befangenheit vorliegt.

(3) Der Prüfbericht kann Hinweise enthalten. Die Hinweise können auch angeben, ob und durch welche Maßnahmen des Cloud-Anbieters bislang nicht erreichte TCDP-Anforderungen noch erfüllt werden können.

(4) Der Prüfgegenstand ist im Prüfbericht genau zu bezeichnen. Insbesondere sind die Funktion des Cloud-Dienstes genau zu beschreiben und abzugrenzen sowie die technischen Einrichtungen einschließlich der für die Erbringung des Cloud-Dienstes maßgeblichen Räume zu beschreiben. Maßgeblich sind Räume, in denen technische Anlagen betrieben werden sowie Arbeitsräume von Personen, die den Cloud-Dienst steuern.

(5) Die Bezeichnung des Prüfgegenstandes kann in einer Anlage zum Prüfbericht erfolgen.

(6) Die Prüfstelle übermittelt der Zertifizierungsstelle einen Entwurf des Prüfberichts zur Stellungnahme. Die endgültige Version des Prüfberichts darf erst nach Stellungnahme der Zertifizierungsstelle an den Cloud-Anbieter übermittelt werden.

(7) Die Prüfstelle stellt den Prüfbericht dem Cloud-Anbieter zur Verfügung und räumt diesem uneingeschränkte Nutzungsrechte ein. Der Cloud-Anbieter darf den Prüfbericht Dritten nur im vollen Wortlaut und unter Angabe des Ausstellungsdatums zur Verfügung stellen und hat solchen Dritten entsprechende Nutzungsbeschränkungen aufzuerlegen. Die Prüfstelle kann sich das Recht zur Veröffentlichung und zur öffentlichen Wiedergabe i.S. des § 15 Abs. 2 UrhG vorbehalten.

§ 3.6 Zwischenprüfung

(1) Auf Antrag des Cloud-Anbieters können Zwischenprüfungen durchgeführt werden.

(2) Aufgrund der Zwischenprüfung hat die Zertifizierungsstelle festzustellen, ob der zertifizierte Cloud-Dienst die TCDP-Anforderungen nach der zertifizierten Schutzanforderungsklasse weiterhin erfüllt.

(3) Die jährliche Zwischenprüfung nach § 5.4 ist frühestens nach Ablauf des sechsten und spätestens bis zum Ablauf des zwölften Monats ab Zertifikatserteilung oder der entsprechenden Zeitpunkte der Folgejahre durchzuführen.

(4) Für die Zwischenprüfung gelten die Anforderungen über die Prüfung entsprechend. Der Umfang der Zwischenprüfung ist so zu wählen, dass die seit der letzten Prüfung erfolgten Änderungen des Cloud-Dienstes geprüft werden. Durch geeignete Stichproben ist festzustellen, ob der Cloud-Dienst insgesamt die TCDP-Anforderungen weiterhin erfüllt.

(5) Der Cloud-Anbieter ist zur Mitwirkung nach Maßgabe von § 3.2 verpflichtet. Er hat insbesondere eine Dokumentation der Änderungen der technischen und organisatorischen Maßnahmen nach Maßgabe von § 3.2 Abs. 2 zu erstellen.

(6) Die Prüfstelle erstellt einen Zwischenprüfbericht und übermittelt diesen rechtzeitig vor Ablauf des Zwischenprüfungszeitraums der Zertifizierungsstelle. § 3.5 gilt entsprechend.

4. Kapitel: Das Zertifizierungsverfahren

§ 4.1 Vertragliche Grundlage

(1) Das Zertifizierungsverfahren beruht auf einem Vertrag zwischen dem Cloud-Anbieter und der Zertifizierungsstelle.

(2) Im Vertrag sind mindestens festzulegen:
a) der Zertifizierungsgegenstand mit Angabe aller für den Betrieb des Cloud-Dienstes relevanten Standorte;
b) die TCDP-Anforderungen in der maßgeblichen Fassung;
c) die Prüfstelle, welche die Prüfung durchführen soll;
d) diese Verfahrensordnung als die für die Zertifizierung maßgebliche Verfahrensregelung;
e) der Zertifizierungsantrag einschließlich der Angabe der beantragten Schutzanforderungsklasse;
f) die Mitwirkungspflichten des Cloud-Anbieters.

