Dr. Axel-Michael Wagner, RA, und Stefan Groß, StB, CISA

Über den Wolken: Die Rechtsprobleme des Cloud Computing aus der Sicht des auslagernden Unternehmens

Das Thema Cloud Computing ist derzeit in aller Munde. Und immer dann, wenn neue Begriffe eingeführt werden, stellt sich meist zunächst für (insbesondere juristische) Berater die Frage, wie sich die neue Technologie – wenn es sich um eine solche handelt – rechtlich einordnen lässt. Auch beim Aufkommen des Internet als „Massenphänomen" Ende der Neunziger Jahre des letzten Jahrhunderts inklusive der vielen dann folgenden „Domainstreitigkeiten" und des „Web 2.0" der letzten Jahre wurde jeweils darüber gerätselt, ob es sich hier um neuartige „rechtsfreie Räume" handelt oder nur um eine „Verlängerung" altbekannter juristischer Probleme in neuem technischen Gewand. Zwischenzeitlich findet man auch in Gerichtsentscheidungen wie selbstverständlich Begriffe wie „Meta-Tag", „Application Service Providing", „personalisierter Online-Videorekorder" und „Facebook-Account".

I. Einleitung

Ein kurzer Rück- und Überblick, bevor es um Cloud Computing selbst geht: Die Welt der Computer hat sich in den beiden letzten Jahrzehnten stark gewandelt. Früher war der einzige Kontakt, den ein PC zur Außenwelt hatte, die Diskette und vielleicht ein angeschlossener Drucker. Unternehmenseigene EDV-Großanlagen wurden mit höchst individuellen Netzstrukturen in einem Rechenzentrum auf dem Betriebsgelände installiert. Die frühen Netzwerkverbindungen ließen es nicht zu, große Datenmengen zu übertragen, schon gar nicht in Echtzeit. Es bildeten sich proprietäre und Insel-Lösungen, aber zunächst keine allgegenwärtige Informationsinfrastruktur vergleichbar dem öffentlichen Straßennetz.

Der Wandel vollzog sich kontinuierlich: Die Netzwerkverbindungen sind universell geworden und verfügen über stetig steigende Übertragungskapazitäten, die einen Austausch beliebig großer Datenmengen in beliebig kurzer Zeit ermöglichen. Zu einer globalen Weltwirtschaft mit Waren gesellte sich die globale „Weltdatenwirtschaft". Der Unterschied zwischen beiden liegt darin, dass die Transportkosten physischer Waren bei Daten (fast) nicht anfallen und Hin- und Rücktransportzeiten keine Rolle spielen. Das, was einen deutschen mittelständischen Betrieb davon abhalten würde, ein reines Waren-Außenlager beispielsweise in Indien zu errichten – wochenlanger teurer Transport hin und zurück –, entfällt bei Daten völlig. Liegt nun der Schwerpunkt des Begriffes „Elektronische Datenverarbeitung" auf der „Verarbeitung", also dem Prozess des Umgehens mit Daten in bestimmter Weise, so geht es künftig von einem rein ökonomischen Standpunkt aus gesehen darum, die Daten dort zu verarbeiten, wo dies am günstigsten ist. Es stellt sich demnach bei einer kosten- und synergieorientierten Betrachtung nur noch die Frage, wo die größte (= höchstmögliche Synergie) Verarbeitungskapazität für Daten in günstigster (= niedrigste Steuern, niedrigste Bau- und Unterhaltungskosten) Form geschaffen und aufrechterhalten werden kann. Verzögerungsfreier und kostenloser Transport der Daten an den beliebigen Ort der Verarbeitung (und wieder zurück) spielen vor dem Hintergrund der Infrastrukturentwicklungen keine wesentliche Rolle mehr. Kein „Internet-Startup" wird daher, wie noch im Jahr 2000, in ein eigenes kleines „Rechenzentrum" mit Serverhardware, unterbrechungsfreier Stromversorgung und Klimatechnik investieren, weil es diese Kapazitäten als externe Dienstleistungen in Anspruch nehmen wird. Gezahlt wird verbrauchsabhängig für die zur Verfügung gestellten Kapazitäten; damit lassen sich die Kosten für Serverleistung flexibel dem Bedarf anpassen und müssen nicht als Fixkosten kalkuliert werden. Da außerdem die Leistung von professionellen, redundanten Rechenzentren im großen Maßstab erbracht werden, die entsprechend überwacht und gepflegt werden, sollte auch das Qualitätsniveau (Verfügbarkeit) bei dieser Form von Outsourcing wesentlich besser sein als bei einer am geringeren eigenen Bedarf orientierten Eigenlösung.

Die Analogie zur globalen Warenwirtschaft eignet sich – trotz der beschriebenen grundlegenden Unterschiede – gut, um die rechtlichen Probleme einer globalen Weltdatenwirtschaft (zu deren Ausprägungen auch das Cloud Computing gehört) zunächst einmal abstrakt zu beschreiben. An den Ländergrenzen enden die Einflussmöglichkeiten des jeweiligen Staates (und des einzelstaatlichen Rechts), der aber in den verschiedensten Situationen ein Interesse daran hat, den grundsätzlich erwünschten Außenhandel zumindest zu regulieren und manchmal auch (erheblich) einzudämmen. Dies geschieht zunächst oft zum Schutz der Wirtschaftsordnung und ihrer einzelnen Teilnehmer, so zum Beispiel, wenn die Ein- oder Ausfuhr von Markenartikeln an die Zustimmung des Markeninhabers gekoppelt wird und widerrechtlich eingeführte Artikel vom Zoll aufgegriffen und vernichtet werden. Weiter soll bisweilen im Interesse der öffentlichen Ordnung verhindert werden, dass als „gefährlich" eingestufte Waren außer Landes gelangen, etwa beim Export militärischen Materials an bestimmte Staaten. Es wäre auch undenkbar, Staatsarchive oder laufende Akten der öffentlichen Verwaltung ins Ausland zu verbringen, weil dann der originäre hoheitliche Zugriff auf diese Akten aus Gründen, die vom Inland aus nicht (mehr) gesteuert werden können, nicht mehr möglich wäre. Neben die generelle „Exportkontrolle" treten weiter Zollvorschriften und spezifische Besteuerungstatbestände bei grenzüberschreitenden Lieferungen oder Funktionsverlagerungen (z. B. bei der Wegzugsbesteuerung).

