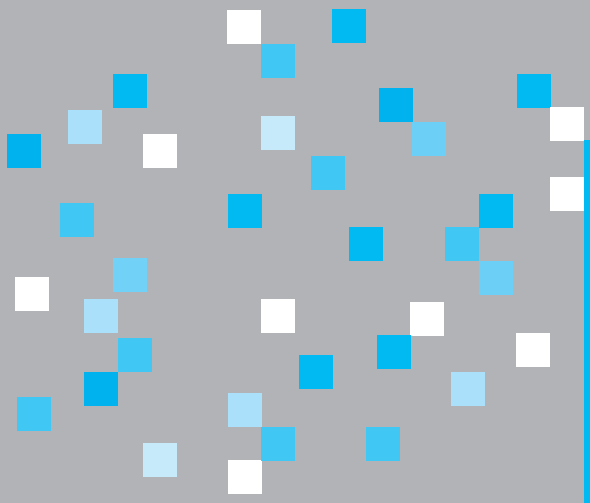
Trusted Cloud



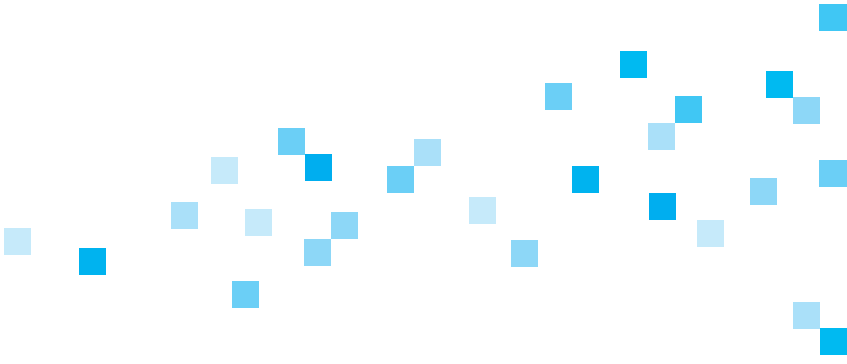
Datenschutzrechtliche Lösungen für Cloud Computing

Ein rechtspolitisches Thesenpapier der AG Rechtsrahmen des Cloud Computing

Arbeitsgruppe Rechtsrahmen des Cloud Computing

Die Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ im Kompetenzzentrum Trusted Cloud bearbeitet rechtliche Aspekte des Cloud Computing mit dem Ziel, die Gestaltung verlässlicher und angemessener rechtlicher Rahmenbedingungen für Cloud Computing zu fördern.

Mitglieder der AG sind neben Vertretern der Projekte des Technologieprogramms Trusted Cloud namhafte Experten aus Wirtschaft, Wissenschaft sowie der öffentlichen Hand. Die AG wird geleitet von Prof. Dr. Georg Borges.



Rechtsrahmen

Datenschutzrechtliche Lösungen für Cloud Computing

Cloud Computing wirft schwierige Rechtsfragen im Bereich des Datenschutzrechts auf.

Dies gilt nicht zuletzt für die Ausgestaltung der Auftragsdatenverarbeitung, die bei Cloud Computing genutzt wird. Dies beruht wesentlich darauf, dass das bisherige Recht der Auftragsdatenverarbeitung auf die aktuelle technische Entwicklung der Datenverarbeitung (Internet, Cloud Computing) nicht eingestellt ist.

Die anstehende Reform des europäischen Datenschutzrechts bietet die Gelegenheit, das Recht der Auftragsdatenverarbeitung an die geänderten technischen und organisatorischen Bedingungen der Datenverarbeitung im Internet und im Cloud Computing anzupassen.

Das nachfolgende Papier zeigt, durch Formulierung und Begründung von insgesamt zehn Thesen, Reformbedarf bei der Rechtsfigur der Auftragsdatenverarbeitung auf und entwirft einen konkreten Reformvorschlag. Im ersten Teil (Thesen 1–5) wird die Notwendigkeit einer gesetzlichen Reform begründet und das Kernelement der notwendigen Reform, die Erfüllung der Überprüfungspflicht des Auftraggebers durch ein Testat, entwickelt. Im zweiten Teil (Thesen 6–10) werden die Elemente dieser Testatlösung im Einzelnen beschrieben.

These 1

Die Auftragsdatenverarbeitung ist ein zentraler Anwendungsfall bei der Nutzung neuer Formen der Datenverarbeitung.

Die Organisation der elektronischen Datenverarbeitung erfährt einen grundlegenden Wandel durch moderne Technologien, insbesondere das Internet. Besonders deutlich wird der Wandel am Beispiel des Cloud Computing.

Das aus Sicht des Datenschutzrechts zentrale Charakteristikum des Cloud Computing besteht darin, dass Datenverarbeitung als „Dienst“ (Service) strukturiert wird. Entsprechend unterscheidet die Cloud-Computing-Definition des NIST (National Institute of Standards and Technology) drei Kategorien von Servicemodellen, die als Software as a Service, Platform as a Service und Infrastructure as a Service bezeichnet werden. Ein solcher Dienst ist, wie schon der Begriff zeigt, darauf angelegt, dass er von einem Dritten angeboten wird. Daher werden beim Cloud Computing, ebenso bei anderen technischen Dienstleistungen, häufig die inhaltliche Gestaltung der Datenverarbeitung einerseits, die technische Steuerung der Datenverarbeitung andererseits, durch unterschiedliche Personen erbracht.

Cloud Computing wird als dominanter technischer Trend der Datenverarbeitung eingeschätzt, der grundsätzlich den gesamten Bereich der Datenverarbeitung erfassen kann, angefangen von der Datenverarbeitung durch Unternehmen jeglicher Größenordnung bis zur staatlichen Verwaltung und einschließlich der privaten Datenverarbeitung. In der Tat ist Cloud Computing die konsequente Fortentwicklung der Datenverarbeitung unter den Bedingungen des Internets. Genauso wie bei der Kommunikation per Internet der physische Standort der Kommunikationspartner unbedeutend wird, wird beim Cloud Computing der Ort von Datenspeicherung und -verarbeitung – zumindest aus technischer Sicht – bedeutungslos.

Im geltenden deutschen Datenschutzrecht wird die Trennung zwischen der Datenverarbeitung als technischem Prozess und der Datenverarbeitung als inhaltlicher Nutzung der Datenverarbeitung maßgeblich durch die Rechtsfigur der Auftragsdatenverarbeitung erfasst (§ 11 BDSG). Dies gilt ebenso im Entwurf der EU-Datenschutz-Grundverordnung, die zwischen dem „für die Verarbeitung Verantwortlichen“ und dem „Auftragsverarbeiter“ unterscheidet.

Wenn also Cloud Computing und damit die organisatorische Trennung zwischen der Datenverarbeitung als technischer Dienstleistung und der inhaltlichen Steuerung und Nutzung der Datenverarbeitung künftig die Realität der Datenverarbeitung prägt, dann wird die Auftragsdatenverarbeitung unter dem Gesichtspunkt des Datenschutzrechts zu einem zentralen Anwendungsfall der Datenverarbeitung.

