Trusted Cloud

Kompetenzzentrum Trusted Cloud

Thesenpapier – Eckpunkte eines Zertifizierungs-verfahrens für Cloud-Dienste

Nr. 12

Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“

Das Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ wird im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) vom Kompetenzzentrum Trusted Cloud in Kooperation mit Projektpartnern des Technologieprogramms Trusted Cloud durchgeführt.

Am Pilotprojekt sind alle maßgeblichen Interessenvertreter beteiligt. Dazu gehören insbesondere Datenschutzbehörden und Privatwirtschaft, d. h. Anbieter und Nutzer von Cloud-Diensten, sowie Stellen mit Erfahrung in der Normung und Zertifizierung von IT-Diensten. Die Zahl der Projektbeteiligten ist begrenzt, um die Arbeitsfähigkeit der Gruppe sicherzustellen. Das Pilotprojekt wird von Prof. Dr. Georg Borges (Universität des Saarlandes) vom Kompetenzzentrum Trusted Cloud geleitet.

Inhaltsverzeichnis

1 Die Zertifizierung von Cloud-Diensten

Die Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ im Kompetenzzentrum Trusted Cloud des Bundesministeriums für Wirtschaft und Energie (BMWi) hat im Thesenpapier „Datenschutzrechtliche Lösungen für Cloud Computing. Ein rechtspolitisches Thesenpapier“ [1] vom September 2012 ein Konzept für eine datenschutzrechtliche Zertifizierung von Cloud-Diensten beschrieben.

Im Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“, das seit November 2013 im Auftrag des BMWi vom Kompetenzzentrum Trusted Cloud in Kooperation mit Projektpartnern durchgeführt wird, werden die zentralen Elemente dieses Konzepts im Detail erarbeitet. Ein wesentlicher Bestandteil dieser Arbeiten betrifft die Beschreibung eines geeigneten Zertifizierungsverfahrens.

→ Herausforderung: effizienter Datenschutz im Cloud Computing

Bei Cloud-Computing-Diensten werden in der Regel Daten im Auftrag des Cloud-Nutzers verarbeitet. Werden dabei personenbezogene Daten verarbeitet, handelt es sich datenschutzrechtlich um eine sogenannte Auftragsdatenverarbeitung im Sinne des § 11 des Bundesdatenschutzgesetzes (BDSG), bei der der Cloud-Nutzer als Auftraggeber, der Cloud-Anbieter als Auftragnehmer tätig wird. Dies hat zur Folge, dass gemäß § 11 Abs. 1 BDSG der Cloud-Nutzer für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich ist. Das geltende deutsche und europäische Datenschutzrecht verlangt ebenso wie der Entwurf der EU-Datenschutz-Grundverordnung (DSGVO) vom Auftraggeber, sich von der Erfüllung der datenschutzrechtlichen Anforderungen auch durch den Auftragnehmer zu überzeugen.

Nutzt ein Unternehmen für die Verarbeitung personenbezogener Daten Cloud-Computing-Dienste, hat es sicherzustellen, dass auch die Datenverarbeitung beim Cloud-Anbieter den datenschutzrechtlichen Vorschriften genügt. Zu diesem Zweck müssen die technischen und organisatorischen Maßnahmen des Cloud-Anbieters überprüft werden. So hat sich der Cloud-Nutzer als Auftraggeber gemäß § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Cloud-Anbieter getroffenen technischen und organisatorischen Maßnahmen zu überzeugen; das Ergebnis dieser Überprüfung ist nach § 11 Abs. 2 Satz 5 BDSG zu dokumentieren. Unterlässt es ein Cloud-Nutzer vorsätzlich oder fahrlässig, sich vor Beginn der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen, stellt dies gemäß § 43 Abs. 1 Nr. 2b BDSG eine Ordnungswidrigkeit dar, die nach § 43 Abs. 3 BDSG mit einer Geldbuße bis zu 50.000 EUR geahndet werden kann.

Eine Überprüfung der technischen und organisatorischen Maßnahmen des Cloud-Anbieters durch jeden einzelnen Cloud-Nutzer würde jedoch zu weit überhöhten Kosten führen und kann jedenfalls von kleinen Unternehmen, die Cloud-Dienste nutzen, nicht aus eigener Kraft durchgeführt werden. Ein weiteres Problem bezüglich der Kontrollpflicht ergibt sich

1 Das Papier ist abrufbar über www.trusted-cloud.de.

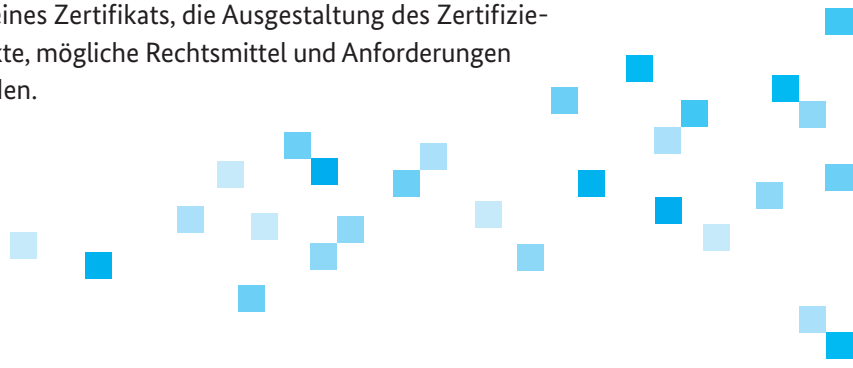
zudem daraus, dass Nutzer häufig viele verschiedene Cloud-Systeme verwenden und zugleich eine Vielzahl von Nutzern auf dieselben Cloud-Systeme zurückgreift. Dies führt dazu, dass beim Cloud Computing jeder Nutzer eine Vielzahl von Diensten kontrollieren müsste und umgekehrt die einzelnen Dienste durch eine Vielzahl von Nutzern kontrolliert würden.

→ Lösung: Zertifizierung von Cloud-Diensten durch unabhängige Dritte

Dieses strukturelle Problem kann durch eine Bündelung der Kontrolle gelöst werden, indem ein geeignetes Zertifizierungsverfahren geschaffen wird, das alle datenschutzrechtlichen Anforderungen an den Auftragsdatenverarbeiter im Cloud Computing, d. h. an den Cloud-Anbieter, umfasst. Dabei würden insbesondere die technischen und organisatorischen Maßnahmen des Cloud-Anbieters von einer fachlich geeigneten und unabhängigen Zertifizierungsstelle auf der Grundlage einheitlicher und anerkannter Kriterien (vgl. Ziffer 4, S. 14) überprüft. Sind alle datenschutzrechtlichen Anforderungen erfüllt, würde dieses Ergebnis durch die Erteilung eines Zertifikats bestätigt werden. Das Ergebnis der Prüfung käme dabei allen Nutzern des geprüften Cloud-Dienstes zugute. Mit einer solchen Zertifizierung könnte sowohl ein hohes Datenschutzniveau gewährleistet als auch eine effiziente Grundlage für die Nutzung von Cloud-Diensten geschaffen werden.

Eine derartige Bündelung der Kontrolle ist grundsätzlich bereits de lege lata zulässig. Denn die nach § 11 Abs. 2 Satz 4 BDSG geforderte Überprüfung muss nicht durch den Auftraggeber persönlich erfolgen, sondern kann auch durch einen unabhängigen Dritten vorgenommen werden. Der Dritte kann die Prüfung auch für mehrere Auftraggeber gleichzeitig durchführen, soweit er für jeden Auftraggeber die jeweils geforderte Prüfung wahrnimmt. Allerdings besteht erhebliche Rechtsunsicherheit in Bezug auf die Anforderungen, die an ein solches Testat bzw. Zertifikat zu stellen sind, sowie hinsichtlich der damit einhergehenden Rechtsfolgen. Eine gesetzliche Regelung einer Zertifizierung besteht derzeit auf Bundesebene nicht.

