

Stellungnahme

Cloud-Strategie der Europäischen Kommission

27. Dezember 2012

Seite 1

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.700 Unternehmen, davon über 1.200 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu gehören fast alle Global Player sowie 800 leistungsstarke Mittelständler und zahlreiche gründergeführte, kreative Unternehmen. Mitglieder sind Anbieter von Software und IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien und der Netzwirtschaft. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Zusammenfassung

Der BITKOM begrüßt die mit Mitteilung vom 27. September 2012 veröffentlichte Strategie der EU-Kommission zur „Freisetzung des Cloud-Computing Potenzials in Europa (kurz: EU-Cloud-Strategie). Der Verband hat Kommentare und Vorschläge entwickelt, die darauf zielen, die EU-Cloud-Strategie zum Erfolg zu führen. Die Kommentare und Vorschläge lassen sich 5 Säulen zuordnen, die der BITKOM als wichtige Erfolgsfaktoren sieht.¹

- Standardisierung im Cloud Computing
- Rechtsrahmen für Cloud Computing (in erster Linie Datenschutzrecht und Vertragsrecht)
- Einsatz von Cloud Computing in der öffentlichen Verwaltung
- Infrastruktur für Cloud Computing sowie
- Internationale Kooperation im Cloud Computing.

Die Kommentare und Anregungen des BITKOM lassen sich folgendermaßen zusammenfassen:

- Standardisierung, Zertifizierung und Selbstverpflichtungen im Cloud Computing:

Der BITKOM unterstreicht die Bedeutung der Standardisierung für die Förderung von Interoperabilität (zwischen verschiedenen Clouds sowie zwischen Cloud-Applikationen und traditionellen IT-Systemen), für Datenportabilität und zur Definition von Datenschutz- und Sicherheitsniveaus. Der Verband begrüßt in dem Zusammenhang die Berufung eines Steering Boards für die European Cloud Partnership (ECP). Der BITKOM erwartet, dass weitere Standardisierungsvorhaben im Cloud Computing einen bedeutenden Einfluss auf den europäischen Cloud-Markt ausüben werden und ist daher bereit, die Steuerungsgruppe bei seiner Arbeit zu unterstützen.

Eine in der EU vereinheitlichte Datenschutzregelung sollte für Cloud Computing auch in einem Zertifikat testiert werden. Darüber hinaus gehende Erwar-

Ansprechpartner
Dr. Mathias Weber
Bereichsleiter IT-Services
Tel.: +49.30.27576-121
m.weber@bitkom.org

Präsident
Prof. Dieter Kempf

Hauptgeschäftsführer
Dr. Bernhard Rohleder

¹ Die Säulen 1 bis 3 folgen den Schlüsselaktionen 1 bis 3 der EU-Cloud-Strategie. Die Säule 4 wird vom BITKOM für maßgeblich gehalten; im Dokument der EU-Kommission wird die Infrastruktur eher beiläufig erwähnt. Die Säule 5 des BITKOM findet sich im Kapitel 4 des EU-Dokumentes („Zusätzliche Politische Schritte“).

Stellungnahme

EU-Cloud-Strategie

Seite 2

tungen oder branchenspezifische Anforderungen von Cloud-Anwendern sollten von den Cloud-Anbietern in freiwilligen Selbstverpflichtungen oder Kodizes attestiert werden, um die notwendige Flexibilität zu wahren und den bürokratischen Aufwand gering zu halten, gleichzeitig aber den Auftraggeber transparent über die Bedingungen der Cloud-Dienstleistung zu informieren.

■ Rechtsrahmen für Cloud Computing:

BITKOM spricht sich für eine praxisgerechte Harmonisierung des Datenschutzes in der EU mit Hilfe der neuen Datenschutz-Grundverordnung aus. Entscheidend sind klare Regelungen zur Auftragsdatenverarbeitung - insbesondere zur Aufteilung der Zuständigkeiten und Verantwortlichkeit.

Die Ankündigungen der EU-Kommission zu Muster-Vertragsformulierungen werden vom BITKOM als eine große Hilfe für Cloud-Verträge angesehen und ausdrücklich begrüßt. Die Muster-Vertragsformulierungen sollten keine zwingenden vertragsrechtliche Vorgaben des Europarechts für Cloud-Computing-Verträge darstellen.

■ Einsatz von Cloud Computing in der öffentlichen Verwaltung:

BITKOM fordert die Vorreiterrolle öffentlicher Verwaltungen bei der Umsetzung von Cloud Computing. Der Verband regt die Erarbeitung eines Strategieplans, eines Stufenplanes und eines Governance-Rahmens zur Umsetzung für Verwaltungs-Clouds in den EU-Ländern an.

■ Infrastruktur für Cloud Computing:

Eine Hochgeschwindigkeits-Breitbandinfrastruktur bildet die Grundlage für das Cloud Computing. Um den Ausbau von Hochgeschwindigkeitsnetzen über die bisherigen Erfolge hinaus zügig mit wettbewerblichen Mitteln voranzubringen, ist es unumgänglich, für ein entsprechendes regulatorisches Umfeld zu sorgen und alle Synergien für den Netzaufbau zu nutzen.

■ Internationale Kooperation im Cloud Computing:

Aufgrund der kleinen Heimatmärkte ist die europäische Koordinierung bezüglich gesetzlicher Anforderungen und Standards notwendig, jedoch global nicht hinreichend. BITKOM setzt sich für eine Neubelebung der transatlantischen Wirtschaftspartnerschaft und Unterstützung der Cloud-Arbeitsgruppe des Transatlantic Economic Council zur Schaffung eines gemeinsamen Cloud-Rechtsrahmens ein.

Stellungnahme

EU-Cloud-Strategie

Seite 3

Inhalt Seite

1. Vorbemerkung zum B2B-Fokus des BITKOM	4
2. Standardisierung im Cloud Computing vorantreiben	5
3. Praxisgerechter Rechtsrahmen für Cloud Computing.....	5
3.1 Für die Auftragsdatenverarbeitung geeignete Harmonisierung des Datenschutzes	5
3.1.1 Vereinheitlichung der Datenschutzregeln für –Cloud-Anbieter	5
3.1.2 Technischen Datenschutz stärken	6
3.1.3 Klare Regelungen für Auftragsdatenverarbeitung	6
3.1.4 Geltung von standardisierten Vertragsklauseln	7
3.1.5 Einführung extraterritorial geltenden Rechts - Beseitigung rechtlicher Grauzonen	8
3.2 Flexibilität durch Selbstverpflichtungen und Zertifizierung	8
3.3 Vertragsrecht für Cloud Computing	10
3.3.1 Cloud-Verträge haben eigene Anforderungen	11
3.3.2 Unverzichtbare Vertragsbestandteile im Cloud Computing	11
3.3.3 Plädoyer für faire und KMU-taugliche Muster-Vertragsklauseln	11
3.3.4 Regelungsbedarf bei rechtlichen „Randbedingungen“ für Cloud Computing	12
3.3.5 Verbraucherschutz in Cloud-Computing-Verträgen austarieren	12
3.3.6 Ablehnung zwingender vertragsrechtlicher Vorgaben des Europarechts für Cloud-Computing-Verträge.....	13
3.4 Öffnung des Zugangs zu Inhalten – Vorschläge und Kommentare	13
4. Public Sector – Förderung einer gemeinsamen Führungsrolle des öffentlichen Sektors durch eine europäische Cloud-Partnerschaft	13
4.1 Orientierung an offenen Standards	13
4.2 Akzeptanz elektronischer Dokumente unterstützen	14
5. Infrastruktur - Breitbandausbau für Cloud Computing	14
6. Stellung von Europa im Cloud Computing und internationale Kooperation	15