These 2

Die Regeln der Auftragsdatenverarbeitung, insbesondere die Anforderungen an den Vertrag und an die Kontrolle des Auftragnehmers durch den Auftraggeber, passen nicht uneingeschränkt zu modernen Formen der Datenverarbeitung und müssen überarbeitet werden.

Die rechtliche Regelung der Auftragsdatenverarbeitung basiert auf einem anderen als dem gegenwärtigen und künftigen technischen Hintergrund und wurde ursprünglich mit Blick auf große IT-Outsourcing-Projekte geschaffen.

→ Auftragsdatenverarbeitung und IT-Outsourcing

Klassische IT-Outsourcing-Projekte haben typischerweise eine lange Vertragsdauer, häufig ein großes wirtschaftliches Volumen und sind regelmäßig von vitaler Bedeutung für das auslagernde Unternehmen, das eine unverzichtbare Grundlage seiner Tätigkeit in andere Hände gibt. Ein typischer Hintergrund des klassischen IT-Outsourcings sind Situationen, in denen ein Unternehmen, das bisher ein eigenes Rechenzentrum betreibt, die Datenverarbeitung auf einen Dritten auslagert.

Zum Bild des klassischen IT-Outsourcings passt die rechtliche Regelung der Auftragsdatenverarbeitung, die durch folgende zentrale Merkmale gekennzeichnet ist:

- Zulässigkeit der Auftragsdatenverarbeitung ohne Einwilligung des Betroffenen;
- primäre Verantwortlichkeit des Auftraggebers für die Datenverarbeitung gegenüber dem Betroffenen;
- eingeschränkte Verantwortlichkeit des Auftragnehmers gegenüber dem Betroffenen (vor allem in Bezug auf die Sicherheit der Datenverarbeitung);
- Weisungsrecht des Auftraggebers;
- umfassende rechtliche Anforderungen an den Vertrag zwischen Auftraggeber und Auftragnehmer;
- Pflicht des Auftraggebers zur sorgfältigen Auswahl des Auftragnehmers und zur kontinuierlichen Überwachung der Datenverarbeitung beim Auftragnehmer.

→ Datenverarbeitung durch Dienstleister in Internet und Cloud Computing

Die Einbeziehung Dritter in die Datenverarbeitung im Zeitalter von Internet und Cloud Computing kann sich vom klassischen IT-Outsourcing erheblich unterscheiden.

Anders als beim klassischen IT-Outsourcing ist die Nutzung von Cloud-Computing-Diensten nicht notwendig ein umfangreiches Projekt von großer Bedeutung, sondern kann auch als Alltag der Datenverarbeitung konzipiert sein, ähnlich wie die Nutzung des Internets. In diesen Fällen werden Cloud-Computing-Dienste als standardisierte Dienstleistung angeboten.

Die Nutzung von Cloud-Computing-Diensten kann auch von geringem Umfang sein oder vorübergehend erfolgen, etwa um Belastungsspitzen aufzufangen. Entsprechend der NIST-Definition soll Cloud Computing mit minimalem Managementaufwand („minimal management effort“) erfolgen können, soll also kurzfristig in Anspruch genommen werden können.

Auch wenn klassisches IT-Outsourcing durch Verwendung von Cloud Computing erfolgen kann, sind wesentliche neue Anwendungsfelder des Cloud Computing dem klassischen IT-Outsourcing diametral entgegengesetzt: hier vitale Bedeutung eines einzelnen Auslagerungsvorgangs, großes Volumen der Transaktion, umfangreiche Verhandlungen, dort auch Alltagsgeschäft, Standardangebote, auch Angebote mit geringerem Umfang oder vorübergehender Bedeutung, auch kurzfristige Inanspruchnahme des Dienstes.

Die Unterschiedlichkeit zwischen diesen verschiedenen Einsatzfeldern von Cloud Computing kann bildlich mit dem Unterschied zwischen der Maßschneiderei (klassisches IT-Outsourcing) und der Konfektionsware (Cloud Computing für „jedermann“) beschrieben werden.

Die rechtliche Regelung der Auftragsdatenverarbeitung ist teilweise am klassischen IT-Outsourcing orientiert und passt daher in vielen Fällen nicht auf neue Formen der Datenverarbeitung. Dies betrifft die umfangreichen Anforderungen an den Vertrag zum einen, die Anforderungen an die Kontrolle des Auftragnehmers zum anderen.

→ Reformbedarf bei den Anforderungen an den Vertrag

Das BDSG stellt umfassende inhaltliche und formale Anforderungen an den Vertrag über die Auftragsdatenverarbeitung, etwa die Schriftlichkeit, die als Schriftform mit eigenhändiger Unterschrift gedeutet wird. Diese Anforderungen führen insgesamt zu einem hohen Aufwand für den Abschluss von Verträgen über Auftragsdatenverarbeitung. Dieser Aufwand war vor dem Hintergrund des klassischen IT-Outsourcings als eines Großprojekts unproblematisch.

Diese Anforderungen passen aber nicht zu den Bedingungen moderner Datenverarbeitung, bei der als Regelfall eine Vielzahl von Datenverarbeitungsdiensten bei unterschiedlichen Anbietern in Anspruch genommen wird. Sie sind insbesondere mit dem Konzept des Cloud Computing, das durch „minimal management effort“ gekennzeichnet sein soll, nicht uneingeschränkt vereinbar.

→ Die Pflicht zur Kontrolle des Auftragnehmers durch den Auftraggeber

Gemäß § 11 Abs. 2 S. 4 BDSG hat sich der Auftraggeber davon zu überzeugen, dass der Auftragnehmer die erforderlichen Maßnahmen zur Gewährleistung der technischen Sicherheit ergriffen hat. Diese Pflicht schließt die Überprüfung der technischen und organisatorischen Maßnahmen vor Ort ein. Unklar ist, ob der Auftraggeber die Überprüfung vor Ort persönlich vorzunehmen hat, wie mitunter gefordert wird. Vor allem ist unklar, durch welche Maßnahmen die Überprüfung durch den Auftraggeber persönlich ersetzt werden kann.

Eine Überprüfung vor Ort durch den Auftraggeber oder dessen Beauftragte entspricht der Realität des klassischen IT-Outsourcings, bei dem ein konkret bezeichnetes Rechenzentrum oder konkrete Server Gegenstand der Dienstleistung waren.

Schon bei Diensten wie der Nutzung von E-Mail-Konten oder Webspace ist diese Situation nicht mehr gegeben. Erst recht wird die Vorstellung, dass der Auftraggeber etwa die Sicherheit einzelner Server oder Serverräume überwacht, im Zeitalter des Cloud Computing realitätsfern. Die Vorteile bei modernen Formen der Datenverarbeitung entstehen durch die gemeinsame Nutzung technischer Ressourcen durch unterschiedliche Datenverarbeitungsvorgänge, bei der viele Nutzer auf einen Rechner oder Server zugreifen und auch mehrere Server oder Rechenzentren parallel eingesetzt werden.