Im November 2013 startete deshalb das BMWi das Pilotprojekt „Datenschutz-Zertifizierung für Cloud Computing“. Es ist in das BMWi-Technologieprogramm „Trusted Cloud“ eingebunden, das innovative, sichere und rechtskonforme Cloud-Computing-Lösungen entwickelt und erprobt. In diesem Pilotprojekt des BMWi werden nicht nur die geltenden Regelungen des BDSG berücksichtigt, sondern auch Fragen erörtert, die für die Ausgestaltung der künftigen DSGVO relevant sind. Im Rahmen des Pilotprojekts sollen die Eckpunkte für ein geeignetes Zertifizierungsverfahren beschrieben werden, wobei im Folgenden insbesondere Inhalt und Rechtswirkung eines Zertifikats, die Ausgestaltung des Zertifizierungsverfahrens, haftungsrechtliche Aspekte, mögliche Rechtsmittel und Anforderungen an die Zertifizierungsstellen erörtert werden.



2 Das Zertifikat

→ Inhalt und Aussage des Zertifikats

Unter Zertifikat versteht das Konzept der AG „Rechtsrahmen des Cloud Computing“ die Wissensbekundung der Zertifizierungsstelle, dass der geprüfte Dienst die datenschutzrechtlichen Anforderungen erfüllt. Gegenstand der Überprüfung im Rahmen der Zertifizierung ist insbesondere die Einhaltung der technischen und organisatorischen Maßnahmen von Cloud-Diensten, die zur Erfüllung der datenschutzrechtlichen Anforderungen erforderlich sind. Das Ergebnis der Zertifizierung ist die Erteilung eines Testats bzw. Zertifikats über die Einhaltung der einschlägigen datenschutzrechtlichen Normen. Vor diesem Hintergrund wird synonym auch der Begriff „Compliance-Zertifikat“ verwendet. In diesem Papier wird von Datenschutz-Zertifizierung gesprochen.

Die Zertifizierung in diesem Sinne ist von Verfahren abzugrenzen, die mit der Erteilung eines Gütesiegels enden, da in einem Gütesiegel-Verfahren nicht nur die einschlägigen rechtlichen Normen maßgebliche Prüfkriterien sind, sondern auch darüber hinausgehende oder abweichende datenschutzrechtliche Bewertungen berücksichtigt werden können. Ebenso ist sie von Verfahren abzugrenzen, bei denen einzelne oder mehrere datenschutzrechtliche Aspekte berücksichtigt werden, aber nicht die Gesamtheit der gesetzlichen (datenschutzrechtlichen) Anforderungen geprüft wird.

Da sich die Prüfung insbesondere darauf bezieht, ob der Cloud-Anbieter die notwendigen technischen und organisatorischen Maßnahmen ergriffen hat, setzt die Prüfung eine Bewertung voraus, welche Maßnahmen erforderlich sind. Nach § 9 Satz 2 BDSG sind Maßnahmen nur dann erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Auch die Anlage zu § 9 BDSG, die die nötigen Kontrollmaßnahmen exemplarisch aufzählt, stellt auf die Art der zu schützenden personenbezogenen Daten ab. So sind umso strengere Anforderungen zu erfüllen, je höher der Schutzbedarf der zu verarbeitenden Daten und des Datenverarbeitungsvorgangs insgesamt ist. Sollen im Rahmen des Cloud-Dienstes besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG, beispielsweise Gesundheitsdaten, verarbeitet werden, haben die technischen und organisatorischen Maßnahmen diesem erhöhten Schutzbedarf Rechnung zu tragen. Cloud-Dienste, die für die Verarbeitung „normaler“ personenbezogener Daten, z. B. Kunden-Stammdaten, ausreichende Sicherheitsmaßnahmen vorsehen, sind daher ggf. für die Verarbeitung von personenbezogenen Gesundheitsdaten ungeeignet. Vor diesem Hintergrund hat das Zertifikat auch eine Aussage darüber zu treffen, für welche Schutzklasse von Daten der Cloud-Dienst geeignet ist. Auf diese Weise kann der Cloud-Nutzer erkennen, ob ein angebotener Cloud-Dienst den Besonderheiten seiner Datenverarbeitung angemessen Rechnung trägt.[2]

2 Zur Bedeutung von Schutzstufen vgl. Papier Kompetenzzentrum Trusted Cloud (Hrsg.), „Schutzklassen in der Datenschutz-Zertifizierung“, April 2015, abrufbar unter www.trusted-cloud.de.

→ Rechtswirkung des Zertifikats

Das Zertifikat stellt eine Wissensbekundung der Zertifizierungsstelle dar, dass der geprüfte Cloud-Dienst die datenschutzrechtlichen Anforderungen erfüllt, insbesondere dass die erforderlichen technischen und organisatorischen Maßnahmen eingehalten werden. Damit ist aber noch keine Aussage darüber getroffen, welche Wirkung einem solchen Zertifikat zukommt.

Die Durchführung eines Zertifizierungsverfahrens durch einen Cloud-Anbieter ist zunächst Ausdruck einer bewussten und gewollten Selbstregulierung. Zertifikate entfalten insofern Marktanreize, als sie Transparenz und Vertrauen schaffen und dadurch für die geprüften Dienste Wettbewerbsvorteile bieten. Dem Nutzer ermöglichen Zertifikate, sich effizient zu informieren und Angebote zu vergleichen.

Darüber hinaus erleichtert die Zertifizierung von Cloud-Diensten dem Nutzer, sich – wie von § 11 Abs. 2 Satz 4 BDSG gefordert – von der Einhaltung der technisch-organisatorischen Maßnahmen durch den Cloud-Anbieter zu überzeugen (vgl. Ziffer 1, Seite 7). Mangels ausdrücklicher Regelung besteht aber erhebliche Rechtsunsicherheit, unter welchen Voraussetzungen die Nutzung eines zertifizierten Dienstes den Cloud-Nutzer tatsächlich davon befreit, sich selbst von der Erfüllung der notwendigen Anforderungen zu überzeugen. Um die nötige Rechtssicherheit zu schaffen, sollte daher die künftige europäische Datenschutz-Grundverordnung (DSGVO) eine Regelung enthalten, wonach ein Unternehmen durch die Nutzung eines gemäß den gesetzlichen Regelungen zertifizierten Cloud-Diensts seine Überzeugungspflicht erfüllen kann. Ein Nutzer könnte dann auf das Zertifikat vertrauen und auch ohne eigene Kontrolle des Cloud-Dienstes diesen datenschutzkonform nutzen.

In der gesetzlichen Grundlage sollte auch geregelt werden, dass der Cloud-Nutzer das Zertifikat tatsächlich einzusehen hat, um den Dienst auf die Geeignetheit für seine beabsichtigte Datenverarbeitung zu prüfen; die bloße Existenz eines Zertifikats für den Dienst sollte demnach die eigene Überzeugungspflicht nicht entfallen lassen. So ist es auch nach derzeitiger Rechtslage zur Vermeidung eines Bußgelds nicht ausreichend, dass die technisch-organisatorischen Maßnahmen objektiv vorliegen. Vielmehr muss sich die verantwortliche Stelle hiervon „überzeugen“; § 11 Abs. 2 Satz 5 BDSG verlangt hierfür eine Dokumentation des Ergebnisses. Einer Einsichtnahme in das Zertifikat bedarf es vor allem auch deshalb, um überhaupt feststellen zu können, ob der vorgesehene Cloud-Dienst für die beabsichtigte Datenverarbeitung, insbesondere im Hinblick auf den Schutzbedarf der zu verarbeitenden Daten, geeignet ist. Beweisen lassen sich Einsichtnahme und Prüfung – wie auch schon bisher – insbesondere durch die Anordnung einer entsprechenden Dokumentationspflicht. Vor diesem Hintergrund sollte die DSGVO eine Regelung enthalten, wonach ein Cloud-Nutzer seine Pflicht, sich vom Vorliegen der technisch-organisatorischen Voraussetzungen zu überzeugen, dadurch erfüllen kann, dass er ein Zertifikat[3] des Cloud-Diensts eingesehen und daraufhin die Geeignetheit des Diensts für die beabsichtigte Datenverarbeitung festgestellt und dokumentiert hat. Sind diese Voraussetzungen erfüllt, kann gegen den Cloud-Nutzer auch dann kein Bußgeld verhängt werden, wenn er sich nicht persönlich von der Einhaltung der technisch-organisatorischen Voraussetzungen überzeugt hat.