Das Problem liegt nun darin, dass physische Waren – eingeschlossen die immer seltener werdenden physisch versendeten Datenträger – an einer begrenzten Zahl von „Transitübergängen" (Flughäfen, Häfen, Grenzübergängen) zumindest stichprobenartig geprüft werden und in hohem Umfang „Begleitdokumente" erstellt werden (Exportpapiere,

internationale Frachtbriefe, Umsatzsteuervoranmeldungen bezüglich Einfuhrumsatzsteuer etc.), mit denen Zulässigkeit, Inhalt und Folgen der Lieferung belegt, geprüft und später nachgewiesen werden können. Der physische Transport ist vergleichbar gemächlich und gut zu kontrollieren, die Kontrolldichte vergleichsweise hoch und die Nachverfolgbarkeit gut. Vergleichbare Mechanismen – z. B. als „angeheftete" Metadaten für die „Ein- und Ausreise" von Daten – sind im Bereich der Datenwirtschaft undenkbar; hier werden derzeit Software und Inhalte (z. B. als Downloads), E-Mails, Datensätze aus ERP-Systemen und alles, was in digitaler Form vorliegt, ohne die Möglichkeit einer (behördlichen) Kontrolle oder Nachverfolgbarkeit über die Landesgrenzen hinaus verschickt. Die Diskussion um die Vorratsdatenspeicherung wirkt demgegenüber fast harmlos; immerhin geht es dort „nur" um die Verbindungsdaten, nicht um die übertragenen Dateninhalte – man kann sich also ausmalen, was passieren würde, wenn z. B. die Zollbehörden den Ländergrenzen überschreitenden Datenwarenverkehr inhaltlich kontrollieren sollten.

Es gibt nun hier auch bisher schon Überschneidungen zwischen grenzüberschreitender Waren- und Datenwirtschaft, etwa im Bereich der Umsatzsteuer, des gewerblichen Rechtsschutzes oder der Exportkontrolle von waffentauglicher Software. Für die rechtliche Einordnung spielt es in den meisten Rechtsgebieten (einmal abgesehen vom Umsatzsteuerrecht) im Grundsatz keine Rolle, ob Informationen auf einem physischen Datenträger physisch verschickt oder durch eine „transnationale" Datenleitung unverkörpert übertragen werden. Insofern erweist sich die Rechtsordnung bisweilen als erstaunlich „weitsichtig", was daran liegt, dass „alte" Formulierungen „neu" interpretiert werden können und so ihren Sinnbezug vergrößern. Manche Regelungsfragen aber, die bislang schlicht keine Bedeutung hatten, stellen sich erst dann, wenn bestimmte tatsächliche Möglichkeiten neu entstehen. So gab es historisch nie ein „Aktenexportrecht" als eigenständiges Rechtsgebiet, weil es ökonomisch keinen Sinn machte, Dokumente in größerem Umfang physisch ins Ausland zu verlagern. Seit jedoch das Interesse an der Verbringung elektronischer Dokumente zur Verarbeitung und Speicherung im Ausland ökonomisch sinnvoll geworden ist – die Möglichkeiten sind schier unbegrenzt –, bildet sich ein bislang nicht so genanntes, spezifisches Gebiet des „Datenexportrechts" aus. Und diese Rechtsmaterie entwickelt sich möglicherweise zunehmend zum Stolperstein für die globale Weltdatenwirtschaft – zumindest aus deutscher und europäischer Sicht. Inhalt der so bezeichneten Vorschriften, die aus den verschiedensten Bereichen der Rechtsordnung stammen, ist jeweils, dass bestimmte Daten nicht über die Grenzen der BRD oder der EU hinaus transportiert („verbracht") bzw. dort gespeichert („gelagert") werden dürfen. Hintergrund ist immer die Gefahr, die Kontrolle über diese Daten zu verlieren, sei es, weil ein Dritter Einblick in die Daten nehmen könnte, ohne dass dies in einer fremden Rechtsordnung effektiv verhindert werden kann, oder sei es, weil die Daten im Inland nicht mehr verfügbar sind, sodass Berechtigte keinen Einblick mehr nehmen können, obwohl sie dies sollen oder dürften. Die systematische Aufarbeitung der sich hier stellenden Probleme wird freilich auch dadurch erschwert, dass der Gesetzgeber nach Art eines „Flickenteppichs" sehr anwendungsspezifische Rechtsnormen erlassen hat, während die hierfür zumeist vorausgesetzten begrifflichen Konzepte der „Datenherrschaft" oder des „Dateneigentums" mit all ihren Voraussetzungen und Konsequenzen völlig diffus bleiben. So hat der Gesetzgeber, nur um ein Beispiel zu nennen, analog der Beschädigung fremder Sachen eine Beschädigung fremder Daten unter Strafe gestellt, ohne auch nur im Ansatz Lösungskonzepte vorzusehen, wie man „fremde" von „eigenen" Daten unterscheiden kann – eine Unterscheidung, die im Bereich des Rechts der physischen Sachen allein Bände von Gesetzen, Rechtsprechung und Literatur füllt.

II. Die Gefahren des Cloud Computing aus rechtlicher Sicht

Cloud Computing in seiner begrifflich weitesten Ausprägung kann aus rechtlicher Sicht abstrakt recht einfach beschrieben werden: Nachdem ein „Dateninhaber" seine Daten jederzeit „irgendwo" mittels der globalen Dateninfrastruktur Internet bei einem sogenannten Cloud-Provider eingespeist hat, liegt jegliche Kapazität der Verarbeitung und Speicherung dieser Daten (und damit diese Daten selbst) zunächst beim Cloud-Provider, später aber möglicherweise geografisch und rechtlich in unbekannten Händen (also „irgendwo"); zu beliebigen Zeitpunkten können die gespeicherten oder verarbeiteten Daten von „irgendwo" aus mittels Internetzugang wieder durch den „Dateninhaber" oder einen Dritten (im Idealfall natürlich nur mit Zustimmung des „Dateninhabers") abgerufen werden. Bezahlt werden derartige Dienste gewöhnlich verbrauchsabhängig wie Strom oder Telefon, also anhand der Intensität der Inanspruchnahme. Es kann nun aus Sicht des ursprünglichen Dateninhabers durchaus unkontrollierbar und unbekannt sein, welcher Rechenzentrumsbetreiber die Daten wo auf der Welt und nach Maßgabe welcher vertraglichen Regelungen mit einem über beliebig viele Zwischenstufen nachgeschalteten „Vorlieferanten" oder „Auftraggeber" speichert und bearbeitet. Es ist daher auch unbekannt, welchen Sicherheitsstandards das jeweilige Rechenzentrum unterliegt, wer (deshalb) sonst noch alles auf die Daten zugreifen kann, ob die Daten nicht durch äußere – auch hoheitliche – Eingriffe vernichtet oder gesperrt werden könnten und welche vertraglichen Regelungen innerhalb der „Datenlieferkette" bestehen bzw. im Streitfalle überhaupt effektiv durchgesetzt werden können. Aus ökonomischen Gründen kann es z. B. sinnvoll sein – wovon der ursprüngliche Dateninhaber im Zweifelsfall gar nichts erfährt –, die Daten über den Tag verteilt immer dorthin in Rechenzentren auf der Welt zu verlegen, wo gerade Nacht ist, weil dort üblicherweise der Strom für den Betrieb (Datenverarbeitung) günstiger ist als untertags. Synergieeffekte durch ressourcenschonende Verteilung der Daten – und damit deren Dezentralität sowie die gemeinsame Speicherung und Verarbeitung mit den Daten anderer „Dateninhaber" auf denselben, virtuell aufgeteilten physischen Ressourcen – ist die entscheidende Neuerung des Cloud Computings. Was genau nun mit den Daten in der Cloud gemacht wird, d. h. welche Funktionen (z. B. Rechenkapazität in einer definierten Software-Umgebung, Archivierung, Bereitstellung von Software-Funktionen, Zurverfügungstellung der innerhalb des Unternehmens verwendeten Kommunikationsplattformen, Rechnungsstellung und -versendung bis hin zur Erbringung ganzer Teil-Geschäftsprozesse) vom Cloud-Provider zur Verfügung gestellt werden muss, hängt vom jeweiligen inhaltlichen Bedarf des ausgliedernden Unternehmens ab und kann sehr unterschiedlich sein.

