



Empfehlungen für den Cloud Computing-Standort Deutschland

■ Impressum

Herausgeber:	BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. Albrechtstraße 10 A, 10117 Berlin-Mitte Tel.: 030.27576-0 Fax: 030.27576-400 bitkom@bitkom.org www.bitkom.org	VOICE Verband der IT-Anwender e.V. Inselkammerstr. 10 82008 Unterhaching Tel.: 089.8982797-15 Fax: 089.8982797-79 Info@voice-ev.org www.voice-ev.org
Ansprechpartner:	Dr. Mathias Weber Tel.: 030.27576-121 m.weber@bitkom.org	Christoph Hecker Tel.: 089.8982797-15 christoph.hecker@voice-ev.org
Verantwortliche Gremien:	BITKOM AK Cloud Computing und Outsourcing AK Datenschutz	VOICE SIG Daten- und Rechtssicherheit in der Cloud
Projektleitung:	Gerald Münzl (House of IT e.V.) Dr. Mathias Weber (BITKOM)	
Copyright:	BITKOM und VOICE 2012	
Grafik/Layout:	Design Bureau kokliko/ Astrid Scheibe (BITKOM)	
Titelbild:	Daniela Stanek (BITKOM)	

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung von BITKOM und VOICE zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen bei BITKOM und VOICE.

Empfehlungen für den Cloud Computing-Standort Deutschland

Verzeichnis der Abkürzungen

AGB	Allgemeine Geschäftsbedingungen
ANSI	American National Standards Institute
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BITKOM	BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BMWi	Bundesministerium für Wirtschaft und Technologie
BSI	Bundesamt für Sicherheit in der Informationstechnik
CCUCDG	Cloud Computing Use Case Discussion Group
CDP	Commissioned Data Processing (Auftragsdatenverarbeitung)
DMTF	Distributed Management Task Force
ECMA	European Computer Manufacturers Association
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
GG	Grundgesetz
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
IT	Informationstechnologie(n), hier meist verstanden als Informations- und Kommunikationstechnologie(n)
ITU	International Telecommunication Union
ITU-T	ITU's Telecommunication Standardization Sector
KMU	Kleine und mittelständische Unternehmen
KoSIT	Koordinierungsstelle für IT-Standards
LTE	Long Term Evolution
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
ÖPP	Öffentlich-Private Partnerschaften
SLA	Service-Level Agreement
W3C	World Wide Web Consortium

Inhaltsverzeichnis

Geleitwort	5
Einleitung: Gibt es eine Cloud-Standortpolitik?	6
1 Optimierung des Rechtsrahmens	9
1.1 Datenschutz	9
1.2 Flexibilität durch Selbstverpflichtungen und Zertifizierung	13
1.3 Entwicklung innovativer Gestaltungsansätze für das rechtliche Verhältnis Cloud-Nutzer – Cloud-Anbieter	14
2 Einsatz von Cloud Computing in der öffentlichen Verwaltung	16
3 Ökosystem-Politik	20
3.1 Infrastruktur	20
3.2 Standardisierung	21
3.3 Vernetzung und Forschungspolitik	23
Anhang: Cloud Computing – Revolution im Business, Chancen, Herausforderungen	25
Kurzprofile: BITKOM und VOICE	27
Autoren und Projektteam	28



Geleitwort



Prof. Dieter Kempf
BITKOM Präsident,
Vorsitzender des Vorstands Datev eG

Cloud Computing markiert einen Paradigmenwechsel in der Bereitstellung und Nutzung von IT-Services, der Anbieter wie Anwender gleichermaßen betrifft. Durch die global skalierbare Cloud Computing-Technologie stellt sich in verschärfter Form die Frage, welche Rolle nationale Standortpolitik spielen kann. Verfügt die Politik über Hebel, um die großen Potenziale des Cloud Computings zu nutzen und weiter zu entwickeln? Oder setzt sich Cloud Computing im Selbstlauf durch? Wir meinen: Cloud Computing und eine moderne Standortpolitik sind auf zweierlei Weise untrennbar miteinander verbunden.

- Cloud Computing macht Standortpolitik möglich und stellt einen Hebel dar, den die Politik für eine positive Entwicklung des Wirtschaftsstandortes Deutschland nutzen kann. So machen Cloud-Technologien eine Restrukturierung der Wertschöpfungsketten möglich, die große Effizienzgewinne verspricht. Der Staat kann in diesem komplexen Prozess eine wichtige Rolle spielen und dort ansetzen, wo es um Koordinierung und



Dr. Thomas Endres
Vorsitzender des Präsidiums, VOICE e.V.

Standardisierung geht. Cloud Computing wird so zu einem interessanten Ansatzpunkt für eine moderne Industriepolitik.

- Standortpolitik macht Cloud Computing möglich. Die rechtlichen Rahmenbedingungen für Cloud Computing haben großen Einfluss auf die Marktentwicklung in Deutschland. Informationsverarbeitung basiert auf Vertrauen. Insofern erweist sich ein gutes Rechtssystem, das auf der einen Seite Vertrauen stiftet und auf der anderen Seite genügend Flexibilität bietet, die Skalierungseffekte durch Cloud Computing zu ermöglichen, als bedeutender standortpolitischer Vorteil.

Im internationalen Wettbewerb werden jene Standorte profitieren, an denen der Staat seine aktivierende Rolle besonders gut wahrnimmt. Mit dem vorliegenden Papier skizzieren BITKOM und VOICE die Eckpunkte einer erfolgreichen Cloud-Standortpolitik. Wir freuen uns auf den Dialog mit der Politik!

Einleitung: Gibt es eine Cloud-Standortpolitik?

Cloud Computing bedeutet einen Paradigmenwechsel in der Bereitstellung und Nutzung von IT-Dienstleistungen. In der Informationswirtschaft „bleibt kein Bit auf dem anderen“. Für die Anwender von IT aller Betriebsgrößenklassen und Branchen sowie für die öffentliche Verwaltung eröffnet Cloud Computing zahlreiche Chancen.¹

Durch die global skalierbare Cloud Computing-Technologie stellt sich in verschärfter Form die Frage, welche Rolle nationale Standortpolitik spielen kann. Verfügt die Politik über Hebel, um die großen Potenziale des Cloud Computings für einen Standort zu nutzen und weiter zu entwickeln? Oder „passiert“ Cloud Computing quasi im Selbstlauf?

BITKOM und VOICE meinen: Cloud Computing und eine moderne Standortpolitik sind auf zweierlei Weise untrennbar miteinander verbunden.