3 In der gesetzlichen Regelung müsste auch festgelegt werden, welche Informationen dem Cloud-Nutzer mit dem Zertifikat bereitgestellt werden müssen.

Das Zertifikat hat auch bei Folgefragen rechtliche Bedeutung, insbesondere wenn es um das Verschulden des Cloud-Nutzers bei Datenschutzverstößen geht. Das Vorliegen eines Zertifikats bindet zwar die Datenschutzaufsichtsbehörden bei der Erfüllung ihrer Beratungs- und Kontrollaufgaben nicht und steht auch dem Erlass von Anordnungen nicht entgegen, wenn die Aufsichtsbehörde die datenschutzrechtlichen Voraussetzungen trotz Vorliegens eines Zertifikats nicht als erfüllt ansieht. Soweit die Datenschutzaufsichtsbehörde aber den Erlass eines Bußgeldes wegen Vorliegens einer Ordnungswidrigkeit erwägt, ist das Zertifikat bei der Prüfung einer schuldhaften Pflichtverletzung zu berücksichtigen. Da der Cloud-Nutzer mit der Einsichtnahme in das Zertifikat aber seine gesetzliche Pflicht grundsätzlich erfüllt, fehlt es regelmäßig an einer schuldhaften Pflichtverletzung. Eine schuldhafte Pflichtverletzung und entsprechend der Erlass eines Bußgeldes kommen daher regelmäßig nur in Betracht, wenn dem Cloud-Nutzer eine andere Pflichtverletzung vorgeworfen werden kann, er etwa von dem Datenschutzverstoß Kenntnis hatte. Entsprechendes gilt für zivilrechtliche Verfahren, wenn etwa Betroffene Schadensersatzansprüche aufgrund einer unzulässigen Datenverarbeitung geltend machen.

Der europäische Gesetzgeber könnte auch regeln, ob und unter welchen Voraussetzungen das Vorliegen eines Zertifikats als geeignete Grundlage für eine sichere Übermittlung in einen Drittstaat und somit als Alternative zum Safe-Harbor-Abkommen oder zum Abschluss von EU-Standardverträgen angesehen werden kann. De lege ferenda könnten einem Zertifikat auch weitere Rechtswirkungen (z. B. Privilegierung zertifizierter Dienste im Rahmen von Vergabeverfahren) beigemessen werden.

Wie eingangs ausgeführt, stellt das Zertifikat eine Wissensbekundung der das Zertifikat vergebenden Stelle dar. Ob es sich dabei um eine privatrechtliche Aussage oder einen Verwaltungsakt (entweder einer als Zertifizierungsstelle tätigen Behörde oder einer privaten Zertifizierungsstelle als Beliehene) handelt, hängt insbesondere von der näheren Ausgestaltung durch die künftige DSGVO oder die auf ihrer Grundlage erlassenen delegierten Rechtsakte ab. Auf die Rechtswirkung des Zertifikats sollte dies keine Auswirkungen haben.

→ Geltungsdauer und Geltungsbereich des Zertifikats

Zertifizierungen von Cloud-Diensten betreffen in ganz wesentlichem Umfang technische und organisatorische Maßnahmen, die aufgrund der technischen Fortentwicklung nur eine begrenzte Gültigkeitsdauer für sich beanspruchen können. Es sollte deshalb vorgesehen werden, dass Zertifikate für Cloud-Dienste maximal drei Jahre gültig sind und danach der Rezertifizierung bedürfen. Es sollte auch eine Regelung über das Erfordernis von Zwischenprüfungen getroffen werden. Für eine Rezertifizierung nach Ablauf der Geltungsdauer sollte ein vereinfachtes Prüfverfahren vorgesehen werden, das sich auf die tatsächlichen oder rechtlichen Änderungen gegenüber der Ausgangszertifizierung bezieht.

Das Zertifikat sollte im gesamten räumlichen Anwendungsbereich der DSGVO gelten, um Cloud-Anbietern und Cloud-Nutzern im gesamten Binnenmarkt Rechtssicherheit zu verschaffen und widersprechende Entscheidungen in verschiedenen Mitgliedstaaten zu vermeiden. Damit wird auch dem Ziel der DSGVO Rechnung getragen, unionsweit ein einheitliches Datenschutzniveau zu gewährleisten und zugleich Unterschiede, die den freien Datenverkehr im Binnenmarkt behindern könnten, zu beseitigen. Das Problem des Zugriffs ausländischer Geheimdienste auf Daten, die in der Cloud gespeichert sind, wird mit einer Zertifizierung jedoch nicht gelöst.

3 Erteilung des Zertifikats

→ Zertifizierungsverfahren

Eingeleitet wird das Zertifizierungsverfahren durch einen Antrag des Cloud-Anbieters, der aus Gründen der Selbstregulierung bzw. zur Erlangung von Wettbewerbsvorteilen für seinen Cloud-Dienst ein Zertifikat anstrebt. Die Durchführung eines Zertifizierungsverfahrens sollte dabei in der DSGVO nicht als Pflicht, sondern als freiwilliges Verfahren ausgestaltet werden. Auf der Grundlage eines Antrags des Cloud-Anbieters auf bzw. nach Abschluss eines Vertrags zur Durchführung eines Zertifizierungsverfahrens prüft die hiermit beauftragte Prüfstelle den Dienst anhand der festgelegten Prüfanforderungen. Auf der Grundlage des Prüfberichts der Prüfstelle, d. h. auf Basis der Aktenlage, entscheidet anschließend die Zertifizierungsstelle, ob die datenschutzrechtlichen Voraussetzungen erfüllt sind und deshalb ein Zertifikat zu verleihen oder zu versagen ist. Das Zertifikat muss von der Zertifizierungsstelle selbst oder einer sonstigen gesetzlich bestimmten Stelle veröffentlicht werden. Dabei sollte auch das Datum der Erteilung und des Ablaufs der Gültigkeit des Zertifikats angegeben werden.

→ Prüfanforderungen und Prüfintensität

Grundlage des Prüfverfahrens sind definierte Prüfanforderungen bzw. Prüfkriterien, d. h. bestimmte Anforderungen, die erfüllt sein müssen, damit ein Zertifikat erteilt werden kann. Im Rahmen des Pilotprojekts „Datenschutz-Zertifizierung für Cloud Computing“ wird zu diesem Zweck ein datenschutzrechtlicher Prüfkatalog für Cloud-Dienste, das „Trusted-Cloud-Datenschutzprofil für Cloud-Dienste“ (TCDP), erarbeitet.[4] Das TCDP konkretisiert die gesetzlichen Anforderungen, die sich aus dem BDSG für Cloud-Dienste ergeben, und stellt damit eine Vorlage auch für die unter der künftigen DSGVO geltenden Vorgaben dar.

Die Prüfanforderungen für die Erteilung des Zertifikats sollten auf gesetzlicher Grundlage für den europäischen Binnenmarkt einheitlich festgelegt werden. Eine Festlegung der Prüfanforderungen in der DSGVO selbst würde zwar eine einheitliche Regelung ermöglichen, aber den Text der Verordnung überfrachten; zudem wäre eine solche Regelung zu unflexibel. Daher sollten die Prüfanforderungen in einem Verfahren festgelegt werden, in dem Aufsichtsbehörden sowie Vertreter von Anbietern und Nutzern der Auftragsdatenverarbeitung beteiligt werden.