Diese extreme Ausprägung ist gleichzeitig auch das Schreckensszenario beispielsweise der Datenschützer und der Finanzbehörden, denn traditionell rechtlich „sensible" Daten im wirtschaftlichen Bereich sind vor allem personenbezogene und steuerlich relevante (Buchhal-

tungs-)Daten. Ihre Verbringung über bestimmte Grenzen hinaus – das können übrigens auch schon Unternehmens- statt Ländergrenzen sein – wird daher zunehmend zumindest an die Einhaltung bestimmter Vorgaben gekoppelt. So bedarf es etwa bei der Aufbewahrung elektronischer Bücher und entsprechender elektronischer Aufzeichnungen im Ausland einer Bewilligung der Finanzverwaltung, die an bestimmte Voraussetzungen geknüpft ist. Ein etwaiger Verstoß kann mit einem Verzögerungsgeld bis zu 250 000 Euro sanktioniert werden (§ 146 Abs. 2b AO). Der Satz des deutschen Grundgesetzes, dass „Eigentum verpflichtet" (Sozialbindung), gilt auch und gerade für den „Dateneigentümer", von dem übrigens gar nicht klar ist, ob es ihn rechtlich überhaupt gibt. Der „Dateneigentümer" darf aufgrund verschiedener Beweggründe mit den Daten eben nicht nach Belieben verfahren, sondern muss Sorgfaltsmaßstäbe und Grenzen im Umgang mit den Daten einhalten, die je nach dem Inhalt der Daten unterschiedlich weit gezogen sind. In erster Linie geht es hier darum, einen (befürchteten) Kontrollverlust des rechtlich primär Verantwortlichen zu vermeiden, und zwar sowohl im Wege des unkontrollierbaren Zugriffs durch Dritte als auch dadurch, dass die Daten außer „Reichweite" gelangen. Und der rechtlich in Deutschland Verantwortliche soll sich dieser (Sozial-)Verantwortung nicht durch Verlagerung von Daten ins Ausland entziehen können; ob nämlich später tatsächlich Daten (unabsichtlich) „verschwunden" sind oder nur (absichtlich) vorenthalten werden, lässt sich aus deutscher (Behörden-)Sicht kaum beantworten.

Es gibt nun vier Möglichkeiten, diese Risiken einzudämmen. Zum Ersten kann die Verbringung außerhalb einer bestimmten „zulässigen Zone" schlechthin verboten und versucht werden, die Einhaltung dieses Verbotes möglichst umfassend zu kontrollieren und zu sanktionieren („Exportverbot"). Das Problem dieser Lösung ist freilich, dass so – neben den faktisch höchst eingeschränkten Kontrollmöglichkeiten – jegliche ökonomischen Vorteile einer Datenverlagerung außerhalb der „zulässigen Zone" komplett zunichte gemacht werden; ein Standortnachteil droht. Zum Zweiten kann die Verbringung an die Einhaltung bestimmter zusätzlicher rechtlicher Vorgaben gekoppelt werden, beispielsweise, indem durch vertragliche oder zwischenstaatliche Abreden versucht wird, ein annähernd gleiches Niveau des Schutzes vor einem Kontrollverlusts zu erreichen („Exportbeschränkungen"). Damit können kostensenkende Synergieeffekte genutzt werden, gleichzeitig aber noch eine gewisse, wenn auch nur rechtlich vermittelte und daher vergleichsweise schwächere Kontrolle über die Daten aufrechterhalten werden. Zum Dritten kann versucht werden – dies ist eine rein technische Lösung –, die Daten durch Verschlüsselung in eine Form zu bringen, welche die Daten für einen Dritten nicht oder nur mit unverhältnismäßig großem Zeitaufwand zugänglich macht. Diese Option könnte für die externe Speicherung, weniger aber für die anderweitige externe Verarbeitung interessant sein, verliert aber durch die sich stetig vergrößernden Rechen- und damit „Schlüsselüberwindungs"-Kapazitäten an Attraktivität. Man wird sich hier zumindest immer vor dem entschlüsselnden Eingriff (fremder) staatlicher Stellen fürchten müssen. Zum Vierten kann auf Vertrauen in die Kompetenz des Verantwortlichen zur verlässlichen Organisation der „Rückholbarkeit" der Daten gesetzt werden: Jemand, der sich in der Vergangenheit rechtskonform verhalten hat, insbesondere also Daten vorlegen konnte, wenn dies notwendig war, bekommt einen Vertrauensvorschuss und darf Daten so lange außer Landes schaffen, wie er weiterhin seinen Vorlagepflichten nachkommt (vgl. § 146 Abs. 2a AO).

Die spezifische Gefahr des Cloud Computing besteht vor diesem Hintergrund darin, dass die „sensiblen" (Unternehmens-)Daten bei Transport, Speicherung und Verarbeitung durch viele „unbekannte Hände" gehen. Man kann diese lokalen Rechenzentrumsbetreiber, Anlagenvermieter, Wartungs-Dienstleister und sonstigen Funktionsträger, die einzelne der als „Cloud Computing" umschriebenen Gesamtleistung erbringen, als „Subunternehmer des Cloud-Providers" bezeichnen. Eine „Kontrolle" zumindest darüber, auf welchem Sorgfaltsniveau mit den Daten tatsächlich umgegangen wird, kann dann verloren gehen, vergleichbar mit dem Kontrollverlust beim Datentransport im Internet: Auch hier weiß systembedingt niemand vorher, welchen Weg die Datenpakete nehmen und durch wessen Hände (Leitungs-, Knotenpunkt- und Serverbetreiber etc.) sie – mit den entsprechenden „Abhör"- und Modifikationsrisiken – geschleust werden. Auch bestehen keine direkten vertraglichen Vereinbarungen mit bzw. zwischen diesen verschiedenen Betreibern. Wenn nun auch noch sensible Unternehmensdaten – gleich, ob aus Unternehmersicht „mission critical" oder als personenbezogene Daten mit besonderer Sozialbindung ausgestaltet – in ein nicht mehr transparentes, internationales Konglomerat von Dienstleistern „geschoben" würden, so die Befürchtung, verliert das Unternehmen die Kontrolle und kann seinen Verpflichtungen bzw. seiner Verantwortung nicht mehr gerecht werden.