Damit wird der Gedanke an eine Ortsbegehung durch den Auftraggeber ad absurdum geführt, da eine Vielzahl von Orten begangen werden müsste, letztlich ohne dass genau bekannt ist, ob ein bestimmter Ort überhaupt genutzt wird. Zwar ist eine Begehung mehrerer Orte möglich, jedoch steigen die Transaktionskosten so stark an, dass die Effizienzvorteile der verteilten Datenverarbeitung zumindest teilweise wieder zunichtegemacht werden.

Umgekehrt wären Prüfungen vor Ort bei Cloud-Anbietern durch eine Vielzahl von Auftraggebern zu befürchten („Prüftourismus“), die vom Auftragnehmer wirtschaftlich und tatsächlich gar nicht gehandhabt werden könnten. Auch würde eine Vielzahl von prüfenden Auftraggebern in den Rechenzentren grundlegenden Anforderungen an Sicherheit und Datenschutz widersprechen.

Zudem wäre die Frage zu stellen, inwieweit insbesondere kleinere und mittlere Auftraggeber in die Lage versetzt werden können, die beim Auftragnehmer getroffenen Maßnahmen fachlich zu bewerten.

→ Notwendigkeit der Reform

Die derzeitigen Anforderungen des BDSG an den Vertrag sowie an die Kontrolle des Auftragnehmers durch den Auftraggeber führen zu überhöhten Transaktionskosten an die Nutzung moderner Formen der Datenverarbeitung mit der Folge, dass die erhofften wirtschaftlichen Vorteile nicht realisiert werden können oder die gesetzlichen Anforderungen in der Praxis nicht beachtet werden.

Daher sollten die gesetzlichen Bestimmungen zur Auftragsdatenverarbeitung so reformiert werden, dass die gesetzlichen Anforderungen unter den Gegebenheiten moderner Formen der Datenverarbeitung ohne Senkung des materiellen Datenschutzniveaus mit angemessenem Aufwand erfüllt werden können.

These 3

Die primäre rechtliche Verantwortlichkeit des Auftraggebers in der Auftragsdatenverarbeitung ist auch im Zeitalter von Internet und Cloud Computing sachgerecht.

Die Grundgedanken der Auftragsdatenverarbeitung passen auch auf moderne Formen der Datenverarbeitung. Die Nutzung von Cloud-Computing-Diensten ist technisch gesehen ebenso ein interner Vorgang innerhalb der datenverarbeitenden Stelle, wie es im klassischen IT-Outsourcing der Fall ist. Es erscheint richtig, dass das Datenschutzrecht eine solche Datenverarbeitung zulässt.

Würde man die Nutzung der Auftragsdatenverarbeitung an die Zustimmung des Betroffenen binden, hätte dies starke Eingriffe in die Organisationsfreiheit zur Folge, die daher auch rechtlich problematisch sein dürften. Vor allem erscheint es angemessen, es Unternehmen und anderen Organisationen zu ermöglichen, die Datenverarbeitung nach ihren Vorstellungen zu organisieren.

Die primäre Verantwortlichkeit des Auftraggebers gegenüber dem Betroffenen sowie den Aufsichtsbehörden ist eine notwendige und angemessene Folge aus dem Umstand, dass die Datenverarbeitung durch den technischen Dienstleister als interner Vorgang innerhalb der verantwortlichen Stelle angesehen wird. Entfiele die Verantwortlichkeit des Auftraggebers, wären die Schutzinteressen des Betroffenen erheblich beeinträchtigt.

Die eingeschränkte Verantwortlichkeit des technischen Dienstleisters als Auftragnehmer erscheint ebenso richtig. Wäre dieser umfassend Adressat der datenschutzrechtlichen Anforderungen, könnte der Betroffene Rechte wie den Anspruch auf Auskunft und Löschung etc. unmittelbar ihm gegenüber geltend machen. Da der Auftraggeber ebenfalls Adressat dieser Ansprüche ist, hätte dies schwierige Abstimmungsprobleme im Verhältnis zwischen Auftraggeber und Auftragnehmer zur Folge. Problematisch erscheint auch, dass der technische Dienstleister die Information über Zulässigkeit der Datenverarbeitung, etwa eine Einwilligung des Betroffenen, regelmäßig nur über den Auftraggeber erhalten kann.

Die im geltenden Recht verankerte, ergänzende Verantwortung des Auftragnehmers für technische Sicherheit hingegen erscheint gerechtfertigt. Diese Gewährleistung der technischen Sicherheit des Datenverarbeitungsvorgangs erfolgt in der Sphäre des Dienstleisters, die der Auftraggeber nur mittelbar beeinflussen kann. Daher erscheint es richtig, die Verantwortung für die technische Sicherheit jedenfalls auch dem Dienstleister aufzuerlegen und ihn insoweit zum unmittelbaren Adressaten des Datenschutzrechts zu machen, wie es das geltende Recht und ebenso der Entwurf der EU-Datenschutz-Grundverordnung vorsehen.

These 4

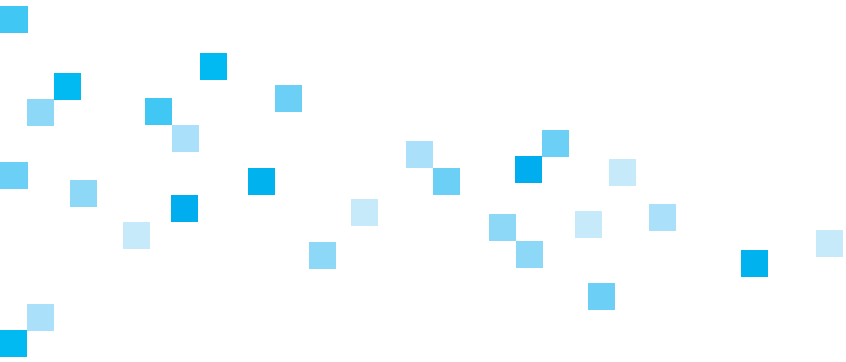
Die Anforderungen an den Vertrag über Auftragsdatenverarbeitung müssen so gefasst werden, dass der Vertragsinhalt vom Auftragnehmer mit den gesetzlich geforderten Inhalten weitgehend vorbereitet und zum Beispiel über Webformulare erfüllt werden kann.

Der Reformbedarf hinsichtlich der gesetzlichen Anforderungen an den Vertrag über Auftragsdatenverarbeitung betrifft zum einen das Schriftlichkeitserfordernis des § 11 Abs. 2 S. 2 BDSG. Die Schriftform des § 126 BGB erscheint im Hinblick auf alternative Dokumentationsmöglichkeiten zur Wahrung eines hinreichenden Datenschutzniveaus jedenfalls de lege ferenda nicht geboten. Der Entwurf der EU-Datenschutz-Grundverordnung verzichtet, wie schon die EU-Datenschutzrichtlinie von 1995, auf das Erfordernis der Schriftlichkeit und hält eine Dokumentation des Vertrages für ausreichend.