- Cloud Computing macht Standortpolitik möglich und stellt einen Hebel dar, den die Politik für eine dynamische Entwicklung des Wirtschaftsstandortes Deutschland nutzen kann. So machen Cloud-Technologien eine Restrukturierung der Wertschöpfungsketten möglich, die große Effizienzgewinne verspricht. Der Staat kann in diesem komplexen Prozess eine wichtige Rolle spielen und dort ansetzen, wo es um Koordination und Standardisierung geht. Cloud Computing wird so zu einem bedeutsamen Ansatzpunkt für eine moderne Industriepolitik.²
- Standortpolitik macht Cloud Computing möglich. Die rechtlichen Rahmenbedingungen für Cloud Computing haben erheblichen Einfluss auf die Marktentwicklung in Deutschland. Informationsverarbeitung basiert auf Vertrauen. Insofern erweist sich ein etabliertes Rechtssystem als bedeutender standortpolitischer Vorteil, wenn es auf der einen Seite Vertrauen stiftet und auf der anderen Seite genügend Flexibilität bietet, um die Skalierungseffekte durch Cloud Computing zu heben.

Im internationalen Wettbewerb werden jene Standorte profitieren, an denen der Staat seine aktivierende Rolle besonders aktiv wahrnimmt. Für den Standort Deutschland sind insbesondere die Auswirkungen von Cloud Computing auf die traditionell starken Anwenderbranchen wie Maschinen- und Anlagenbau, Automobilindustrie, Energiewirtschaft und Logistik wichtig.³

Als ein führender Wirtschaftsstandort hat Deutschland den Anspruch, nicht nur Absatzmarkt, sondern auch Anbieter für Cloud-Technologien zu sein. Die Voraussetzungen dafür sind gegeben, und das unter anderem über den IT-Gipfel sehr gut etablierte Zusammenwirken von Politik und Wirtschaft spielt dabei eine besonders wichtige Rolle.

¹ Der Anhang (S. 25) gibt eine Definition von Cloud Computing und fasst die Bedeutung von Cloud Computing für Wirtschaft und Verwaltung zusammen.

² Vgl. BITKOM 2012, Wirtschaftspolitisches Grundsatzpapier. www.bitkom.org

³ Vgl. Anhang S. 25

Hierauf gilt es aufzubauen. Vor diesem Hintergrund haben die in BITKOM und VOICE⁴ vertretenen Unternehmen optimierungsbedürftige Rahmenbedingungen beleuchtet und daraus Handlungsempfehlungen an die Politik abgeleitet.

Drei BITKOM/VOICE-Ziele für Cloud Computing:

1. Deutschland wird Cloud Computing-Kompetenzstandort Nummer 1 in Europa – mit dem Ziel, durch zügigen und breiten Einsatz von Cloud Computing einen möglichst hohen wirtschaftlichen Effekt in Wirtschaft und Verwaltung zu erreichen
2. Deutschland prägt durch eine enge Kooperation von Informationswirtschaft und Anwenderbranchen das Business Web als zentrale Organisationsplattform für den B2B-Sektor.
3. Mit optimierten Rahmenbedingungen zum Einsatz von Cloud Computing vermittelt die Politik allen IT-Anwenderbranchen Innovations- und Wachstumsimpulse.

Agenda einer Cloud-Standortpolitik

Das vorliegende Papier identifiziert Ansatzpunkte für die weitere Ausgestaltung des Cloud-Standortes Deutschland, aus denen sich drei Säulen einer erfolgreichen Cloud-Standortpolitik ableiten lassen (vgl. Abbildung 1).



Abbildung 1: Drei Säulen der Cloud-Standortpolitik

⁴ Vgl. die Kurzprofile auf Seite 27

■ Optimierung des Rechtsrahmens:

Den größten Hebel für eine erfolgreiche Cloud-Politik bildet ein international abgestimmter, verlässlicher und optimierter Rechtsrahmen (vgl. Kapitel 1). In Deutschland herrscht ein ausgeprägtes Bewusstsein für Sicherheit und Datenschutz. Das kann auch zur Geschäftsentwicklung von Cloud-Angeboten aus Deutschland heraus beitragen. Es kommt nun darauf an, geeignete Mittel zur Umsetzung dieser Leitlinien zu wählen. Als sinnvoller Ansatzpunkt erscheint der „Export“ der in Deutschland akzeptierten Politikvorstellungen nach Europa: So kann der einheitliche, für Unternehmen attraktive Markt geschaffen werden. Das Gegenteil dieser europäischen Cloud-Politik ist die isolierte Weiterentwicklung nationaler Gesetzgebung, die dem Cloud-Markt die Dynamik rauben kann. Dies ist kein Argument für die Absenkung, sondern für den richtigen Rahmen von Datenschutz-Standards.

■ Einsatz von Cloud Computing in der öffentlichen Verwaltung:

Cloud-Computing ist eine Schlüsseltechnologie für den öffentlichen Sektor (vgl. Kapitel 2) und leistet wesentliche Beiträge, die hier geltenden komplexen Anforderungen an IT zu erfüllen. Durch die hohe Flexibilität und Effizienzgewinne können Behörden kommende Herausforderungen – Budgetrestriktionen sowie Versorgung der gesamten Bevölkerung unter Bedingungen des demografischen Wandels meistern. Eine vom öffentlichen Sektor genutzte Cloud muss hohen Sicherheitsanforderungen entsprechen.

■ Ökosystem-Politik:

Eine Cloud-Standortpolitik muss auf Cloud-Ökosysteme ausgerichtet sein (vgl. Kapitel 3): Cloud-Infrastrukturen bieten die Grundlage für ein breites Partnernetzwerk, um Applikationen und Dienstleistungen anzubieten. Diese Ökosysteme bestehen einerseits aus großen Anbietern von Cloud-Technologieplattformen, andererseits aus Spezialisten, die solche Plattformen an die Anwendungsbereiche und lokalen Bedingungen anpassen. Eine wohlverstandene „deutsche Cloud“ ist nichts anderes als ein Ökosystem, das sich am Standort Deutschland entfaltet und hier Arbeitsplätze, Wertschöpfung und Technologie-Know-how schafft – sowohl in der IT-, als auch in den bedeutenden Anwenderbranchen.

1 Optimierung des Rechtsrahmens

Cloud Computing entwickelt sich mit hoher Dynamik. Es reicht also nicht aus, sich auf verlässliche, Vertrauen stiftende Rahmenbedingungen zu verlassen. Dynamische Entwicklungen erfordern Flexibilität. Eine sinnvolle Kombination aus einem vorgegebenen Rechtsrahmen und Flexibilität sichernden Instrumenten wie Selbstverpflichtungen und Zertifizierungen wird hier entscheidend.