Bei dieser Betrachtung stellt sich Cloud Computing – Juristen versuchen ja immer zunächst, gleichartige Fallgestaltungen im Analogiewege heranzuziehen – als Steigerung und Internationalisierung der bereits als „Rechenzentrumsverträge" bzw. IT-Outsourcing bezeichneten Sachverhalte und Risikolagen dar. Hier wie dort gibt es zunächst einmal einen „Provider", also einen Dienstleister, der verspricht, abstrakt Rechen- und Speicherkapazität bereitzustellen. Während dies beim klassischen Modell aber ein geografisch bekanntes Rechenzentrum mit einem einzigen Betreiber (dem Outsourcing-„Provider" und Vertragspartner) betraf (und Verträge mit ausländischen Outsourcing-„Providern" waren früher eher selten anzutreffen), werden die Daten beim Cloud Computing – je nach Ausgestaltung – weltweit in Rechenzentren beliebiger „Unterprovider" in unvorhersehbarer Weise verteilt, zu denen nur noch höchst mittelbare Vertragsbeziehungen bestehen, sodass die Durchsetzung von Rechten des ursprünglichen Auftraggebers beliebig verwässert wird.

III. Die derzeitige rechtliche Situation und die Folgen für Cloud-Provider

Der Gesetzgeber hat in diesem Bereich, wenn man dies flapsig so sagen wollte, „alles und nichts" geregelt. Alles, weil es viele Vorschriften gibt, welche letztlich die Weitergabe von Daten an Dritte von Voraussetzungen abhängig machen oder verbieten, sodass hier in einigen Bereichen klare Vorgaben herrschen, an denen man nolens volens nach derzeitiger Rechtslage nicht vorbeikommt. Nichts, weil in Kernfragen eine geradezu verblüffende Rechtsunsicherheit herrscht, sodass man beinahe auf die böse Idee kommen könnte, der Gesetzgeber wolle die Kosten der Normierung auf die Wirtschaft verlagern, indem diese entgeltlich die Gerichte in Anspruch nehmen möge, um den bestehenden Lücken durch höchstrichterliche Rechtsfortbildung beizukommen. Zu diesen offenen Fragen gehört zum Beispiel nach wie vor die genaue Definition der „personenbezogenen Daten", etwa, ob und wann solche Daten bei ausreichender Verschlüsselung ihren Personenbezug verlieren und damit außerhalb des Einflussbereichs des

Schlüsselinhabers selbst nicht mehr dem Datenschutzrecht unterliegen. Dieses Thema wird juristisch unter dem Etikett des „relativen" oder „absoluten" Personenbezuges diskutiert.

Eine solche Gemengelage macht die Beurteilung des Cloud Computings schwierig, weil es sich – wie so oft – um Rechtsprobleme handelt, die bei der Gestaltung und Risikoeinschätzung eine entscheidende Rolle spielen, die aber (wenn nicht zufällig durch anderweitige „Präzedenzfälle") nur in der Rückschau „vom grünen Tisch" aus aufgelöst werden, nämlich nach einem jahrelangen Rechtsstreit, oder überhaupt nicht (z. B. bei einem Vergleich oder wenn es zu keinem Klageverfahren kommt). Die Anklage des gestaltenden Juristen, dass in Zeiten eines zunehmend und wohl unvermeidlich unpräziser werdenden Gesetzgebers in Deutschland viel zu wenig geklagt (bzw. richtiger: richterlich entschieden) wird, soll hier nicht angestimmt werden; es ist ein offenes Geheimnis, dass jeder gestaltende Anwalt zumindest bei jedem komplexeren Fall zwangsläufig an Rechtsfragen gerät, von denen seine weitere Empfehlung abhängt, die aber nie höchstrichterlich entschieden wurden und daher nicht abschließend bewertet werden können. Und da Jura keine Arithmetik ist – schon gar nicht im Datenschutzrecht als reinem „Abwägungsrecht" –, kann man die Ergebnisse auch nicht mit hoher Wahrscheinlichkeit „ausrechnen". Anhand dieser Ausgangslage und unter Berücksichtigung ihrer Interessenlage als (im positiven Sinne) „Datenschutzlobbyisten" erklärt sich daher auch ohne Weiteres, warum die Rechtsauffassungen der Datenschutzbeauftragten der Länder in diesem Bereich bislang sehr restriktiv sind. Auch jeder gestaltende Rechtsanwalt ist gegenüber seinem Mandanten verpflichtet, den sichersten Weg zu empfehlen, also so vorsichtig wie möglich zu agieren, und dies bedeutet im Umfeld des Cloud Computings zunächst einmal, die rechtlichen Bedenken so gravierend wie möglich zu formulieren. Dass damit (stark auf Internationalisierung oder technische Verschlüsselung setzende) Geschäftskonzepte behindert werden und deutsche Anbieter im internationalen Vergleich – insbesondere gegenüber den USA – zurückfallen, ist da nur ein Kollateralschaden, der als Preis der Verteidigung des hehren Persönlichkeits- und Öffentlichkeitsschutzes zumindest der Politik bislang akzeptabel erschien.

Eine weitere Facette, die bisher in der juristischen Diskussion kaum beachtet wurde, ist die generelle „Corporate Governance"-Frage: Darf ein Geschäftsleiter unternehmenskritische Daten „in die Cloud" verlagern, wenn er faktisch die Kontrolle über die Daten verliert und dies eventuell auch rechtlich nicht effektiv verhindern kann? Derartige Fragestellungen werden organhaftungsrechtlich – auch wenn das rechtlich eigentlich nicht so vorgesehen ist – häufig nach der Prämisse „Nachher ist man immer schlauer" behandelt: Wenn sich ein Risiko später verwirklicht, wird schlussgefolgert, dass dieses Risiko auch seinerzeit schon hätte gesehen werden können, und dann liegt es nahe, dass es seinerzeit schuldhaft unterschätzt wurde. Dabei geht es nicht einmal nur darum, sich an (häufig unklares) geltendes Recht zu halten („Compliance" im engeren Sinne), sondern auch darum, operative Risiken im Kernbereich des Geschäftsbetriebes (mission critical) – d. h. die Kern-EDV-Prozesse – beherrschbar und verantwortungsvoll zu gestalten (im Rahmen der sog. „business judgement rule"). Ohne funktionierendes EDV-System sind bekanntlich die heutigen Unternehmen allenfalls stillstehende Produktionsmaschinen und ratlose Arbeiter. Diese Thematik besteht ganz unabhängig von der Frage, ob aufgrund von Verbotsnormen bestimmte Daten nicht „exportiert" werden dürfen; es geht dann vielmehr darum, ob man als gewissenhafter Kaufmann und Geschäftsleiter wichtige Daten ins Ausland verlagern sollte.