§ 4.2 Voraussetzungen der Zertifizierung

(1) Die Erteilung des Zertifikats setzt eine Prüfung des Cloud-Dienstes nach dieser Verfahrensordnung durch eine Prüfstelle voraus. Der Cloud-Anbieter hat die Prüfstelle zu benennen und die Akkreditierung der Prüfstelle nachzuweisen. Sie wird vermutet, wenn die Prüfstelle auf einer Liste der Zertifizierungsstelle im Sinne des § 2.6 verzeichnet ist.

(2) Nach Vertragsabschluss benennt die Zertifizierungsstelle dem Cloud-Anbieter und der Prüfstelle einen verantwortlichen Zertifizierer.

(3) Die Prüfstelle benennt der Zertifizierungsstelle den verantwortlichen Prüfer, den sie mit der Prüfung betraut hat.

(4) Der Zertifizierer stimmt den Prüfgegenstand, den Prüfumfang, die Prüfdauer und den Zeitplan der Prüfung mit dem verantwortlichen Prüfer sowie der Zertifizierungsstelle und dem Cloud-Anbieter ab. Gegenstand der Abstimmung sind auch beabsichtigte Anerkennungen vorliegender Zertifikate.

(5) Die Zertifizierungsstelle kann sich das Recht vorbehalten, an der Vor-Ort-Prüfung ganz oder teilweise teilzunehmen. Sie darf jedoch keine Prüfungshandlungen durchführen oder in das Prüfverfahren eingreifen.

§ 4.3 Bewertung der Prüfung

(1) Die Zertifizierungsstelle stellt durch eine Bewertung des Prüfberichts fest, ob die Prüfung ordnungsgemäß erfolgte, insbesondere den Anforderungen dieser Verfahrensordnung entspricht, und ob der Cloud-Dienst die TCDP-Anforderungen in der beantragten Schutzanforderungsklasse erfüllt.

(2) Die Zertifizierungsstelle kann von der Prüfstelle weitere Erläuterungen oder Ergänzungen des Prüfberichts verlangen.

(3) Die Zertifizierungsstelle kann im Benehmen mit der Prüfstelle Auskünfte und Nachweise vom Cloud-Anbieter erheben, soweit dies für die Zertifizierungsentscheidung erforderlich ist.

§ 4.4 Anerkennung von TCDP-Zertifikaten

(1) Die Zertifizierungsstelle anerkennt TCDP-Zertifikate für Bestandteile von Cloud-Diensten im Umfang von deren Gültigkeit und Schutzanforderungsklasse, sofern diese in Übereinstimmung mit dieser Verfahrensordnung erteilt wurden.

(2) Das Zertifikat kann im Fall der Anerkennung über die volle Gültigkeitsdauer nach § 5.3 erteilt werden. Das Zertifikat ist zu widerrufen, soweit ein anerkanntes Zertifikat erlischt. Dies gilt nicht, wenn der betreffende Bestandteil unverzüglich erneut zertifiziert wird und das Zertifikat anerkannt werden kann, oder wenn der Bestandteil unverzüglich durch eine Änderungszertifizierung nach § 4.9 in das Zertifikat für den Cloud-Dienst einbezogen wird.

(3) Die Zertifizierungsstelle überwacht die Gültigkeit der anerkannten Zertifikate. Sie weist den Cloud-Anbieter rechtzeitig auf den bevorstehenden Ablauf von Gültigkeitsdauern anerkannter Zertifikate hin.

§ 4.5 Anerkennung anderer Zertifikate

(1) Die Zertifizierungsstelle kann andere Zertifikate anerkennen, wenn sie einem TCDP-Zertifikat materiell und verfahrensmäßig gleichwertig sind. Sie stellt fest, mit welcher Schutzklasse und welchem Wiederherstellbarkeitsniveau das Zertifikat anerkannt wird.

(2) Eine materielle Gleichwertigkeit liegt vor, wenn das andere Zertifikat auf Anforderungen beruht, die denen des TCDP im Hinblick auf das Schutzniveau vergleichbar sind oder diese übertreffen.