Die gesetzlichen Anforderungen an den Inhalt des Vertrags müssen so gestaltet sein, dass sie grundsätzlich per Internet erfüllt werden können. Dabei ist zu bedenken, dass zahlreiche Dienste zur Verringerung von Transaktionskosten vom Auftragnehmer als standardisierte Dienstleistungen angeboten werden, wie es bei Miete von Speicherplatz und zahlreichen Cloud-Computing-Diensten der Regelfall ist. In diesem Fall muss der Auftraggeber die Anforderungen an den Vertragsinhalt mit zumutbarem Aufwand erfüllen können. Dies ist etwa der Fall, wenn vom Auftragnehmer ein Formular mit dem gesetzlich vorgegebenen Inhalt eines Vertrags über Auftragsdatenverarbeitung – einschließlich des Weisungsrechts – vorbereitet wird, das vom Nutzer, der verantwortlichen Stelle, durch Einfügen der spezifischen Angaben vervollständigt wird. Bei diesem Vorgehen wird auch die – für eine Dokumentation ausreichende – Textform eingehalten.

Dieses Vorgehen wird in der Praxis bei standardisierten Diensten zum Einsatz kommen. Bei komplexeren, insbesondere individualisierten Diensten wird auch der Vertrag individuell gestaltet und auf anderem Wege abgeschlossen.

Die Erfüllbarkeit der gesetzlichen Anforderungen durch Webformulare durch Verzicht auf die Schriftform sollte, um Rechtsunsicherheit zu vermeiden, im Gesetz explizit ermöglicht werden.



These 5

Das wesentliche Problem des Kontrollerfordernisses kann gelöst werden, wenn die Kontrolle durch den Auftraggeber durch das von einem unabhängigen Dritten erstellte Testat ersetzt werden kann, das die Durchführung der Kontrolle im gesetzlich angeordneten Umfang bescheinigt. Die Ersetzbarkeit der Überprüfung durch ein Testat ist gesetzlich festzuschreiben.

Zur Lösung der mit dem Kontrollerfordernis verbundenen Schwierigkeiten sind unterschiedliche Ansätze denkbar, insbesondere der vollständige Verzicht zum einen, die Modifikation zum anderen.

→ Schutzlücken bei Verzicht auf Kontrolle

Der Verzicht auf das Kontrollerfordernis würde bedeuten, dass sich die Pflichten des Auftraggebers auf die Auswahl eines geeigneten Auftragnehmers und die vertragliche Verpflichtung des Auftragnehmers zur Erfüllung der gesetzlichen Anforderungen an den Datenschutz beschränken. Insoweit entstünden jedoch Schutzlücken, da der Auftragnehmer nur eingeschränkt Adressat der datenschutzrechtlichen Anforderungen ist.

Vor allem könnte ohne Kontrolle nicht verhindert werden, dass unseriöse Auftragnehmer, die nach außen datenschutzkonformes Verhalten vorgeben – und damit auswahlfähig sind, tatsächlich aber die datenschutzrechtlichen Anforderungen nicht einhalten –, mit der Datenverarbeitung betraut werden.

→ Haftung ist kein Ersatz für Kontrolle

Eine andere Lösung wäre eine Einstandspflicht des Auftraggebers. Danach müsste der Auftraggeber uneingeschränkt für den Auftragnehmer einstehen, wie es § 11 BDSG vorsieht. In diesem Fall würde sich aus dem Haftungsrisiko ein Eigeninteresse des Auftraggebers zur Überwachung ergeben.

Das Konzept einer Verhaltenssteuerung durch Haftung, wie es dem Zivilrecht entspricht, ist prinzipiell überzeugend. Im Datenschutzrecht ist es aber derzeit keine überzeugende Alternative, da die Verhaltenssteuerung durch zivilrechtliche Verantwortlichkeit derzeit nicht funktioniert. Die schon bisher im BDSG enthaltene – dem Gesetzeswortlaut nach strenge – zivilrechtliche Haftung für Datenschutzverstöße hat bisher keine nennenswerte praktische Bedeutung, da die Berechnung eines Schadens schwierig ist.

→ Modifikation der Überwachungspflicht

Als überzeugende Lösung bleibt daher derzeit die Modifikation des Kontrollerfordernisses in der Weise, dass die bestehenden Schwächen beseitigt werden.

Ein zentrales Problem der Kontrolle in der modernen Datenverarbeitung ist, wie dargestellt, dass der einzelne Nutzer viele unterschiedliche Systeme nutzt und zugleich eine Vielzahl von Nutzern auf dieselben Ressourcen zurückgreift, sodass bei der Auftragsdatenverarbeitung jeder Nutzer eine Vielzahl von DV-Systemen kontrollieren müsste und einzelne Systeme durch eine Vielzahl von Nutzern kontrolliert würden.

Dieses strukturelle Problem kann durch Bündelung der Kontrolle beseitigt werden. Im Idealfall sollte jedes System durch eine eigenständige Instanz geprüft werden, die Prüfung sollte allen Nutzern zugutekommen.

Eine solche Bündelung ist schon de lege lata zulässig. Die nach § 11 Abs. 2 S. 4 BDSG geforderte Überprüfung muss nicht durch den Auftraggeber persönlich, sondern kann auch durch einen unabhängigen Dritten erfolgen. Der Dritte kann die Prüfung auch für mehrere Auftraggeber gleichzeitig durchführen, soweit er für jeden Auftraggeber die jeweils geforderte Prüfung wahrnimmt.

Es wird diskutiert, ob die Kontrolle durch den Auftragnehmer erfolgen kann, etwa aufgrund eines detaillierten Fragenkatalogs des Auftraggebers. Dagegen spricht, dass dies dem Wesen der Kontrolle als Überprüfung durch einen anderen als den Kontrollierten nicht entspricht. Im Übrigen könnten die Eigenkontrollen das Auftreten unseriöser Anbieter nicht verhindern.

Eine verstärkte staatliche Aufsicht von Cloud-Dienstleistern durch Datenschutzbehörden kann weder die konkrete Überprüfung des Auftragnehmers ersetzen noch die Risiken einer solchen Eigenkontrolle vermeiden, da eine flächendeckende Überprüfung durch Datenschutzbehörden aus Kapazitätsgründen ausgeschlossen ist.

Als beste Lösung erscheint daher die Überprüfung durch unabhängige Dritte. Diese Dritten müssen für eine sachgerechte Prüfung Gewähr bieten, also insbesondere auch die entsprechende fachliche Eignung aufweisen.

Die Überprüfung müsste dokumentiert werden. In der Auftragsdatenverarbeitung könnte der jeweilige Auftraggeber durch die Dokumentation auch Dritten, etwa der Aufsichtsbehörde, nachweisen, dass eine Überprüfung erfolgte.

Eine solche Prüfungsdokumentation kann durch ein Testat des Prüfers abgeschlossen werden, das die Erfüllung der gesetzlichen Anforderungen im Verantwortungsbereich des Auftragnehmers bestätigt.

Die Überprüfung durch unabhängige Dritte kann auch vom Auftragnehmer initiiert werden. Es ist also möglich, dass der Auftragnehmer eine Überprüfung durchführen lässt und die Dokumentation nebst Testat der Prüfung dem Auftraggeber zur Verfügung stellt mit der Folge, dass die anlassfreie Prüfung der von dem Testat umfassten Gegenstände durch den Auftraggeber nicht mehr erforderlich ist.