Die Grenze des Cloud Computing – zumindest aus deutscher Sicht – liegt daher insgesamt neben der räumlichen Beschränkung in der vertraglichen Gestaltbarkeit. Von den Anbietern wird man nach derzeitiger Rechtslage (dazu im Einzelnen noch unten) erstens verlangen, geografisch eingeschränkte Clouds mit definierten physischen „Außengrenzen" anzubieten (Eingrenzung der „Exportländer"), und zweitens, Vertragskonzepte vorzulegen, die den Cloud-Providern erhebliche Verantwortlichkeiten auferlegen (Übernahme von Compliance-Verantwortlichkeiten). Dies wird ein vernünftiger Cloud-Provider jedoch kaum akzeptieren können, weil er unter Risikogesichtspunkten derartige Regelungen möglichst eins zu eins in die Sub-Provider-Verhältnisse spiegeln müsste, die Sub-Provider aber, zumeist mit Sitz im ferneren Ausland und, selbst wenn es sich um verbundene Gesellschaften des Cloud-Providers handelt, nicht gewillt sein werden, deutsche Verantwortlichkeitsstandards und den darauf eventuell noch aufbauenden Wunsch nach entsprechendem Versicherungsschutz zu akzeptieren. Noch komplizierter wird es dann, wenn man einen möglichst langfristigen Vertrag abschließen will und sich in unserer schnelllebigen Zeit aus wirtschaftlichen Gründen später der internationale „Stand der Technik" (weiter) entgegen dem deutschen Sicherheits- und Kontrollbewusstsein entwickelt. Dann sind dem Cloud-Provider und den Sub-Providern die Hände gebunden: Synergie- und Rationalisierungspotenziale werden sich nur eingeschränkt realisieren lassen, weil man sich an alte, sehr restriktive Verträge zu halten hat. Diese Probleme münden selbstverständlich für die deutschen bzw. europäischen Auftraggeber in ein Preisdilemma: Ein hiesigen Rechtsmaßstäben genügender Cloud-Zugang wird vermutlich wesentlich teurer sein als der Zugang zu einer international marktüblichen Cloud. Und die „deutsche Cloud" (bzw. „europäische Cloud") selbst wird letztlich anders beschaffen sein als eine internationale, solange der deutsche (oder europäische) Gesetzgeber die Sozialbindung des Dateneigentümers immer stärker ausformuliert.

Man kann also zunächst einmal resümieren: Cloud Computing ist vom rechtlichen Standpunkt aus IT-Outsourcing, nur (wegen der Synergieeffekte) günstiger, (geografisch) weiträumiger und mit einer größeren faktischen Unsicherheit verbunden. Dabei umfasst „Sicherheit" in diesem Zusammenhang mindestens zwei unterschiedliche Facetten: Es geht um tatsächliche Sicherheit, zum Beispiel in Bezug auf Viren, Verlust und sonstigen Eingriffen in die Daten auf dem Transport oder innerhalb virtualisierter Server-Umgebungen – diese Sicherheit ist oft als Wettlauf zwischen Schadsoftware und Entschlüsselungskapazität einerseits sowie Schadsoftware-Abwehr und Verschlüsselungstiefe andererseits zu sehen –, es geht aber auch um rechtliche Sicherheit, insbesondere in Bezug auf die Vertragsgestaltung in mehrstufigen, internationalen Vertragsverhältnissen. Letzteres zeigt sich zum Beispiel bei der effektiven Durchsetzung rechtlicher Ansprüche „an Ort und Stelle", etwa wenn der Cloud-Provider oder sein Sub-Provider die Herausgabe der Daten an den ursprünglich Verantwortlichen verweigern. Man stelle sich den deutschen Mittelständler vor, der verzweifelt versucht, vor indonesischen Gerichten die Herausgabe von unternehmenskritischen Daten eines dortigen Sub-Providers und Rechenzentrumsbetreibers zu erklagen, nachdem sein „eigentlicher" Auftragnehmer, ein US-amerikanischer Cloud-Provider, in Insolvenz gefallen ist, wenn der Sub-Provider-Vertrag selbst aus lediglich zwei E-Mails besteht und der Sub-Provider behauptet, er habe die Daten

damals an ein Rechenzentrum in Brasilien weitergeleitet und auch keine Back-ups mehr zurückgehalten.

IV. Einzelprobleme

Im Folgenden sollen überschlägig die hauptsächlichen Problemfelder des Datenexports außerhalb der Sphäre des ursprünglichen „Dateneigentümers", insbesondere aber außerhalb der EU oder – in der Cloud – an einen nur mittelbar bekannten oder sogar gänzlich unbekannten Speicherungs- bzw. Verarbeitungsort dargestellt werden. Dabei wird auf „klassische" Exportbeschränkungen bei speziellen Datentypen – z. B. kriegswaffenfähige Software – sowie auf besondere Vorgaben, die der Cloud-Provider möglicherweise zu beachten hat – z. B. telekommunikationsrechtliche Vorschriften –, nicht gesondert eingegangen.

1. Gesetzliche und vertragliche Rechtspositionen an den Daten

Daten können schon aufgrund ihres Inhalts oder aufgrund einer rechtlichen Verknüpfung Beziehungen zu Dritten aufweisen; damit haben Dritte (das kann auch der Staat sein) irgendeine Form von „Rechtsposition" an diesen Daten. Das „Dateneigentum" wird also auf Basis der Sozialverbindlichkeit zugunsten dieser Dritten eingeschränkt. Damit ergeben sich Interessenkonflikte zwischen dem „Dateneigentümer" einerseits und dem berechtigten Dritten andererseits.