(3) Eine verfahrensmäßige Gleichwertigkeit liegt vor, wenn das andere Zertifikat in einem Zertifizierungsverfahren erteilt wurde, das eine dieser Verfahrensordnung vergleichbare Gewähr für die ordnungsgemäße Prüfung und Zertifizierung bietet.

(4) Folgende Zertifikate gelten als materiell und verfahrensmäßig gleichwertig:
- Zertifikate nach ISO 27001 auf der Basis IT-Grundschutz;
- Testate nach SOC 2;
- Zertifikate nach BSI-Anforderungskatalog Cloud Computing.

(5) Die Zertifizierungsstelle hat die Anerkennung, insbesondere hinsichtlich der Schutzklasse und des Wiederherstellbarkeitsniveaus, zu begründen.

(6) Im Fall der Anerkennung gilt § 4.4 Abs. 2 bis 3 entsprechend.

§ 4.6 Entscheidung der Zertifizierungsstelle

(1) Die Zertifizierungsstelle entscheidet auf der Grundlage des Prüfberichts, der Bewertung durch den Zertifizierer und, soweit erforderlich, weiterer Feststellungen über die Verleihung des Zertifikats.

(2) Das Zertifikat ist im beantragten Umfang zu erteilen, wenn der Cloud-Dienst die entsprechenden TCDP-Anforderungen erfüllt.

(3) Das Zertifikat kann mit Einschränkungen erteilt werden, wenn zwar die TCDP-Anforderungen für den beantragten Zertifikatsumfang nicht erfüllt sind, aber die Anforderungen eines geringeren Umfangs erfüllt sind. Insbesondere kann das Zertifikat mit einer geringeren Zertifikatsdauer oder für eine geringere Schutzklasse erteilt werden.

(4) Soweit ein Cloud-Dienst die TCDP-Anforderungen nicht erfüllt, ist die Erteilung des Zertifikats abzulehnen.

(5) Soweit die Entscheidung hinter dem Antrag zurückbleibt, ist dies zu begründen.

(6) Die Zertifizierungsentscheidung ist dem Cloud-Anbieter mitzuteilen. Die Zertifizierungsentscheidung muss alle Informationen zu anerkannten Zertifikaten und die Angaben nach § 4.5 Abs. 5 enthalten.

§ 4.7 Nachbesserung

(1) Die Zertifizierungsstelle kann dem Cloud-Anbieter vor oder nach einer Entscheidung über die Erteilung des Zertifikats Gelegenheit zur Nachbesserung sowie zur Modifikation seines Zertifizierungsantrags geben.

(2) Soweit der Cloud-Dienst aufgrund der Nachbesserung die TCDP-Anforderungen entsprechend dem ursprünglichen oder modifizierten Zertifizierungsantrag erfüllt, ist das Zertifikat entsprechend zu erteilen.

§ 4.8 Widerspruch

(1) Der Cloud-Anbieter kann gegen eine Entscheidung, durch die er beschwert ist, Widerspruch bei der Zertifizierungsstelle einlegen. Der Widerspruch ist zu begründen. Eine Beschwer liegt vor, wenn die Zertifizierungsentscheidung hinter dem Antrag zurückbleibt.

(2) Der Widerspruch ist in Textform innerhalb einer Frist von 4 Wochen nach Zugang der Zertifizierungsentscheidung einzureichen.

(3) Die Zertifizierungsstelle prüft, ob der Widerspruch begründet ist.

(4) Soweit sich der Widerspruch gegen die Prüfung oder die Feststellungen der Prüfstelle richtet, informiert die Zertifizierungsstelle die Prüfstelle über den Widerspruch und holt eine Stellungnahme der Prüfstelle ein.

(5) Soweit der Widerspruch begründet ist, ändert die Zertifizierungsstelle die Zertifizierungsentscheidung. Soweit die Zertifizierungsstelle dem Widerspruch nicht abhilft, ist dies zu begründen.

(6) Die Entscheidung über den Widerspruch einschließlich Begründung ist dem Cloud-Anbieter in Textform mitzuteilen.