Stellungnahme

EU-Cloud-Strategie

Seite 4

1. Vorbemerkung zum B2B-Fokus des BITKOM

Der BITKOM regt an, für die von der Kommission geplanten Schlüsselaktionen und begleitenden politischen Schritte zukünftig eine klare inhaltliche und sprachliche Trennung zwischen den Kommunikations- und Geschäftsfeldern

- Business-to-Consumer (B2C) und
- Business-to-Business (B2B)

vorzunehmen und dies auch durch eine durchgängig einheitliche Verwendung von Begriffen zu dokumentieren. Der BITKOM schlägt deshalb vor, die Bezeichnungen

- „Verbraucher“ für private Konsumenten von Cloud-Diensten und
- „Unternehmen“ für gewerbliche Konsumenten

einzuführen.

Dem BITKOM ist durchaus bewusst, dass eine Reihe der von der Kommission geplanten Maßnahmen gleichermaßen sowohl den B2C- als auch den B2B-Bereich betreffen; beispielsweise im Bereich „Mobile Banking“, im Gesundheitswesen, in der Kommunikation mit Behörden oder auch im Hinblick auf das Urheberrecht.

Trotzdem bietet nur eine klare Trennung zwischen beiden Bereichen die Chance, zielgruppenspezifische Maßnahmen zu initiieren, deren Vorteile für die jeweilige Nutzergruppe aufzuzeigen und die erzielten Ergebnisse gezielt und verständlich zu kommunizieren.

Eine Trennung erscheint auch deshalb sinnvoll, weil Privatpersonen in ihren Rollen als Verbraucher und Bürger im B2C-Umfeld andere Erwartungen und Anforderungen an die Service-Qualität der Cloud-Dienste hinsichtlich Verfügbarkeit oder Ausfallsicherheit haben als Unternehmen im B2B-Umfeld. Ähnliches gilt in Bezug auf Datensicherheit (Data Security), Datenschutz (Data Privacy) und Regelgerechtes Verhalten (Compliance).² Zudem müssen Unternehmen im Gegensatz zu Verbrauchern sehr viel mehr rechtliche Anforderungen bei der Nutzung von IT-Systemen und damit auch von Cloud-Diensten beachten, z.B. handels- und steuerrechtliche Archivierungsanforderungen oder Pflichten zur Risikoerkennung und Risikovermeidung.

Diesen spezifischen Anforderungen sind durch unterschiedliche bzw. sich ergänzende, den beiden Nutzergruppen angepasste EU-Maßnahmen Rechnung zu tragen.

Demgegenüber scheint die in dem EU-Dokument vorgenommene Unterscheidung in große und kleine Unternehmen weniger sinnvoll. Weil sich auch und gerade Kleinunternehmen durch eine Cloud-Nutzung große Chancen auf globalen Märkten eröffnen, haben diese prinzipiell die gleichen Anforderungen wie große Unternehmen z.B. in Bezug auf Datenschutz, Datensicherheit und Compliance. Nicht zuletzt gelten für kleine Unternehmen auch dieselben rechtlichen Regelungen wie für große Unternehmen.

Der BITKOM setzt sich dafür ein, dass kleine und mittelständische Unternehmen nicht zusätzlich mit bürokratischen Regulierungen überfordert werden.

² Das Speichern von Urlaubsfotos in der Cloud, ein mobiler Musik-Download durch einen Endverbraucher oder die freiwillige Veröffentlichung von privaten Informationen auf Facebook hat tendenziell einen anderen Grad an Schutzbedürftigkeit als die Verarbeitung von unternehmens- oder behördenkritischen Daten. Hier sind erhöhte Anforderungen z.B. durch Anonymisierung, Pseudonymisierung personenbezogener Informationen, durch eine hohe Qualität der verwendeten Verschlüsselungsalgorithmen oder durch Rechtssicherheit der Prozesse zu erfüllen.

Stellungnahme

EU-Cloud-Strategie

Seite 5

Da die höchste gesamtwirtschaftliche Bedeutung des Cloud-Computing im B2B-Umfeld liegt und dort die Dringlichkeit einer Problemlösung am größten ist, konzentriert sich der BITKOM in dieser Stellungnahme auf den B2B-Bereich.

2. Standardisierung im Cloud Computing vorantreiben

Standardisierung zur Förderung von Interoperabilität (zwischen verschiedenen Clouds sowie zwischen Cloud-Applikationen und traditionellen IT-Systemen), Datenportabilität und zur Definition von Datenschutz- und Sicherheitsniveaus ist für die weitere Entwicklung des Cloud-Marktes notwendig.

Der BITKOM begrüßt, dass das am 19.11.2012 von der EU eingesetzte Steering Board für die European Cloud Partnership (ECP) beabsichtigt, als Teil ihres Arbeitsprogrammes eine Liste existierender und sich in Entwicklung befindlicher Cloud-relevanter Standards vom European Telecommunications Standards Institute (ETSI) entwickeln zu lassen. Ein Bericht in Form einer Cloud-Standard-Roadmap soll noch im Jahr 2013 durch die Kommission veröffentlicht werden.³ Der BITKOM erwartet, dass weitere Standardisierungsvorhaben im Cloud Computing einen bedeutenden Einfluss auf den europäischen Cloud-Markt ausüben werden. Der Verband ist daher bereit, seine Einschätzungen und Erfahrungen einzubringen und sich an Diskussionen und Round Tables der Steuerungsgruppe zu beteiligen.

3. Praxisgerechter Rechtsrahmen für Cloud Computing

3.1 Für die Auftragsdatenverarbeitung geeignete Harmonisierung des Datenschutzes

BITKOM spricht sich für eine praxisgerechte, für die Auftragsdatenverarbeitung geeignete Harmonisierung des Datenschutzes in der EU mit Hilfe einer neuen Datenschutz-Verordnung aus.

Neben dem Gesichtspunkt der Einheitlichkeit und dem Anwendungsbereich ist vor allem auch darauf zu achten, dass die zukünftige Verordnung auch inhaltlich keine neuen Hürden aufbaut bzw. bestehende Rechtsunsicherheiten für das Cloud Computing im geltenden Recht beseitigt. Hierbei sind vor allem

- der technische Datenschutz zu stärken,
- klare Regelungen für Auftragsdatenverarbeitung zu erlassen und
- rechtliche Grauzonen zu beseitigen.