Folgende Beispiele mögen dies verdeutlichen: Beziehen sich Daten inhaltlich auf Personen, so liegen personenbezogene Daten im Sinne des Datenschutzrechts vor, sodass sich Rechte der „Betroffenen" ergeben, wie mit diesen Daten umzugehen ist (Verarbeitung, Weitergabe, Löschen etc.). Sind Daten Teil eines nicht abgeschlossenen Telekommunikationsvorgangs im Sinne des Telekommunikationsgesetzes, so unterliegen sie dem Telekommunikationsgeheimnis, sodass sich Rechte der „Telekommunikationsteilnehmer" ergeben, wie mit diesen Daten umzugehen ist (Verbot der Kenntnisbeschaffung). Stellen Daten inhaltlich urheberrechtlich geschützte Werke dar, so unterliegen sie dem Urheberrecht, sodass sich Rechte der „Urheber" oder „Lizenzgeber" ergeben, wie mit diesen Daten umzugehen ist (Vervielfältigung, Verbreitung, Bearbeitung, Öffentliche Zugänglichmachung etc.). Sind Daten (als Produkte, z. B. veräußerte Software oder Nutzdaten) mit Marken kenntlich gemacht, so unterliegen die Kennzeichnungen dem Markenrecht, sodass sich Rechte der „Markeninhaber" ergeben, wie mit diesen Daten umzugehen ist (Ein- und Ausfuhr etc.). Unterliegen Daten vertraglichen Verpflichtungen, etwa der Pflicht zur Geheimhaltung (Geheimhaltungsvereinbarungen) oder der Pflicht zur Benutzung nur in bestimmten (Zweck-)Grenzen, so gibt es schuldrechtliche Ansprüche gegen den „Dateneigentümer" dahin gehend, dass dieser die vertraglichen Grenzen einhält. Unterstehen Daten einem besonderen Geheimnisschutz, z. B. mandatsbezogene Daten eines Rechtsanwalts, so gibt es berufsrechtliche Vorgaben.

Da eine Verbringung dieser „gebundenen" Daten außerhalb definierter Sphären (Sphäre des „Dateneigentümers", BRD, EU – „grüne Zone") die Rechtspositionen der Berechtigten gefährden könnte (insbesondere könnte z. B. eine ausländische Rechtsordnung diese „Gebundenheit" gar nicht vorsehen oder die Durchsetzbarkeit dieser Rechtspositionen eingeschränkt sein), sehen verschiedene Schutzrechte „Exportbeschränkungen" vor. Und auch bei Geheimhaltungsvereinbarungen könnte es sich anbieten – eventuell im Sinne ergänzender Vertragsauslegung sogar herauszulesen sein –, dass der „Informationsgeber" dem „Informationsnehmer" vorschreibt, die Daten nicht außerhalb eines Landes zu verbringen, damit die Durchsetzungsrisiken, denen ein vertraglicher Löschungsanspruch später ausgesetzt ist, nicht überhandnehmen. Die Beschränkungen können verschiedener Natur sein; grundsätzlich zulässig aber ist die Verbringung außerhalb der „grünen Zone", wenn (sämtliche) an den Daten Berechtigten dieser Verbringung dediziert zustimmen. Ohne solche Zustimmung im Einzelfall kann eine Exportbeschränkung entfallen, wenn bestimmte Vorgaben der jeweiligen Schutzrechtsmaterie erfüllt werden, beispielsweise der Empfänger der Daten (außerhalb der „grünen Zone") sich bestimmten Verpflichtungen unterwirft. Im Bereich des Telekommunikationsgesetzes beispielsweise ist hingegen noch völlig ungeklärt, ob beispielsweise ein deutsches Unternehmen, das seinen Angestellten die Unternehmens-EDV für private E-Mails zur Verfügung stellt und damit Anbieter von Telekommunikationsdienstleistungen für die Angestellten sein könnte, sämtliche E-Mails zentral auf einem Server in Frankreich oder Indien verwalten darf, weil damit ein „Umweg" der Daten (insbesondere wenn sie aus Deutschland versendet werden) und damit eine an sich unzulässige Zeitverzögerung des geschützten Telekommunikationsvorganges verbunden ist. Hier fehlt bislang eine Ausdifferenzierung des zugehörigen „Exportrechts".

Jede Einführung von Cloud Computing muss sich daher matrixartig mit der Frage beschäftigen, welche rechtliche Qualität die in der Cloud zu verarbeitenden Daten aufweisen, welche Rechtspositionen sich hieraus für dritte Berechtigte ergeben und wie sichergestellt wird, dass diese Rechtspositionen gewahrt bleiben bzw. durchsetzbar sind. Im Idealfall sind die Daten „unbemakelt", es „kleben" also keine Drittrechte an ihnen, und der „Dateneigentümer" kann tatsächlich völlig nach eigenem Belieben verfahren. Im „worst case" sind die Daten vielfach „bemakelt" und die an den Daten „klebenden" Drittrechte verlangen einen erheblichen Aufwand im Sinne einer Strukturierung der Organisation und der Prozesse beim „Dateneigentümer", einer Einhaltung von Exportbeschränkungen oder der Implementierung und Aufrechterhaltung von Schutzmaßnahmen (dazu unten).

2. Vorhaltepflichten

Daten können inhaltlich später einmal möglicher Gegenstand der Prüfmaterie staatlicher Stellen (oder – bei vereinbarten Audit-Rechten – auch von Vertragspartnern) sein; denn die öffentliche Hand hat ein Interesse daran, dass die Daten für sie zugänglich sind, also im Einflussbereich der Behörden oder der Gerichte (vgl. § 258 Abs. 1 HGB) vorgehalten werden. Auch hier findet sich also ein Interesse an „Exportbeschränkungen". Diese Regelungen korrespondieren mit Verpflichtungen, bestimmte Daten für einen bestimmten Zeitraum aufzubewahren und den prüfenden Stellen Zugriff auf diese Daten einzuräumen.

So sind nach § 146 Abs. 2 AO Handelsbücher und Aufzeichnungen des Kaufmanns in der BRD zu „führen" und „aufzubewahren". Unter bestimmten qualifizierenden Voraussetzungen kann die Finanzbehörde jedoch bewilligen, dass dies in einem EU- oder EWR-Staat stattfindet (§ 146 Abs. 2a AO). Für die darüber hinausgehenden handelsrechtlichen Unterlagen (§ 257 HGB) ist bislang kein besonderer Aufbewahrungsort geregelt; nach der entsprechenden Regelung zum Datenzugriff der Finanzverwaltung („Einsicht in die gespeicherten Daten nehmen", § 147 Abs. 6 AO) ist bezüglich all dieser weiteren Unterlagen lediglich sicherzustellen, dass die Daten „während der Dauer der Aufbewahrungsfrist jederzeit verfügbar sind, unverzüglich

lesbar gemacht und maschinell ausgewertet werden können" (§ 147 Abs. 2 AO).

Im Rahmen einer Einführung von Cloud Computing muss daher vorab geprüft werden, ob sich hieraus die Notwendigkeit zur räumlichen Begrenzung der Cloud auf die BRD, zur Einholung einer Bewilligung der Finanzverwaltung oder zur Separierung von „exportbeschränkten" Daten und Aufbewahrung (ggf. Spiegelung) dieser Daten in der BRD ergibt.