■ 1.1 Datenschutz

Harmonisierung des Datenschutzes in der EU

Obwohl bereits die Datenschutz-Richtlinie von 1995 die Vollharmonisierung der Datenschutz-Vorschriften in Europa bringen sollte, sieht die Realität in den Mitgliedsstaaten anders aus. Für Cloud Computing Anbieter und ihre Kunden ergeben sich Schwierigkeiten vor allem daraus, dass die Einzelstaaten bei der Umsetzung unterschiedliche Anforderungen festgelegt haben und die Datenschutzbehörden sich auch hinsichtlich ihrer Auslegungen und Gepflogenheiten unterscheiden. Die aktuell geltende Datenschutz-Richtlinie verweist in Artikel 4 auf das einzelstaatliche Recht des Mitgliedsstaats, in dem der für die Verarbeitung Verantwortliche oder sein rechtlicher Vertreter ansässig ist oder dem er aus anderen Gründen unterliegt. Maßgeblich für die Vertragsbeziehung mit dem Auftragnehmer ist das einzelstaatliche Recht des für die Verarbeitung Verantwortlichen; ausgenommen hiervon sind die technischen und organisatorischen Vorkehrungen, mit denen der Auftragnehmer die sichere und gesetzeskonforme Verarbeitung gewährleisten muss.⁵ Diese technischen und organisatorischen Pflichten ergeben sich aus den Rechtsvorschriften des EU-Mitgliedsstaats, in dem der Auftragnehmer seinen Sitz hat.⁶

Die Schwierigkeiten, die durch die unterschiedlichen einzelstaatlichen Umsetzungen sowie unterschiedliche Vorgehensweisen der Aufsichtsbehörden ergeben, vervielfachen sich, wenn ein Anbieter von Cloud-Services im Auftrag seiner Kunden Daten verarbeitet und diese Dienstleistung in mehr als einem oder zwei Mitgliedsstaaten anbietet. Im Extremfall müsste ein solcher Cloud-Betreiber für ein und dasselbe Dienstleistungsangebot 27 einzelstaatliche Rechtsvorschriften und -auslegungen einhalten und berücksichtigen. Dies setzt hoch spezialisiertes juristisches Fachwissen voraus. Die Gestaltung des Unternehmens, die Beobachtung rechtlicher Änderungen und die jeweils erforderliche Anpassung daran wären so kostspielig und aufwändig, dass sie den technischen Betrieb beeinträchtigen würden.

Klare und einheitliche rechtliche Vorgaben zum Datenschutz würden dagegen die Chance bieten, eine technisch anspruchsvolle einheitliche Umsetzung der Vorgaben ohne unangemessenen Aufwand zu gewährleisten. Die jetzt begonnene Neugestaltung des europäischen Datenschutz-Rechtsrahmens bietet die Chance, die bestehenden Regelungen mit Blick auf neue Geschäftsmodelle zu überarbeiten und mit einheitlichen Regeln gleiche Wettbewerbsbedingungen für alle in Europa tätigen Anbieter zu schaffen.

⁵ Das ist meist der Auftraggeber.

⁶ Vgl. Artikel 17 Absatz 3 der Datenschutzrichtlinie.

Agenda

- Praxisgerechte, für die Auftragsdatenverarbeitung geeignete Harmonisierung des Datenschutzes in der EU mit Hilfe einer neuen Datenschutz-Verordnung
- Die vollharmonisierten europäischen Vorgaben sollen für alle Auftragsdatenverarbeiter 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 Mitgliedsstaat 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.

Verwendung von Standardvertragsklauseln

Standardvertragsklauseln sind für die Auftragsdatenverarbeitung ein wichtiges Instrument zur rechtskonformen vertraglichen Ausgestaltung von datenverarbeitenden Dienstleistungen.

Die Verwendung von Standardvertragsklauseln ist insbesondere Voraussetzung für den Datenexport in Drittstaaten, wie er im Rahmen von Cloud Computing Angeboten öfter vorkommt. Allerdings gibt es im Cloud Computing auch oftmals Konstellationen, in denen ein europäischer Anbieter Daten seines europäischen Kunden bei Unterauftragnehmern in Drittstaaten verarbeiten lässt (zum Beispiel werden dort angebotene Speicherkapazitäten in Anspruch genommen). Momentan darf allerdings der europäische Anbieter im Gegensatz zu

außereuropäischen Anbietern gegenüber seinem außereuropäischen Unterauftragsverarbeiter nicht die EU-Standardvertragsklauseln verwenden.⁷ Das bedeutet, dass ein außereuropäischer Cloud-Anbieter ein Standardverfahren an die Hand bekommt, nach dem er Daten im Auftrag eines europäischen Kunden (für die Verarbeitung Verantwortlichen) mithilfe außereuropäischer Unterauftragnehmer verarbeiten darf, während dies einem europäischen Cloud-Anbieter verwehrt bleibt.

Es wäre wünschenswert, dass europäische Cloud-Anbieter dieselben standardisierten Vertragsklauseln sowohl im Verhältnis zum Kunden als auch im Verhältnis zu inner- und außereuropäischen Unterauftragnehmern verwenden können. Dies würde sowohl bürokratischen Aufwand reduzieren als auch zu mehr Transparenz und Rechtsklarheit führen.

⁷ 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.

Agenda

- Klarstellung der EU-Kommission, dass die Standardvertragsklauseln von europäischen Cloud-Anbietern auch bei Vertragsverhältnissen innerhalb der EU verwendet werden dürfen
- Neufassung oder Änderung der Standardvertragsklauseln so, dass sie auch von europäischen Cloud-Anbietern verwendet werden können, die Unterauftragnehmer außerhalb der EU beschäftigen möchten.

Beseitigung der Benachteiligung deutscher Anbieter bei Datentransfers in Drittstaaten

Deutsche Anbieter werden durch den bis zum Inkrafttreten der geplanten EU-Verordnung geltenden § 3 (8) BDSG im Vergleich zu anderen Anbietern in der EU dadurch benachteiligt, dass die Privilegierung der Auftragsdatenverarbeitung möglicherweise nur beim Datentransfer innerhalb der EU oder dem EWG-Wirtschaftsraum besteht.⁸ Dem gesetzlichen Wortlaut zufolge liegt eine Auftragsdatenverarbeitung nur vor, wenn der Cloud-Anbieter die personenbezogenen Daten in der EU oder dem EWR erhebt oder verwendet. Die EU-Datenschutz-Richtlinie 95/46 sieht dagegen auch die Privilegierung für Auftragsdatenverarbeitung beim Datentransfer in sichere Drittländern vor wie auch für Datentransfers in Drittländer ohne angemessenes Datenschutzniveau, sofern der für die Verarbeitung Verantwortliche ausreichend Garantien hinsichtlich der Privatsphäre, des Schutzes der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet – insbesondere durch entsprechende Vertragsklauseln.⁹ In Umsetzung dieser Regelung hat die EU-Kommission

Standardvertragsklauseln verabschiedet, die die weisungsgebundene Weitergabe von personenbezogenen Daten, also die Auftragsdatenverarbeitung, zum Gegenstand haben.¹⁰ Diese Entscheidung steht im Gegensatz zum gegenwärtigen gesetzlichen Wortlaut in Deutschland.