3.1.1 Vereinheitlichung der Datenschutzregeln für –Cloud-Anbieter

Der BITKOM begrüßt das Vorhaben der Kommission, eine Datenschutz-Grundverordnung zu erlassen, grundsätzlich sehr. BITKOM regt an:

- Die vollharmonisierten europäischen Vorgaben sollten für alle Auftragsverarbeiter gelten, die in Europa Dienste anbieten, unabhängig davon, ob diese Anbieter auch in einem Mitgliedsstaat die Auftragsdatenverarbeitung betreiben.
- Dabei sollte die Datenverarbeitung eines Cloud-Anbieters - egal für welchen Kunden (für die Verarbeitung Verantwortlichen) und egal in welchem Mit-

³ Damit werden wesentliche Empfehlungen und Schlussfolgerungen umgesetzt, die in folgender Studie enthalten sind: Das Normungs- und Standardisierungsumfeld von Cloud Computing - Eine Untersuchung aus europäischer und deutscher Sicht unter Einbeziehung des Technologieprogramms „Trusted Cloud“. Studie von Booz&Co. und FZI für das Bundesministerium für Wirtschaft und Technologie (BMWi), Februar 2012, verfügbar als Download auf <http://www.trusted-cloud.de/de/878.php>

Stellungnahme

EU-Cloud-Strategie

Seite 6

gliedsstaat dieser ansässig ist, dem Recht bzw. der Aufsicht des Mitgliedsstaats unterliegen, in dem der Cloud-Anbieter seinen Hauptsitz hat. Bei Cloud-Anbietern, die nicht in einem Mitgliedsstaat ansässig sind, sollte ebenfalls nur eine Aufsichtsbehörde zuständig sein und diese nach objektiven Kriterien festgelegt werden. Es muss sichergestellt werden, dass die Beteiligten auf Nutzer- und Anbieterseite nicht mit unterschiedlichen Auslegungen durch die Aufsichtsbehörden konfrontiert werden.

3.1.2 Technischen Datenschutz stärken

BITKOM regt an, die Instrumente des technischen Datenschutzes im aktuell vorliegenden Entwurf der EU-Kommission für eine Datenschutz-Verordnung zu stärken.

IT-Technologie ist ein wichtiger „Enabler“ des Datenschutzes. Durch Verschlüsselung, Pseudonymisierung und Anonymisierung kann der Datenschutz wirksam erhöht werden. Daten, die mit einem ausreichenden Niveau verschlüsselt in die Cloud gegeben werden, könnten ohne weiteres Risiko vom Cloud-Anbieter behandelt werden wie nicht-personenbezogene Daten. Technischer Datenschutz ist allerdings aufwändig und oft mit Kosten verbunden. Um die Möglichkeiten des technischen Datenschutzes zu nutzen, muss der Gesetzgeber dazu die richtigen Anreize setzen. Diese Perspektive sollte im anstehenden Review des europäischen Datenschutzes beachtet werden. Dort sollten Anreize für die Pseudonymisierung und Anonymisierung von zu verarbeitenden personenbezogenen Daten gesetzt werden, indem noch deutlicher herausgestellt wird, dass anonymisierte Daten keine personenbezogenen Daten sind und indem für die Verarbeitung pseudonymisierter Daten gezielt erleichterte Bedingungen geschaffen werden, wie dies teilweise im deutschen Datenschutzrecht schon heute der Fall ist⁴.

3.1.3 Klare Regelungen für Auftragsdatenverarbeitung

Entscheidend für die Weiterentwicklung von Cloud Computing sind außerdem klare Regelungen zur Auftragsdatenverarbeitung - insbesondere zur Aufteilung der Zuständigkeiten und Verantwortlichkeit. Die im Entwurf vorgeschlagenen Vorschriften zur Auftragsverarbeitung passen strukturell nicht auf einige Formen des Cloud Computings und würden diese daher erschweren. Um Praxistauglichkeit zu erreichen, sollte klargestellt werden, dass die Auftragsverarbeitung grundsätzlich zulässig ist. Die vorgeschlagenen Regelungen sollten unter Berücksichtigung der folgenden Punkte noch sorgfältig überarbeitet werden:

- Die Verantwortung von Verantwortlichem und Auftragsverarbeiter sollten weiterhin klar getrennt sein und der Auftragsverarbeiter nur in dem vertraglich bestimmten Rahmen für die Datenverarbeitung verantwortlich sein. Das beinhaltet auch die Bestimmungen über die Sicherheit der Auftragsverarbeitung. Allein der Verantwortliche kann bestimmen, wie wichtig die Daten für ihn sind und wie sie geschützt werden müssen. Die Verteilung der Verantwortlichkeit zwischen Verantwortlichem und Auftragsverarbeiter (Art. 22, 24, 26, 27, 28 des Verordnungsentwurfs) wird aus dem Entwurf nicht ausreichend deutlich.⁵

⁴ Vgl. Bundesdatenschutzgesetz, § 5 (3).

⁵ In zahlreichen Vorschriften werden der Verantwortliche und der Auftragsverarbeiter gleichzeitig genannt. Im Sinne einer klaren Verantwortlichkeitszuordnung auf die verantwortliche Stelle müssten in den entsprechenden Vorschriften der Bezug zum Auftragsverarbeiter gestrichen werden.

Stellungnahme

EU-Cloud-Strategie

Seite 7

- Über die vertraglich vereinbarten Pflichten hinaus sollten Auftragsverarbeiter nur für diejenigen Pflichten verantwortlich sein, die in ihrem Aufgabenbereich liegen, wie z.B. die notwendigen Schutzvorkehrungen zu treffen (z.B. Privacy by Design) und angemessene Sicherheitssysteme einzusetzen.
- Dementsprechend sollten sich Kunden, denen durch entsprechende Zertifizierung⁶ im Vorfeld bestätigt wird, dass entsprechende Sicherheitsstandards eingehalten werden, darauf verlassen dürfen, ohne ihrerseits zusätzlichen Kontrollpflichten nachkommen zu müssen. Gegenstand des Testats ist die gesetzlich geforderte Überprüfung des Auftragnehmers durch den Auftraggeber anhand eines standardisierten Anforderungskatalogs.⁷ Die Ersetzbarkeit der Überprüfung des Auftragnehmers durch ein Testat sollte gesetzlich verankert werden.
- Es sollte eine erleichterte Vertragsgestaltung bei Auftragsverarbeitern (Cloud-Anbieter) eingeführt werden, wenn deren Dienstleister (z.B. für die Wartung von Betriebsanlagen) geeignete Zertifikate oder Binding Corporate Rules nachweisen können. In diesen Fällen wären auch Problemanalysen durch den Dienstleister zulässig, selbst wenn dieser seinen Sitz in einem ansonsten nicht-sicheren Drittland hat. Für die Zulässigkeit von Problemanalysen durch den Dienstleister in einem ansonsten nicht-sicheren Drittland gelten zwei weitere Voraussetzungen: Erstens ist die Weitergabe und denkbare Kenntnisnahme von personenbezogenen Daten nur ein technisch unvermeidliches Ereignis im Rahmen einer Problemanalyse. Und zweitens ist eine Problemanalyse erforderlich, um z.B. den Betrieb aufrecht zu erhalten bzw. zu gewährleisten.
Nach geltender Rechtslage wäre dies nur über direkte Vertragsverhältnisse zwischen allen Verarbeitungs-Verantwortlichen und allen gegebenenfalls eingebundenen Dienstleistern des Auftragsverarbeiters möglich.
- möglich.