Ein solches Testat wäre regelmäßig zu erneuern, genauso wie die Überprüfung durch den Auftraggeber persönlich in regelmäßigen Abständen erforderlich ist. Auch Elemente wie laufende Berichte (Monitoring) ließen sich durch Testierung feststellen und wären Bestandteil des Testats, soweit eine entsprechende gesetzliche Verpflichtung besteht.

Dies führt dazu, dass die gesetzlich erforderliche Überprüfung durch das Testat eines unabhängigen Dritten ersetzt werden kann, soweit die testierte und im Einzelnen dokumentierte Prüfung die vom jeweiligen Auftraggeber geforderte Kontrolle abdeckt.

→ Notwendigkeit der gesetzlichen Klarstellung

Die Ersetzbarkeit der eigenen Überprüfung durch das Testat eines unabhängigen Dritten im Rahmen des § 11 Abs. 2 S. 4 BDSG entspricht heute der ganz überwiegenden Auffassung in Wissenschaft und Praxis. Es besteht aber noch erhebliche Rechtsunsicherheit in Bezug auf die Rechtsfolgen des Testats, insbesondere auf die Wirkung, dass aufgrund des Testats die eigene Kontrolle vor Ort entbehrlich wird. Vor allem sind die Anforderungen an ein solches Testat unklar.

Daher ist eine gesetzliche Regelung erforderlich, die ausdrücklich vorsieht, dass – unter den gesetzlich zu definierenden Voraussetzungen – die Pflicht zur Kontrolle durch den Auftraggeber durch Vorlage des Testats eines unabhängigen Dritten über die Durchführung der gesetzlich angeordneten Überprüfung ersetzt werden kann. Die Pflicht zur anlassbezogenen Überprüfung bliebe hiervon unberührt.

These 6

Gegenstand des Testats ist die gesetzlich geforderte Überprüfung des Auftragnehmers durch den Auftraggeber anhand eines standardisierten Anforderungskatalogs.

Der Gegenstand des Testats ist aus dessen Funktion abzuleiten. Gegenstand der Überprüfung, die durch das Testat ersetzt werden soll, ist die Einhaltung der technischen und organisatorischen Maßnahmen, die zur Erfüllung der datenschutzrechtlichen Anforderungen erforderlich sind.

Die erforderlichen technischen und organisatorischen Maßnahmen orientieren sich am Einzelfall und sind aufgrund einer Abwägung von Schutzerfordernis und Aufwand der Maßnahme zu ermitteln. Daher können die im Einzelfall gesetzlich erforderlichen Maßnahmen nicht generell festgelegt werden.

Dies schließt einheitliche Testate jedoch nicht aus. Dabei ist zum einen zu berücksichtigen, dass ein Großteil der Anforderungen an die technischen und organisatorischen Maßnahmen für eine Vielzahl von Datenverarbeitungsvorgängen gleich ist. So unterscheiden sich, bildlich gesprochen, etwa die Anforderungen an die Sicherung des Zugangs zu Serverräumen nicht danach, ob Buchhaltungsdaten aus einer Metzgerei oder einer Bäckerei verarbeitet werden. Daher könnten für die meisten Anwendungsbereiche ähnliche Anforderungen formuliert werden.

Der gesetzliche Maßstab legt bei den technischen und organisatorischen Maßnahmen ein Mindestmaß fest und schließt es nicht aus, dass höhere Anforderungen erfüllt werden. Daher können die Divergenzen, die sich im Rahmen einer einzelfallorientierten Abwägung ergeben würden, dadurch aufgefangen werden, dass für die Testierung ein hoher Schutzmaßstab zugrunde gelegt wird, bei dem sicher angenommen werden kann, dass die im Einzelfall geforderten gesetzlichen Anforderungen erfüllt werden.

Durch diesen Effekt ergibt sich durch ein Testierungsverfahren ein Gewinn an Datenschutz, der für den Auftraggeber ein zusätzlicher Anreiz für die Nutzung einer Cloud-Lösung sein kann. Die Anbieter von Auftragsdatenverarbeitung werden hierdurch nicht stärker belastet, da sie aus Effizienzgründen ohnehin ein einheitliches Schutzniveau anstreben und dabei ein hohes Schutzniveau wählen, um den Schutzbedürfnissen unterschiedlicher Kundengruppen gerecht zu werden.

Die gesetzlichen Anforderungen an die technischen und organisatorischen Maßnahmen werden für die praktische Durchführung der Überprüfung in einem Anforderungskatalog zusammengefasst, der Grundlage der Prüfung und damit des Testats ist. Das Testat erstreckt sich im Umfang auf die geprüften Maßnahmen. Damit können die gesetzlichen Anforderungen für Standard-Clouddienste und Standard-Datenverarbeitung abgedeckt werden.

Soweit aufseiten des Auftraggebers, insbesondere aufgrund der Art der Daten (z. B. Gesundheitsdaten) oder der Art der Datenverarbeitung, besondere gesetzliche Anforderungen bestehen, sind diese vom Testat nicht erfasst. Es bleibt insoweit beim Erfordernis der Eigenüberwachung. Allerdings werden sich auch für besondere Anwendungen in vielen Fällen Fallgruppen bilden lassen, die dann wiederum Gegenstand eines spezifischen Testats (z. B. Testat für die Auslagerung der Verarbeitung von Gesundheitsdaten) sein können. Entsprechendes gilt, soweit das Risikoprofil der Datenverarbeitung durch besondere technische Schutzmaßnahmen (z. B. Verschlüsselung) verändert wird.

These 7

Die Prüfkriterien für die Erteilung des Testats sind auf gesetzlicher Grundlage für den europäischen Binnenmarkt einheitlich festzusetzen. Die Festlegung der Prüfkriterien sollte durch ein Verfahren erfolgen, in dem Datenschutzbehörden sowie Vertreter von Anbietern und Nutzern der Auftragsdatenverarbeitung beteiligt werden.

Wenn die Überprüfung des Diensteanbieters zum Zwecke der Testaterteilung anhand eines standardisierten Prüfkatalogs erfolgen soll, ist zu klären, durch welche Institution die Prüfkriterien des Katalogs oder der Kataloge festgesetzt werden sollen.

Das Verfahren zur Festlegung der Prüfkriterien sollte eine Reihe grundlegender Anforderungen erfüllen:

- Die Prüfkriterien sollen im Binnenmarkt einheitlich sein, da sonst die durch die Verordnung angestrebte Vereinheitlichung in diesem wichtigen Punkt wieder verloren ginge.
- Die Kriterien sollen an die Veränderungen der Datenverarbeitung angepasst werden können, damit die Schutzziele bei Veränderung technischer oder organisatorischer Gegebenheiten erreicht werden können.
- Die Kriterien sollen durch eine Institution oder in einem Verfahren festgelegt werden, das die Interessen aller Beteiligter, insbesondere des Datenschutzes und der Anbieter und Nutzer von Diensten, einbezieht.