§ 4.9 Änderungszertifizierung

(1) Die Zertifizierungsstelle kann die Zertifikatsaussage auf Antrag des Cloud-Anbieters durch eine Änderungszertifizierung ändern, wenn eine erneute Zertifizierung einen unangemessen hohen Aufwand erfordern würde. Im Fall der Änderung besteht das Zertifikat mit seiner ursprünglichen Geltungsdauer fort.

(2) Eine Änderungszertifizierung kann insbesondere bei Änderungen des Cloud-Dienstes oder bei Änderung des TCDP erfolgen. Für das Verfahren der Änderungszertifizierung gelten die Bestimmungen über das Zertifizierungsverfahren entsprechend. Für die Prüfung im Rahmen der Änderungszertifizierung gilt § 3.6 entsprechend.

5. Kapitel: Das Zertifikat

§ 5.1 Erteilung und Inhalt des Zertifikats

(1) Die Zertifizierungsstelle erteilt dem Cloud-Anbieter entsprechend der Zertifizierungsentscheidung ein Zertifikat.

(2) Das Zertifikat enthält folgende Angaben:
- a) den Cloud-Anbieter, ggf. als Kurzbezeichnung;
- b) den Zertifizierungsgegenstand, ggf. als Kurzbezeichnung;
- c) die Zertifizierungsstelle;
- d) die Bezeichnung der maßgeblichen Fassung des TCDP, ggf. als Kurzbezeichnung;
- e) die Wissensbekundung, wonach der zertifizierte Cloud-Dienst die Datenschutzanforderungen des BDSG für Auftragsdatenverarbeitung gemäß TCDP in der jeweiligen Fassung für eine konkrete Schutzklasse und ein konkretes Wiederherstellbarkeitsniveau erfüllt (Zertifizierungsaussage); die Schutzklasse wird angegebenen als Schutzklasse „I“, „II“ oder „III“, das Wiederherstellbarkeitsnievau als Wiederherstellbarkeitsniveau „normal“, „hoch“ oder „sehr hoch“;
- f) eine eindeutige Zertifikatsnummer;
- g) die Gültigkeitsdauer des Zertifikats;
- h) eine Anlage mit den Angaben nach Abs. 3;
- i) das TCDP-Prüfzeichen.

(3) Die Anlage zum Zertifikat enthält folgende Angaben:
- a) die eindeutige Bezeichnung des Cloud-Anbieters;
- b) die eindeutige Bezeichnung des Zertifizierungsgegenstandes;
- c) die Bezeichnung dieser Verfahrensordnung als maßgebliche Verfahrensgrundlage;
- d) die Bezeichnung der angewendeten Regelwerke der Zertifizierungsstelle;
- e) die eindeutige Bezeichnung des Prüfberichtes und der Prüfstelle;
- f) die genaue Bezeichnung der maßgeblichen Fassung des TCDP;
- g) das Prüfergebnis.

(4) Das Zertifikat oder die Anlage können folgende weitere Elemente enthalten:
- a) Unternehmenskennzeichen der Zertifizierungsstelle;
- b) die Unterschrift eines Vertretungsberechtigten der Zertifizierungsstelle;
- c) die Beschreibung des Zertifizierungsgegenstandes;
- d) Hinweise der Zertifizierungsstelle.

(5) Bei Verwendung des Zertifikatsmusters nach Anlage 1) gelten die Anforderungen nach Abs. 2 und 3 als gewahrt.

(6) Die Zertifizierungsstelle vergibt für jedes Zertifikat eine eindeutige Zertifikatsnummer. Sie setzt sich zusammen aus der eindeutigen Bezeichnung der Zertifizierungsstelle, der Angabe TCDP und einer innerhalb der Zertifizierungsstelle eindeutigen Nummer (Beispiel: ZERTIFIZIERUNGSSTELLE-TCDP-0001).

§ 5.2 Veröffentlichung des Zertifikats

Die Zertifizierungsstelle führt ein Verzeichnis der Zertifikate und veröffentlicht das Zertifikat nebst Anlage während der Gültigkeitsdauer und weiterer zehn Jahre auf einer öffentlich zugänglichen Internetseite. Die Zertifikate müssen leicht zugänglich sein.