3.1.4 Geltung von standardisierten Vertragsklauseln

BITKOM regt eine Klarstellung durch die EU-Kommission an, dass die Standardvertragsklauseln von europäischen Cloud-Anbietern auch bei Vertragsverhältnissen innerhalb der EU verwendet werden dürfen. Die Standardvertragsklauseln sollten so neu gefasst oder geändert werden, dass sie auch von europäischen Cloud-Anbietern verwendet werden können, die Unterauftragnehmer außerhalb der EU beschäftigen möchten.

Bis Ende 2013 wird die Kommission mit den Interessenträgern Musterbedingungen für das Cloud-Computing zur Verwendung in Leistungsvereinbarungen zwischen Cloud-Anbietern und gewerblichen Cloud-Nutzern aufstellen und dabei der Entwicklung des EU-Rechts auf diesem Gebiet Rechnung tragen.-Diese Maßnahme ist sehr zu begrüßen, denn verbindliche Standardvertragsklauseln sind für die Auftragsdatenverarbeitung ein wichtiges Instrument zur rechtskonformen vertraglichen Ausgestaltung von IT-Dienstleistungen. Sie dienen auch der Verkürzung und Vereinfachung von Vertragsverhandlungen und sparen den Beteiligten damit Kosten. Die Verwendung von Standardvertragsklauseln ist insbesondere Voraussetzung für den Export personenbezogener Daten in Drittstaaten, wie er im Rahmen von Cloud-Computing-Angeboten öfter vorkommt. Allerdings gibt es im Cloud Computing auch oftmals Konstellationen, in

⁶ Auf Fragen der Zertifizierung geht die Stellungnahme im Unterkapitel 3.2 im Detail ein.

⁷ Vorschlag der Rechtsarbeitsgruppe der Trusted-Cloud-Initiative des Bundesministeriums für Wirtschaft und Technologie. Vgl.: http://www.trusted-cloud.de/documents/Thesenpapier_Datenschutz.pdf

Stellungnahme

EU-Cloud-Strategie

Seite 8

denen ein europäischer Anbieter personenbezogene Daten seines europäischen Kunden bei Unterauftragnehmern in Drittstaaten verarbeiten lässt⁸. Momentan darf allerdings der europäische Anbieter im Gegensatz zu nicht-europäischen Anbietern gegenüber seinem nicht-europäischen Unterauftragsverarbeiter nicht die EU-Standardvertragsklauseln verwenden.⁹ Das bedeutet, dass ein nichteuropäischer Cloud-Anbieter ein Standardverfahren an die Hand bekommt, nach dem er Daten im Auftrag eines europäischen Kunden (für die Verarbeitung Verantwortlichen) mithilfe nichteuropäischer Unterauftragnehmer verarbeiten darf, während dies einem europäischen Cloud-Anbieter verwehrt bleibt. Hierin liegt ein Wettbewerbsnachteil für europäische Cloud-Anbieter.

Europäische Cloud-Anbieter sollten daher dieselben standardisierten Vertragsklauseln sowohl im Verhältnis zum Kunden als auch im Verhältnis zu inner- und außereuropäischen Unterauftragnehmern verwenden können. Dies würde Wettbewerbsnachteile verringern, bürokratischen Aufwand reduzieren und auch zu mehr Transparenz und Rechtsklarheit führen.

3.1.5 Einführung extraterritorial geltenden Rechts - Beseitigung rechtlicher Grauzonen

BITKOM regt eine transatlantische Initiative zur Beseitigung rechtlicher Grauzonen an, die durch die Einführung extraterritorial geltenden Rechts entstanden sind. Nicht nur für Cloud Anbieter, sondern für alle datenverarbeitenden Unternehmen, die auf beiden Seiten des Atlantiks Datenverarbeitung durchführen, stellen gegenläufige rechtliche Verpflichtungen aus der amerikanischen und der europäischen Rechtsordnung eine erhebliche Rechtsunsicherheit dar. Es sollte an einem gemeinsamen Verständnis gearbeitet werden, unter welchen Voraussetzungen Unternehmen zur Herausgabe von personenbezogenen Daten zur Bekämpfung des Terrorismus verpflichtet werden können. Entsprechend sollten dann auch die Pflichten aus dem jeweiligen Datenschutzrecht angepasst werden.

3.2 Flexibilität durch Selbstverpflichtungen und Zertifizierung

BITKOM regt an, Erleichterungen für die Wahrnehmung der Weisungs- und Kontrollbefugnisse des Cloud-Kunden bei Inanspruchnahme von Cloud-Diensten zu schaffen - durch Förderung von Selbstverpflichtungen¹⁰ und Verhaltenskodizes sowie deren Anerkennung als Nachweis zur Erfüllung der Sorgfalts- und Kontrollpflichten des Cloud-Kunden. Es sollten freiwillige Zertifikate mit

⁸ Zum Beispiel werden dort angebotene Speicherkapazitäten in Anspruch genommen.

⁹ Vgl. Ziffer 23 des Beschlusses 2010/87/EU. Ein europäischer Cloud-Anbieter, der einige Verarbeitungsaufgaben an Unterauftragnehmer vergeben möchte, muss die im Kommissionsbeschluss 2010/87/EU niedergelegten Standardvertragsklauseln verwenden. Er kann sie aber nicht unmittelbar übernehmen. Da die Standardvertragsklauseln ausschließlich den direkten Datenexport durch den für die Verarbeitung Verantwortlichen an nichteuropäische Unterauftragsverarbeiter zulassen (vgl. Ziffer 5 des Beschlusses 2010/87/EU der Kommission), muss ein europäischer Cloud-Anbieter seine Kunden als die für die Verarbeitung der Daten Verantwortlichen davon überzeugen, dass sie in eigenen Verträgen mit nichteuropäischen Unterauftragsverarbeitern die Standardvertragsklauseln übernehmen. Erst wenn den rechtlichen Vorschriften mit solchen Datenschutzvereinbarungen Genüge getan wurde, kann der Cloud-Anbieter die Verträge seinerseits unterzeichnen. Diese direkt zwischen Kunden und Unterauftragsverarbeitern geschlossenen Datenschutzvereinbarungen, die je nach Zahl der Unterauftragnehmer sehr zahlreich sein können, müssten dann natürlich zusätzlich zu den innereuropäischen Datenschutzvereinbarungen abgeschlossen werden, mit denen der Kunde und der Cloud-Anbieter diejenigen Verarbeitungsleistungen rechtlich absichern, die der europäische Cloud-Anbieter selbst erbringt.