In der Praxis bedeutet eine fehlende Privilegierung für den Datentransfer in Drittstaaten im Rahmen einer Auftragsdatenverarbeitung, dass die Weitergabe an Cloud-Anbieter nur zulässig ist, wenn gesetzliche Erlaubnistatbestände hierfür vorliegen: Die Übermittlung müsste also beispielsweise durch überwiegende Interessen des Cloud-Kunden oder Cloud-Anbieters gerechtfertigt sein oder durch die Einwilligung des Betroffenen. Ersteres würde eine erhebliche Rechtsunsicherheit mit sich bringen, letzteres ist nicht immer praktikabel. Diese Beschränkung besteht in anderen EU-Ländern soweit ersichtlich nicht. Für deutsche Cloud-Kunden besteht daher bei der Nutzung von Cloud-Services insofern eine erhöhte Rechtsunsicherheit, welche bis zum Inkrafttreten der EU-Datenschutzverordnung bestehen wird, wenn der deutsche Gesetzgeber sie nicht beseitigt.

⁸ § 3 (8) BDSG: Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

⁹ EU-Datenschutz-Richtlinie 95/46 Art. 25 (1) und Art 26 (2).

¹⁰ Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (Bekannt gegeben unter Aktenzeichen K(2010) 593), Amtsblatt Nr. L 039 vom 12/02/2010 S. 0005 – 0018.

Agenda

Klarstellung in § 3 (8) BDSG, dass die Privilegierung der Auftragsdatenverarbeitung entsprechend der geltenden EU-Datenschutz-Richtlinie 95/46 auch beim Datentransfer in sichere Drittländer oder mit ausreichenden Garantien des Verantwortlichen auch in Drittländer ohne angemessenes Datenschutzniveau vorgesehen wird.

Stärkung des technischen Datenschutzes

IT-Technologie ist ein wichtiger „Enabler“ des Datenschutzes. Durch Verschlüsselung, Pseudonymisierung und Anonymisierung kann der Datenschutz wirksam erhöht werden – oftmals effizienter als durch das rechtliche Instrument der Einwilligung. 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 insbesondere im anstehenden Review des europäischen Datenschutzes beachtet werden.

Agenda

Stärkung der Instrumente des technischen Datenschutzes im aktuell vorliegenden Entwurf der EU-Kommission für eine Datenschutz-Verordnung.

Voraussetzungen für staatliche Zugriffe auf personenbezogene Daten im Kontext der Terrorbekämpfung

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.

Agenda

Transatlantische Initiative zur Beseitigung rechtlicher Grauzonen, die durch die Einführung extraterritorial geltenden Rechts entstanden sind.

■ 1.2 Flexibilität durch Selbstverpflichtungen und Zertifizierung

Cloud-Kunden, die personenbezogene Daten in die Cloud geben, tragen die Verantwortung, dass diese in Abhängigkeit vom 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 Cloud-Infrastruktur 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 freiwilligen 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. Damit würde die Ausübung des Selbstbestimmungsrechts durch den Betroffenen und die Verantwortungsübernahme durch die verantwortlichen Stellen optimal unterstützt.

Mit der Anerkennung der Vorlage von Selbstverpflichtungen als Nachweis für die Erfüllung der Kontrollpflichten des für die Verarbeitung Verantwortlichen werden

Vor-Ort-Kontrollen vermieden, die bei der Vielzahl von Cloud-Kunden nicht nur extremen Aufwand, sondern auch ein erhebliches Gefährdungspotential für die Datensicherheit zur Folge haben könnten. Die Gesetzesbegründung zur BDSG-Änderung 2009 weist explizit darauf hin, dass ein externes Audit oder ein vom Dienstleister vorgelegtes schlüssiges Datensicherheitskonzept genügen können.

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 Datensicherheitsniveau besteht. Hierfür müssen entsprechende Nachweise in Form von freiwilligen 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. Die branchenspezifische Konformität, die materiell-rechtliche Zulässigkeit und die technisch-organisatorische Sicherheit der Datenverarbeitung sind als feste Bestandteile der Prüfung anzusehen.

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. Gemeinsam geschaffene Standards, insbesondere auch zu Umfang und Inhalten der Datenschutz-Dokumentation, können sowohl für die Selbstverpflichtung als auch für das Zertifizierungsverfahren erfolgreich verwendet werden. Für die Unternehmen kann sich so ein harmonischer Dreiklang ergeben aus Umsetzung der Standards, Selbstverpflichtung und Nachprüfung durch unabhängige sachverständige Prüforganisationen, in Abhängigkeit auch von Größe, Wachstum und Entwicklung der eigenen Dienstleistungen der Cloud-Anbieter.

Erweiterung des Ansatzes der Selbstverpflichtungen über den Datenschutz hinaus

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.

Agenda

- Erleichterungen für die Wahrnehmung der Weisungs- und Kontrollbefugnisse des Cloud-Kunden bei Inanspruchnahme von Cloud-Diensten schaffen durch Förderung von Selbstverpflichtungen und Verhaltenskodizes sowie deren Anerkennung als Nachweis zur Erfüllung der Sorgfalts- und Kontrollpflichten des Cloud-Kunden
- Etablierung freiwilliger Zertifikate mit einheitlichen und transparenten Prüfverfahren durch sachverständige Dritte als Nachweis der Erfüllung der Kontrollpflichten des für die Datenverarbeitung Verantwortlichen
- Anforderungen an die Datensicherheit im Rahmen von Cloud-Dienstleistungen weiter entwickeln und entsprechenden Rahmen für Zertifizierungen setzen

■ 1.3 Entwicklung innovativer Gestaltungsansätze für das rechtliche Verhältnis Cloud-Nutzer – Cloud-Anbieter

Um den Wirtschaftsstandort Deutschland als ein internationales Zentrum für Cloud-basierte Dienstleistungen zu etablieren und die damit verbundenen Innovations- und Wachstumsimpulse zu schaffen, halten BITKOM und VOICE auch die Prüfung von innovativen Ansätze zur Weiterentwicklung der Rahmenbedingungen für das Verhältnis Anwender und Anbieter für sinnvoll. Bestehende Rechtsunsicherheiten, die Cloud-Nutzer bei der Nutzung von Cloud Diensten belasten, sollten durch praxisnahe Regelungen beseitigt werden.