3. Jahresabschlussprüfung

Im Rahmen der Jahresabschlussprüfung hat der Prüfer auch die Buchführung einzubeziehen (§ 317 Abs. 1 HGB). Die Organe der Gesellschaften unterliegen umfangreichen Auskunfts- und Vorlageverpflichtungen (§ 320 HGB). Sowohl kann daher im Rahmen der Jahresabschlussprüfung die Prüfung der Ordnungsgemäßheit der Auslagerung von EDV-Funktionen und der dabei angewendeten Prozesse eine große Rolle spielen als auch können, im Falle des Outsourcings, diese Prüfungen den ausgelagerten Funktionen „folgen". Mit der Auslagerung wesentlicher rechnungslegungsrelevanter Funktionen (dazu gehören z. B. die Verarbeitung von Daten über Geschäftsvorfälle in einem Rechenzentrum, die zentrale Abwicklung des Rechnungswesens über ein Shared Service Center oder die Erledigung standardisierter Geschäftsprozesse) rückt das interne Kontrollsystem des Outsourcing-Anbieters in den Fokus des Interesses und mithin die Frage, ob durch die eingerichteten Kontrollen Risiken entstehen können, die wiederum beim auslagernden Unternehmen zu Mängeln in der Rechnungslegung führen können. Jahresabschlussprüfer sind gehalten, das gesamte – also auch das auf den Dienstleister (Cloud-Provider) ausgelagerte – interne Kontrollsystem einer Beurteilung zu unterziehen, um einen Nachweis für dessen Angemessenheit und Wirksamkeit zu erlangen. Damit sich die Jahresabschlussprüfer beim Dienstleister nicht die „Klinke in die Hand geben", unterziehen sich diese vielfach „freiwillig" einer Prüfung ihres dienstleistungsbezogenen internen Kontrollsystems, um aktiv den Nachweis über die Ordnungsmäßigkeit liefern zu können. Insbesondere für Dienstleister, die vom Ausland aus agieren, kann die Latte der deutschen Ordnungsmäßigkeits- und Sicherheitsanforderungen recht hoch liegen, weswegen es schon aus Sicht der Geschäftsführung eines auslagernden Unternehmens unabdingbar erscheint, einen solchen Nachweis zu fordern, allein um seiner eigenen Verantwortung nachgekommen zu sein.

4. Schutzmaßnahmen

Unabhängig von der geografischen Belegenheit von Daten – die in der Cloud minütlich wechseln kann – werden an den „Dateneigentümer" in verschiedenen Vorschriften Anforderungen daran gestellt, welche Maßnahmen er (im Interesse der Inhaber anderer Rechtspositionen an den Daten) ergreifen muss, wenn er mit bestimmten Daten umgehen möchte. Bereits 1995 hat die EU dies in der EU-Datenschutzrichtlinie so formuliert, dass „*der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muss, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang – insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden – und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind*". Im Wandel der Zeit ergeben sich ständig neue „Bedrohungen für Daten", die sämtlich unter diese generische Beschreibung fallen, und da allein auf die „erforderlichen" Maßnahmen abgestellt wird, gibt es hier auch zunächst einmal keine Kosten- oder Aufwandsgrenzen. Auch aus Sicht einer verantwortungsvollen Unternehmensführung wird man daher in ähnlicher Weise verlangen können, dass mindestens „mission critical"-Daten durch Maßnahmen geschützt werden, die dem Stand der Technik entsprechen. Insbesondere wird hier die Verschlüsselung der Datenübertragung vom „Dateneigentümer" zum Cloud-Provider vorausgesetzt, zum Teil aber auch Verschlüsselungsmaßnahmen beim Cloud-Provider selbst gefordert, die natürlich (bislang) dann kaum möglich sind, wenn innerhalb der Cloud inhaltliche Operationen mit den Daten vorgenommen werden sollen („Verarbeitung"). Daneben stehen Abschottungsmaßnahmen durch Virtualisierung, Virenschutz, Filtertechniken und dergleichen. Die erforderlichen Schutzmaßnahmen sind unabhängig davon zu betrachten, ob bei ausreichender Verschlüsselung und fehlender Herrschaft des Cloud-Providers über den Schlüssel z. B. die rechtliche Qualifikation von Daten als personenbezogen entfällt.

Das Besondere ist nun, dass diese rechtliche Verantwortung für die Datenintegrität und Datenauthentizität, gleich aus welcher juristischen Verpflichtung des „Dateneigentümers" sie im Einzelnen herrühren mag, bei jeder Form des Outsourcings der Daten – also auch in die Cloud hinein – weitergegeben werden muss. Auch wenn es hierfür verschiedenste Produkte in Form von Software geben mag, sind diese immer nur so gut wie die Organisation bzw. die ausführenden Personen, die sie installieren, überwachen und warten. Das Level an eigener Verantwortung im Umgang mit „eigenen" Daten ist daher eins zu eins an sämtliche Dienstleister (Cloud-Provider) weiterzugeben, was zunächst im Wege entsprechender Vertragsregelungen – möglicherweise unter Bezugnahme auf internationale Standards oder Zertifizierungen, die dem Cloud-Provider verliehen wurden –, darüber hinaus aber auch im Wege der nachfolgenden Überwachung der Einhaltung eben dieser Regelungen geschieht. Es muss also neben der Gestaltung auch ein Controlling von Vertragsbeziehungen geben, wenn die Verantwortlichkeit für Schutzmaßnahmen auf einen Dritten übertragen werden sollen. Überträgt der Dritte seinerseits die Verantwortung an einen Sub-Dienstleister, muss er mit diesem gleichartige Vertragsbeziehungen abschließen und überwachen. Die Konditionen des Erstvertrages müssen also weitergereicht werden – in einer internationalen Cloud mit verschiedenen „Vor-Ort-Providern" ein nahezu unmögliches Unterfangen mit zusätzlichen Barrieren in Sachen Vertragssprache und anwendbares Recht.

Bei der Vertragsgestaltung mit dem Cloud-Provider ist daher darauf zu achten, dass die sich aus den vorstehenden Anforderungen ergebenden notwendigen Regelungsinhalte vereinbart werden (vgl. für den Bereich des Datenschutzes § 11 BDSG). Dabei sind ggf. Folgerisiken bei suboptimalen Vertragsgestaltungen mit wirtschaftlichen und Effizienzvorteilen abzuwägen.