¹⁰ Selbstverpflichtungen auf Community- und Verbandsebene sind individuellen Selbstverpflichtungen von Unternehmen vorzuziehen.

Stellungnahme

EU-Cloud-Strategie

Seite 9

einheitlichen und transparenten Prüfverfahren durch sachverständige Dritte als Nachweis der Erfüllung der Kontrollpflichten des für die Datenverarbeitung Verantwortlichen etabliert werden. Schließlich sind die Anforderungen an die Datensicherheit im Rahmen von Cloud-Dienstleistungen weiter zu entwickeln und entsprechende Rahmen für Zertifizierungen zu setzen.

- Cloud-Kunden, die personenbezogene und andere schützenswerte Daten in die Cloud geben, tragen die Verantwortung, dass diese entsprechend deren unterschiedlich ausgeprägten Schutzbedarf angemessen geschützt werden. Der Schutzbedarf ist abhängig davon, welche Gefahren für die Rechte und Freiheiten der Betroffenen mit der konkreten Verarbeitung einhergehen. Entscheidender Faktor neben der Art der Daten ist der inhaltliche und infrastrukturelle Kontext der Datenverarbeitung. Um dieser Verantwortung gerecht zu werden, müssen Cloud-Kunden ihre Dienstleister sorgfältig aussuchen und überprüfen. Für die Auswahl brauchen sie Angaben, anhand derer sie die Eignung eines Anbieters für ihre Datenverarbeitungszwecke erkennen können. Was die Kontrollpflichten angeht, so sind sie für den Cloud-Kunden oftmals nicht umfassend selbst zu bewältigen, da es einer Cloud-Infrastruktur immanent ist, dass sie gerade nicht an bestimmte Orte gebunden ist..
- Ein guter Ansatz für mehr Transparenz und Unterstützung der Cloud-Kunden bei ihren Kontrollpflichten ist ein abgestimmtes System von qualitativ vergleichbaren Arten von Nachweisen, wie z.B. Selbstverpflichtungen, branchenspezifische Verhaltenskodizes und Zertifizierungen, die imstande sind, die Konformität der Datenverarbeitung mit den gesetzlichen Vorschriften – und den besonderen Anforderungen des jeweiligen Unternehmens oder bestimmter Branchen – festzustellen und gegenüber den Betroffenen zu bezeugen.
- Ein solches System würde sowohl dem Betroffenen, der seine Daten in eine Cloud gibt, als auch der verantwortlichen Stelle, die die Cloud für Unternehmensdaten nutzt, die Entscheidung erleichtern, welcher Nachweis in der für sie relevanten Situation sinnvoll und angemessen ist.¹¹
- Mit der Anerkennung der Vorlage von Selbstverpflichtungen als Nachweis für die Erfüllung der Kontrollpflichten des für die Verarbeitung Verantwortlichen werden Vor-Ort-Kontrollen vermieden.
- Es wird Konstellationen geben, in denen ein Bedarf des Anbieters oder des Kunden nach einem besonderen Nachweis für die Einhaltung der Datenschutzvorschriften bzw. besonderer Vorkehrungen für ein hohes Datenschutz und Datensicherheit-Niveau besteht. Hierfür müssen entsprechende Nachweise in Form von Zertifizierungen gefördert und anerkannt werden.
- Um dieser Zielsetzung gerecht zu werden, sollte die Zertifizierung eine angemessene Prüftiefe und -weite aufweisen. Der Bedarf des einzelnen Cloud-Kunden oder -Nutzers ist - abhängig von seinem Kontext - sehr unterschiedlich. „Allgemeine“ Zertifikate würden daher eher verwirren als nutzen. Deshalb ist es unentbehrlich, einen allgemeingültigen Rahmen der Zertifizierung zu erarbeiten und innerhalb dieses Rahmens die branchenspezifischen Anforderungen zu ermitteln, die dann für die Zertifizierung geprüft würden.
- Um die externen Aufwände der Zertifizierung für die Unternehmen zu minimieren, sollte die Zertifizierung als eine nachträgliche Überprüfung der internen Prozesse zum Datenschutz konzipiert werden. Die Dokumentation der

¹¹ Damit würde die Ausübung des Selbstbestimmungsrechts durch den Betroffenen und die Verantwortungsübernahme durch die verantwortlichen Stellen optimal unterstützt.

Stellungnahme

EU-Cloud-Strategie

Seite 10

inneren Prozesse und die Zertifizierung sollten zudem auf den gleichen Prinzipien beruhen.

- Zertifizierungsmöglichkeiten sollten einem einheitlichen, objektiven Standard folgen, der eine Vergleichbarkeit der Anbieter und ihrer Datenschutzmaßnahmen ermöglicht. 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.¹² Dabei sind Möglichkeiten zu schaffen, welche die Schutzbedürftigkeit der Daten berücksichtigen.¹³ Das Testat sollte 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.¹⁴ Bei der Spezifizierung von Zertifizierungen sind neben den notwendigen Mindest-Qualitätsstandards auch die Kosten-Nutzen-Aspekte für Cloud-Provider zu betrachten.
- Die Voraussetzungen der Akkreditierung von testierenden Stellen sollten in einem Verfahren von Vertretern der Datenschutz-Aufsichtsbehörden und Vertretern der Auftraggeber und Auftragnehmer von Auftragsdatenverarbeitung festgelegt werden. Die Akkreditierung sollte für den gesamten Geltungsbereich der EU-Datenschutz-Verordnung gelten und durch geeignete, insbesondere fachlich qualifizierte und unabhängige Stellen erfolgen. Die EU-Datenschutz-Verordnung sollte die Anforderungen an die Akkreditierungsstellen im Grundsatz regeln, jedoch die Benennung der Akkreditierungsstellen den Mitgliedsstaaten überlassen.
- Neben dem Datenschutz gibt es noch eine Reihe weiterer Themen, bei denen es sinnvoll ist, Anbietern die Möglichkeit zu geben, für ihren Dienst die rechtliche Eignung selbst zu erklären. Ergänzend zu den datenschutzrechtlichen Selbstverpflichtungen kann eine Selbsterklärung Aussagen zu Compliance mit nationalen Rechtsordnungen, Interoperabilität, Datenportabilität und zur Servicequalität enthalten und somit redundante Zertifikate und den damit verbundenen Zertifizierungsaufwand ersetzen.
- Bei der Zertifizierung ist es wichtig, dass Normen und Zertifizierungen sich an bereits bestehende und allgemein in der Branche akzeptierte Ansätze wie z.B. ISO 27001 anlehnen, die um essentielle Cloud-Spezifika ergänzt werden. Dies schafft einen erheblichen Geschwindigkeitsvorteil und vermeidet gleichzeitig wettbewerbsrelevante Mehrkosten durch neue Zertifizierungen.

