Trusted Cloud

Kompetenzzentrum Trusted Cloud

Thesenpapier – Datenschutz-Zertifizierung durch private Stellen

Nr. 6

Arbeitsgruppe „Rechtsrahmen des Cloud Computing“

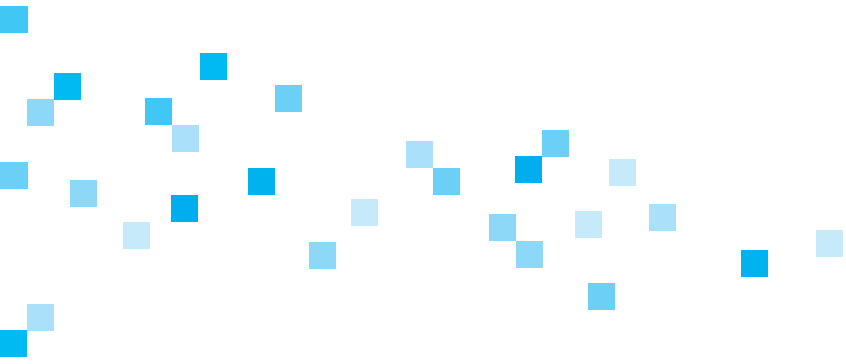
Cloud Computing kann in Deutschland nur wirtschaftlich erfolgreich sein, wenn die rechtlichen Rahmenbedingungen eine effiziente Nutzung von Cloud-Diensten ermöglichen. Ein innovationsfreundlicher Rechtsrahmen ist daher von besonderer Bedeutung. Für die rechtlichen Aspekte von Cloud Computing hat das Bundesministerium für Wirtschaft und Energie (BMWi) daher innerhalb des Kompetenzzentrums Trusted Cloud eine eigene Arbeitsgruppe einrichten lassen.

In der Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ erarbeiten Experten aus Wirtschaft, Anwaltschaft und Wissenschaft sowie Vertreter aus Datenschutzbehörden gemeinsam mit Projektbeteiligten aus dem Trusted-Cloud-Programm Lösungsvorschläge für rechtliche Herausforderungen. Sie wird geleitet von Prof. Dr. Georg Borges. Themenschwerpunkte sind u. a. Datenschutz, Vertragsgestaltung, Urheberrecht sowie Haftungsfragen und Strafbarkeitsrisiken. Darüber hinaus wird ein Pilotprojekt zur datenschutzrechtlichen Zertifizierung von Cloud-Diensten durchgeführt, das Impulse für die rechtssichere Nutzung von Cloud Computing und die Gewährleistung eines hohen Datenschutzniveaus setzen soll.

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 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 Bedeutung der datenschutzrechtlichen Compliance-Zertifizierung

Die Bedeutung von Zertifizierungen im Bereich des Datenschutzes und die rechtliche Einordnung der Zertifizierung als öffentliche Aufgabe oder private Tätigkeit folgen aus der aktuellen Diskussion zu einer datenschutzrechtlichen Compliance-Zertifizierung und zum Entwurf der europäischen Datenschutz-Grundverordnung.

→ Bedarf an einer datenschutzrechtlichen Compliance-Zertifizierung

Die Zertifizierung im Bereich des Datenschutzes ist Gegenstand einer vielschichtigen Diskussion, in der sehr unterschiedliche Ziele und Ansätze einer solchen Zertifizierung vertreten werden. Dabei zeigt sich in jüngster Zeit, dass insbesondere ein Bedarf an einer Zertifizierung von Diensten besteht, in der die Erfüllung der datenschutzrechtlichen Anforderungen durch den zertifizierten Dienst geprüft und durch ein Zertifikat bestätigt wird.

Die Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ hat in ihrem im September 2012 veröffentlichten Dokument „Datenschutzrechtliche Lösungen für Cloud Computing. Ein rechtspolitisches Thesenpapier“[1] ein Konzept für eine solche Zertifizierung einschließlich ihrer zentralen Elemente beschrieben.

→ Gegenstand der datenschutzrechtlichen Compliance-Zertifizierung

Unter Zertifizierung versteht das Konzept der AG Rechtsrahmen die Wissensbekundung der Zertifizierungsstelle über die Erfüllung der datenschutzrechtlichen Anforderungen an den geprüften Dienst. Ergebnis der Zertifizierung in diesem Zusammenhang ist deshalb die Erteilung eines Testats über die Einhaltung der einschlägigen rechtlichen Normen. Insofern wird zutreffend synonym auch der Begriff „Compliance-Zertifikat“ verwendet.

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

Im Pilotprojekt „Datenschutz-Zertifizierung für Cloud Computing“ des BMWi-Technologieprogramms „Trusted Cloud“ werden die Elemente einer datenschutzrechtlichen Compliance-Zertifizierung für Cloud-Dienste ausgearbeitet.[2] Das Pilotprojekt beruht auf dem Konzept der AG Rechtsrahmen und strebt an, die Kernelemente einer datenschutzrechtlichen Compliance-Zertifizierung zu erarbeiten. Dabei werden auf der Grundlage der gesetzlichen Anforderungen einheitliche Prüfanforderungen, das Trusted Cloud-Datenschutzprofil für Cloud-Dienste, entwickelt.

1 Das Papier ist abrufbar über www.trusted-cloud.de.
2 Siehe zum Pilotprojekt unter www.trusted-cloud.de/569.php.

2 Zertifizierung durch Behörden oder private Stellen?

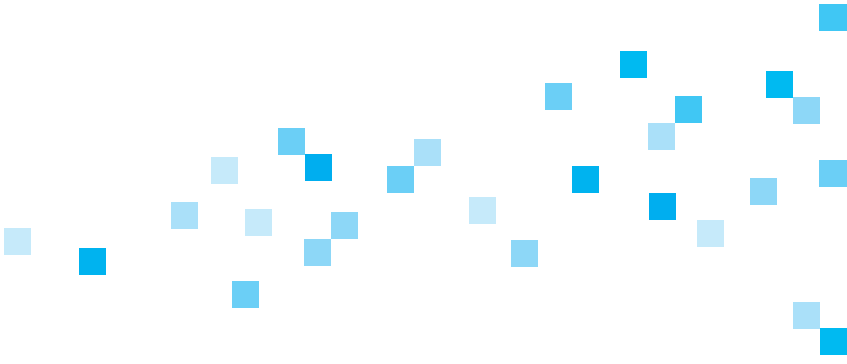
Im Rahmen einer datenschutzrechtlichen Compliance-Zertifizierung ist es von zentraler Bedeutung, ob das Zertifizierungsverfahren als ein öffentlich-rechtliches oder als ein privatrechtliches Verfahren ausgestaltet ist und ob die Zertifizierungsstelle eine Behörde oder ein privates Unternehmen ist.