§ 5.3 Gültigkeitsdauer. Erneute Zertifizierung

(1) Das Zertifikat wird für eine Gültigkeitsdauer von längstens drei Jahren erteilt. Die Frist beginnt mit dem im Zertifikat ausgewiesenen Datum der Erteilung.

(2) Der Cloud-Anbieter kann vor oder nach Ablauf der Gültigkeitsdauer beantragen, den Cloud-Dienst nach Maßgabe dieser Verfahrensordnung erneut zu prüfen und zu zertifizieren.

(3) Für die erneute Prüfung und Zertifizierung gelten die Regeln zur (ersten) Prüfung und Zertifizierung. Der Cloud-Anbieter kann die Prüfstelle, die die vorherige Prüfung durchgeführt hat, oder eine andere Prüfstelle beauftragen. Er kann die Zertifizierungsstelle, die das vorherige Zertifikat erteilt hat, oder eine andere Zertifizierungsstelle beauftragen. Die Zertifizierungsstelle kann das erneute Zertifikat bei rechtzeitiger Beantragung auf das Datum unmittelbar nach Ablauf der Gültigkeitsdauer des vorangegangenen Zertifikats ausstellen.

§ 5.4 Überwachung

(1) Der Cloud-Dienst bedarf während der Gültigkeitsdauer des Zertifikats der Überwachung in Form einer jährlichen Zwischenprüfung gemäß § 3.6.

(2) Die Zertifizierungsstelle erinnert den Cloud-Anbieter und die Prüfstelle rechtzeitig an eine anstehende Zwischenprüfung und weist auf die Folge des Unterbleibens der Zwischenprüfung (§ 5.6) hin. Erfolgt die Zwischenprüfung nicht in der Frist nach § 3.6 Abs. 3, ergreift die Zertifizierungsstelle Maßnahmen gemäß § 5.6 Abs. 3 bis 7.

(3) Die Zertifizierungsstelle bewertet den Zwischenprüfbericht. § 4.3 gilt entsprechend.

(4) Die Zertifizierungsstelle entscheidet auf der Grundlage des Zwischenprüfberichts des Prüfers, der Bewertung durch den Zertifizierer und, soweit erforderlich, weiterer Feststellungen unverzüglich über die Aufrechterhaltung, Einschränkung, Aussetzung oder den Widerruf des Zertifikats. § 4.6 Abs. 6 gilt entsprechend.

§ 5.5 Prüfzeichen

(1) Die Erteilung des Zertifikats berechtigt den Cloud-Anbieter, für den zertifizierten Cloud-Dienst das Prüfzeichen nach Anlage 2) nach Maßgabe der Prüfzeichenbedingungen des Prüfzeicheninhabers zu führen.

(2) Das Prüfzeichen darf nur während der Gültigkeit des Zertifikats geführt werden.

(3) Das Prüfzeichen enthält ausschließlich folgende Angaben:

a) das graphische Prüfzeichen;
b) die Zertifikatsnummer;
c) die Gültigkeitsdauer;
d) die Bezeichnung TCDP mit Angabe der Schutzklasse [I, II, III];
e) die Angabe des Wiederherstellbarkeitniveaus [normal, hoch, sehr hoch];
f) die Angabe der Internetseite, auf der das TCDP veröffentlicht ist.

(4) Die Zertifizierungsstelle stellt das Prüfzeichen aus und stellt es dem Cloud-Anbieter graphisch in elektronischer Form zur Verfügung.

§ 5.6 Einschränkung, Aussetzung oder Widerruf des Zertifikats

(1) Der Cloud-Anbieter kann jederzeit die Einschränkung, Aussetzung oder den Widerruf des Zertifikats beantragen. Dem Antrag ist zu entsprechen, soweit dem nicht schwerwiegende Gründe entgegenstehen.

(2) Der Cloud-Anbieter ist verpflichtet, die Zertifizierungsstelle unverzüglich detailliert zu informieren, wenn ihm bekannt wird, dass die Voraussetzungen für die Erteilung des Zertifikats nicht vorlagen oder nicht mehr vorliegen.

