Mit Recht in der Cloud

Cloud Computing bietet große Chancen – für Unternehmen aller Branchen. Aber: Der rechtliche Rahmen muss stimmen.

Wie kann der Datenschutz in der Cloud eingehalten werden? Wer haftet, wenn Daten verlorengehen sollten? Was passiert, wenn der Cloud-Dienst nicht zur Verfügung steht? Die Cloud steckt voller juristischer Herausforderungen. Im Rahmen des Technologieprogramms Trusted Cloud arbeiten Experten an Lösungsansätzen.

In vielen Bereichen gehört Cloud Computing längst zum Alltag: Privatpersonen nutzen Cloud Computing bei webbasierenden E-Mail-Diensten oder verwalten ihre Fotos und sonstige Dateien im Internet. Dokumente, Bilder, Videos und Musik sind so überall abrufbar – egal ob mit dem Tablet-PC, Laptop oder Smartphone. Auch immer mehr Unternehmen setzen Cloud-Lösungen ein. Denn Cloud Computing bietet ihnen vielfältige Möglichkeiten: Über die Cloud können mittelständische Firmen auf innovative Technologien zugreifen, die bislang vor allem großen Unternehmen vorbehalten waren. Sie müssen nicht mehr selbst in eine große IT-Infrastruktur investieren, da sie unterschiedliche Ressourcen von professionellen IT-Anbietern quasi mieten können. Gezahlt wird verbrauchsabhängig nur für die tatsächlich benötigten Leistungen. Gleichzeitig können die Mitarbeiter bequem auch mobil auf ihre Daten zugreifen. Diese Flexibilität wird den typischen Anforderungen eines Unternehmens oftmals besser gerecht als bisherige firmeneigene IT-Systeme. Durch die hohe Nachfrage und den raschen technischen Fortschritt gehört Cloud Computing mit hohen jährlichen Wachstumsraten zu den wichtigsten Trends der IT-Branche weltweit. Auch in Deutschland hat Cloud Computing mittlerweile eine starke Dynamik erreicht.

Noch gibt es aber auch Gründe, die Unternehmen zögern lassen, die Cloud zu nutzen. Unklare Haftungsbedingungen, offene Fragen beim Urheberrecht und Sorgen beim Thema Datenschutz gelten verbreitet als ein Hemmnis für den Einsatz von Cloud Computing. Das Technologieprogramm Trusted Cloud des Bundesministeriums für Wirtschaft und Technologie (BMWi) nimmt sich diesen Herausforderungen im Rahmen einer Arbeitsgruppe an (siehe Kasten 1).

Zuverlässigkeit, Sicherheit, Verfügbarkeit und Datenschutz sind wichtige Voraussetzungen, um das notwendige Vertrauen der Anwender in Cloud-Dienste zu etablieren. Daher werden im Technologieprogramm Trusted Cloud innovative, sichere und rechtskonforme Cloud-Computing-Lösungen in 14 Projekten entwickelt und erprobt. Von diesen neuen, cloud-basierten Diensten sollen insbesondere mittelständische Unternehmen profitieren. Die Vorteile von Cloud Computing werden anhand konkreter Pilotanwendungen verdeutlicht und in unterschiedlichen Branchen eingesetzt – von Industrie und Handwerk über den Gesundheitssektor bis hin zum öffentlichen Sektor. Das dafür bereitgestellte Fördervolumen beträgt rund 50 Millionen Euro. Durch Eigenbeiträge der Projektpartner liegt das Gesamtvolumen von Trusted Cloud bei rund 100 Millionen Euro. An den 14 Projekten sind insgesamt 36 Unternehmen verschiedener Branchen, 27 wissenschaftliche Einrichtungen und vier weitere Institutionen beteiligt. Neben der Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ werden auch in den einzelnen Projekten eine Reihe spezieller rechtlicher Fragen behandelt.

1. Datenschutz und Zertifizierung

Herausforderung: Die Prüfpflichten des Cloud-Nutzers

Wer Cloud Computing nutzt, möchte sich darauf verlassen können, dass seine Daten sicher sind. Gerade vor dem Hintergrund aktueller Debatten um Datenschutz machen sich immer mehr Anwender von Cloud Computing Gedanken über die Sicherheit ihrer Daten. Es ist besonders wichtig, dass die Anforderungen des Datenschutzrechts zum Schutz der Privatsphäre und zur Verhinderung von Datenmissbrauch beachtet werden. Mitunter machen neue Technologien wie Cloud Computing es jedoch schwierig, die Anforderungen des deutschen Datenschutzrechts in der Praxis zu erfüllen.