BITKOM und VOICE werden dazu den Dialog zwischen Anwender- und Anbieterseite und der Politik intensivieren. Unter dem Stichwort „Shared Data – Shared Responsibility“ wird unter anderem geprüft, wie eine ausgewogene Verteilung der Verantwortlichkeiten für Datenschutz und Datensicherheit im Verhältnis zwischen Cloud-Kunden

und Cloud-Dienstleistern zukünftig bei neuen Konstellationen aussehen kann und welche regulatorischen Maßnahmen sinnvoll wären. Bis zum IT-Gipfel 2012 werden erste Ergebnisse dieser Diskussion angestrebt.

Insbesondere bei Dienstleistungsangeboten aus der Public Cloud lassen sich – entsprechend dem auf Skalierung und Standardisierung beruhenden Geschäftsmodell der Cloud-Dienstleister – die für die klassische Auftragsdatenverarbeitung entwickelten Weisungsrechte und Kontrollbefugnisse des Cloud-Kunden in der Praxis oft kaum umsetzen. Um die breite Nutzung von Cloud-Diensten zu befördern, müssen die Bedingungen für die Cloud-Nutzung so ausgestaltet sein, dass Cloud-Nutzer keine unbekannteren oder unüberschaubaren Risiken eingehen müssen, gegen die sie sich nicht befriedigend absichern können. Hierzu beitragen können z. B. auch die im Abschnitt 1.2 erwähnten Selbstverpflichtungen und Zertifizierungen sowie klare Vorgaben für die Datensicherheit in der Cloud und entsprechende rechtliche Rahmenbedingungen. Berücksichtigt werden muss auch, dass die volle Ausnutzung

der Cloud-spezifischen Skalierungs-Vorteile meist nur bei Inanspruchnahme von internationalen Angeboten möglich ist. Bedingung hierfür ist eine Vereinfachung der bestehenden Vorgaben zumindest für gängige Datenverarbeitungsprozesse für Daten von niedrigem Sensitivitätsgrad.

Bei der weiterführenden Diskussion über die zukünftigen Rahmenbedingungen für das Verhältnis Cloud-Kunde – Cloud-Anbieter sollten daher folgende Ansätze genauer betrachtet werden:

Agenda

- Klassifizierungen und katalogartige Zweckbestimmungen zur Nutzung von Datenkategorien, für die aufgrund geringerer Datensensitivität zur Nutzung von Cloud-Diensten erleichterte Bedingungen gelten, entwickeln (einschließlich solcher, die als Funktionsübertragung anzusehen sind)
- Anforderungen an die Datensicherheit im Rahmen der technischen und organisatorischen Maßnahmen auf Cloud-Dienstleistungen weiter entwickeln und einen Rahmen für Selbstverpflichtungen und Zertifizierungen setzen
- Erleichterungen für die Wahrnehmung der Weisungs- und Kontrollbefugnisse des Auftraggebers bei Inanspruchnahme von Cloud-Diensten schaffen und dazu insbesondere auf noch näher zu entwickelnde Zertifizierungen des Cloud-Dienstleisters vertrauen
- Prüfung alternativer Regelungsmodelle für eine sach- und risikogerechte Verteilung der Verantwortlichkeiten im Verhältnis Cloud-Kunde und Cloud-Anbieter bei neuen Geschäftsmodellen (wie z. B. die datenschutzrechtliche Eigenhaftung bei Verstößen gegen die Grundsätze der Datensicherheit und im Falle von Datensicherheitspannen ab dem Übergabepunkt und die gesamtschuldnerische Haftung von Auftraggeber und Auftragnehmer für Datensicherheitsverstöße).

2 Einsatz von Cloud Computing in der öffentlichen Verwaltung

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 entgegen. Aber auch die strategische Ausrichtung ist in vielen Bereichen noch offen. So haben sich einige kommunale bzw. Dienstleistungszentren der Länder für eine Umsetzung von Private Clouds entschieden, die inhouse betrieben werden und den Anforderungen an Sicherheit und Datenschutz genügen. Die mit Cloud einhergehenden Skalen- und Konsolidierungseffekte sind in dieser Konstellation vergleichsweise gering, da weder die Anzahl der vorhandenen öffentlichen Rechenzentren (ca. 400) noch die Anzahl der Server, die trotz Virtualisierung auf Lastspitzen ausgelegt sind, reduziert wird. Überdies werden Anwendungen (IT-Services) von mehreren IT-Dienstleistern neu entwickelt, ohne die Potentiale wiederverwendbarer Anwendungen zu nutzen.

Die öffentlichen Verwaltungen in Deutschland müssen eine Vorreiterrolle in Sachen Cloud-Standardisierung übernehmen. Andere Länder – insbesondere die USA und Großbritannien – sind hier deutlich weiter¹¹. Im Wettbewerb um die Ansiedlung internationaler Unternehmen ist auch die Verwaltungsinfrastruktur neben Verkehrs-anbindung und Steuern ein Standortfaktor.

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.

Strategie und Stufenplan für deutsche Verwaltungs-Clouds

Im IT-Planungsrat wollen Bund, Länder und Kommunen Initiativen starten, um IT-Infrastrukturen zur Kosteneinsparung gemeinsam nutzen zu können¹². Benötigt werden ein Strategiepapier und ein Stufenplan zur Umsetzung für deutsche Verwaltungs-Clouds, an denen sich alle Verwaltungsebenen ausrichten können, sowie ein Governance-Rahmen für Cloud Computing für die öffentlichen Verwaltungen.

In der Gesamtumsetzungsplanung sollten verschiedene Ziele definiert werden, die bei der Entwicklung einer Cloud-Strategie Orientierungen geben; sie betreffen beispielsweise konkrete Maßnahmen zur Koordinierung der Zusammenarbeit und zur Vereinbarung von Standards. Stufenkonzepte für die Umsetzung und Roll-out sind zu entwickeln und gegebenenfalls durch Leuchtturmprojekte zu untermauern.