3.3 Vertragsrecht für Cloud Computing

Mit einer europäischen Cloud-Strategie und den daraus abgeleiteten Maßnahmen besteht die Chance, den vertragsrechtlichen Aufwand für internationale Cloud-Computing-Verträge zu reduzieren.

Bei der Diskussion um eine Fortentwicklung des Rechtsrahmens für Cloud-Verträge darf jedoch nicht vergessen werden, dass die Unternehmen bereits eine funktionierende Praxis in der Gestaltung von Cloud-Verträgen auf der Basis nationaler Rechtsordnungen etabliert haben.

¹² Vgl.: http://www.trusted-cloud.de/documents/Thesenpapier_Datenschutz.pdf

¹³ Z.B. müssen medizinische Daten oder Daten, die einem Berufsgeheimnis unterliegen, durch höherwertige Schutzmaßnahmen abgesichert werden als Adressdaten eines Onlinegewinnspiels.

¹⁴ Vgl.: http://www.trusted-cloud.de/documents/Thesenpapier_Datenschutz.pdf

Stellungnahme

EU-Cloud-Strategie

Seite 11

3.3.1 Cloud-Verträge haben eigene Anforderungen

Die Gestaltung von Cloud-Verträgen muss zwar vielfach Anforderungen berücksichtigen und Vertragsabreden konzipieren, die aus anderen rechtlichen Gestaltungen bereits bekannt sind. Es wäre jedoch nicht angemessen, Geschäftsmodelle des Cloud Computings in vorhandene Muster für andere vertragliche Konstellationen zu pressen. In diesem Sinne ist ein Vergleich zwischen Cloud Computing und Outsourcing sowie zwischen den dafür jeweils geltenden rechtlichen Anforderungen nicht zielführend. Cloud-Leistungen sind meistens sehr spezifisch und auf einen bestimmten, klar definierten Zweck beschränkt, setzen kein vorheriges Vergabeverfahren voraus und sind auch nicht mit einem Personalübergang verbunden.

Ebenso wenig passt das europäische Kaufrecht für Cloud-Verträge und ist als Rechtsgrundlage für solche Verträge nicht geeignet. Es ist bereits fraglich, ob das Herunterladen digitaler Inhalte aus dem Internet schon als Cloud-Dienst anzusehen ist. Geschäftsbeziehungen im Cloud Computing basieren überwiegend auf Miete und Dienstvertrag. Außerdem ist derzeit nicht absehbar, wann und ob überhaupt die Verordnung zum Europäischen Kaufrecht in Kraft treten wird. Eine Unterstützung für die Gestaltung von Cloud-Verträgen hilft in der Praxis aber nur weiter, wenn sie schnell gewährt wird sowie angemessene und einfach zu verstehende Vertragsgestaltungen ermöglicht.

3.3.2 Unverzichtbare Vertragsbestandteile im Cloud Computing

Auf bestimmte Vertragsbestandteile kann in Cloud Computing-Geschäftsbeziehungen nicht verzichtet werden. Hierzu gehören beispielsweise die Festlegung von Leistungsparametern in Service Level Agreements (SLA) und die Abgrenzung von Aufgaben und Verantwortlichkeiten zwischen Cloud-Anbieter und Cloud-Nutzer. SLA dienen auch dazu, um festzustellen, ob und in welchem Umfang die vereinbarte Cloud-Leistung erbracht wurde und ob ggf. Gewährleistungsansprüche oder Vertragsstrafen geltend gemacht werden können. Wenn die EU-Kommission Beispiele für ausgewogene SLA vorschlagen würde, wäre dies für die Vertragspraxis sicher hilfreich.

3.3.3 Plädoyer für faire und KMU-taugliche Muster-Vertragsklauseln

Vertragsbedingungen für Cloud-Verträge sowohl im B2B-Bereich als auch im B2C-Bereich sollten Fragen zur Aufbewahrung und Rück- bzw. Weiterübertragung der Daten nach Vertragsende, Offenlegung und Integrität der Daten, zum Datenschutz, zum Speicherort von Daten, zur Abgrenzung der Datenverantwortlichkeit zwischen Cloud-Anbieter und Cloud-Nutzer, zur Haftung für Störungen des Cloud-Dienstes und für Datenverlust, zur Einschaltung von Unterauftragnehmern und zur Beilegung von Streitigkeiten aus der Cloud-Geschäftsbeziehung beantworten. Es wäre daher für die Vertragspraxis eine große Hilfe und eine gute Orientierung, wenn die EU-Kommission möglichst bis Ende 2013 Überlegungen zur vertraglichen Regelung dieser Fragen in Form von Muster-Vertragsformulierungen veröffentlichen würde. Wegen der unterschiedlichen Interessenlage sollten voneinander unabhängige Musterbedingungen für Verträge mit Verbrauchern (B2C) und für Verträge zwischen Unternehmen (B2B) geschaffen werden. Als Unterscheidungskriterium könnte die Kaufmanneigenschaft des Cloud-Kunden herangezogen werden. Tritt der Cloud-Kunde als Kaufmann auf, gelten die B2B-Regeln. In beiden Konstellationen sollten sich solche Musterklauseln für Cloud-Verträge an den Regelungen für Dienst- und Mietverträge orientieren, um die typischen Vertragsbeziehungen im Cloud Com-

Stellungnahme

EU-Cloud-Strategie

Seite 12

puting adäquat abzubilden. Die Regelungen dürften jedoch nicht zu kompliziert sein, müssten auf das jeweilige Cloud-Geschäftsmodell angepasst werden können und für die Vertragsparteien des Cloud-Vertrages fakultativ sein.

Bei der Gestaltung von Mustervertragsbedingungen durch die EU muss auch darauf geachtet werden, dass die Klauseln dem jeweiligen innerstaatlichen Recht entsprechen und nicht z.B. an einer nationalen AGB-Kontrolle scheitern. Denn für die Cloud-Anbieter muss Rechtssicherheit über die Wirksamkeit der Muster-Vertragsklauseln bestehen.

Bei der Forderung nach fairen Vertragsbedingungen im Cloud Computing für kleine Unternehmen (und Verbraucher) darf nicht vergessen werden, dass kleine Unternehmen vielfach auch als Cloud-Anbieter auftreten. Damit dies nicht gefährdet wird, wäre darauf zu achten, dass die vertragsrechtlichen Vorgaben in Cloud-Musterverträgen auch von kleinen Unternehmen erfüllt werden können und sie nicht überfordern.