Ein zentrales Problem des Datenschutzrechts im Cloud Computing ergibt sich durch die so genannte Auftragsdatenverarbeitung. Dabei muss der Auftraggeber die Sicherheit der Datenverarbeitung beim Auftragnehmer überwachen. Diese Überprüfung soll gewährleisten, dass die Daten sicher verarbeitet werden und Unbefugte keinen Zugriff darauf erhalten. Daher muss auch die Sicherheit vor Ort überprüft werden, beispielsweise in den Serverräumen eines Rechenzentrums, auch wenn dies nicht notwendig durch den Auftraggeber persönlich erfolgen muss.

Beim Cloud Computing ist Auftraggeber der Cloud-Nutzer. Dies kann beispielsweise ein kleines Unternehmen oder ein Start-up sein, das Kundendaten für die Rechnungsstellung in einer kostengünstigen Cloud-Lösung verarbeitet. Auftragnehmer ist der Cloud-Anbieter. Bei ihm könnte es sich um ein großes Unternehmen handeln, das tausende kleine Unternehmen mit Cloud-Diensten versorgt. Soll nun jedes dieser tausend kleinen Unternehmen die Serverräume des großen Cloud-Anbieters inspizieren? Und woher soll es die Kompetenz

Kasten 1: Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ im Kompetenzzentrum Trusted Cloud

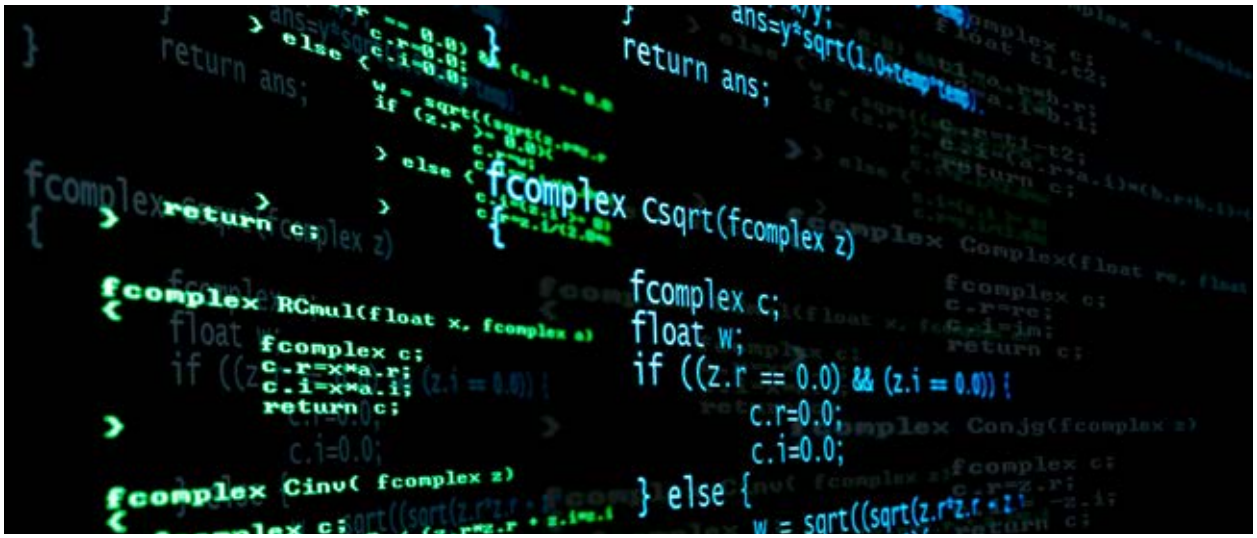
Für die rechtlichen Aspekte von Cloud Computing hat das BMWi innerhalb des Kompetenzzentrums Trusted Cloud eine eigene Arbeitsgruppe einrichten lassen. Sie wird von Prof. Dr. Georg Borges, Jura-Professor an der Ruhr-Universität Bochum, geleitet. In der Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ erarbeiten Experten aus Wirtschaft, Anwaltschaft und Wissenschaft sowie Vertreter aus Datenschutzbehörden gemeinsam mit Projektbeteiligten aus dem Trusted-Cloud-Programm Lösungen für rechtliche Herausforderungen. Bisher hat sich die Arbeitsgruppe folgenden Themenschwerpunkten gewidmet:

1. Datenschutz und Zertifizierung

2. Cloud-Computing-Verträge

3. Haftung im Cloud Computing

4. Urheberrecht und Lizenzen



dafür haben? Wie soll es die hohen Kosten eines externen Gutachters tragen? Auch eine Selbstkontrolle des Anbieters erscheint im Hinblick auf eine unabhängige Kontrolle problematisch. Hier ist eine Lösung gefragt, die den Schutz von Daten gewährleistet und zugleich praxistaugliche Überprüfungsmaßnahmen bietet.

Lösung: Zertifizierung von Cloud-Anbietern

Die Überprüfung könnte zukünftig durch eine Zertifizierung erfolgen. Der Anbieter kann seinen Cloud-Dienst durch eine unabhängige Institution bzw. Sachverständige prüfen lassen und erhält ein Zertifikat – sofern die gesetzlichen Anforderungen erfüllt sind. Der Cloud-Nutzer kann auf dieses Zertifikat vertrauen. Es ermöglicht ihm, den Cloud-Dienst zu nutzen, ohne möglicherweise gegen Datenschutzrecht zu verstoßen.

Die Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ hat hierzu ein rechtspolitisches Thesenpapier „Datenschutzrechtliche Lösungen für Cloud Computing“ erarbeitet.

Es wurde auf dem „Jahreskongress Trusted Cloud“ im November 2012 vorgestellt und mit der Fachöffentlichkeit diskutiert. Ziel ist es, in der künftigen Europäischen Datenschutz-Grundverordnung eine solche Möglichkeit der Datenschutz-Zertifizierung von Cloud-Diensten zu verankern. Die Bundesregierung hat wesentliche Aspekte aus dem Konzept aufgegriffen und einen Gesetzgebungsvorschlag in die europäischen Verhandlungen eingebracht. Der aktuelle Kompromissvorschlag wurde von der irischen Ratspräsidentschaft sowie von der Ratsarbeitsgruppe in seinen wesentlichen Grundgedanken positiv aufgenommen.

Unabhängig vom europäischen Gesetzgebungsverfahren gilt es nun, das Konzept der Datenschutz-Zertifizierung von Cloud-Diensten praktisch umzusetzen. Dies ist schwierig, da das deutsche Datenschutzrecht eine solche Zertifizierung zwar zulässt, sie aber nicht ausdrücklich nennt und erst recht nicht im Einzelnen regelt. Das BMWi ist im Gespräch mit Datenschutzbehörden, Wirtschaft und anderen Institutionen, etwa der Stiftung Datenschutz, um eine solche Zertifizierung zu ermöglichen.

So einfach und überzeugend der Gedanke der Zertifizierung ist, so muss doch vieles bedacht werden, um Missbrauch auszuschließen. Es muss gewährleistet werden, dass nur seriöse Institutionen ein Zertifikat verleihen können. Daher sollen nur akkreditierte Prüfstellen ein Zertifikat vergeben. Wenn das Zertifikat zu Unrecht vergeben wurde oder der Cloud-Anbieter die Anforderungen nicht mehr erfüllt, muss das Zertifikat widerrufen werden können. Auch für Schäden muss eine Regelung gefunden werden. Vor allem muss ganz genau und bis ins Detail geklärt sein, welche Voraussetzungen erfüllt werden müssen, damit das Zertifikat verliehen wird, denn sonst würden die Cloud-Anbieter ungleich behandelt.