Die erforderlichen technischen und organisatorischen Maßnahmen orientieren sich grundsätzlich am Einzelfall und sind aufgrund einer Abwägung von Schutzerfordernis und Aufwand der Maßnahme zu ermitteln (vgl. § 9 BDSG). Daher können die im Einzelfall gesetzlich erforderlichen Maßnahmen nicht generell festgelegt werden. Dies schließt einheitliche Zertifikate jedoch nicht aus. Dabei ist zunächst zu berücksichtigen, dass ein Großteil der Anforderungen an die technischen und organisatorischen Maßnahmen für eine Vielzahl von Datenverarbeitungsvorgängen gleich ist. Daher könnten für die meisten Anwendungsbereiche ähnliche Anforderungen formuliert werden. Soweit auf Seiten des Auftraggebers insbesondere aufgrund der Art der Daten, z. B. Gesundheitsdaten, besondere

4 Kompetenzzentrum Trusted Cloud (Hrsg.), „Trusted-Cloud-Datenschutzprofil für Cloud-Dienste (TCDP) – v.0.9“, April 2015, abrufbar unter www.trusted-cloud.de.

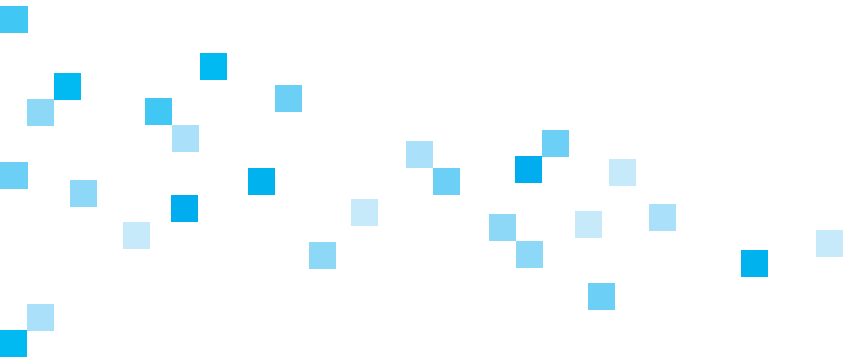
gesetzliche Anforderungen bestehen, lassen sich Fallgruppen bilden, die im Rahmen der Zertifizierung berücksichtigt und im Zertifikat durch die Angabe einer entsprechenden Schutzklasse ausgewiesen werden können. Entsprechendes gilt, wenn das Risikoprofil der Datenverarbeitung durch besondere technische Schutzmaßnahmen (z. B. Verschlüsselung) verändert wird.[5]

Im Hinblick auf die Prüfintensität, die dem Zertifizierungsverfahren zugrunde liegt, ist von entscheidender Bedeutung, dass Transparenz gegenüber dem Cloud-Anbieter, aber vor allem auch gegenüber dem Cloud-Nutzer hergestellt wird. So ist bei der Regelung des Zertifizierungsverfahrens möglichst konkret und verständlich darzulegen, wie die Prüfung im Rahmen der Zertifizierung abläuft und wie detailliert die einzelnen Anforderungen überprüft werden. Dabei ist es für die Zertifizierung eines Cloud-Diensts regelmäßig erforderlich, die Einhaltung der technisch-organisatorischen Maßnahmen beim Cloud-Anbieter vor Ort zu überprüfen.

→ Kosten des Zertifizierungsverfahrens

Da der Aufwand eines Zertifizierungsverfahrens maßgeblich von den (erst noch festzulegenden) Prüfanforderungen und der (ebenfalls erst noch zu regelnden) Prüftiefe abhängt, ist im Rahmen des Pilotprojekts keine konkrete Aussage zu den voraussichtlichen Kosten eines Zertifizierungsverfahrens möglich.

Eine gesetzliche Kostenregelung für ein Zertifizierungsverfahren wird nicht als notwendig angesehen. Vielmehr sollte dies, soweit es sich um eine privatwirtschaftliche Dienstleistung handelt, dem Markt überlassen bleiben. Zwar sollten die Einnahmen den Zertifizierungsstellen eine kostendeckende Tätigkeit und auch die Erwirtschaftung von Gewinnen ermöglichen. Zugleich sollten die Kosten für die Cloud-Anbieter aber erschwinglich sein und insbesondere keine abschreckende Wirkung entfalten, da andernfalls die gewünschte Verbreitung von Zertifikaten auf dem Markt erheblich beeinträchtigt würde.



5 Vgl. Papier „Schutzklassen in der Datenschutz-Zertifizierung“ (Fn. 2).

4 Prüfstellen und Zertifizierungsstellen

→ Differenzierung zwischen Prüfstelle und Zertifizierungsstelle

Im Rahmen der datenschutzrechtlichen Zertifizierung sind zwei Schritte erforderlich: In einem ersten Schritt erfolgt eine Prüfung des Cloud-Dienstes anhand der maßgeblichen Prüfanforderungen, die in einem Prüfbericht zu dokumentieren ist (siehe Seite 11). In einem zweiten Schritt ist auf der Grundlage der dokumentierten Prüfung über die Verleihung bzw. Versagung oder eingeschränkte Verleihung des beantragten Zertifikats zu entscheiden. Die Stelle, die die Prüfung vornimmt, wird dabei als Prüfstelle, die Stelle, die über die Vergabe des Zertifikats entscheidet, als Zertifizierungsstelle bezeichnet. Jedenfalls bei funktionaler Betrachtungsweise sind demnach Prüf- und Zertifizierungsstelle voneinander zu unterscheiden.

Mit der funktionalen Trennung von Prüfung und Zertifizierung ist eine rechtlich-organisatorische Unterscheidung von Prüfstelle und einer Zertifizierungsstelle nicht vorgegeben. Es sprechen aber gute Gründe dafür, die Unterscheidung von Prüf- und Zertifizierungsstelle auch in organisatorischer Hinsicht vorzusehen und entsprechend beiden Stellen separate Aufgabenkreise zuzuweisen und auch eine rechtliche Trennung zumindest zuzulassen. Dies ermöglicht es, dass sich spezialisierte Einheiten herausbilden, die sich mit der Prüfung oder Zertifizierung befassen. In dieser Weise sind im Bereich des Datenschutzes und der IT-Sicherheit eine Vielzahl von Zertifizierungsverfahren organisiert. Die organisatorische und rechtliche Trennung von Prüfungsstelle und Zertifizierungsstelle kann daher als bewährter Standard angesehen werden.

Die rechtliche Trennung von Prüf- und Zertifizierungsstellen erfordert es, beiden separate Aufgabenkreise zuzuweisen. Zudem entstehen eigenständige Rechtsbeziehungen zwischen der Prüfstelle und dem Cloud-Anbieter einerseits und der Zertifizierungsstelle und dem Cloud-Anbieter andererseits. Diese Rechtsbeziehung kann in Form eines privatrechtlichen Vertrags oder eines Verwaltungsverfahrens gestaltet sein. Dabei sollte jedenfalls die Rechtsbeziehung zwischen Prüfstelle und Cloud-Anbieter als privatrechtliches Verhältnis ausgestaltet sein, wie es der bisherigen Praxis entspricht. Die Rechtsbeziehung zwischen Cloud-Anbieter und Zertifizierungsstelle kann nach dem Papier „Datenschutz-Zertifizierung durch private Stellen“[6] sowohl privatrechtlich als auch öffentlich-rechtlich ausgestaltet sein.

Der Cloud-Anbieter ist demnach Vertragspartner der Prüfstelle und steht in einer Rechtsbeziehung zur Zertifizierungsstelle. Entsprechend hat der Cloud-Anbieter die Wahl, an welche Prüfstelle und an welche Zertifizierungsstelle er sich wendet. Diese Wahlmöglichkeit sollte nicht eingeschränkt werden, damit sich ein Markt für Prüfung und Zertifizierung von Cloud-Diensten entwickeln kann.