(3) Wenn die Zertifizierungsstelle aufgrund Mitteilung des Cloud-Anbieters, der Prüfstelle oder eines Dritten oder aufgrund sonstiger Umstände Grund zur Annahme hat, dass die Voraussetzungen für die Zertifikatserteilung nicht vorlagen oder nicht mehr vorliegen, ergreift sie unverzüglich die erforderlichen Maßnahmen, um das Vorliegen der Voraussetzungen festzustellen. Die Zertifizierungsstelle kann insbesondere feststellen, dass eine Zwischenprüfung zur Aufrechterhaltung des Zertifikats erforderlich ist.

(4) Wenn die Zertifizierungsstelle die Erforderlichkeit einer Zwischenprüfung feststellt, setzt sie dem Cloud-Anbieter eine angemessene Frist zur Durchführung der Zwischenprüfung. Die Zertifizierungsstelle hat dem Cloud-Anbieter deutlich zu beschreiben, unter welchen Aspekten Zweifel an der Einhaltung der Zertifizierungsvoraussetzungen bestehen. Die Frist kann auf Antrag des Cloud-Anbieters verlängert werden.

(5) Die Zertifizierungsstelle kann das Zertifikat für die Dauer des Feststellungsverfahrens aussetzen. Im Fall der Aussetzung darf das Prüfzeichen nicht geführt werden. Der Cloud-Anbieter hat die Nutzer seines Cloud-Dienstes über die Aussetzung zu informieren.

(6) Die Zertifizierungsstelle trifft aufgrund ihrer Feststellungen, ggf. auf der Grundlage des Zwischenprüfungsberichts, die zur Einhaltung des TCDP erforderlichen Maßnahmen. Sie kann das Zertifikat einschränken, aussetzen oder widerrufen. Die Zertifizierungsstelle gibt dem Cloud-Anbieter vor ihrer Entscheidung Gelegenheit zur Stellungnahme. Die Entscheidung ist zu begründen und dem Cloud-Anbieter in Textform zuzustellen. Auf Antrag des Cloud-Anbieters kann eine Änderungszertifizierung erfolgen.

(7) Das Zertifikat ist zu widerrufen, wenn
a) die Zertifizierungsstelle feststellt, dass die Voraussetzungen für die Erteilung des Zertifikats nicht vorlagen oder nicht mehr vorliegen;
b) eine Zwischenprüfung nicht oder nicht innerhalb der Frist nach Abs. 4 durchgeführt wird;
c) der Inhaber des TCDP feststellt, dass das TCDP die gesetzlichen Anforderungen des BDSG oder die an dessen Stelle tretenden gesetzlichen Bestimmungen nicht oder nicht mehr erfüllt. Dies gilt nicht, wenn der Cloud-Anbieter unverzüglich eine Änderungszertifizierung nach einer neuen Version des TCDP beantragt und diese

unverzüglich durchgeführt wird.

(8) Der Widerruf oder die Einschränkung des Zertifikats werden drei Wochen nach Zustellung der Entscheidung über den Widerruf oder die Einschränkung wirksam. Die Aussetzung wird sofort wirksam. § 4.8 gilt entsprechend.

§ 5.7 Änderung des Cloud-Dienstes

(1) Wenn der Cloud-Anbieter oder der Anbieter eines Bestandteils eine Änderung des Cloud-Dienstes oder des Bestandteils vornimmt oder vorzunehmen beabsichtigt, die dazu führen kann, dass das Zertifikat zu widerrufen oder einzuschränken ist, ist der Cloud-Anbieter verpflichtet, die Zertifizierungsstelle unverzüglich über die beabsichtigte oder bereits erfolgte Änderung des Cloud-Dienstes zu informieren.

(2) Wenn die Zertifizierungsstelle aufgrund Mitteilung des Cloud-Anbieters, der Prüfstelle oder eines Dritten oder aufgrund sonstiger Umstände von der Änderung eines zertifizierten Cloud-Dienstes erfährt, die zu einer geänderten Beurteilung des Cloud-Dienstes im Hinblick auf das erteilte Zertifikat führen kann, ergreift sie unverzüglich die erforderlichen Maßnahmen, um festzustellen, ob die Voraussetzungen der Zertifizierung auch für den geänderten Cloud-Dienst vorliegen. § 5.6 gilt entsprechend.