3.3.4 Regelungsbedarf bei rechtlichen „Randbedingungen“ für Cloud Computing

Gesetzlicher Regelungsbedarf besteht bei den rechtlichen „Randbedingungen“ für Cloud Computing, also bei den Vorschriften, die bestimmte Anforderungen an Daten und an den Umgang mit Daten stellen (Datenverarbeitung, -nutzung, -zugang und -speicherung). Diese Anforderungen müssten europaweit vereinheitlicht und für die Datenverarbeitung im Wege des Cloud Computings optimiert werden.

So sind beispielsweise die Datensicherheit (Haftung des Cloud-Anbieters bei Datenverlust), die Insolvenzsicherheit der Daten (ordnungsgemäße Datenrückgabe im Insolvenzfall des Anbieters), Datenschutz und Archivierungsanforderungen noch nicht EU-weit vereinheitlicht und auf Cloud-Anwendungen ausgerichtet.

3.3.5 Verbraucherschutz in Cloud-Computing-Verträgen austarieren

Wie bereits ausgeführt, unterscheiden sich Cloud-Vertragsbeziehungen zwischen Unternehmen (B2B) einerseits und Cloud-Vertragsbeziehungen zu Verbrauchern (B2C) andererseits deutlich.

Bei den Vertragsbedingungen für Cloud-Computing-Verträge im B2C-Geschäftsverkehr müssen die Interessen der Verbraucher und die Möglichkeiten der Cloud-Anbieter in einen angemessenen Ausgleich gebracht werden. Dabei ist zu berücksichtigen, dass die Kostenvorteile von Cloud-Angeboten nur realisiert werden können, wenn ihr Charakter als leicht skalierbare Standard-Leistung erhalten bleibt. Des Weiteren muss gewährleistet sein, dass Vertragsbedingungen in B2C-Cloud-Verträgen im Einklang mit nationalem Verbraucherschutzrecht stehen und damit Rechtssicherheit bieten. Zugleich müssen standardisierte Vertragsbedingungen in ihrem jeweiligen Regelungsbereich abschließend verwendet werden können. Diese Anforderungen sind besonders wichtig, wenn kleine und mittelständische Unternehmen als Anbieter von Cloud-Leistungen auftreten. Der besondere Nutzen von standardisierten Vertragsklauseln besteht gerade in der Vereinheitlichung und in der Möglichkeit eines umfassenden Anwendungsbereiches.

Stellungnahme

EU-Cloud-Strategie

Seite 13

3.3.6 Ablehnung zwingender vertragsrechtlicher Vorgaben des Europarechts für Cloud-Computing-Verträge

Die Erarbeitung von Mustervertragsklauseln für den B2B- und den B2C-Bereich ist zu begrüßen. Von der Vorgabe eines zwingenden europäischen Vertragsrechts sollte dagegen abgesehen werden, da sie nicht sachgerecht wären. Die Vielgestaltigkeit einzelner Cloud-Geschäftsmodelle erfordert eine erhebliche Flexibilität der vertragsrechtlichen Regelungen und steht einer einheitlichen zwingenden Gesetzesregelung im Wege. Folglich kann es keinen einheitlichen und fest definierten gesetzlichen Vertragstyp „Cloud-Vertrag“ geben.

3.4 Öffnung des Zugangs zu Inhalten – Vorschläge und Kommentare

Um die Wertschöpfung mit Cloud-Musik-Angeboten in einem europäischen Binnenmarkt zu fördern, ist eine Flexibilisierung und Modernisierung von Verwertungsgesellschaften notwendig. Die Regulierung ihrer De-facto-Monopole durch staatliche Aufsicht und Kontrolle darf auch ihre Tochtergesellschaften nicht ausschließen.

Wir betrachten daher die mit dem vorliegenden Entwurf einer Richtlinie über kollektive Rechtewahrnehmung in Europa adressierten Problemstellungen als wichtige Weichenstellungen für die Schaffung eines europäischen Binnenmarktes für kreative Inhalte. Die dort adressierten Handlungsfelder greifen jedoch vielfach zu kurz.¹⁵

4. Public Sector – Förderung einer gemeinsamen Führungsrolle des öffentlichen Sektors durch eine europäische Cloud-Partnerschaft

BITKOM hat in einem gemeinsam mit VOICE - Verband der IT-Anwender e.V. entwickelten Positionspapier¹⁶ gefordert, den Einsatz von Cloud Computing in der öffentlichen Verwaltung zu forcieren. Die in diesem Positionspapier enthaltenen Empfehlungen gehen konform mit der Schlüsselaktion 3 in der EU-Cloud-Strategie. Die Kommentare und Hinweise gelten für die Situation in Deutschland und müssten für die anderen EU-Länder verifiziert werden.

Cloud Computing liefert für die vielfältigen Anforderungen des öffentlichen Dienstes gute Lösungen. Bislang werden die Chancen aber gerade im öffentlichen Sektor kaum genutzt. Der breiten Anwendung von Cloud Computing in der öffentlichen Verwaltung stehen Bedenken zu Sicherheit und Datenschutz sowie Vergabe- und Haushaltsrecht entgegen. Aber auch die strategische Ausrichtung ist in vielen Bereichen noch offen.

Funktionierende Pilotprojekte der öffentlichen Verwaltung können wichtige Initialzündungen und Benchmarks für die Wirtschaft sein. Sie stärken das Vertrauen in die neue Technologie und erhöhen ihre Akzeptanz.

BITKOM fordert die Vorreiterrolle öffentlicher Verwaltungen bei der Umsetzung von Cloud Computing. Der Verband regt die Erarbeitung eines Strategiepapiers, eines Stufenplanes und eines Governance-Rahmens zur Umsetzung für Verwaltungs-Clouds in den EU-Ländern an.

4.1 Orientierung an offenen Standards

Die Öffentlichen Verwaltungen müssen beispielgebend sein, indem sie sich auf Standards für die öffentlichen Verwaltungen festlegen, Interoperabilität zwischen

¹⁵ Für weitere Details sei auf die ausführliche Stellungnahme zum aktuellen Richtlinien-Entwurf verwiesen.: http://www.bitkom.org/de/themen/59922_73400.aspx

¹⁶ Vgl. BITKOM/VOICE, Februar 2012, „Empfehlungen für den Cloud Computing-Standort Deutschland“

Stellungnahme

EU-Cloud-Strategie

Seite 14

Cloud-Diensten durch Nutzung der Standards und Prozessen ermöglichen, bei der Ausschreibung öffentlicher Cloud-Projekte die Einhaltung von Standards vorgeben und einfordern sowie verstärkt in Cloud Computing investieren. Vertrauen in Cloud Anbieter kann nur durch offene Standards entstehen. Offene Standards werden international entwickelt und müssen in den entsprechenden nationalen Gremien berücksichtigt werden. Die Aussagen im Abschnitt 2 gelten auch für die Öffentliche Verwaltung.