Mit Art. 91c Grundgesetz wurde der Grundstein für die Zusammenarbeit zwischen Bund und Ländern gelegt, der insbesondere die Bereiche Standards, Sicherheit und IT-Netze betrifft. Bisher fehlen aber gesetzliche Grundlagen, um personenbezogene bzw. sensible Daten zwischen zwei unterschiedlichen Standorten über eine gemeinsam genutzte Infrastruktur zu übertragen. Damit wird die Etablierung einer IT-Kooperation zu einem schwierigen Unterfangen. Vergleichbar für die Erstellung einer Strategie ist die Government Cloud Strategie in Großbritannien, umgesetzt durch die G-Cloud¹³ Initiative. Ein anderes Beispiel liefert Frankreich. Der Staat investiert in eine Public Private Partnership knapp 300 Millionen Euro in die Schaffung einer Government Cloud.¹⁴

¹¹ s. z. B. die G-Cloud in UK (<http://www.cabinetoffice.gov.uk/content/government-ict-strategy>) und die dortige Festlegung auf offene Standards.

¹² Memorandum des IT-Planungsrats vom 30.06.2011; <http://www.it-planungsrat.de/SharedDocs/Pressemitteilungen/DE/2011/Memorandum%20des%20IT-Planungsrats.html>

¹³ Cloudbook, UK Government CIO Council, Retrieved January 17, 2012. <http://www.cabinetoffice.gov.uk/content/government-ict-strategy>

¹⁴ <http://www.lemondeinformatique.fr/actualites/lire-285-millions-d-euros-pour-andromede-le-cloud-souverain-francais-41990.html> (abgerufen 29.02.2012)

Agenda

- Erarbeitung eines Strategiepapiers, eines Stufenplanes und eines Governance-Rahmens zur Umsetzung für deutsche Verwaltungs-Clouds durch den IT-Planungsrat
- Vorreiterrolle öffentlicher Verwaltungen bei der Umsetzung von Cloud Computing.

Orientierung an offenen Standards

Die öffentlichen Verwaltungen müssen beispielgebend sein, indem sie sich auf Standards festlegen, Interoperabilität in ihren eigenen Cloud-Diensten durch Nutzung der Standards und Prozessen ermöglichen, bei der Ausschreibung öffentlicher Cloud-Projekte die Einhaltung von Standards vorgeben und einfordern und dabei die Ergebnisse des Theseus-Programms berücksichtigen sowie verstärkt in Cloud Computing investieren.

Vertrauen in Cloud-Anbieter kann nur durch offene Standards erfolgen, die dem sogenannten Vendor-Lock-in entgegenstehen. Offene Standards werden international auf Basis von Use-Cases entwickelt und sollten in den entsprechenden Gremien des IT-Planungsrats berücksichtigt werden.

Agenda

Integration offener Standards in den Bereichen Interoperabilität und Sicherheit aus den verschiedenen Standardisierungsgremien und Industriekonsortien¹⁵.

Akzeptanz von Standardgeschäftsvorfällen für Interaktionen zwischen Verwaltungen und Wirtschaft

Es sollten die Rahmenbedingungen für eine Akzeptanz von Standardgeschäftsvorfällen für Interaktionen zwischen Verwaltungen und Wirtschaft hergestellt werden. Viele Verwaltungsleistungen sind gebührenpflichtig. Online-Transaktionen scheitern bei diesen Dienstleistungen an der fehlenden Online-Bezahlungsfunktion.

Denn der Nutzwert von E-Government-Angeboten für den Kunden und für die Verwaltung hängt davon ab, dass der gesamte Leistungsprozess durchgängig elektronisch umgesetzt wird. Ein Beispiel, wie eine Umsetzung erfolgen kann, liefert der Freistaat Sachsen¹⁶. Hier finden sich auch Beispiele für die notwendigen Anpassungen des öffentlichen Kassenrechts.

¹⁵ NIST, DMTF, ISO, OASIS, W3C, IETF, ETSI, ITU-T, CCUCDG, usw.

¹⁶ Freistaat Sachsen, Basiskomponente Zahlungsverkehr <http://www.egovernment.sachsen.de/54.htm> (abgerufen am 01.03.2012)

Agenda

Akzeptanz von Standardgeschäftsvorfällen für Interaktionen zwischen Verwaltungen und Wirtschaft herstellen.

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. Diese Herausforderung betrifft gleichermaßen Bund, Länder, Kommunen; die Schaffung einer gemeinsamen wettbewerbsoffenen Public Key Infrastructure (PKI) als Grundlage für Dokumentenmanagement und Archivierungssysteme könnte somit eine Aufgabe des IT-Planungsrats sein.

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. Diese lässt sich durch Zertifikate sicherstellen. Empfehlenswert ist daher der Aufbau einer interoperablen wettbewerbsoffenen Public Key Infrastructure für die knapp 5 Millionen öffentlich Bediensteten in Deutschland.

Einige Berufsgruppen wie etwa Notare¹⁷ oder auch einige Verwaltungsverfahren wie das elektronische Abfallnachweisverfahren¹⁸ oder der elektronische Handel mit Emissionszertifikaten¹⁹ liefern Modelle für moderne vollelektronische Verfahren. Um Interoperabilität der Lösungen in Bundesbehörden, Ländern und Kommunen zu gewährleisten und damit Zertifikate ohne Umwege anerkannt werden können, bedarf es einer gemeinsamen wettbewerbsoffenen PKI und einer zukunftsgerichteten Signaturpolitik von Bund, Ländern und Kommunen.

Agenda

Gesetzliche Regelungen (wie z. B. das E-Government-Gesetz²⁰) für die Akzeptanz elektronischer Dokumente forcieren.

¹⁷ Zum Einsatz der elektronischen Signatur im Notariat <http://www.elrv.info/de/signaturkarte/informationen-zur-elektronischen-signatur.php> (abgerufen am 01.03.2012)

¹⁸ Hierzu insbesondere die Mitteilung der Bund/Länder-Arbeitsgemeinschaft Abfall (LAGA) Ifd Nr. 27 - Vollzugshilfe zum abfallrechtlichen Nachweisverfahren; zum elektronischen Abfallnachweisverfahren und dem Einsatz der qualifizierten elektronischen Signatur vgl. ab S. 67 ff http://www.zks-ab-fall.de/nn_7576/DE/Service/Publikationen/Informationsschriften/M27,templateId=raw,property=publicationFile.pdf/M27.pdf (abgerufen am 01.03.2012)

¹⁹ Umweltbundesamt, DEHSt – Deutsche Emissionshandelsstelle; zur virtuellen Poststelle und dem Einsatzfeld der qualifizierten elektronischen Signatur http://www.dehst.de/DE/Service/Haeufig-gestellte-Fragen/Virtuelle-Poststelle/virtuelle-poststelle_node.html (abgerufen am 01.03.2012)

²⁰ Vgl. Stellungnahme http://www.bitkom.org/files/documents/Stellungnahme_BITKOM_E-Government_Gesetz_V.2.0.pdf

BSI-Eckpunktpapier um Klassifikation sensibler Daten ergänzen

Unsicherheiten im Umgang mit sensiblen Daten führen eher dazu, nichts in die Cloud zu legen als darüber nachzudenken, was in die Cloud kann. Deswegen scheint es

sinnvoll, das Eckpunktpapier des BSI „Sicherheitsempfehlungen für Cloud Computing“²¹ um eine Klassifikation von sensiblen Daten (Sicherheitslevel normal, hoch, sehr hoch) zu erweitern, und es sollte eine entsprechende Zuordnung der Daten vorgenommen werden, die in Relation zu den Sicherheitsstandards der Cloud-Anbieter zu stellen ist.