Die schwierigsten Fragen in diesem Zusammenhang betreffen das Verhältnis zwischen Prüfstelle und Zertifizierungsstelle. Aufgrund der organisatorischen und rechtlichen Trennung besteht im Rahmen der Zertifizierung nicht notwendig ein Rechtsverhältnis zwischen ihnen. Bisher schränken Zertifizierungsstellen in ihren Zertifizierungsbedingungen oft

6 Das Papier ist abrufbar über www.trusted-cloud.de.

die Wahl der Prüfstelle ein, indem nur bestimmte Prüfstellen zugelassen werden. Dies erscheint auf der Grundlage der bisherigen Rechtslage, in der es an einer gesetzlichen Qualitätssicherung für Prüfstellen und für Prüfungen fehlt, sinnvoll. Im Rahmen einer gesetzlich fundierten Datenschutz-Zertifizierung ist dies jedoch wohl nicht mehr geboten. Stattdessen könnte der europäische Gesetzgeber auch ein System installieren, wonach an die Prüfstelle und die Prüfung einschließlich des Prüfberichts qualitative Anforderungen gestellt werden und im Gegenzug die Zertifizierungsstelle die Prüfung jeder Prüfstelle akzeptieren muss, die diese Anforderungen erfüllt. Denkbar wäre schließlich auch, der Zertifizierungsstelle trotz Vorliegens gesetzlicher qualitativer Anforderungen die Möglichkeit einzuräumen, eigene Anforderungen an Prüfstellen oder Prüfberichte zu stellen. Dies wäre aber nur dann zu rechtfertigen, wenn eine hinreichende Wahlmöglichkeit zwischen Zertifizierungsstellen für den Cloud-Anbieter besteht. Die Zertifizierungsstelle sollte aber in jedem Fall die Möglichkeit haben, Anforderungen an Sprache und, soweit nicht gesetzlich geregelt, Form des Prüfberichts zu formulieren.

→ Anforderungen an die Zertifizierungs- und Prüfstellen

Unabhängig davon, ob Prüf- und Zertifizierungsstelle Teil derselben Einrichtung oder rechtlich eigenständig organisiert sind, ist gesetzlich festzulegen, welche Anforderungen an Zertifizierungs- und Prüfstellen zu stellen sind und ob die Zertifizierung durch private oder öffentliche Stellen erfolgen soll.

Die Möglichkeit, datenschutzrechtliche Compliance-Zertifikate nach der DSGVO zu vergeben, ist nicht auf Aufsichtsbehörden zu beschränken, sondern muss auch durch private Stellen erfolgen können. Dies sollte in der DSGVO klargestellt werden.[7]

Hinsichtlich der Frage, welche inhaltlichen Anforderungen an Zertifizierungsstellen zu stellen sind, ist zu berücksichtigen, dass sowohl Cloud-Anbieter als auch Cloud-Nutzer nur dann von angebotenen Zertifikaten Gebrauch machen, wenn sie den Zertifikaten vertrauen können. Dies setzt voraus, dass auf die von den Zertifizierungsstellen getroffenen Aussagen Verlass ist. Um die Qualität und Akzeptanz von Zertifikaten auf dem Markt und bei den Aufsichtsbehörden sicherzustellen, kommt daher der Eignung und Unabhängigkeit der Zertifizierungsstellen große Bedeutung zu. Zur Konkretisierung dieser Voraussetzungen sollten gesetzliche Anforderungen festgelegt werden, die von den Zertifizierungsstellen zu erfüllen sind. So sollte die Eignung der Zertifizierungsstelle insbesondere im Hinblick auf Fachkunde, Organisation und Ressourcen nachgewiesen werden müssen; dies gilt vor allem für die persönliche und fachliche Eignung der zertifizierenden Personen. Die Zertifizierungsstelle muss ihre Tätigkeit zudem unabhängig, d. h. insbesondere unbeeinflusst von sachfremden Erwägungen, ausüben. Um Interessenkollisionen und Abhängigkeitsverhältnisse so weit wie möglich auszuschließen, muss das Verfahren transparent ausgestaltet und das Prüfergebnis objektiv nachvollziehbar dargelegt werden.

Diese Vorgaben gelten in gleicher Weise für die Prüfstellen. Auch insoweit müssen Eignung und Unabhängigkeit gewährleistet sein, um nicht die Aussagekraft und Akzeptanz der Zertifikate zu gefährden. Denn dadurch, dass die Zertifizierungsstelle über die Vergabe des Zertifikats auf der Grundlage des Prüfberichts entscheidet und sie den Prüfbericht

7 Vgl. Thesenpapier „Datenschutz-Zertifizierung durch private Stellen“.

nur anhand der Aktenlage auf Plausibilität überprüfen kann, ist sicherzustellen, dass den im Prüfbericht dargestellten Fakten vertraut werden kann. Eine gesetzliche Regelung der Anforderungen an die Prüfung und den Prüfbericht ist daher notwendig. Dabei sollte auch das Format des Prüfberichts, etwa durch ein Muster, festgelegt werden, um die Nutzung von Prüfberichten im gesamten Binnenmarkt zu ermöglichen.

→ Akkreditierungsverfahren

Um die qualitativen Anforderungen an die Prüfstellen und die Zertifizierungsstellen sicherzustellen, sollte eine Akkreditierung dieser Stellen vorgesehen werden. Im Rahmen eines solchen Akkreditierungsverfahrens würde dabei von einer Akkreditierungsstelle geprüft, ob die Prüfstelle und die Zertifizierungsstelle die obigen Anforderungen im Hinblick auf Eignung und Unabhängigkeit (noch) erfüllen. Dadurch könnte die erforderliche Qualifikation der Zertifizierungsstelle gewährleistet und Rechtssicherheit für Cloud-Anbieter und Cloud-Nutzer geschaffen werden.

Im Interesse eines funktionierenden Binnenmarkts und eines einheitlichen Datenschutzniveaus sollte die Akkreditierung für den gesamten Geltungsbereich der DSGVO gelten. Eine Prüfstelle könnte demnach aufgrund der Akkreditierung im gesamten Geltungsbereich der Verordnung Prüfungen durchführen, eine Zertifizierungsstelle könnte im gesamten Geltungsbereich der Verordnung über die Verleihung von Zertifikaten entscheiden. Dadurch wäre zugleich sichergestellt, dass sich der Geltungsbereich der Akkreditierung mit dem des Zertifikats deckt, da auch das Zertifikat unionsweit gelten soll.

Die Akkreditierung sollte durch geeignete, insbesondere fachlich qualifizierte und unabhängige Stellen erfolgen. Zu diesem Zweck sollte die DSGVO die Anforderungen an die Akkreditierungsstellen im Grundsatz regeln, die Benennung der Akkreditierungsstellen aber den Mitgliedstaaten überlassen. Von einer unmittelbaren Festlegung der Akkreditierungsstellen auf europäischer Ebene ist insofern abzuraten, als dadurch erheblich in die mitgliedstaatliche Kompetenz der Verwaltungsorganisation eingegriffen würde.

5 Rücknahme des Zertifikats, Haftung und Rechtsmittel

→ Rücknahme des Zertifikats

Wenn der zertifizierte Dienst die Voraussetzungen für das Zertifikat nicht mehr erfüllt oder sich herausstellt, dass die Voraussetzungen von Anfang an nicht vorgelegen haben, stellt sich die Frage nach der Fortgeltung eines Zertifikats. Sowohl im Fall des anfänglichen Fehlens von (wesentlichen) Voraussetzungen als auch im Fall des nachträglichen Entfallens entspricht das Zertifikat nicht (mehr) der tatsächlichen Situation und hätte daher nicht vergeben werden dürfen bzw. dürfte nicht mehr vergeben werden. Während unwesentliche Änderungen in beiden Fällen irrelevant sein dürften, ist fraglich, welche Konsequenzen wesentliche Abweichungen nach sich ziehen.