Aus diesen Zielen ergibt sich eine Vorklärung für die Auswahl des geeigneten Verfahrens:

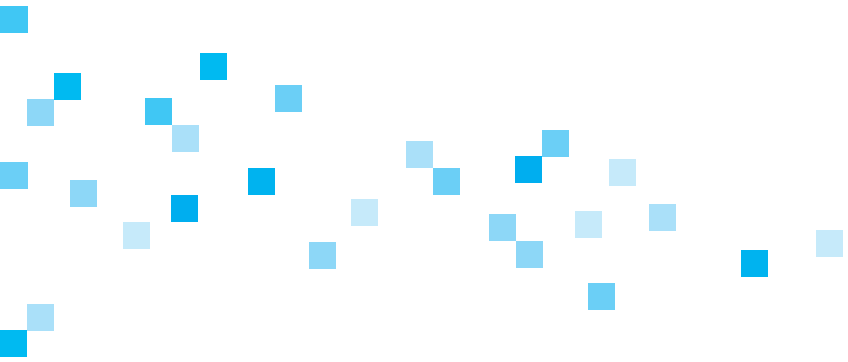
- Die theoretisch denkbare Möglichkeit, die Prüfkriterien durch die testierende Stelle selbst bestimmen zu lassen, würde den genannten Zielen nicht gerecht. Sie würde zu divergierenden Anforderungen führen. Zudem bestünde für die testierende Stelle ein Anreiz, die Prüfkriterien zu niedrig anzusetzen.
- Wegen des Ziels der Einheitlichkeit sollte die Bestimmung der Prüfkriterien auch nicht den einzelnen Mitgliedstaaten überlassen werden.
- Eine Festlegung der Prüfkriterien in der Verordnung selbst würde zwar eine einheitliche Regelung herbeiführen. Dies würde den Text der Verordnung jedoch überfrachten und vor allem wäre diese Regelungstechnik zu unflexibel.
- Die Prüfkriterien könnten durch einen delegierten Rechtsakt der EU-Kommission festgelegt werden. Allerdings fehlt der Kommission die eigene Sachkunde hierfür. Daher müssten die Aufsichtsbehörden sowie Datenschutzexperten aus Wirtschaft und Wissenschaft einbezogen werden, damit deren Kompetenz genutzt werden kann. Vorzugswürdig sind daher Lösungen, die eine solche Beteiligung sichern.
- Die Verordnung könnte den Europäischen Datenschutzausschuss (heute: Art. 29 Arbeitsgruppe) beauftragen, die Kriterien festzulegen. Hierfür sprechen mehrere Gesichtspunkte. Die Datenschutzbehörden sind schon nach geltendem Recht damit betraut, die Einhaltung der gesetzlichen Anforderungen zu überprüfen, und verfügen daher über breite Erfahrung und große Sachkunde. Weiterhin handelt es sich um Stellen, die entsprechend der EU-Datenschutzrichtlinie mit fachlicher Unabhängigkeit ausgestattet sind.

Allerdings würde die Festlegung der Prüfkriterien durch Datenschutzbehörden dem Ziel, dass die Interessen aller Beteiligten bei der Konkretisierung berücksichtigt werden, nicht uneingeschränkt gerecht. Insbesondere könnte die Sachkunde der Anwender und Anbieter der Dienste nicht einbezogen werden.

- Mit der Festlegung könnte eine neue Institution beauftragt werden, in der alle Beteiligten vertreten sind. Allerdings besteht eine solche Institution auf europäischer Ebene derzeit nicht. Die Errichtung einer neuen Institution für einen so begrenzten Zweck wie der Festlegung von Prüfkriterien erscheint nicht sinnvoll.
- Die Kriterien könnten auch in einem Verfahren abgestimmt werden, in dem Prüfkriterien durch Einbeziehung von Datenschutzbehörden und weiterer Interessengruppen in einem Abstimmungsverfahren festgelegt werden. Dieses Verfahren könnte vom Europäischen Datenschutzausschuss administriert werden.
  Dieses Vorgehen ist funktional mindestens gleichwertig gegenüber der Festlegung durch eine eigene Institution und kann auf bestehende Strukturen zurückgreifen. Zugleich wäre eine umfassende Beteiligung aller Interessengruppen garantiert.

Im Ergebnis erscheint es notwendig, die Prüfkriterien auf europäischer Ebene in einem Verfahren festzulegen, in dem die Kompetenz aller Beteiligten unmittelbar einbezogen wird.

Organisatorisch erscheint es vorzugswürdig, die Prüfkriterien durch ein Abstimmungsverfahren unter Einbeziehung der Datenschutzbehörden und der Anwender zu ermitteln. Dieses Abstimmungsverfahren sollte durch den Europäischen Datenschutzausschuss administriert werden, wobei vorausgesetzt wird, dass diesem im Zuge der ihm ohnehin nach dem Entwurf der EU-Datenschutz-Grundverordnung zukommenden Bedeutung auch die notwendige administrative Infrastruktur zur Verfügung steht.



These 8

Das Testat sollte (auch) durch qualifizierte private Stellen vergeben werden. Die Eignung der testierenden Stelle sollte durch eine Akkreditierung nachgewiesen werden. Die testierende Stelle sollte für fehlerhafte Testate haften.

Wenn die Überprüfung des Auftragnehmers durch ein Testat ersetzt werden können soll, ist zu klären, durch welche Institution das Testat erteilt werden soll.

→ Testaterteilung als private Wirtschaftstätigkeit

Bei dieser Frage ist zu berücksichtigen, dass aufgrund der Entwicklung der Datenverarbeitung (Internet, Cloud Computing) voraussichtlich sehr viele Dienste eine datenschutzrechtliche Auftragsdatenverarbeitung enthalten und daher möglicherweise sehr viele Testate benötigen werden.

Es ist daher erforderlich, dass eine hinreichende Kapazität zur Erteilung von Testaten besteht. Die Erteilung durch staatliche Stellen dürfte daher schon aus diesem Grunde nicht ratsam sein. Zudem wäre eine Begrenzung dieser Tätigkeit auf staatliche Stellen wohl auch rechtlich problematisch. Bei Öffnung der Testaterteilung als wirtschaftliche Tätigkeit kann sich auch ein Markt für Testatanbieter entwickeln.

Es spricht daher alles dafür, dass das Testat (auch) durch private Stellen erteilt werden kann.

→ Notwendigkeit qualitativer Anforderungen an die testierende Stelle

Wenn die Testate (auch) durch private Stellen erteilt werden können, ist zu klären, welche Anforderungen an die testierende Stelle zu stellen sind. Eine Möglichkeit wäre es, auf gesetzliche Anforderungen an die testierende Stelle gänzlich zu verzichten und die Durchführung einer adäquaten Prüfung vor Testaterteilung durch eine Haftung der testierenden Stelle für unzutreffende Testate zu sichern. Allerdings weist das Haftungsmodell im Bereich des Datenschutzes generell Schwächen auf. Auch eine strafrechtliche oder ordnungsrechtliche Verantwortlichkeit bei falscher Testaterteilung kann alleine nicht sicherstellen, dass Testate nur durch qualifizierte Stellen erteilt werden. Daher sind qualitative Anforderungen an die testierende Stelle notwendig.

Die EU-Datenschutz-Grundverordnung sollte deshalb die Notwendigkeit, dass die testierende Stelle die fachliche und persönliche Eignung zur Testaterteilung aufweist, ausdrücklich festschreiben.