Diese Frage ist bisher nicht umfassend gesetzlich geregelt. Das Konzept der AG Rechtsrahmen des Cloud Computing spricht sich dafür aus, dass die Zertifizierung durch geeignete private Stellen erfolgt. Die Anforderungen an private Zertifizierungsstellen und an das Zertifizierungsverfahren sollten nach diesem Konzept gesetzlich geregelt sein.

So heißt es in These 8 des Thesenpapiers wie folgt: „Das Testat sollte (auch) durch qualifizierte private Stellen vergeben werden. […]“[3]

These 10 führt ergänzend dazu u. a. aus: „Die Akkreditierung sollte durch geeignete, insbesondere fachlich qualifizierte und unabhängige Stellen erfolgen. Die EU-Datenschutz-Grundverordnung sollte die Anforderungen an die Akkreditierungsstellen im Grundsatz regeln, die Benennung der Akkreditierungsstellen den Mitgliedstaaten überlassen.“

Im Rahmen der europäischen Datenschutz-Grundverordnung können entscheidende Weichenstellungen für den rechtlichen Charakter der Zertifizierung erfolgen.



3 AG Rechtsrahmen, Datenschutzrechtliche Lösungen für Cloud Computing (Fn. 1), These 8 (S. 18).

3 Rechtliche Grundlagen der datenschutzrechtlichen Compliance-Zertifizierung

Eine allgemeine gesetzliche Regelung der datenschutzrechtlichen Compliance-Zertifizierung besteht bisher in Deutschland auf Bundesebene nicht; der eine solche Regelung erlaubende § 9a BDSG von 2001 wurde bislang nicht ausgefüllt. In Einzelfällen sieht das Gesetz eine datenschutzrechtliche Compliance-Zertifizierung vor. So ist nach § 18 Abs. 3 Nr. 4, 2. Halbs. De-Mail-Gesetz die Erfüllung der datenschutzrechtlichen Anforderungen an den De-Mail-Dienst durch ein Zertifikat der BfDI nachzuweisen. Auf Landesebene besteht in Schleswig-Holstein auf Grundlage des § 4 Abs. 2 LDSG die Datenschutzgütesiegelverordnung[4], die die Vergabe eines Datenschutzgütesiegels regelt. In Bremen wurde 2004 auf Grundlage von § 7b BremDSG die Bremische Datenschutzauditverordnung (BremDSAuditV) erlassen, auf deren Basis ein Bremisches Datenschutzaudit-Gütesiegel vergeben werden kann, jedoch ausschließlich für öffentliche Stellen des Landes Bremen. Mit Ende 2014 tritt die BremDSAuditV außer Kraft. Seit 2011 sind die öffentlichen Einrichtungen Mecklenburg-Vorpommerns durch § 5 Abs. 2 DSG M-V gehalten, vorrangig zertifizierte IT-Produkte einzusetzen. Das Prüfverfahren dazu ist im Benehmen mit dem Landesbeauftragten für den Datenschutz durchzuführen[5].

Gesetzliche Regeln zu Aspekten der Zertifizierung bestehen vor allem auf europäischer Ebene in Form der Verordnung 765/2008.[6] In Ausführung der Verordnung wurden in den Mitgliedstaaten Gesetze über Akkreditierungen erlassen, in Deutschland durch das Akkreditierungsstellengesetz (AkkStelleG).[7] Die Bedeutung der Verordnung 765/2008 und des AkkStelleG für eine datenschutzrechtliche Zertifizierung ist nicht abschließend geklärt. Soweit die datenschutzrechtliche Zertifizierung künftig durch die europäische Datenschutz-Grundverordnung geregelt werden sollte, ginge diese der VO 765/2008 jedoch vor.

Die europäische Datenschutz-Grundverordnung könnte eine gesetzliche Regelung der datenschutzrechtlichen Zertifizierung bringen oder jedenfalls entscheidende Weichen stellen. Jedoch ist derzeit noch unklar, welche Position die Verordnung enthalten wird.

4 Landesverordnung über ein Datenschutzgütesiegel (Datenschutzgütesiegelverordnung – DSGSVO) vom 30.11.2013 (GVOBl. 2013, S. 536).
5 Landesrechtliche Erwähnungen finden sich darüber hinaus in § 11c Brandenburgisches Datenschutzgesetz und § 4 Abs. 2 i.V.m. § 10a Datenschutzgesetz Nordrhein-Westfalen.
6 Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften zur Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates, ABl. EU Nr. L 218/30 vom 13.08.2008.
7 Gesetz über die Akkreditierungsstelle (AkkStelleG) vom 31.07.2009, BGBl. I S. 2625.

4 Datenschutz-Zertifizierung im Entwurf der Datenschutz-Grundverordnung

Der Entwurf der Europäischen Kommission zur Datenschutz-Grundverordnung (DSGVO) enthält in Art. 39 eine – sehr allgemeine – Bezugnahme auf Zertifizierungen, enthält aber keine Festlegungen in Bezug auf den rechtlichen Charakter der Zertifizierung und die Eigenschaften der Zertifizierungsstelle. In der Diskussion der Datenschutz-Grundverordnung im Europäischen Parlament und im Ministerrat sind auch zu Art. 39 weitreichende Änderungsvorschläge erarbeitet worden.