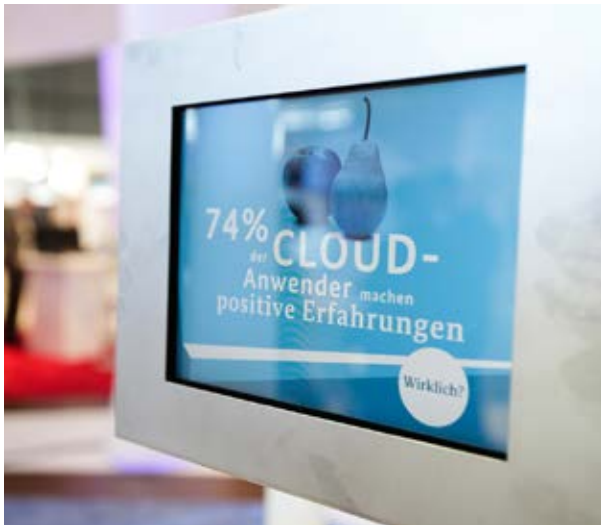
2. Vertragsrecht im Cloud Computing

Nur eine sorgfältige Vertragsgestaltung kann interessengerechte Risikoverteilung sicherstellen

Leistungen aus der Cloud werden im Regelfall nur aufgrund eines Vertrages erbracht. Je nach Cloud-Dienst stellen die Anbieter dazu meist Musterverträge bereit, die die Rechtsbeziehungen zwischen Anbieter und Nutzer regeln sollen. Bei privaten Nutzern besteht

wegen der großen Marktmacht der Anbieter häufig keine Möglichkeit, auf die vom Anbieter gestellten Bedingungen Einfluss zu nehmen.

Unternehmen, die Teile ihrer IT in die Cloud auslagern, haben dagegen als begehrte Kunden oft deutlich mehr Möglichkeiten, auf die Gestaltung des Vertrages einzuwirken. Weil die gesetzlichen Vorschriften vielerorts nicht auf Cloud-Dienste zugeschnitten sind und sich der Nutzer durch die Auslagerung der eigenen Datenverarbeitung häufig in eine starke Abhängigkeit zu den Diensteanbietern begibt, ist eine interessengerechte und angemessene Risikoverteilung im Vertrag wichtig. Die Möglichkeit einer rechtssicheren vertraglichen Ausgestaltung kann entscheidend dafür sein, ob Cloud Computing eine gangbare Alternative zum klassischen Outsourcing darstellt, und ist daher ein für die Akzeptanz des Geschäftsmodells maßgeblicher Faktor.



Das BMWi informiert auf der CeBIT über das Thema Cloud Computing auf diversen Touch Screens.

Eine detaillierte Leistungsbeschreibung schafft Rechtssicherheit

Die Notwendigkeit einer sorgfältigen Vertragsgestaltung zeigt sich bereits bei der Leistungsbeschreibung. Bei Cloud-Diensten muss diese vertraglich detailliert ausgestaltet werden. Ein Cloud-Dienst lässt sich nicht ohne weiteres in „klassische“ Vertragstypen wie Kauf- oder Mietvertrag einordnen. Zudem können mehrere Leistungen vorgesehen sein, die unterschiedlich zu klassifizieren sind. Während zum Beispiel die Bereitstellung von Speicherplatz oder Rechenleistung meist eher mietvertraglichen Charakter aufweist, wird die Anfertigung von Sicherheitskopien der Kundendaten eher als Werkvertrag anzusehen sein.

Eine Einordnung in die „klassischen“ Vertragstypen des Bürgerlichen Gesetzbuches (BGB) ist aber vorteilhaft, weil sich aus dieser die Rechte der Parteien bei Leistungsstörungen wie zum Beispiel Verzug oder Schlechtleistung ergeben. Auch die Regeln des BGB zu Allgemeinen Geschäftsbedingungen (AGB), denen alle Verträge unterliegen, die für eine mehrfache Verwendung vorgesehen sind, orientieren sich am einschlägigen Vertragstyp. Insbesondere können einseitig benachteiligende oder dem Vertragszweck widersprechende vertragliche Regelungen nach AGB-Recht unwirksam sein. Für die Entscheidung, ob eine Klausel dem Vertragszweck widerspricht, ist wiederum entscheidend, um welchen Vertragstyp es sich handelt.

Werden in Verträgen die Leistungspflichten daher nicht eindeutig und für die jeweilige Teilleistung differenziert geregelt, ist oft fraglich, welche Vorschriften anwendbar sind, woraus sich für beide Parteien Rechtsunsicherheiten ergeben können.

Leitlinien zur Vertragsgestaltung notwendig

Die Festlegung der zu erbringenden Leistungen erfolgt von Anbieterseite in der Praxis häufig im Rahmen so genannter Service Level Agreements (SLAs). Die Anbieter staffeln den Umfang und die Qualität der zu erbringenden Leistungen und knüpfen entsprechende Vergütungsregelungen an die Servicequalität.