5. Durchsetzbarkeit

Häufig wird in der Praxis vergessen, dass Recht haben und Recht bekommen zweierlei sind. Der beste Vertrag auf dem Papier bei der Weitergabe von Verantwortung nützt nichts, wenn er später nicht effektiv durchgesetzt werden kann. Damit ist nicht einmal die klassische mehrjährige Dauer eines Rechtsstreits vor den deutschen Zivilgerichten gemeint, sondern vielmehr die Durchsetzung in einer „Dienstleisterkette". Da eigene vertragliche Ansprüche nur gegenüber dem eige-

nen Dienstleister bestehen und dieser seinerseits Ansprüche gegen den Sub-Dienstleister hat, gerät ein Streit „entlang der Kette“ zur Geduldsprobe. Die Rechtsfindung wird dabei immer der faktischen Entwicklung hinterherhinken: So schnell, wie sich Daten vernichten, verlagern oder zweckentfremdet verwenden lassen, ist kein Gericht der Welt.

Die Frage ist, welche Ansprüche überhaupt von entscheidender Relevanz sind. Hier gibt es zwei wichtige Themenfelder: Den Anspruch auf Herausgabe der Daten des „Dateneigentümers“ – schließlich befinden sich die Daten irgendwo in der Cloud in der Hardware-Besitzsphäre eines Dritten – und den Anspruch auf Einhaltung der vereinbarten Schutzmaßnahmen einschließlich der Geheimhaltung der Dateninhalte durch den Cloud-Provider (der ja theoretisch die Daten zur Kenntnis nehmen könnte, wenn diese nicht lediglich verschlüsselt abgespeichert werden, was zumindest bei einer „Verarbeitung“ von Daten innerhalb der Cloud wohl kaum durchzuhalten ist).

Mehr noch: Um die Ernsthaftigkeit zu demonstrieren, mit welcher der „Dateneigentümer“ auf „seine“ Daten in der Cloud achtet, wird der „Dateneigentümer“ gezwungen sein, bei entsprechenden Vertragsverstößen des Cloud-Providers diesen auch tatsächlich zur Haftung heranzuziehen und/oder zu einem anderen Cloud-Provider zu wechseln. Mit einem „Zurücklehnen“ mit Hinweis auf einen weitreichenden Vertragsschutz, der aber nicht effektiv eingefordert wird, wird der „Dateneigentümer“ seiner – wie immer inhaltlich ausgestalteten – Verantwortung nicht gerecht.

Bei der Gestaltung von Verträgen mit Cloud-Providern sollte daher daran gedacht werden, möglichst effektiv durchsetzbare Regelungen zu schaffen. Dies betrifft insbesondere das anwendbare Recht, den Gerichtsstand und möglicherweise eine schnelle Entscheidungsmöglichkeit durch ein Schiedsgericht. Auch sollte darüber nachgedacht werden, Ansprüche des Cloud-Providers gegen nachgelagerte (Sub-) Sub-Dienstleister an den ursprünglichen Auftraggeber abzutreten, auch und gerade in mehrstufigen Verhältnissen. Können Rechte auf Herausgabe etc. nicht mehr geltend gemacht werden, weil die Daten nicht mehr vorhanden sind, so sollten neben Schadensersatzansprüchen Vertragsstrafen in angemessen abschreckender Höhe treten. Hinzu kommen Sicherungsinstrumente wie Banksicherheiten und die Forderung nach Versicherungsschutz.

V. Fazit

Cloud Computing ist aus rechtlicher Sicht nichts kategorisch Neues, sondern stellt eine Weiterentwicklung bereits bekannter Phänomene dar. In einigen Bereichen werden aber erst durch die Mehrstufigkeit der Vertragsverhältnisse und die Ortslosigkeit der Daten, d. h. die enorme Geschwindigkeit des – z. T. unvorhersehbaren und unkontrollierbaren – internationalen Ortswechsels, Probleme sichtbar, die sich in dieser Intensität so vorher noch nicht gestellt haben. Nach derzeitiger Gesetzeslage gibt es viele Stolpersteine, die dazu führen können, eine Cloud z. B. auf die BRD zu beschränken – was den mit der (internationalen) Cloud angestrebten Synergieeffekten zuwiderläuft. Die Cloud-Provider werden sich für ihre deutschen Kunden mit denselben Fragestellungen zu beschäftigen haben wie die Anwender selbst. Hierzu zählt die Frage, welcher faktische und rechtliche Sicherheitsstandard geboten werden kann, sodass ein verantwortungsvoller Geschäftsleiter überhaupt unternehmenskritische Daten in die Cloud geben kann. Aber selbst eine in diesen Beziehungen hochsichere Cloud kann auf der anderen Seite nicht die Regelungen des deutschen Gesetzgebers im Bereich des „Datenexportrechts“ ignorieren. Es muss also ein austariertes Konzept, je nach der juristischen Klassifikation der Daten, geben, welche Grenzen welche Daten überschreiten dürfen und welche nicht. Dies könnte z. B. in einem – enorm aufwendigen – Konzept enden, sämtliche (Unternehmens-)Daten jeweils mit einem Metadatensatz über die „zulässige Verbringungszone“ zu versehen; die Schwierigkeit besteht hier freilich darin, wer wann diese Klassifikation vornimmt, prüft und ggf. korrigiert. Der hier auf die auslagernden Unternehmen zukommende Prüfungsaufwand ist immens, von der Erhebung der notwendigen Informationen hin zur rechtlichen Bewertung, über die Aufstellung entsprechender Leitlinien und die Abstimmung z. B. mit den Arbeitnehmervertretungen bis hin zum Auffinden eines Cloud-Providers, der dies dann auch so umsetzen kann. Die Kostenersparnis der Cloud ist also mit erheblichen Anfangsinvestitionen verbunden, was nicht zuletzt auch daran liegt, dass – nach Maßstäben des Informationszeitalters – „uralte“ Gesetzesregelungen immer wieder für aufsehenerregende Theorien und Gerichtsurteile sorgen (werden), welche das Vorhaben „Cloud“ unter Compliance-Gesichtspunkten für das auslagernde Unternehmen aufs Neue in Frage stellen oder von fragwürdigen Vorabinvestitionen abhängig machen. Es ist eben eine Binsenweisheit, dass Juristerei immer beliebig kompliziert betrieben werden kann. Die EU-Kommission will 2012 eine europäische Strategie für das Cloud Computing vorstellen, die, das lässt sich zweckpessimistisch sagen, sicherlich – neben der Behebung bestehender Probleme – neue Probleme schaffen und das zersplitterte „Informationsrecht“ mitnichten auf umfassend dogmatisch fundierte Beine stellen wird. Aber mit Rechtsunsicherheiten haben die Wirtschaft und ihre Berater bislang noch immer leben müssen.

// Autoren

Dr. Axel-Michael Wagner ist Rechtsanwalt und Partner der multidisziplinären Kanzlei Peters, Schönberger & Partner (PSP) in München.

Stefan Groß ist Steuerberater, Certified Information Systems Auditor und Partner der multidisziplinären Kanzlei Peters, Schönberger & Partner (PSP) in München.