Der am 12. März 2014 verabschiedete Entwurf des Europäischen Parlamentes[8] sieht eine umfangreiche Regelung zur Zertifizierung in Art. 39 DSGVO (EP) vor. Die zentrale Grundlage soll Art. 39 Abs. 1a DSGVO (EP) sein, der wie folgt lautet: „Jeder für die Verarbeitung Verantwortliche oder Auftragsverarbeiter kann bei jeder Aufsichtsbehörde in der Union für eine angemessene Gebühr unter Berücksichtigung der Verwaltungskosten eine Zertifizierung darüber beantragen, dass die Verarbeitung personenbezogener Daten im Einklang mit dieser Verordnung durchgeführt wird […].“

Die hier genannte Zertifizierung entspricht im Grundgedanken dem Konzept der datenschutzrechtlichen Compliance-Zertifizierung, wie sie auch im Thesenpapier der AG „Rechtsrahmen des Cloud Computing“ entwickelt wird.

Im Vorschlag des Europäischen Parlaments wird die Zertifizierung jedoch vor allem als Aufgabe der Aufsichtsbehörden gesehen. Dies ergibt sich aus Art. 39 Abs. 1a DSGVO (EP), aber auch aus Art. 39 Abs. 1d DSGVO (EP), dessen letzter Satz lautet: „Die endgültige Zertifizierung erteilt die Aufsichtsbehörde.“

Das Europäische Parlament spricht sich demnach dafür aus, dass eine Zertifizierung durch die Aufsichtsbehörden möglich sein soll und dass die verantwortliche Stelle einen Anspruch auf Zertifizierung gegen die Aufsichtsbehörden hat. Der rechtliche Charakter des Zertifizierungsverfahrens wird im Vorschlag des Europäischen Parlaments nicht abschließend festgelegt. Es wird auch nicht eindeutig geregelt, ob die Zertifizierung den Aufsichtsbehörden vorbehalten sein soll oder ob auch private Stellen die Möglichkeit haben sollen, ein Compliance-Zertifikat mit der Bedeutung des Art. 39 Abs. 1d DSGVO (EP) auszustellen.

Im aktuellen Entwurf der italienischen Ratspräsidentschaft vom 3. Oktober 2014[9] wird die Ergänzung des Art. 39 durch einen Art. 39a vorgeschlagen, in dem die Anforderungen an die Zertifizierung und das zugrunde liegende Zertifizierungsverfahren näher geregelt werden. Nach Art. 39a Abs. 1 DSGVO (RP) muss die Zertifizierungsstelle unabhängig sein und über eine hinreichende Sachkunde verfügen. Sie muss weiterhin auch akkreditiert sein. Art. 39a Abs. 2 DSGVO (RP) nennt mehrere Bedingungen für die Akkreditierung von Zertifizierungsstellen. Der Entwurf des Ministerrats geht also davon aus, dass die Zertifizierung jedenfalls auch eine Aufgabe privater, akkreditierter Zertifizierungsstellen ist.

8 Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), ordentliches Gesetzgebungsverfahren: erste Lesung).

9 Ratsdokument Nr. 13772/14 vom 3.10.2014, abrufbar unter http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2013772%202014%20INIT.

5 Gründe für eine Zertifizierung durch Aufsichtsbehörden[10] oder private Stellen

Die Frage, ob die Datenschutz-Zertifizierung nach der Datenschutz-Grundverordnung durch Aufsichtsbehörden oder durch private Stellen erteilt werden soll, ist im Licht der Vor- und Nachteile der in Betracht kommenden Optionen zu bewerten.

→ Zertifizierung als Aufgabe der Aufsichtsbehörden

Für die Einordnung der datenschutzrechtlichen Compliance-Zertifizierung als Aufgabe öffentlicher Träger, insbesondere der Aufsichtsbehörden, können gewichtige Argumente genannt werden.

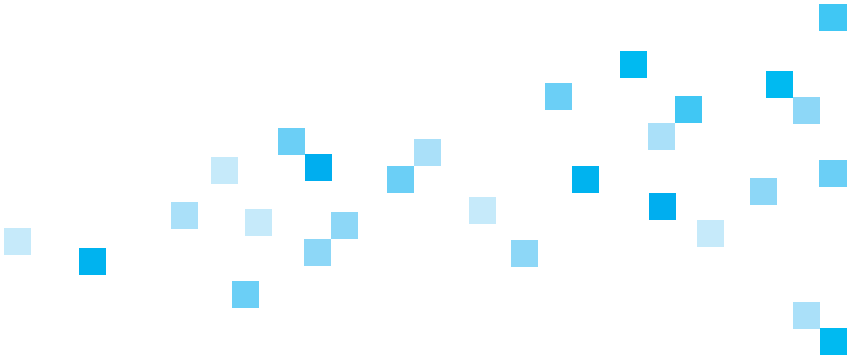
- Aufsichtsbehörden haben aufgrund ihrer Kontrolltätigkeit eine klare Vorstellung von den Anforderungen datenschutzrechtlicher Vorschriften und können deshalb die Datenschutzkonformität eines Datenumgangs sachgerecht beurteilen.
- Eine Zertifizierung durch Aufsichtsbehörden kann für das Unternehmen Rechtssicherheit schaffen, da anzunehmen ist, dass die Behörde bei ihrer Aufsichtstätigkeit einer von ihr vorgenommenen Zertifizierung nicht widersprechen wird. Damit würde die Zertifizierung jedenfalls eine faktische Selbstbindung der Aufsichtsbehörde auslösen.
- Behördliche Zertifizierungsverfahren einschließlich der Kostenregelung können vom Staat durch Verwaltungsnormen transparent geregelt werden und unterliegen einer rechtsstaatlichen Kontrolle.
- Aufsichtsbehörden können als Zertifizierer dienen, wenn keine geeigneten privaten Anbieter zur Verfügung stehen, und sind deshalb ein wichtiges Instrument, um der Wirtschaft den Zugang zur Zertifizierung zu ermöglichen.

10 Der Begriff umfasst in Anlehnung an die Terminologie des Entwurfs der Datenschutz-Grundverordnung die Datenschutzaufsichtsbehörden sowie sonstige Stellen, die eine Aufsichtsfunktion wahrnehmen, insbesondere die Datenschutzbeauftragten des Bundes und der Länder.

→ Zertifizierung als Aufgabe privater Stellen

Für die Einordnung der datenschutzrechtlichen Compliance-Zertifizierung als Aufgabe privater Stellen, insbesondere geeigneter Unternehmen, sprechen ebenfalls wichtige Gründe.