Insbesondere dann, wenn wesentliche Voraussetzungen nachträglich entfallen, könnte daran gedacht werden, dass die rechtliche Wirkung des Zertifikats, wonach die Cloud-Nutzer auf das Zertifikat vertrauen dürfen, automatisch entfällt. Denn der angebotene Dienst entspricht dann nicht mehr dem Dienst, der der Zertifizierung zugrunde lag und für den das Zertifikat erteilt wurde. Jedoch stünde dennoch eine Wissensbekundung (vgl. Ziffer 2, S. 8) der Zertifizierungsstelle im Raum, auf die Cloud-Nutzer des zertifizierten Diensts vertrauen und auch vertrauen dürfen. Um den von ihr geschaffenen Vertrauenstatbestand zu beseitigen, muss die Zertifizierungsstelle daher ihre Wissensbekundung ausdrücklich zurücknehmen, wenn nach Vergabe des Zertifikats wesentliche Voraussetzungen entfallen. Aus Gründen der Rechtssicherheit muss dies in derselben Weise veröffentlicht werden, in der die Vergabe des Zertifikats bekannt gemacht wurde.

Dem Cloud-Anbieter sollte gesetzlich untersagt werden, das Zertifikat nach einer Rücknahme weiter zu führen. Damit die Zertifizierungsstelle bei Änderungen das Zertifikat ggf. zurücknehmen kann, muss der Cloud-Anbieter der Zertifizierungsstelle gegenüber zur Meldung verpflichtet sein, wenn er feststellt, dass sich (wesentliche) Aspekte des Diensts geändert haben bzw. ändern. Diese Verpflichtung sollte gesetzlich geregelt werden. Erhält die Zertifizierungsstelle eine solche Meldung, hat sie zu prüfen, ob sie das Zertifikat zurücknimmt oder ob der Dienst – beispielsweise weil der Cloud-Anbieter unverzüglich eine Nachbesserung vornimmt – weiterhin den datenschutzrechtlichen Anforderungen genügt. Eine solche Meldepflicht des Cloud-Anbieters bei Veränderungen bzw. eine damit einhergehende Pflicht der Zertifizierungsstelle zur erneuten Prüfung würde dazu führen, dass ein Zertifikat einen Cloud-Dienst nicht statisch im Sinne einer Momentaufnahme bewertet, sondern einen dynamischen Prozess einer kontinuierlichen Qualitätskontrolle ermöglicht. Damit Cloud-Anbieter zuverlässig ihrer Pflicht nachkommen, Änderungen des Diensts der Zertifizierungsstelle zu melden, sollte ein Verstoß gegen diese Pflicht in geeigneter Weise sanktioniert werden können.

Das Vertrauen des Cloud-Nutzers in das Zertifikat muss bis zu dessen Rücknahme geschützt sein. Erst im Fall einer Rücknahme darf der Cloud-Nutzer nicht mehr auf das Zertifikat vertrauen und muss sich selbst von der Einhaltung der datenschutzrechtlichen Anforderungen beim Cloud-Anbieter überzeugen und ggf. den Cloud-Anbieter wechseln. Dieser Grundsatz sollte ausdrücklich gesetzlich geregelt sein. Dieser Vertrauensschutz stärkt die Akzeptanz von Zertifizierungen. Dies wiederum dient letztlich dem Datenschutz und der Datensicherheit, da zertifizierte Dienste eine erheblich größere Gewähr dafür bieten, dass objektiv die datenschutzrechtlichen Anforderungen beachtet werden.

Auch wenn sich nachträglich herausstellt, dass ein Cloud-Dienst von Anfang an nicht die datenschutzrechtlichen Voraussetzungen erfüllt hat und daher kein Zertifikat hätte erteilt werden dürfen, ist eine Rücknahme des Zertifikats erforderlich. Denn auch in diesem Fall vertrauen die Cloud-Nutzer dem Zertifikat und gehen davon aus, dass der Cloud-Dienst unbedenklich genutzt werden kann. Stellt die Zertifizierungsstelle beispielsweise infolge einer Meldung des Cloud-Anbieters oder aufgrund eines Hinweises eines Cloud-Nutzers fest, dass die Voraussetzungen für die Erteilung des Zertifikats (von Anfang an) nicht vorlagen, hat sie das Zertifikat zurückzunehmen und die Rücknahme in gleicher Weise wie die ursprüngliche Erteilung zu veröffentlichen. Die Rücknahme des Zertifikats darf dabei keine Rückwirkung entfalten, sondern nur für die Zukunft wirken, da Cloud-Nutzer auf das Vorliegen eines Zertifikats vertrauen können müssen. Aus Gründen der Qualitätssicherung und im Hinblick auf etwaige Datenschutzverstöße, die infolge eines zu Unrecht erteilten Zertifikats möglicherweise begangen wurden, bedarf es im Gegenzug jedoch einer haftungsrechtlichen Korrektur.

→ Haftung bei fehlerhafter Zertifizierung

Zertifikate können sich als falsch erweisen. Ein Zertifikat ist falsch, wenn der zertifizierte Dienst entgegen der Aussage des Zertifikats die datenschutzrechtlichen Anforderungen nicht oder nicht mehr erfüllt. Aufgrund eines fehlerhaften Zertifikats können dem Cloud-Anbieter, Cloud-Nutzern oder Betroffenen Schäden entstehen. Es stellt sich die Frage, ob diesen Schadensersatzansprüche gegen die Zertifizierungsstelle zustehen.

Schäden aufgrund fehlerhafter Zertifikate

Erhält ein Cloud-Dienst ein Zertifikat, obwohl die Voraussetzungen nicht vorliegen, nehmen Cloud-Nutzer einen Dienst in Anspruch, der nicht den datenschutzrechtlichen Vorgaben genügt. Vor diesem Hintergrund können infolge einer fehlerhaften Zertifizierung dem Cloud-Nutzer Schäden entstehen. Dies ist beispielsweise dann der Fall, wenn der Cloud-Nutzer wegen fehlender Datenschutzkonformität des Cloud-Dienstes den Cloud-Anbieter wechseln muss und hierdurch Kosten entstehen oder wenn Maßnahmen der Aufsichtsbehörde zu Kosten führen oder gar ein Bußgeld wegen unzulässiger Datenverarbeitung verhängt werden sollte (wobei bei Vorliegen eines gültigen Zertifikats in der Regel ein Verschulden des Cloud-Nutzers zu verneinen sein wird, s. o.).[8]

Kommt es infolge der fehlerhaften Zertifizierung zu unzulässigen Datenerhebungen, -verarbeitungen oder -nutzungen und entsteht Betroffenen dadurch ein Schaden, haben darüber hinaus auch die Betroffenen gemäß § 7 Satz 1 BDSG grundsätzlich einen Schadensersatzanspruch gegen den Cloud-Nutzer. Allerdings entfällt nach § 7 Satz 2 BDSG die Ersatzpflicht, soweit der Cloud-Nutzer die nach den Umständen des Falles gebotene Sorgfalt beachtet hat. Davon dürfte auszugehen sein, wenn der Cloud-Nutzer auf einen zertifizierten Cloud-Dienst zurückgegriffen hat (vgl. Ziffer 2, S. 9). Nimmt der Cloud-Nutzer einen zertifizierten Dienst in Anspruch, haftet er demnach regelmäßig nicht für Datenschutzverstöße, die sich daraus ergeben, dass in Wirklichkeit der Cloud-Dienst nicht die

8 Siehe zu Haftungsszenarien beim Cloud Computing den Leitfaden der AG „Rechtsrahmen des Cloud Computing", „Haftungsrisiken beim Cloud Computing", April 2015, abrufbar unter www.trusted-cloud.de.

datenschutzrechtlichen Anforderungen erfüllt. Beruht das fehlerhafte Zertifikat nicht auf falschen Angaben des Cloud-Anbieters, sondern auf einer fehlerhaften Prüfung der Zertifizierungsstelle, wird daher eine Haftung des Cloud-Anbieters meist zu verneinen sein, weil auch ihm eine schuldhafte Pflichtverletzung dann kaum zur Last gelegt werden kann. Denn angesichts der Erteilung des Zertifikats kann auch der Cloud-Anbieter davon ausgehen, dass sein Dienst den gesetzlichen Vorgaben genügt; anderes dürfte nur dann gelten, wenn der Cloud-Anbieter weiß oder wissen muss, dass sein Dienst trotz der Zertifizierung die datenschutzrechtlichen Anforderungen nicht erfüllt.