Auch für die potenziellen Nutzer lassen sich Unwägbarkeiten vor allem durch eine detaillierte Beschreibung der zu erbringenden Leistungen und des jeweils anzuwendenden Mängelrechts beseitigen. So ist jederzeit für die Parteien vorhersehbar, welche Maßnahmen sie zu treffen haben und was vom Vertragspartner erwartet werden kann.

Um hier Hilfestellung für Unternehmen zu bieten, sollen möglichst differenzierte Leitlinien ausgearbeitet werden, die für häufig vorkommende vertragliche Konstellationen Hinweise zu Art und Umfang der Leis-

tungsbeschreibung enthalten. Sie können, wenn von unabhängiger Seite erarbeitet, Grundlage einer Einigung bei Interessenkonflikten zwischen den Vertragsparteien sein.

Besondere Bedeutung hat insofern das Spannungsverhältnis zwischen den Interessen der Vertragspartner, das in Bezug auf die Verfügbarkeit der Dienste besteht. Bei Cloud-Diensten findet überwiegend die komplette Datenverarbeitung beim Anbieter statt, sodass im Falle fehlender Verfügbarkeit, zum Beispiel wenn die Login-Webseite nicht verfügbar ist oder ein Server abstürzt, keinerlei Verarbeitung stattfinden kann. Auch eine prozentual geringe Ausfallzeit des Dienstes kann je nach Umfang der Auslagerung im Ernstfall schlimmstenfalls einen Betriebsstillstand beim Nutzer hervorrufen. Der Nutzer möchte daher eine möglichst hundertprozentige Verfügbarkeitsgarantie erhalten. Für den Anbieter besteht dagegen ein hohes Schadensersatzrisiko, wenn er zu hohe Verfügbarkeiten garantiert und bei einem Ausfall des Systems für Schäden des Kunden einstehen muss.

Checklisten helfen, wichtige Punkte zu beachten

Für kleinere Unternehmen liegt die besondere Schwierigkeit der Vertragsgestaltung darin, zu erkennen, welche Vertragsaspekte besonders relevant sind und welche Punkte sinnvollerweise zumindest grob geregelt werden sollten. In vielen Fällen können durch klare Regelungen Konflikte vermieden und Planungssicherheit geschaffen werden:

- Vergütungsmodelle können passgenau auf die Bedürfnisse des Nutzers zugeschnitten werden.
- Vereinbarungen über regelmäßige Datensicherungen sind unentbehrlich, um das Risiko eines Datenverlusts zu minimieren.
- Genaue Regelungen zum Ablauf der Vertragsbeendigung helfen beim Exit-Management. Über die Vertragslaufzeit und Kündigungsmöglichkeiten hinaus ist die Portabilität der Daten ein zentraler Gesichtspunkt, um einen Umstieg auf einen anderen Anbieter oder den Rückzug aus Cloud-basierter Verarbeitung zu ermöglichen.
- Eine Wahl des Gerichtsstandes und derjenigen nationalen Rechtsordnung, nach der sich die Rechtsbeziehungen der Parteien richten sollen, ist unter dem Gesichtspunkt der Rechtssicherheit stets empfehlenswert. Sind diese Informationen nicht angegeben, lassen sie sich jederzeit (anhand der einschlägigen Normen) ermitteln.

Soll eine umfängliche Vertragsgestaltung erfolgen, die alle relevanten Punkte berücksichtigt, so kann dies schnell die im Unternehmen vorhandenen rechtlichen Kenntnisse übersteigen. Um einen Überblick über eventuell regelungsbedürftige Punkte zu ermöglichen, erarbeitet die Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ derzeit einen Vorschlag für Checklisten, anhand derer weiterer Beratungs- bzw. Gestaltungsbedarf ermittelt werden kann.