- Audits und Zertifizierungen durch private Stellen sind im Bereich der Informationstechnologie weit verbreitet und haben sich bewährt. Diese umfassen auch schon datenschutzrechtliche Anforderungen.
- Wenn die Zertifizierung als private Wirtschaftstätigkeit erfolgen kann, können Marktmechanismen genutzt werden. Durch Wettbewerb können sich effiziente und kostengünstige Zertifizierungen herausbilden. Dies gewährleistet, dass das vom Europäischen Parlament angestrebte Ziel einer erschwinglichen und kostengünstigen Zertifizierung erreicht wird.
- Die freiwillige Zertifizierung sollte von der behördlichen Kontrolle durch Aufsichtsbehörden getrennt sein, da es sonst leicht zu einer Vermischung von Aufsichtstätigkeit und gebührenfinanzierter Zertifizierung kommen kann.
- Aufsichtsbehörden können aufgrund einer Zertifizierungstätigkeit, durch die sie Einnahmen erzielen, hinsichtlich ihrer sonstigen Beratungsaufgaben, aber auch hinsichtlich ihrer Kontrolltätigkeit befangen sein.
- Aufsichtsbehörden haben nicht die erforderlichen Kapazitäten, um den gesamten Zertifizierungsbedarf der Privatwirtschaft abzudecken. Diese Kapazitäten können auch nur mit Schwierigkeiten aufgebaut werden, da nicht gesichert ist, dass das entsprechende Personal der Aufsichtsbehörden anderweitig eingesetzt werden kann. Es sind daher problematische Verzögerungen bei der Erteilung von Zertifikaten zu erwarten.[11]
- Wenn zahlreiche Zertifizierungsanträge eingehen und diese innerhalb einer bestimmten Frist erledigt sein müssen, kann dies aufgrund der beschränkten Kapazitäten der Aufsichtsbehörden auch dazu führen, dass andere Aufgaben nicht mehr angemessen erfüllt werden können.



11 Im Bereich des Schienenverkehrs wird in Deutschland derzeit eine Gesetzesänderung vorbereitet, die die bisher dem Eisenbahn-Bundesamt vorbehaltene Zulassung von Schienenfahrzeugen für private Prüfunternehmen öffnet, um bisher eingetretene Verfahrensverzögerungen zu vermeiden.

→ Keine Beschränkung der Compliance-Zertifizierung auf Aufsichtsbehörden

Der Vorschlag des Europäischen Parlaments zu einem neu gefassten Art. 39 DSGVO (EP) kann dahin verstanden werden, dass die datenschutzrechtliche Compliance-Zertifizierung den Aufsichtsbehörden vorbehalten sein soll. Der Vorschlag könnte auch dahingehend verstanden werden, dass zwar private Stellen Zertifizierungen vergeben können, dass aber jedenfalls die zentrale rechtliche Wirkung des Zertifikats nach Art. 26 der Entwürfe zur DSGVO einem von den Aufsichtsbehörden verliehenen Zertifikat vorbehalten sein soll. Nach Art. 26 darf der Auftraggeber auf eine Zertifizierung im Sinne des Art. 39 vertrauen.[12] Damit wäre faktisch eine Beschränkung auf Aufsichtsbehörden begründet, da die Compliance-Zertifizierung gerade auf die Wirkung des Art. 26 abzielt.

Eine Monopolisierung der datenschutzrechtlichen Compliance-Zertifizierung bei den Aufsichtsbehörden wäre problematisch. Eine Notwendigkeit, die Zertifizierung staatlichen Stellen vorzubehalten, ließe sich nur begründen, wenn private Stellen die erforderliche Unabhängigkeit und Eignung nicht aufwiesen. Dies wird man auch im Bereich der datenschutzrechtlichen Zertifizierung nicht annehmen können. Prüfungen und Zertifizierungen werden in den meisten Bereichen, namentlich bei der Zertifizierung technischer Produkte, von privaten Stellen durchgeführt. Dies gilt auch bei Produkten mit hohen Sicherheitsanforderungen. Auch der europäische Gesetzgeber setzt in anderen Bereichen auf ein Modell der Zertifizierung durch private Stellen. Insoweit ist an die Verordnung 765/2008[13] zu erinnern, die für Produktzertifizierungen nach bestimmten Normen eine Akkreditierung privater Zertifizierungsstellen („Konformitätsbewertungsstellen“) vorsieht.

Die Nutzung von Marktmechanismen für die Ermittlung angemessener Preise erscheint auch im Bereich der datenschutzrechtlichen Prüfungen und Zertifizierungen richtig. Allerdings ist es – insbesondere bei privatwirtschaftlicher Zertifizierung im Wettbewerb – erforderlich, die Einhaltung hinreichender Prüfanforderungen durch gesetzliche Anforderungen an die Zertifizierungsstellen und das Zertifizierungsverfahren zu sichern, wie es das Konzept der AG „Rechtsrahmen des Cloud Computing“ und der Entwurf der Ratspräsidentschaft vorsehen.[14]

Die Regelung zur Zertifizierung in der zu verabschiedenden DSGVO sollte dahin gehen, die Zertifizierung sowohl durch private Stellen als auch durch Aufsichtsbehörden zuzulassen. Damit könnte auch den unterschiedlichen Situationen in den Mitgliedstaaten Rechnung getragen werden. So mag es Mitgliedstaaten geben, in denen eine staatliche Stelle schon deswegen erforderlich ist, weil ein Markt für eine rein privatwirtschaftlich organisierte Zertifizierung nicht besteht. Es ist aber auch möglich, dass in einigen Mitgliedstaaten der Aufbau eines öffentlichen Verwaltungsapparats (einschließlich entsprechender Verwaltungsverfahrensregeln) zur umfassenden Durchführung der Zertifizierungen nicht zu leisten ist und daher Marktmechanismen greifen sollten, um ein funktionierendes Zertifizierungssystem zeitnah und erfolgreich zu realisieren.