→ Sicherung der Anforderungen durch Akkreditierung

Wenn die testierende Stelle qualitativen gesetzlichen Anforderungen genügen muss, ist zu klären, wie die Erfüllung der Anforderungen gesichert wird. Auch insoweit bestehen unterschiedliche Möglichkeiten.

- Nur theoretisch kommt in Betracht, die Anforderungen an die Qualifikation der testaterteilenden Stelle abstrakt-generell in der Verordnung zu beschreiben, auf eine formale Absicherung der Qualifikation aber zu verzichten. In diesem Fall wäre es Sache des Auftraggebers, der auf ein Testat vertrauen möchte, zu ermitteln, ob die testierende Stelle die gesetzlichen Voraussetzungen erfüllt, da das Testat nur dann gültig wäre. Dieses Risiko ist dem Auftraggeber jedoch nicht zumutbar. Zudem wird ihm in einer Vielzahl von Fällen die erforderliche Sachkunde fehlen. Dieser muss darauf vertrauen können, dass die Stelle, die ein Testat erteilt, hierzu auch befugt ist.
- Ebenfalls eher theoretisch erscheint die Möglichkeit, die Testate einem bestimmten Berufsstand vorzubehalten oder von einer staatlichen Prüfung abhängig zu machen, ähnlich wie die Abschlussprüfung des Jahresabschlusses gemäß § 319 HGB Wirtschaftsprüfern vorbehalten ist. Diese Anforderung erscheint für das Testat weit überzogen. Denkbar erscheint hingegen, bestimmte Berufsgruppen oder Stellen von vornherein als geeignet zu bestimmen.
- Die Berechtigung zur Testaterteilung könnte von einer Prüfung der testierenden Stelle abhängig gemacht werden, etwa im Wege der Zertifizierung oder Akkreditierung. Für ein solches Modell existieren zahlreiche Vorbilder. Ein solches Modell, das eine Ex-ante-Überprüfung der testierenden Stelle durch das gesetzliche Erfordernis einer Akkreditierung sicherstellt, kann die erforderliche Qualifikation der Stelle für die Testaterteilung sichern und Rechtssicherheit für den Auftraggeber herstellen.

Daher sollte die Eignung der testierenden Stelle durch eine gesetzlich vorgeschriebene Überprüfung (Akkreditierung) der testierenden Stelle gesichert werden.

→ Sicherung der ordnungsgemäßen Testierung durch Haftung

Das Modell einer Akkreditierung kann die qualitativen Anforderungen an die testierende Stelle sicherstellen. Es kann aber allein die Qualität der Überprüfung im Rahmen der Testierung nicht sichern.

Daher sollte in der Verordnung ergänzend eine zivilrechtliche Haftung der testierenden Stelle für fehlerhafte Testierung vorgesehen werden. Die zivilrechtliche Haftung sollte durch eine Verantwortlichkeit für unzureichende Testierung nach Ordnungswidrigkeitenrecht flankiert werden, damit entsprechende Eingriffsbefugnisse für staatliche Stellen bestehen.

These 9

Die Voraussetzungen der Akkreditierung von testierenden Stellen sollten in einem Verfahren von Vertretern der Datenschutzaufsichtsbehörden und Vertretern der Auftraggeber und Auftragnehmer von Auftragsdatenverarbeitung festgelegt werden. Die Akkreditierung sollte für den gesamten Geltungsbereich der EU-Datenschutz-Grundverordnung gelten.

Wenn die Akkreditierung gesetzlich vorgeschrieben sein soll, ist zu klären, welche Voraussetzungen an die Akkreditierung zu stellen sind und welche Stelle die Anforderungen konkretisiert.

Insoweit bestehen ähnliche Optionen wie bei der Festlegung der inhaltlichen Anforderungen an das Testat. Die dort genannten Ziele, insbesondere die Einheitlichkeit der Anforderungen sowie die Möglichkeit der Anpassung an veränderte Entwicklungen, sollten auch für die Anforderungen an die Akkreditierung gelten.

→ Festlegung von Grundsätzen in der Verordnung

Die Bestimmung der Anforderungen sollte nicht den einzelnen Mitgliedstaaten überlassen werden, sondern einheitlich auf europäischer Ebene erfolgen, um die Einheitlichkeit der Anforderungen sicherzustellen.

Eine detaillierte Bestimmung der Anforderungen an die Akkreditierung in der Verordnung erscheint nicht sinnvoll, da sie den Text der Verordnung überfrachten und der Regelung der Akkreditierung jegliche Flexibilität nehmen würde.

Daher sollten die Voraussetzungen der Akkreditierung in allgemeiner Form in der Verordnung beschrieben werden, damit eine hinreichende Grundlage für die Konkretisierung besteht.

→ Konkretisierung der Anforderungen

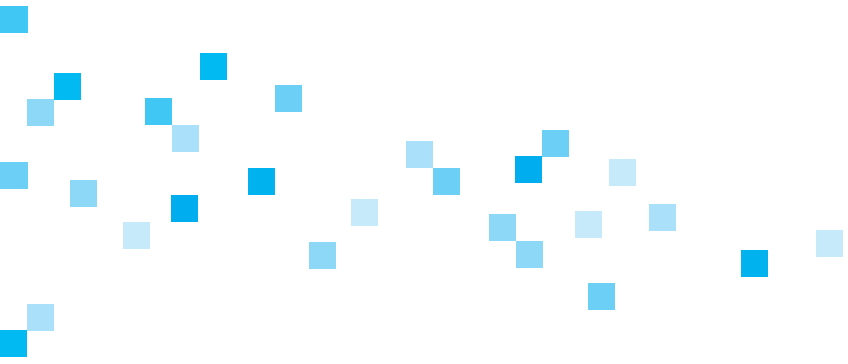
Wenn die Verordnung die Voraussetzungen der Akkreditierung im Grundsatz festlegt, ist weiter zu klären, welche Stelle die Anforderungen konkretisiert. Die Konkretisierung sollte einheitlich für den Binnenmarkt erfolgen, da sonst die Einheitlichkeit der Anforderungen verloren ginge.

Entsprechend der Festlegung der Prüfkriterien für die Erteilung des Testats erscheint es überzeugend, die Anforderungen an die Akkreditierung in einem Verfahren festzulegen, in dem die Kompetenz der Datenschutzaufsichtsbehörden wie der Auftraggeber und Auftragnehmer von Auftragsdatenverarbeitung unmittelbar einbezogen wird.
Auch dieses Abstimmungsverfahren sollte durch den Europäischen Datenschutzausschuss administriert werden.

→ Geltungsbereich der Akkreditierung

Wenn die testierenden Stellen im Binnenmarkt eine Akkreditierung erhalten sollen, ist von Bedeutung, ob die Akkreditierung nur für den Sitzstaat der testierenden Stelle oder für den gesamten Binnenmarkt gilt.

Insoweit erscheint es zwingend, dass die Akkreditierung für den gesamten Geltungsbereich der Verordnung gilt, sodass die testierende Stelle aufgrund der Akkreditierung für den gesamten Geltungsbereich der Verordnung Testate erteilen kann. Nur dann entspricht die Akkreditierung dem Geltungsbereich des Testats, das ebenfalls für den gesamten Anwendungsbereich der Verordnung gilt.