3. Urheberrecht und Lizenzen

Die urheberrechtliche Verantwortlichkeit liegt überwiegend bei den Anbietern

Spannende Fragen stellen sich auch im urheberrechtlichen Bereich. Anbieter von Cloud-Diensten stellen ihren Kunden häufig von Drittunternehmen entwickelte Software zur Verfügung. An der Software besteht dabei regelmäßig ein Urheberrecht des Herstellers. Bei der Nutzung der Dienste kann es daher zu urheberrechtlich relevanten Handlungen kommen, für die ein Nutzungsrecht (Lizenz) erforderlich ist. Bei einer Nutzung ohne entsprechende Lizenz drohen Unterlassungsklagen und Haftung auf Schadensersatz. Um Haftungsrisiken auszuschließen, müssen daher die erforderlichen Nutzungsrechte eingeräumt und die für die Beschaffung verantwortliche Partei ermittelt werden. Welche Lizenzen erforderlich sind, ist dabei vom Einzelfall abhängig. Praktisch relevant ist vor allem die Frage, ob der Nutzer urheberrechtsrelevante Handlungen vornimmt und daher ebenfalls einer Lizenz bedarf.

Auf Seite des Anbieters stellt schon die Installation der Software eine zustimmungsbedürftige Vervielfältigung dar. Auch das Abspielen eines Programms erfordert, dass eine Programmkopie in den Arbeitsspeicher des Anbieters geladen wird. Der Anbieter benötigt daher stets eine Lizenz des Programmherstellers zur Vervielfältigung.

Beim Bereitstellen der Software besteht Uneinigkeit darüber, ob eine öffentliche Zugänglichmachung vorliegt, oder ob Cloud Computing insofern eine eigene, nicht gesetzlich geregelte Nutzungsart darstellt. Nimmt man Letzteres an, so muss vertraglich exakt vereinbart werden, welche Handlungen zugelassen sein sollen, um ein Nutzungsrecht einzuräumen.

Die Handlungen des Nutzers sind hingegen nicht relevant. Denn die Nutzung erfordert keine eigenständige Vervielfältigung. Auch die Vervielfältigung beim Anbieter ist ihm meist nicht zurechenbar, da typischerweise nicht für jeden Nutzer eine neue Programmkopie erstellt wird (sog. Mandantenfähigkeit). Die dem Zugriff dienende Benutzeroberfläche ist im Regelfall nicht schutzfähig. Wenn der Nutzer aufgrund der technischen Ausgestaltung jeweils eigenständige Programmkopien beim Anbieter erzeugt oder spezielle Software des Anbieters nutzt, um auf dessen Dienste zuzugreifen, kann aber auch für ihn eine Lizenzierung erforderlich sein.

In ihrem Arbeitspapier „Lizenzierungsbedarf beim Cloud Computing“ hat die Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ diese und weitere Fragestellungen detailliert erörtert.

4. Haftung im Cloud Computing

Haftungsfragen sind teilweise noch ungelöst

Wie bei jeder Art der Datenverarbeitung birgt auch Cloud Computing das Risiko eines Datenverlustes oder einer unbefugten Offenbarung von Daten an Dritte. Die Daten sind dabei in besonderem Maße dem Einflussbereich des Nutzers entzogen. Abgesehen von vertraglichen Regelungen zu Datensicherung und Sicherheitsmaßnahmen hat er hier kaum Einflussmöglichkeiten.

Bei einer unbefugten Offenbarung stellen sich überwiegend die gleichen Fragen wie bei jeder anderen Form der externen Datenverarbeitung: Bei personenbezogenen Daten können sich Ansprüche aus dem Datenschutzrecht, bei Geheimnissen aus dem Strafrecht ergeben. Daneben kommt immer eine Haftung wegen Verletzung vertraglicher Pflichten in Betracht.

Schwierige Rechtsprobleme können sich bei Datenverlusten ergeben. Der Anbieter haftet aus dem Vertrag, sofern er die Pflichtverletzung fahrlässig oder vorsätzlich begangen hat. Es stellt sich aber jedenfalls die Frage nach dem konkreten Wert der Daten: Entstandene Schäden sind vom Geschädigten grundsätzlich unter Angabe der Schadenshöhe festzustellen. Diese lässt sich bei einem Verlust kaum ermitteln. Oftmals wird nicht einmal rekonstruierbar sein, welche Daten genau vorhanden waren. Die unmittelbaren Kosten, zum Beispiel für die Neubeschaffung der Daten oder die erneute Eingabe in die Datenverarbeitungssysteme, können einigermaßen beziffert werden – die Kosten für spätere betriebliche Auswirkungen oder Imageschäden hingegen nicht. Es besteht daher häufig die Notwendigkeit, im Vertrag Pauschalbeträge für bestimmte Schadensszenarien festzusetzen, um wenigstens Kosten und Aufwand für die Schadensermittlung zu begrenzen.