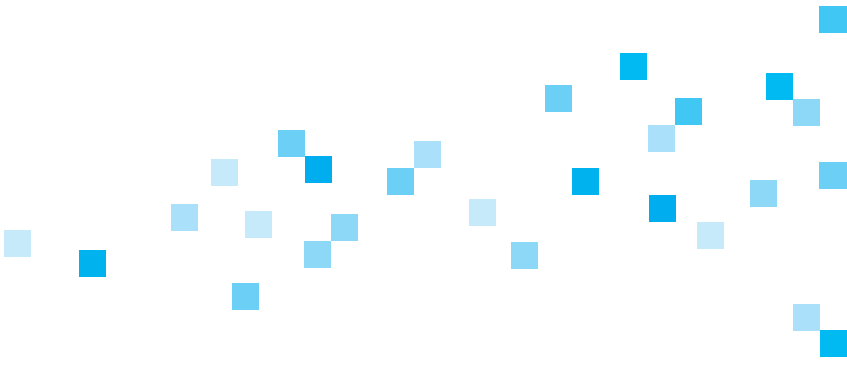
Eine Beschränkung der Zertifizierung auf Aufsichtsbehörden ist daher abzulehnen.

12 Vgl. Art. 26 Abs. 2 lit. a DSGVO (RP); Art. 26 Abs. 3 lit. a DSGVO (EP).
13 Vgl. Fn. 6.
14 Vgl. Thesen 6–10 Thesenpapier AG Rechtsrahmen (Fn. 1); Art. 39a DSGVO (RP).

6 Schlussfolgerungen

Datenschutzrechtliche Compliance-Zertifizierungen, wie sie auch im Entwurf der Datenschutz-Grundverordnung vorgesehen sind, leisten einen wichtigen Beitrag zur Rechtssicherheit und zur Verbesserung des Datenschutzniveaus bei modernen IT-Dienstleistungen, insbesondere im Cloud Computing.

Die Möglichkeit, datenschutzrechtliche Compliance-Zertifizierungen nach der europäischen Datenschutz-Grundverordnung zu vergeben, ist nicht auf Aufsichtsbehörden zu beschränken, sondern muss auch durch private Stellen erfolgen können. Dies sollte in der Datenschutz-Grundverordnung klargestellt werden.



Anhang

Entwurf der Europäischen Kommission für eine „Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)“ vom 25. 1. 2012 mit Änderungsvorschlägen des Europäischen Parlaments i. d. F. des Beschlusses vom 12. 3. 2014 und des Europäischen Rates i. d. F. des Entwurfs der Ratspräsidentschaft vom 3. 10. 2014.

EU-KOMMISSION	EUROPÄISCHES PARLAMENT	EUROPÄISCHER RAT
Erwägung 77	**Erwägung 77**	**Erwägung 77**
Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsmechanismen sowie Datenschutzsiegel und -prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Erzeugnisse und Dienstleistungen ermöglichen.	Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsmechanismen sowie Datenschutzsiegel und standardisierte Datenschutzprüfzeichen eingeführt werden, die den betroffenen Personen einen raschen, zuverlässigen und überprüfbaren Überblick über das Datenschutzniveau einschlägiger Erzeugnisse und Dienstleistungen ermöglichen. Ein „Europäisches Datenschutzsiegel“ sollte auf europäischer Ebene eingeführt werden, um unter betroffenen Personen Vertrauen und für die für die Verarbeitung Verantwortlichen Rechtssicherheit zu schaffen sowie gleichzeitig die Verbreitung europäischer Datenschutzstandards außerhalb der EU zu fördern, indem es nicht-europäischen Unternehmen vereinfacht wird, Zugang zu europäischen Märkten zu erhalten, indem sie sich zertifizieren lassen.	Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Erzeugnisse und Dienstleistungen ermöglichen.
Artikel 39: Zertifizierung	**Artikel 39: Zertifizierung**	**Artikel 39: Zertifizierung**
1. Die Mitgliedstaaten und die Kommission fördern insbesondere auf europäischer Ebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -zeichen, anhand deren betroffene Personen rasch das von für die Verarbeitung Verantwortlichen oder von Auftragsverarbeitern gewährleistete Datenschutzniveau in Erfahrung bringen können. Die datenschutzspezifischen Zertifizierungsverfahren dienen der ordnungsgemäßen Anwendung dieser Verordnung und tragen den Besonderheiten der einzelnen Sektoren und Verarbeitungsprozesse Rechnung.	1. Die Mitgliedstaaten und die Kommission fördern insbesondere auf europäischer Ebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -zeichen, anhand deren betroffene Personen rasch das von für die Verarbeitung Verantwortlichen oder von Auftragsverarbeitern gewährleistete Datenschutzniveau in Erfahrung bringen können. Die datenschutzspezifischen Zertifizierungsverfahren dienen der ordnungsgemäßen Anwendung dieser Verordnung und tragen den Besonderheiten der einzelnen Sektoren und Verarbeitungsprozesse Rechnung.	1. Die Mitgliedstaaten, der Europäische Datenschutzausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen, die von für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern durchgeführt werden, eingehalten wird. Den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen wird Rechnung getragen.