4.2 Akzeptanz elektronischer Dokumente unterstützen

Für den medienbruchfreien Ablauf elektronischer Verwaltungsprozesse ist es notwendig, elektronisch erstellte Dokumente und Urkunden anzuerkennen, die u.U. in einer Cloud-Umgebung, beispielsweise einem elektronischen Safe, abgelegt und Verwaltungen wiedervorgelegt werden können.

Eine querschnittliche Herausforderung für alle Verwaltungsebenen und alle Fachressorts ist der Übergang von der bisherigen hybriden Aktenführung hin zum einem vollständig elektronischen Dokumentenmanagement.

Das Nebeneinander von elektronischen Dokumenten und Papierdokumenten verteuert und behindert elektronische Workflows.

Eine wichtige Basis für Dokumentenmanagementsysteme der Verwaltungsebenen und die Mitzeichnungsverfahren bei mehrstufigen Verwaltungsentscheidungen ist der Einsatz von elektronischen Signaturen. Elektronische Signaturen gewährleisten im Binnenverhältnis die Integrität, Authentizität und eine beweissichere Unterschrift sowie Zeitstempelfunktionen. Auch die Archivierung erfordert eine langfristige Überprüfbarkeit.

Auf der anderen Seite wird empfohlen, für weniger komplexe Verfahren die Vorschriften und Gesetze so zu vereinfachen, dass elektronische Dokumente einfach genutzt werden können. So könnten z. B. die Prinzipien der eRechnung ohne Signatur als zertifikatsfreie Basis für elektronische Dokumente etabliert werden. Dann ist ein innerbetriebliches bzw. -behördliches Kontrollverfahren mit Prüfpfad für Authentizität und Integrität ausreichend – was zu signifikanten Prozessverbesserungen führt. Als Beispiel kann ZUGFeRD herangezogen werden, der vom BITKOM favorisierte neue Standard für elektronische Rechnungen.

5. Infrastruktur - Breitbandausbau für Cloud Computing

Aus Sicht des BITKOM werden im internationalen Wettbewerb jene Standorte profitieren, an denen Cloud Services schnell, sicher und einfach verfügbar sind.

Eine moderne Breitbandinfrastruktur ist hierbei Grundvoraussetzung und Basis zugleich für eine breite Nutzung Cloud-basierter Innovationen in Wirtschaft, Wissenschaft und Gesellschaft. Der Ausbau neuer Infrastrukturen ist für Europa von herausragender gesellschafts- und wirtschaftspolitischer Bedeutung.

Die reibungslose Cloud-basierte Speicherung und Verarbeitung von Daten erfordert hohe Übertragungskapazitäten und in dieser Konsequenz eine Infrastruktur, die in den Ballungszentren, aber auch im ländlichen Raum breitbandig zur Verfügung steht. Die bisherigen Ansätze, mittels Infrastrukturprogrammen die Breitband-Versorgung zu verbessern, haben in den vergangenen Jahren zur signifikanten Schließung sogenannter „weißer Flecken“ geführt. Nach wie vor stehen die Anbieter vor der Herausforderung, massiv in die Infrastruktur investieren zu müssen.

Um den Ausbau von Hochgeschwindigkeitsnetzen über die bisherigen Erfolge hinaus zügig mit wettbewerblichen Mitteln voranzubringen, ist es unumgänglich,

Stellungnahme

EU-Cloud-Strategie

Seite 15

für ein entsprechendes regulatorisches Umfeld zu sorgen und alle Synergien für den Netzaufbau zu nutzen. Regulierung darf kein Risiko für Investitionen sein, sondern muss die Auswirkungen auf Investitionen und Arbeitsplätze mehr als bislang berücksichtigen.

6. Stellung von Europa im Cloud Computing und internationale Kooperation

Der BITKOM unterstützt ausdrücklich die in Unterkapitel 4.2 der EU-Cloud-Strategie angekündigte internationale Kooperation. Eine solche Kooperation ist insbesondere für die Förderung des Wachstums europäischer IT-Unternehmen bedeutsam. Bekanntlich ist die Internationalisierung nach wie vor eine Hürde, die IT-Unternehmen zu einem relativ frühen Zeitpunkt nehmen müssen, um langfristig wachsen zu können. Aufgrund der kleinen Heimatmärkte ist die europäische Koordinierung bezüglich gesetzlicher Anforderungen und Standards notwendig, jedoch global nicht hinreichend. BITKOM setzt sich für eine Neubelebung der transatlantischen Wirtschaftspartnerschaft und Unterstützung der Cloud-Arbeitsgruppe des Transatlantic Economic Council zur Schaffung eines gemeinsamen Cloud-Rechtsrahmens ein.

Cloud-Computing nimmt in einer solchen transatlantischen Wirtschaftsagenda eine Schlüsselstellung ein, da es die zentrale Wirtschaftsplattform der Zukunft sein wird. Mit der Entwicklung eines transatlantischen Cloud-Marktes, der durch geringe Transaktionskosten und hohes Vertrauen geprägt ist, wird eine der prägenden Infrastrukturen des 21. Jahrhunderts definiert.

Die EU sollte ihre führende Rolle in den Bereichen Datenschutz und –sicherheit auch in internationalen Gremien nutzen und ihre Stärken in den Bereichen Software as a Service sowie Business Process as a Service gezielt ausbauen. In diesem Sinne sollte Unterkapitel 4.2 um konkrete Maßnahmen ergänzt werden:

- Unterstützung der Cloud-Arbeitsgruppe des Transatlantic Economic Council zur dauerhaften Verankerung einer gemeinsamen Cloud-Perspektive: Alle Gesetzgebungs- und Verordnungsmaßnahmen, die Cloud Computing betreffen, sollten regelmäßig dem Transatlantic Economic Council zur Bewertung der Auswirkungen auf den transatlantischen Wirtschaftsraum vorgelegt werden.
- Stärkung der Konvergenzbestrebungen zwischen den Rechtssystemen: Langfristig ist die Konvergenz der Rechtsnormen zum Thema Cloud Computing ein wichtiges Ziel. Zu diesem Zweck sollten Regierungsvertreter beider Seiten frühzeitig in laufende Gesetzgebungsverfahren eingebunden werden.
- Stärkung von Brückenmechanismen wie „Safe Harbor“: Brückenmechanismen, die die Unterschiede zwischen den Rechtssystemen wirtschaftsfreundlicher gestalten, sind von strategischer Bedeutung. Diese hohe Bedeutung spiegelt sich zurzeit nur unzureichend in der politischen Arbeit wider. BITKOM wirbt für eine Weiterentwicklung von Safe Harbor, die unter anderem eine Härtung der Umsetzungs- und Kontrollmechanismen auf beiden Seiten des Atlantiks beinhaltet.
- Etablierung gemeinsamer Forschungsschwerpunkte im Bereich Cloud Computing, um mittelfristig die Konvergenz der Cloud-Politik zu fördern (Datenschutz, Verschlüsselung, Protokollierung von Datenzugriffen, Standardisierung)
- Unterstützung der multilateralen und bilateralen Gespräche der EU zu Cloud-Computing-Fragen.