Agenda

Erweiterung des Eckpunktpapiers „Sicherheitsempfehlungen für Cloud Computing“ um eine Klassifikation sensibler Daten

Öffentlich-Private Partnerschaften im IT-Bereich politisch unterstützen

Öffentlich-Private Partnerschaften im IT-Bereich können dazu beitragen, die Herausforderungen in der öffentlichen Verwaltung zu bewältigen. Schuldenbremse und demographischer Wandel zwingen die öffentliche Verwaltung zu erhöhter Automatisierung, um altersbedingte Abgänge zu kompensieren und weitere Effizienzsteigerungen zu erreichen. Politische Unterstützung ist

deshalb notwendig, weil nicht nur Effizienzpotentiale ausgenutzt werden sollen, die modernes E-Government mit sich bringt, sondern auch die Reduzierung des Verwaltungspersonals, verursacht durch den demografischen Wandel. Dies impliziert den positiven Effekt der Demografie, weil sich Personalabbau ohne Entlassung realisieren lässt²², und unterstützt gleichzeitig Cloud Computing mit einem hohen Potential zur Konsolidierung, Effizienzsteigerung und Flexibilität.

Agenda

Politische Unterstützung Öffentlich-Privater Partnerschaften im IT-Bereich.

²¹ Bundesamt für Sicherheit in der Informationstechnik, 2011, <https://www.bsi.bund.de>

²² ÖPP im IT- und Dienstleistungsbereich: Marktüberblick und kritische Erfolgsfaktoren, Band 5, ÖPP Deutschland AG, 2011, siehe auch bereits Public Sector: IT-Outsourcing und Public Private Partnerships, 2008 http://www.bitkom.org/files/documents/PPP_ITO_E-Government_fin.pdf

3 Ökosystem-Politik

Eine Cloud-Standortpolitik sollte sich auf Cloud-Ökosysteme ausrichten - breite Partnernetzwerke, die auf der Basis marktrelevanter Cloud-Infrastrukturen gebildet werden, um Applikationen und Dienstleistungen webbasiert anzubieten. Derartige Ökosysteme entwickeln sich bisher vor allem rund um große Anbieter von Cloud-Infrastrukturen und Technologieplattformen. Sie bieten zahlreichen nationalen und internationalen Partnern die Chance, die Plattformen ergänzende Cloud-Anwendungen zu entwickeln und anzubieten.

Mittelfristig werden sich einige Cloud-Netzwerke stärker thematisch fokussieren, um branchenspezifische Dienste (beispielsweise für die öffentliche Verwaltung) zu offerieren, die ganz gezielt die jeweiligen Anforderungen im Hinblick auf die Art und Ausgestaltung der Dienste, aber auch im Hinblick auf Standards und vertragliche Feinheiten adressieren. Unternehmen der Anwenderbranchen werden nicht selten selbst Anbieter webbasierter Dienstleistungen und könnten sich in unterschiedlichen Rollen in Ökosysteme integrieren.

■ 3.1 Infrastruktur

Ökosysteme können sich nur herausbilden, wenn sie fördernde Rahmenbedingungen vorfinden.

Eine moderne Breitbandinfrastruktur ist die Grundvoraussetzung für eine breite Nutzung Cloud-basierter Innovationen in Wirtschaft, Wissenschaft und Gesellschaft.

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 von Bund und Ländern, 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.

Die Strategie verschiedener Unternehmen ist es, auf einen Technologiemix zu setzen. Neben klassischen, kabelgebundenen Breitband-Anschlüssen gewinnen mobilfunkbasierte Lösungen an Relevanz, z. B. durch den neuen Mobilfunkstandard LTE (Long Term Evolution). Hierdurch kann es gelingen, Cloud-basierte Anwendungen überall in Deutschland zum Erfolg zu führen.

Allerdings werden die Handlungsspielräume für Investitionen durch die Infrastrukturanbieter als Folge intensiver regulatorischer Vorgaben zunehmend kleiner.

Durch regulatorische Preissenkungen drohen wichtige Finanzmittel aus dem Markt genommen zu werden, die für Investitionen nicht mehr zur Verfügung stehen. Um den Ausbau von Hochgeschwindigkeitsnetzen über die bisherigen Erfolge hinaus zügig mit wettbewerblichen Mitteln voranzubringen, ist es daher unumgänglich, auch 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.

Dafür muss die Regulierung zunächst ausreichend Anreize für Investoren setzen, zuvorderst also Rechts- und Planungssicherheit schaffen. Große Kostenblöcke für die notwendigen Investitionen entfallen auf Tiefbauarbeiten und die Verlegung der Inhouse-Netze. Um hier Synergien zu nutzen müssen die Kabelkanalanlagen aller Netzbranchen (Strom, Energie, Wasser) und die vorhandenen Inhouse-Netze zur Verfügung gestellt werden. Zudem sind Anreize für Investitionen in moderne Gebäudenetze zu verstärken, indem entsprechende Bauvorschriften etwa in Form von Pflichten zur Mitverlegung von Leerrohren bei Modernisierungs- und Sanierungsvorhaben angepasst

bzw. geschaffen werden. Auch durch eine konsequente Umsetzung der EU-Richtlinien sollten alle Möglichkeiten und Spielräume für die Schaffung investitionsfreundlicher Rahmenbedingungen genutzt werden.