EU-KOMMISSION	EUROPÄISCHES PARLAMENT	EUROPÄISCHER RAT
	1a. Jeder für die Verarbeitung Verantwortliche oder Auftragsverarbeiter kann bei jeder Aufsichtsbehörde in der Union für eine angemessene Gebühr unter Berücksichtigung der Verwaltungskosten eine Zertifizierung darüber beantragen, dass die Verarbeitung personenbezogener Daten im Einklang mit dieser Verordnung durchgeführt wird, insbesondere mit den Grundsätzen der Artikel 5, 23 und 30, den Pflichten der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter und den Rechten der betroffenen Person.	1a. Zusätzlich zur Einhaltung durch die unter diese Verordnung fallenden für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter können auch datenschutzspezifische Zertifizierungsverfahren, Siegel oder Prüfzeichen, die gemäß Absatz 2a genehmigt worden sind, vorgesehen werden, um nachzuweisen, dass die für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter, die gemäß Artikel 3 nicht unter diese Verordnung fallen, im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen nach Maßgabe von Artikel 42 Absatz 2 Buchstabe e geeignete Garantien bieten. Diese für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter gehen mittels vertraglicher Instrumente oder auf andere Weise die verbindliche und durchsetzbare Verpflichtung ein, die geeigneten Garantien auch im Hinblick auf die Rechte der betroffenen Personen anzuwenden.
	1b. Die Zertifizierung ist freiwillig, erschwinglich und über ein transparentes und nicht übermäßig aufwendiges Verfahren zugänglich.	
	1c. Die Aufsichtsbehörden und der Europäische Datenschutzausschuss arbeiten im Rahmen des Kohärenzverfahrens gemäß Artikel 57 zusammen, um ein harmonisiertes datenschutzspezifisches Zertifizierungsverfahren zu gewährleisten, einschließlich harmonisierter Gebühren innerhalb der Union.	
	1d. Während des Zertifizierungsverfahrens kann die Aufsichtsbehörde spezialisierte dritte Prüfer akkreditieren, die Prüfung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters für sie durchzuführen. Dritte Prüfer verfügen über ausreichend Personal, sind unparteiisch und in Bezug auf ihre Aufgaben frei von Interessenkonflikten. Aufsichtsbehörden entziehen die Akkreditierung, wenn es Grund zu der Annahme gibt, dass der Prüfer seine Aufgaben nicht korrekt erfüllt. Die endgültige Zertifizierung erteilt die Aufsichtsbehörde.	

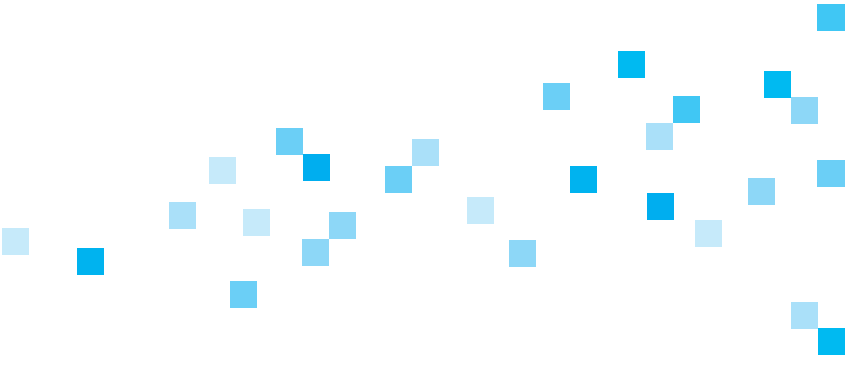
EU-KOMMISSION	EUROPÄISCHES PARLAMENT	EUROPÄISCHER RAT
	1e. Die Aufsichtsbehörden erteilen den für die Verarbeitung Verantwortlichen oder Auftragsverarbeitern, denen nach der Prüfung zertifiziert wird, dass sie personenbezogene Daten im Einklang mit dieser Verordnung verarbeiten, das standardisierte Datenschutzzeichen mit der Bezeichnung „Europäisches Datenschutzsiegel“.	
	1f. Das „Europäische Datenschutzsiegel“ ist so lange gültig, wie die Verarbeitungsprozesse des zertifizierten für die Verarbeitung Verantwortlichen oder des zertifizierten Auftragsverarbeiters weiter vollständig dieser Verordnung entsprechen.	
	1g. Unbeschadet des Absatzes 1f ist die Zertifizierung höchstens fünf Jahre gültig.	
	1h. Der Europäische Datenschutzausschuss richtet ein öffentliches elektronisches Register ein, in dem die Öffentlichkeit Einsicht in alle gültigen und ungültigen Zertifikate, die von den Mitgliedstaaten ausgestellt wurden, nehmen kann.	
	1i. Der Europäische Datenschutzausschuss kann auf eigene Initiative zertifizieren, dass ein technischer Standard zur Verbesserung des Datenschutzes mit dieser Verordnung vereinbar ist.	
2. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die in Absatz 1 genannten datenschutzspezifischen Zertifizierungsverfahren einschließlich der Bedingungen für die Erteilung und den Entzug der Zertifizierung sowie der Anforderungen für die Anerkennung der Zertifizierung in der Union und in Drittländern festzulegen.	2. Die Kommission wird ermächtigt, nachdem sie den Europäischen Datenschutzausschuss um eine Stellungnahme ersucht hat und nach Anhörung von Interessenträgern, insbesondere Industrieverbänden und nichtstaatlichen Organisationen, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen für die in den Absätzen 1a bis 1h genannten datenschutzspezifischen Zertifizierungsverfahren einschließlich der Bedingungen für die Akkreditierung der Prüfer, der Bedingungen für die Erteilung und den Entzug der Zertifizierung sowie der Anforderungen für die Anerkennung der Zertifizierung in der Union und in Drittländern festzulegen. Mit diesen delegierten Rechtsakten werden den betroffenen Personen durchsetzbare Rechte übertragen.	2. Eine Zertifizierung gemäß diesem Artikel mindert nicht die Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung dieser Verordnung und berührt nicht die Aufgaben und Befugnisse der Aufsichtsbehörde, die gemäß Artikel 51 oder 51a zuständig ist.

EU-KOMMISSION	EUROPÄISCHES PARLAMENT	EUROPÄISCHER RAT
		2a. Eine Zertifizierung nach diesem Artikel wird durch die Zertifizierungsstellen nach Artikel 39a oder gegebenenfalls durch die zuständige Aufsichtsbehörde anhand der von der zuständigen Aufsichtsbehörde genehmigten Kriterien oder – gemäß Artikel 57 – durch den Europäischen Datenschutzausschuss erteilt.
3. Die Kommission kann technische Standards für Zertifizierungsverfahren sowie Datenschutzsiegel und -zeichen und Verfahren zur Förderung und Anerkennung von Zertifizierungsverfahren und Datenschutzsiegeln und -zeichen festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren angenommen.	3. Die Kommission kann technische Standards für Zertifizierungsverfahren sowie Datenschutzsiegel und -zeichen und Verfahren zur Förderung und Anerkennung von Zertifizierungsverfahren und Datenschutzsiegeln und -zeichen festlegen. Die entsprechenden Durchführungsrechtsakte werden in Übereinstimmung mit dem in Artikel 87 Absatz 2 genannten Prüfverfahren angenommen.	3. Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter, der die von ihm durchgeführte Verarbeitung dem Zertifizierungsverfahren unterwirft, stellt der Zertifizierungsstelle nach Artikel 39a oder gegebenenfalls der zuständigen Aufsichtsbehörde alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung und gewährt ihr den in diesem Zusammenhang erforderlichen Zugang zu seinen Verarbeitungstätigkeiten.
		4. Die Zertifizierung wird einem für die Verarbeitung Verantwortlichen oder einem Auftragsverarbeiter für eine Höchstdauer von drei Jahren erteilt und kann unter denselben Bedingungen verlängert werden, solange die einschlägigen Voraussetzungen weiterhin erfüllt werden. Sie wird durch die Zertifizierungsstellen nach Artikel 39a oder gegebenenfalls durch die zuständige Aufsichtsbehörde widerrufen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden.
		5. Der Europäische Datenschutzausschuss nimmt alle Zertifizierungsverfahren und Datenschutzsiegel in ein Register auf und veröffentlicht sie in geeigneter Weise, z. B. über das Europäische E-Justiz-Portal.