These 10

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.

Soweit die testierende Stelle durch Akkreditierung ihre Qualifikation nachweisen muss, ist zu klären, welche Stelle die Akkreditierung erteilen soll. Eine unmittelbare Festlegung der für die Akkreditierung zuständigen Stellen auf europäischer Ebene, sei es in der EU-Datenschutz-Grundverordnung, durch delegierten Rechtsakt der Kommission oder durch den Europäischen Datenschutzausschuss, erscheint insoweit problematisch, als sehr stark in die Organisation des Datenschutzes eingegriffen würde, die wohl den Mitgliedstaaten obliegt. Daher scheidet diese Möglichkeit aus.

Die Anforderungen an die akkreditierende Stelle sollten abstrakt-generell in der EU-Datenschutz-Grundverordnung geregelt werden. Insoweit sollte die Verordnung regeln, dass die Akkreditierung nur durch Stellen erfolgen kann, die die fachliche Eignung sowie Unabhängigkeit aufweisen, wie es etwa bei Datenschutzaufsichtsbehörden gegeben ist.

Es erscheint überzeugend, die Bestimmung der akkreditierenden Stelle im Übrigen den Mitgliedstaaten zu überlassen, da die Gegebenheiten in Bezug auf die Organisation des Datenschutzes in den einzelnen Mitgliedstaaten divergieren. Die Gefahr divergierender Standards im Binnenmarkt ist dadurch stark gemildert, dass sowohl die Anforderungen an die Akkreditierung als auch die Verantwortlichkeit bei falscher Akkreditierung auf europäischer Ebene geregelt werden. Es geht hier also eher um eine organisatorische Frage als um Divergenzen in Bezug auf die Schutzstandards.

Das Thesenpapier zur Auftragsdatenverarbeitung

Das rechtspolitische Thesenpapier „Datenschutzrechtliche Lösungen für Cloud Computing“ wurde durch Mitglieder der Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ unter der Leitung von Prof. Dr. Georg Borges erarbeitet und im September 2012 durch die gesamte Arbeitsgruppe einstimmig verabschiedet.

Die Arbeitsgruppe empfiehlt das in dem Papier beschriebene Konzept zur Umsetzung durch den Gesetzgeber.

→ Mitwirkende

Dr. Thorsten Behling, KPMG Rechtsanwaltsgesellschaft mbH

Josef Bergner, Kommunale Informationsverarbeitung Baden-Franken

Prof. Dr. Georg Borges, Ruhr-Universität Bochum

Mathias Cellarius, SAP AG

Dr. Alexander Duisberg, Bird & Bird LLP

Dr. Jens Eckhardt, JUCONOMY Rechtsanwälte

Alexander Glaus, Deutsche Bank AG

Björn Hajek, Infineon Technologies AG

Wulf Hartmann, Bundesverband deutscher Banken e. V.

Dr. Marc Hilber, Oppenhoff & Partner

Dr. Hubert Jäger, Uniscon universal identity control GmbH

Kristian Klodt, QSC AG

Rudi Kramer, DATEV eG

Steffen Kroschwald, Universität Kassel

Johannes Landvogt, Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)

Ulrich Lepper, Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Ninja Marnau, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Dr. Jan Geert Meents, DLA Piper UK LLP

Matthias Rüdiger, ITDZ Berlin

Stephan Sädtler, Universität Passau

Gunther Schiefer, Karlsruher Institut für Technologie (KIT)

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

Prof. Dr. Jürgen Taeger, Universität Oldenburg

Barbara Trusch, HSH Soft- und Hardware Vertriebs GmbH

Dr. Claus-Dieter Ulmer, Deutsche Telekom AG

Thomas von Bülow, 1&1 Internet AG

Magda Wicker, Universität Kassel

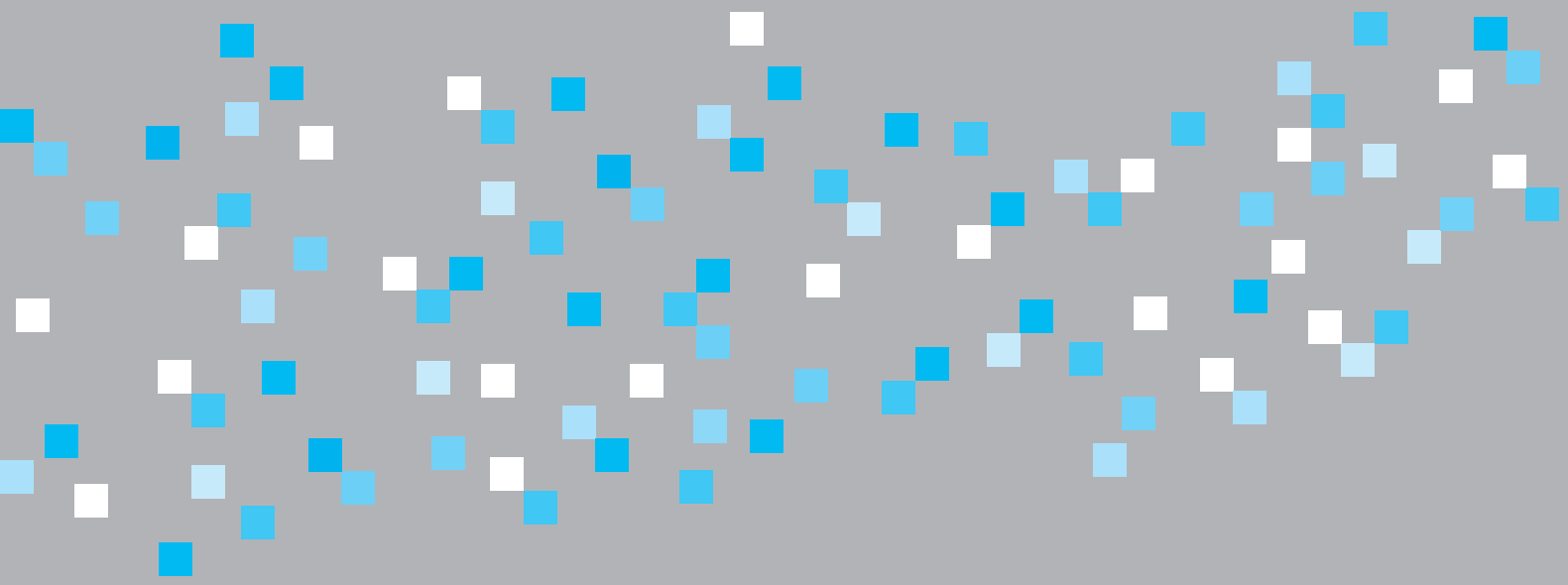
Impressum

Herausgeber
Kompetenzzentrum Trusted Cloud
AG Rechtsrahmen des Cloud Computing
Telefon +49 (0)30 880 04 22 01
E-Mail: kompetenzzentrum@trusted-cloud.de
www.trusted-cloud.de

Gestaltung
A&B One Kommunikationsagentur, Berlin

Druck
vierC print+mediafabrik, Berlin

Stand: Oktober 2012



www.trusted-cloud.de