Daneben kommt eine deliktische Haftung für Datenverlust in Betracht. Diese ist vor allem von Bedeutung, wenn zwischen dem Dateninhaber und dem Cloud-Anbieter keine vertragliche Beziehung bestand, etwa wenn Datenbestände des Kunden eines Cloud-Nutzers verlorengehen. Hierbei handelt es sich juristisch gesehen um einen sehr jungen und überaus umstrittenen Bereich, in dem selbst die Frage, ob und unter welchen

Umständen Daten überhaupt schutzfähig sind, umstritten ist. Gerade beim Cloud Computing, bei dem die Daten nicht einzelnen physikalischen Datenträgern zugewiesen werden können, stellt sich dabei die Frage, ob ein Datum an sich Eigentumsqualität besitzen kann.

Ergebnisse und Ausblick

Datenschutz, Nutzungsrechte, Vertragsrecht und Haftungsfragen – die juristischen Herausforderungen bei Cloud Computing sind komplex. Das Technologieprogramm Trusted Cloud des BMWi bietet die Gelegenheit, dass schon bei der Entwicklung innovativer Cloud-Computing-Dienste Lösungsansätze für diese Herausforderungen gefunden und Beiträge für rechtskonformes Cloud Computing geleistet werden. Bisher hat das BMWi wichtige Impulse im Bereich Datenschutz durch einen Zertifizierungsvorschlag gesetzt.

Die AG Rechtsrahmen des Cloud Computing arbeitet derzeit an einem Arbeitspapier zu den zentralen vertraglichen Fragen des Cloud Computing. Außerdem erstellt sie eine Handreichung inklusive einer Checkliste, die sich vorrangig an mittelständische Unternehmen richtet. Diese soll die für Cloud-Computing-Verträge wichtigen Regelungspunkte enthalten und Hilfestellung bei der Erarbeitung individueller Vertragswerke leisten.

Mehr zum Technologieprogramm Trusted Cloud: www.trusted-cloud.de

Kontakt: Jennifer Welp
Referat: Entwicklung konvergenter IKT

Kasten 2: Datenschutz in der Cloud: Drei Beispiele aus dem Technologieprogramm Trusted Cloud

In allen Projekten des Technologieprogramms Trusted Cloud spielt Datenschutz eine wichtige Rolle. Hier einige Beispiele:

Das Projekt **TRESOR** entwickelt für die Übermittlung von Patientendaten ein sicheres Cloud-Ökosystem, das auf die gesetzlichen Vorschriften sowie Sicherheits- und Datenschutzrichtlinien für Gesundheitsinstitutionen ausgerichtet ist. Die Daten werden dabei durch innovative Zugriffskontrollen geschützt. Ergänzend zu bekannten Sicherungsverfahren wird hier die Möglichkeit der Identifikation durch ortsbasierte Authentifizierung und Autorisierung geschaffen. Nur autorisierte Anwender, die sich zusätzlich an einem bestimmten Ort wie beispielsweise in einem Krankenhaus befinden, können auf die Daten eines bestimmten Patienten zugreifen.

Das Projekt **SkIDentity** erarbeitet für Anwender in Unternehmen ein standardisiertes und sicheres Authentifizierungssystem für Cloud-Anwendungen. Nur wer über einen Kartenleser den richtigen Ausweis vorlegen kann, erhält Zugriff auf die Anwendung und die darin enthaltenen Daten. Dafür setzt SkIDentity auf schon bestehende sichere elektronische Ausweise wie den neuen Personalausweis oder Mitarbeiterausweise. Das ist deutlich sicherer als eine Anmeldung durch Benutzernamen und Passwort.

An einer „versiegelten“ Cloud-Computing-Infrastruktur wird im Rahmen des Projektes **Sealed Cloud** gearbeitet. Dadurch können nicht einmal der Cloud-Anbieter und seine Mitarbeiter auf die Daten der Kunden zugreifen. Das System besteht aus einer speziellen Verschlüsselung, einem neuartigen Verfahren des so genannten Data Clean-up um den Zugriff auf unverschlüsselte Daten zu verhindern, sowie einer Überprüfung der Integrität der Software und des Systemverhaltens durch Auditoren.