EU-KOMMISSION	EUROPÄISCHES PARLAMENT	EUROPÄISCHER RAT
		Artikel 39a **Zertifizierungsstelle und -verfahren** 1. Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 52 und 53 wird die Zertifizierung von einer Zertifizierungsstelle erteilt, die über das geeignete Fachwissen hinsichtlich des Datenschutzes verfügt. Jeder Mitgliedstaat teilt mit, ob diese Zertifizierungsstellen akkreditiert wurden von (a) der gemäß Artikel 51 oder 51a zuständigen Aufsichtsbehörde und/oder (b) der nationalen Akkreditierungsstelle, die gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten im Einklang mit EN-ISO/IEC 17065/2012 und mit den zusätzlichen von der gemäß Artikel 51 oder 51a zuständigen Aufsichtsbehörde festgelegten Anforderungen benannt wurde.
		2. Die Zertifizierungsstelle nach Absatz 1 kann zu diesem Zweck nur akkreditiert werden, wenn (a) sie ihre Unabhängigkeit und ihr Fachwissen hinsichtlich des Gegenstands der Zertifizierung zur Zufriedenheit der zuständigen Aufsichtsbehörde nachgewiesen hat; (aa) sie sich verpflichtet hat, die Kriterien nach Artikel 39 Absatz 2a, die von der gemäß Artikel 51 oder 51a zuständigen Aufsichtsbehörde oder – gemäß Artikel 57 – von dem Europäischen Datenschutzausschuss genehmigt wurden, einzuhalten; (b) sie Verfahren für die Erteilung, die regelmäßige Überprüfung und den Widerruf der Datenschutzsiegel und -prüfzeichen festgelegt hat;

EU-KOMMISSION	EUROPÄISCHES PARLAMENT	EUROPÄISCHER RAT
		Artikel 39a **Zertifizierungsstelle und -verfahren** (c) sie Verfahren und Strukturen festgelegt hat, mit denen sie Beschwerden über Verletzungen der Zertifizierung oder die Art und Weise, in der die Zertifizierung von dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter umgesetzt wird oder wurde, nachgeht und diese Verfahren und Strukturen für betroffene Personen und die Öffentlichkeit transparent macht; (d) sie zur Zufriedenheit der zuständigen Aufsichtsbehörde nachweist, dass ihre Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.
		3. Die Akkreditierung der Zertifizierungsstellen nach Absatz 1 erfolgt anhand der Kriterien, die von der gemäß Artikel 51 oder 51a zuständigen Aufsichtsbehörde oder, gemäß Artikel 57, von dem Europäischen Datenschutzausschuss genehmigt wurden. Im Fall einer Akkreditierung nach Absatz 1b ergänzen diese Anforderungen diejenigen, die in der Verordnung 765/2008 und in den technischen Vorschriften, in denen die Methoden und Verfahren der Zertifizierungsstellen beschrieben werden, vorgesehen sind.
		4. Die Zertifizierungsstelle nach Absatz 1 ist unbeschadet der Verantwortung, die der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter für die Einhaltung dieser Verordnung hat, für die angemessene Bewertung, die der Zertifizierung oder dem Widerruf einer Zertifizierung zugrunde liegt, verantwortlich. Die Akkreditierung wird für eine Höchstdauer von fünf Jahren erteilt und kann unter denselben Bedingungen verlängert werden, solange die Stelle die Anforderungen erfüllt.
		5. Die Zertifizierungsstelle nach Absatz 1 teilt der zuständigen Aufsichtsbehörde die Gründe für die Erteilung oder den Widerruf der beantragten Zertifizierung mit.

EU-KOMMISSION	EUROPÄISCHES PARLAMENT	EUROPÄISCHER RAT
		6. Die Anforderungen nach Absatz 3 und die Kriterien nach Artikel 39 Absatz 2a werden von der Aufsichtsbehörde in leicht zugänglicher Form veröffentlicht. Die Aufsichtsbehörde übermittelt diese auch dem Europäischen Datenschutzausschuss. Der Europäische Datenschutzausschuss nimmt alle Zertifizierungsverfahren und Datenschutzsiegel in ein Register auf und veröffentlicht sie in geeigneter Weise, z. B. über das Europäische E-Justiz-Portal.
		(6a) Unbeschadet der Bestimmungen des Kapitels VIII widerruft die zuständige Aufsichtsbehörde oder die nationale Akkreditierungsstelle die Akkreditierung einer Zertifizierungsstelle nach Absatz 1, wenn die Voraussetzungen für ihre Akkreditierung nicht oder nicht mehr erfüllt sind oder wenn die Stelle Maßnahmen ergreift, die nicht mit dieser Verordnung vereinbar sind.
		7. Die Kommission wird ermächtigt, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Kriterien und Anforderungen festzulegen, die für die in Absatz 1 genannten datenschutzspezifischen Zertifizierungsverfahren zu berücksichtigen sind [, einschließlich der Bedingungen für die Erteilung und den Widerruf der Zertifizierung sowie der Anforderungen für die Anerkennung der Zertifizierung und der Anforderungen für ein standardisiertes „Europäisches Datenschutzsiegel“ in der Union und in Drittländern].
		(7a) Der Europäische Datenschutzausschuss gibt der Kommission gegenüber eine Stellungnahme zu den Kriterien und Anforderungen, auf die in Absatz 7 Bezug genommen wird, ab.
		8. Die Kommission kann technische Standards für Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen und Verfahren zur Förderung und Anerkennung von Zertifizierungsverfahren und Datenschutzsiegeln und -prüfzeichen festlegen. Die betreffenden Durchführungsrechtsakte werden in Übereinstimmung mit dem Prüfverfahren nach Artikel 87 Absatz 2 erlassen.