6. Kapitel: Schlussbestimmungen

§ 6.1 Fortgeltung der Zertifikate nach einem DSGVO-Standard

(1) Die Beteiligten des Pilotprojekts wünschen und erwarten, dass nach Abschluss des Pilotprojekts nach dem Vorbild des TCDP ein Datenschutz-Standard für Cloud-Dienste auf der Grundlage der DSGVO entwickelt wird. Dabei sollte eine Anerkennung durch den Europäischen Datenschutz-Ausschuss nach Art. 42 DSGVO angestrebt werden.

(2) Die Projektbeteiligten wünschen, dass der in Abs. 1 genannte Standard eine Überleitung von TCDP-Zertifikaten aufgrund einer Änderungs- oder Überleitungszertifizierung zulässt, so dass TCDP-Zertifikate mit Maßgeblichkeit der DSGVO am 25. Mai 2018 möglichst lückenlos durch eine Zertifizierung nach dem neuen Standard auf Grundlage der DSGVO abgelöst werden können.

(3) Das Zertifikat erlischt mit Inkrafttreten der DSGVO am 25. Mai 2018, es sei denn, dass zu diesem Zeitpunkt (i) eine Übergangszertifizierung auf einen dem TCDP entsprechenden Standard zur Umsetzung der DSGVO erfolgt ist oder (ii) ein solches Zertifizierungsverfahren durch Abschluss eines entsprechenden Prüfvertrags eingeleitet ist oder (iii) die Europäische Kommission oder der Europäische Datenschutzausschuss eine andere Übergangsregelung geschaffen hat und deren Bedingungen für die Fortgeltung des Zertifikats erfüllt sind.

§ 6.2 Änderungen

Änderungen der Verfahrensordnung erfolgen durch den Inhaber oder Verwalter des TCDP.

Anlage 1) Zertifikatsmuster

Zertifikat

Die Zertifizierungsstelle der << Name >>

bescheinigt hiermit dem Unternehmen

<< Musterfirma >>

<< Musterstraße 99 >>

<< 123456 Musterort >>

für den Dienst

<< Name Cloud-Dienst >>

die Erfüllung der Datenschutzanforderungen für die Auftragsdatenverarbeitung gemäß dem

TCDP, Version 1.0,

Schutzklasse [I, II, III],

Wiederherstellbarkeitsniveau [normal, hoch, sehr hoch].

Die Prüfanforderungen sind in der Anlage zum Zertifikat referenziert. Die Anlage ist Bestandteil des Zertifikats und besteht aus 2 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem zugehörigen Prüfbericht und stellt eine Wissensbekundung der Zertifizierungsstelle dar, dass der geprüfte Dienst die Datenschutzanforderungen für die Auftragsdatenverarbeitung gemäß TCDP erfüllt.

Dieses Zertifikat mit der Registriernummer ZERTIFIZIERUNGSSTELLE-TCDP-0001 ist gültig bis zum tt.mm.jjjj.

Ort, tt.mm.jjjj

Vorname, Name
Leiter Zertifizierungsstelle

Prüfzeichen

Zertifizierungsstelle
Anschrift
www.zertstelle.de

www.tcdp.de

Zertifizierungssystem

Die Zertifizierung wurde auf Basis der folgenden Rahmenbedingungen durchgeführt:

- „Verfahrensordnung für Zertifizierungen nach dem Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP), Version 1.0,

Prüfbericht

- „Prüfbericht für << Name des Cloud-Dienstes >> “, Berichtsversion << Versionsnummer >> vom << Datum >>, << Name Prüfstelle >>

Prüfanforderungen

- „Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP), Version 1.0

Die Prüfanforderungen sind veröffentlicht auf den Seiten

- www.tcdp.de

Prüfgegenstand

Prüfgegenstand ist der Dienst << Name des Cloud-Dienstes >>.

<< ggf. weitere Beschreibung >>

Prüfergebnis

- Der Prüfgegenstand erfüllt die Datenschutzanforderungen für die Auftragsdatenverarbeitung gemäß Trusted Cloud-Datenschutzprofil (TCDP) für die Schutzklasse << [I, II, III] >> und das Wiederherstellbarkeitsniveau << [normal, hoch, sehr hoch] >>.

Anlage 2) Muster des Prüfzeichens

[Hinweis: Im Original farbig]