Auch Schäden des Cloud-Anbieters sind bei fehlerhaften Zertifikaten nicht ausgeschlossen, da der Cloud-Anbieter etwa bei Rücknahme von Zertifikaten regelmäßig Aufwendungen hat und ggf. Kunden verliert. Ob sich hieraus ein Schadensersatzanspruch gegen die Zertifizierungsstelle ableiten lässt, wird wohl nur im Einzelfall zu klären sein, da der Cloud-Anbieter die Ursache durch Anbieten eines datenschutzwidrigen Dienstes selbst gesetzt hat.

Haftung aufgrund fehlerhafter Zertifizierung

Soweit wegen fehlerhafter Zertifizierung Schäden beim Cloud-Anbieter, beim Cloud-Nutzer oder bei Betroffenen entstehen, kann sich eine Haftung der Zertifizierungsstelle oder der Prüfstelle aus verschiedenen Rechtsgrundlagen ergeben.

Eine vertragliche Haftung kommt jedoch wohl nur gegenüber dem Cloud-Anbieter in Betracht, da nur dieser in einer Vertragsbeziehung zur Prüfstelle und zur Zertifizierungsstelle steht. Es ist auch nicht gesichert, dass diese Verträge als Verträge mit Schutzwirkung zugunsten des Cloud-Nutzers oder gar der Betroffenen anzusehen sind. Ohnehin ist das Rechtsinstitut des Vertrags mit Schutzwirkung zugunsten Dritter nicht in jedem Mitgliedstaat bekannt. Daher ist es notwendig, eine gesetzliche Regelung zur Haftung von Prüfstelle und Zertifizierungsstelle bei fehlerhafter Prüfung bzw. Zertifizierung zu schaffen.

Erweist sich eine Zertifizierung als fehlerhaft, kommen demnach – bei entsprechender gesetzlicher Regelung – Schadensersatzansprüche von Cloud-Anbietern, Cloud-Nutzern und Betroffenen in Betracht. Angesichts der Regelung in § 8 BDSG, die – wenn auch nur für öffentliche Stellen – eine Gefährdungshaftung anordnet, erscheint es auch für den Fall einer fehlerhaften Prüfung oder Zertifizierung nicht von vornherein ausgeschlossen, eine Gefährdungshaftung vorzusehen. Solange aber jedenfalls selbst Cloud-Anbieter und Cloud-Nutzer nur verschuldensabhängig haften (vgl. § 7 Satz 2 BDSG), dürfte eine Gefährdungshaftung für fehlerhafte Prüfungen oder Zertifizierungen unverhältnismäßig sein. Vor diesem Hintergrund sollte in die DSGVO bzw. in einen delegierten Rechtsakt eine Regelung aufgenommen werden, wonach eine Haftung der Prüfstelle und der Zertifizierungsstelle von einer schuldhaften Pflichtverletzung abhängig ist.

Eine Haftung der Prüfstelle oder der Zertifizierungsstelle würde demnach voraussetzen, dass diese ihre Pflichten im Rahmen der Prüfung oder Zertifizierungsverfahren vorsätzlich oder fahrlässig verletzt haben. Eine Haftung kann sich demnach zum einen aus einer fehlerhaften Prüfung des Cloud-Diensts, zum anderen aus einer falschen Entscheidung hinsichtlich der Zertifikatsvergabe ergeben. Entscheidende Voraussetzung ist jeweils eine Pflichtverletzung.

Die Hauptpflicht der Prüfstelle besteht in der ordnungsgemäßen Prüfung des Cloud-Dienstes anhand der maßgeblichen Prüfanforderungen. Daher erscheint es wesentlich, die Anforderungen an eine ordnungsgemäße Prüfung möglichst genau zu definieren. Da insoweit bisher keine spezifische gesetzliche Regelung besteht, sollte diese für den gesamten Binnenmarkt geschaffen werden.

Die Hauptpflicht der Zertifizierungsstelle besteht in der pflichtgemäßen Entscheidung über die Vergabe eines Zertifikats auf der Grundlage der von der Prüfstelle vorgenommenen Prüfung. Eine Haftung kommt dabei sowohl für den Fall in Betracht, dass ein Zertifikat zu Unrecht vergeben wurde, als auch für den Fall, dass ein erteiltes Zertifikat nicht zurückgenommen wurde, obwohl die Voraussetzungen des Zertifikats nicht mehr vorliegen.

Zur Begrenzung der Haftung von Prüfstelle und Zertifizierungsstelle könnte die gesetzliche Festlegung einer Haftungshöchstgrenze erwogen werden. Zusätzlich könnten sich Prüfstellen und Zertifizierungsstellen durch den Abschluss einer entsprechenden Haftpflichtversicherung absichern. Der Gesetzgeber könnte auch die Pflicht zum Abschluss einer hinreichenden Haftpflichtversicherung vorsehen.

Im Fall einer fehlerhaften Zertifizierung könnte die zivilrechtliche Haftung der Zertifizierungsstelle durch Befugnisse staatlicher Stellen flankiert werden. Denkbar wären insoweit sowohl Anordnungen der Aufsichtsbehörden gegenüber der Prüfstelle und der Zertifizierungsstelle als auch die Verhängung von Bußgeldern auf der Grundlage von (hierfür zu schaffenden) Ordnungswidrigkeitstatbeständen.

→ Rechtsmittel

Dem Cloud-Anbieter muss im Hinblick auf sein Rechtsschutzinteresse die Möglichkeit einer gerichtlichen Überprüfung der von der Zertifizierungsstelle getroffenen Entscheidung ermöglicht werden, wenn die Zertifizierungsstelle das Zertifikat versagt, nur eingeschränkt erteilt (z. B. nur für bestimmte Schutzklassen) oder zurücknimmt. Ob auch Dritten, beispielsweise Cloud-Nutzern, Betroffenen, Wettbewerbern oder Aufsichtsbehörden, der Rechtsweg gegen eine Entscheidung der Zertifizierungsstelle offenstehen sollte, erscheint hingegen zweifelhaft. Vielmehr dürften hierfür andere Wege vorzugswürdig sein, um deren Interessen angemessen Rechnung zu tragen. Während Cloud-Nutzer und Betroffene in der Regel bereits über die Möglichkeit einer Haftung der Zertifizierungsstelle ausreichend geschützt sein dürften, können Aufsichtsbehörden gegen die Zertifizierungsstelle im Fall einer fehlerhaften Zertifizierung ggf. mittels Anordnungen oder auch durch die Verhängung von Bußgeldern vorgehen.

Welcher Rechtsweg dem Cloud-Anbieter offensteht, d. h., ob er den Zivil- oder den Verwaltungsrechtsweg zu beschreiten hat, richtet sich danach, ob es sich dabei um eine privatrechtliche oder eine öffentlich-rechtliche Streitigkeit handelt (vgl. § 40 Abs. 1 der Verwaltungsgerichtsordnung). Dies hängt wiederum insbesondere von der Rechtsnatur des Zertifikats ab, d. h. von der Frage, ob das Zertifikat privat- oder öffentlich-rechtlich ausgestaltet wird. Maßgeblich hierfür ist die nähere Ausgestaltung durch die künftige DSGVO. Da der Rechtsweg von Mitgliedstaat zu Mitgliedstaat – abhängig von der nationalen Rechtsordnung – unterschiedlich ausfallen kann, sollte die DSGVO die Mitgliedstaaten nur verpflichten, Rechtsmittel gegen die Versagung, Einschränkung oder Rücknahme eines Zertifikats vorzusehen; die Ausgestaltung des Rechtswegs sollte dann den Mitgliedstaaten überlassen werden.