Das Thesenpapier zur Datenschutz-Zertifizierung durch private Stellen

Das rechtspolitische Thesenpapier „Datenschutz-Zertifizierung durch private Stellen“ wurde vom Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ und von der Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ erstellt.

→ Mitwirkende/Autoren

Dr. Thorsten B. Behling, WTS Rechtsanwaltsgesellschaft mbH

Oliver Berthold, Berliner Beauftragter für Datenschutz und Informationsfreiheit

Prof. Dr. Georg Borges, Kompetenzzentrum Trusted Cloud

Dirk Bungard, Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Mathias Cellarius, SAP SE

Dr. Astros Chatziastros, TMF e.V.

Susanne Dehmel, BITKOM

Thomas Doms, TÜV TRUST IT GmbH Unternehmensgruppe TÜV Austria

Dr. Alexander Duisberg, Bird & Bird LLP

Günther Eble, Kommunale Informationsverarbeitung Baden-Franken

Alexander Glaus, Deutsche Bank AG

Björn Hajek, LL.M., Infineon Technologies AG

Dr. Marc Hilber, LL.M., Oppenhoff & Partner

Claudia Husz, regio IT

Dr. Hubert Jäger, Uniscon universal identity control GmbH

Nicolas Kölsch, WTS Consulting

Rudi Kramer, DATEV eG

Thomas Kranig, Bayerisches Landesamt für Datenschutzaufsicht

Steffen Kroschwald, Universität Passau

Johannes Landvogt, Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Dirk Piesker, Deutsche Telekom AG

Patrick Quellmalz, VOICE e.V.

Christoph Rechsteiner, SAP SE

Frederick Richter, Stiftung Datenschutz

Stephan Sädtler, Universität Passau

Gunther Schiefer, Karlsruher Institut für Technologie

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

Antonius Sommer, TÜViT GmbH

Dr. Christoph Sutter, TÜViT GmbH

Karin Vedder, Bayerisches Landesamt für Datenschutzaufsicht

Dr. Joseph Walenta, Deutsches Herzzentrum Berlin

Dr. Mathias Weber, BITKOM

Andreas Weiss, Eurocloud Deutschland_eco e.V.

Magda Wicker, Universität Kassel

Monika Wojtowicz, TÜViT GmbH

Impressum

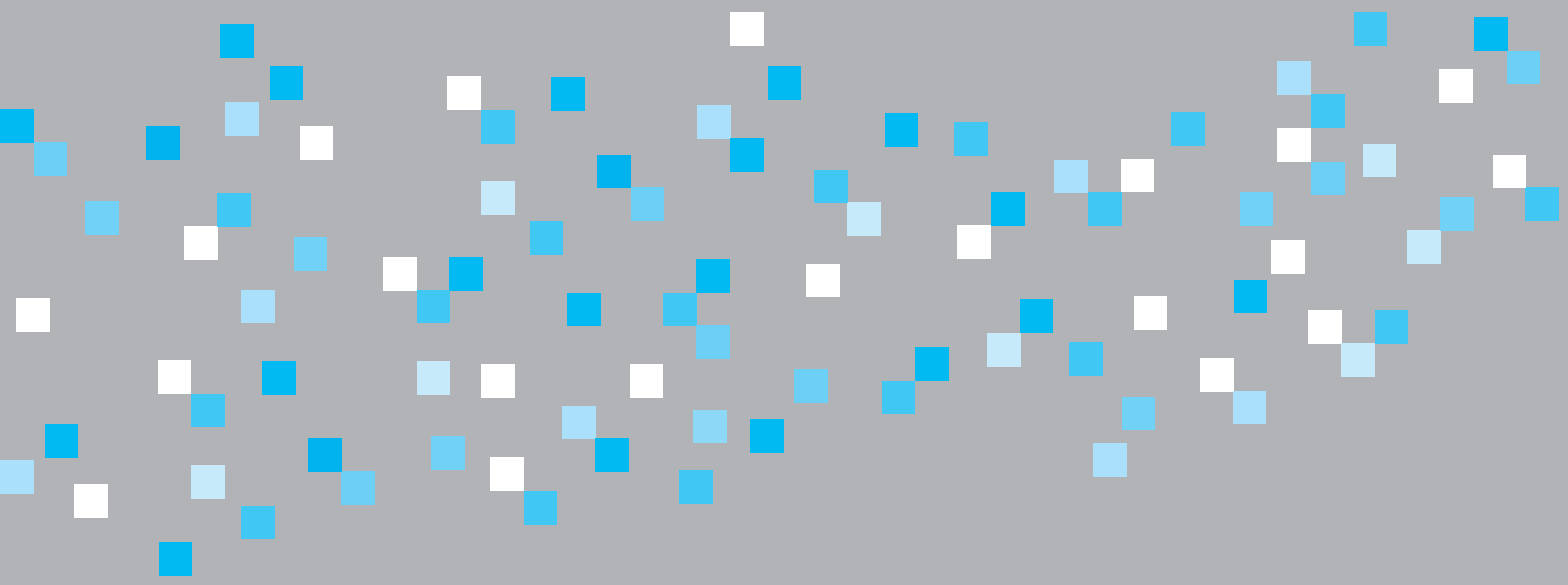
Herausgeber
Kompetenzzentrum Trusted Cloud
Arbeitsgruppe „Rechtsrahmen des Cloud Computing“
E-Mail: kompetenzzentrum@trusted-cloud.de
www.trusted-cloud.de

Im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi)

Gestaltung
A&B One Kommunikationsagentur, Berlin

Druck
DCM Druck Center Meckenheim

Stand: Februar 2015



www.trusted-cloud.de