6 Fazit

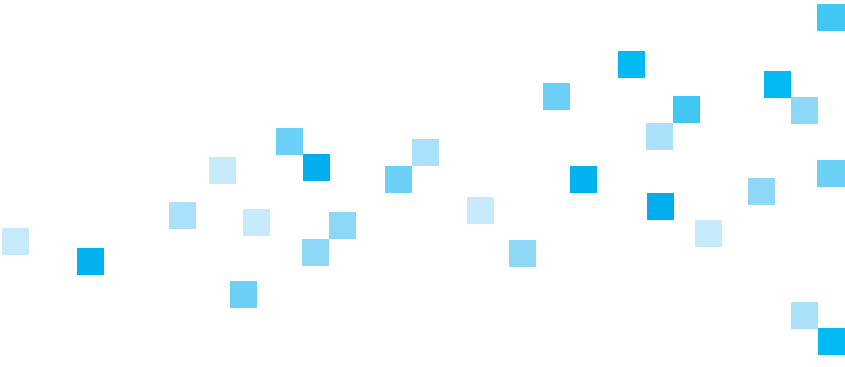
Die Datenschutz-Zertifizierung kann ein sehr erfolgreiches Modell für die Sicherung des Datenschutzes bei der Bereitstellung und Inanspruchnahme von Cloud-Diensten sein. Insbesondere ermöglicht sie eine effiziente datenschutzrechtliche Überprüfung von Cloud-Diensten und stärkt damit den Datenschutz.

Voraussetzung einer erfolgreichen Datenschutz-Zertifizierung ist ein leistungsfähiges und effizientes Zertifizierungsverfahren, das die Erfüllung der Anforderungen an eine ordnungsgemäße Prüfung und Zertifizierung von Cloud-Diensten sichert und zugleich eine kostengünstige Zertifizierung ermöglicht.

Wegen der wesentlichen Bedeutung des Zertifizierungsverfahrens für die Datenschutz-Zertifizierung sollte der europäische Gesetzgeber die Eckpunkte des Zertifizierungsverfahrens regeln. Dabei sollten insbesondere die in diesem Papier genannten Aspekte geregelt werden:

- Prüfung und Zertifizierung nach einheitlichen Maßstäben auf gesetzlicher Grundlage
- Gültigkeit der Zertifizierung für den gesamten Binnenmarkt
- Erfüllung der Überprüfungspflicht des Cloud-Nutzers durch Einsichtnahme in das Zertifikat
- Schutz des Vertrauens des Cloud-Nutzers in das Zertifikat
- Trennung von Prüfstellen und Zertifizierungsstellen mit eigenen Aufgabenkreisen
- Prüfung und Zertifizierung durch akkreditierte Prüfstellen und Zertifizierungsstellen
- Auswahl und Beauftragung von Prüf- und Zertifizierungsstelle durch den Cloud-Anbieter
- Akkreditierung von Prüf- und Zertifizierungsstellen durch geeignete Akkreditierungsstellen
- Rücknahme des Zertifikats bei Fehlen der Voraussetzungen
- Haftung der Prüfstelle und der Zertifizierungsstelle bei Pflichtverletzungen

Mit einem derartigen qualitativ hochwertigen und effizienten Verfahren der Datenschutz-Zertifizierung können Datenschutz und eine effiziente Bereitstellung und Nutzung von Cloud-Diensten gleichermaßen erreicht werden.



Autoren

Prof. Dr. Georg Borges, Kompetenzzentrum Trusted Cloud, Universität des Saarlandes

Oliver Berthold, Berliner Beauftragter für Datenschutz und Informationsfreiheit

Mathias Cellarius, SAP SE

Susanne Dehmel, BITKOM e.V.

Thomas Doms, TÜV Trust IT GmbH

Dr. Alexander Duisberg, Bird & Bird LLP

Dagmar Hartge, Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

Claudia Husz, regio iT GmbH

Dr. Hubert Jäger, Uniscon universal identity control GmbH

Thomas Kranig, Bayerisches Landesamt für Datenschutzaufsicht

Johannes Landvogt, Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Jan Lichtenberg, Deutsche Telekom AG

Peter Niehues, regio iT GmbH

Christoph Rechsteiner, SAP SE

Frederick Richter, Stiftung Datenschutz

Gabriel Schulz, Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern

Dr. Christoph Sutter, TÜV Informationstechnik GmbH

Karin Vedder, Bayerisches Landesamt für Datenschutzaufsicht

Dr. Thilo Weichert, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Monika Wojtowicz, TÜV Informationstechnik GmbH

Ursula Zabel, Berliner Beauftragter für Datenschutz und Informationsfreiheit

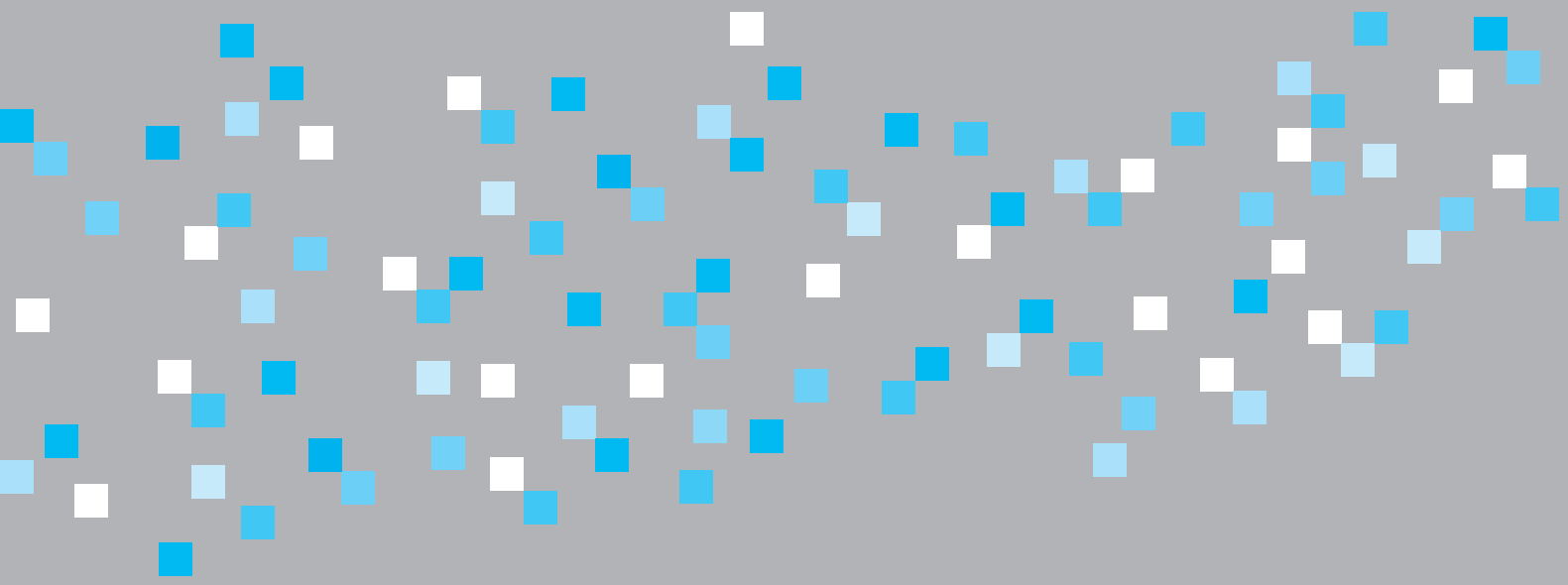
Impressum

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)
Gestaltung
A&B One Kommunikationsagentur, Berlin

Druck
DCM Druck Center Meckenheim

Stand: April 2015



www.trusted-cloud.de