Open-Access-Modelle können ebenso den Ausbau von Glasfaserinfrastrukturen bis zum Endkunden/Haus (FTTH/FTTB) fördern. Diese können ein ausgewogenes Verhältnis von Investitionsanreizen und Wettbewerbssicherung gewährleisten. Bei Einhaltung der Open-Access-Regeln

sollen Unternehmen und Investoren die Sicherheit haben, dass selbst für den Fall, dass Marktbeherrschung festgestellt werden sollte, auf konkrete Regulierungseingriffe verzichtet wird. Konsistente Infrastrukturpolitik bedeutet schließlich auch, die politische Forderung nach einem schnellen flächendeckenden Breitbandausbau ohne Einsatz von Steuergeldern nicht durch immer neue Markteingriffe zu konterkarieren. Für potentielle Investoren wird damit genau das falsche Signal gesetzt.

Agenda

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. Regulierung darf kein Risiko für Investitionen sein, sondern muss die Auswirkungen auf Investitionen und Arbeitsplätze mehr als bislang berücksichtigen.

■ 3.2 Standardisierung

Als Grundlage von Ökosystemen spielen offene Standards eine große Rolle, die eine umfassende Interoperabilität und eine hohe Verfügbarkeit der Cloud-Services ermöglichen.

Die Politik sollte Standardisierungsvorhaben auf europäischer Ebene unterstützen und gerade kleine und mittelständische Unternehmen in dem Prozess nicht außen vor lassen. Ziel muss es sein, offene Standards voranzutreiben, denn davon profitieren alle Marktteilnehmer²³.

Cloud Computing baut auf Vertrauen in die Zuverlässigkeit, Verfügbarkeit und Sicherheit von Technologien und Prozessen auf Basis von Standards.

Zwar existiert heute eine Reihe von Standards, die Teilaspekte von Cloud Computing abdecken. Aber selbst in Verbindung mit den zurzeit weltweit häufig punktuell und isoliert laufenden Standardisierungsinitiativen²⁴, hat dies noch nicht zu umfassenden, leicht handhabbaren, aufeinander abgestimmten und allgemein akzeptierten Standards geführt.

Die Festlegung solcher Standards z. B. in Bezug auf technische, organisatorische und funktionale Interoperabilität zwischen Cloud-Diensten und Dienstleister ist aber die Voraussetzung, um Geschäftsprozesse über die Grenzen einzelner Cloud-Dienste hinweg effizient zu ermöglichen und deren Rechtssicherheit zu gewährleisten.

²³ „Das Normungs- und Standardisierungsumfeld von Cloud Computing“, Berlin, März 2012, Untersuchung aus europäischer und deutscher Sicht unter Einbeziehung des Technologieprogramms „Trusted Cloud“ im Auftrag des Bundesministerium für Wirtschaft und Technologie (BMWi).

Erstellt von Booz & Company in Kooperation mit dem FZI Forschungszentrum Informatik

²⁴ z. B. NIST, DMTF, IEEE, ISO, ANSI, OASIS, W3C, ECMA oder IETF

Einbindung der Wirtschaft in Standardisierungsvorhaben der öffentlichen Verwaltung

Bei laufenden und geplanten Standardisierungsvorhaben der öffentlichen Hand sollte die Privatwirtschaft frühzeitig eingebunden werden. Damit wird sichergestellt, dass deren Anforderungen hinsichtlich Interoperabilität und Praktikabilität erfüllt werden. Ein Beispiel für mangelnde Interoperabilität bestehender Standards zeigt die Bedeutung dieser Empfehlung: Die Finanzverwaltung hat in den

letzten Jahren konsequent ihr Ziel nach mehr Automatisierung bei der Betriebsprüfung vorangetrieben und dazu auch ein Export-Format für das Rechnungswesen definiert, das letztlich alle Anbieter in ihre Produkte integrieren mussten. Leider war das Format eben nur aus dem Blickwinkel der deutschen Betriebsprüfung entworfen. Es enthält dafür verdichtete Daten, aus denen, mangels geeigneter Referenzierung, die Originaldaten nicht rekonstruierbar sind. Somit sind mit diesem Format die Anforderungen an die Interoperabilität nicht erfüllt.

Agenda

Frühzeitige Einbindung der Privatwirtschaft in Standardisierungsvorhaben der öffentlichen Hand.

Verstärkt Leuchtturmprojekte aufsetzen, die Best Practices liefern

Leuchtturmprojekte können Vorbilder und Best Practices für Verwaltung und Wirtschaft liefern. Das Trusted Cloud Programm des Bundesministeriums für Wirtschaft und Technologie (BMWi) ist ein erster Schritt, konkrete Pilotanwendungen im Bereich Cloud Computing zu initiieren. Darüber hinaus sind weitere Forschungsprojekte zu fördern, um offene technische und organisatorische Standards zu definieren.

Dazu zählen z. B. Standards:

- in Bezug auf die Bereitstellung von Daten in offenen Formaten für Datenmigration, die Portabilität von Daten zwischen den verschiedenen Cloud-Typen untereinander (Private, Hybrid und Public Clouds) und für Cloud-Backup-Lösungen,
- zur Sicherstellung eines einfachen Anbieterwechsels,
- in Bezug auf Service-Level-Agreements, Allgemeine Geschäftsbedingungen.

Das Vorhandensein und die Nutzung von Cloud-Standards helfen auch und gerade mittelständischen Unternehmen,

- die Implementierungs- und Integrationskosten von Cloud Computing zu verringern,
- eine gewisse Provider-Unabhängigkeit sicherzustellen,
- die Audit- und Governance-Prozesse transparenter zu machen und zu erleichtern,
- die Sicherheits- und Geschäftsrisiken zu verringern und damit
- das Vertrauen in Cloud Computing zu stärken.

Solche Standardisierungsinitiativen können natürlich nicht isoliert in Deutschland durchgeführt werden. Sie müssen eingebettet sein in internationale Aktivitäten mit dem Ziel, weltweit akzeptierte Normen bereitzustellen.

Agenda

Verstärkt Leuchtturmprojekte aufsetzen, die Best Practices liefern.

■ 3.3 Vernetzung und Forschungspolitik

Der Begriff des Cloud-Ökosystems lässt sich auch weiter fassen, sodass beispielsweise das Ökosystem „Deutsche Cloud“ sämtliche Cloud-Aktivitäten privatwirtschaftlicher Unternehmen, des öffentlichen Bereichs sowie der Forschungseinrichtungen und Hochschulen in Deutschland umfasst. Die Herausforderung besteht dann darin, die Aktivitäten möglichst gut zu bündeln. Die Vernetzung von Unternehmen und Forschungseinrichtungen gilt es zu forcieren, wobei ein besonderes Augenmerk auf umsetzbare Geschäftsmodelle und eine kurze Zeit bis zur Marktreife von Produkten oder Services gelegt werden sollte²⁵.

Durch den zunehmenden Einsatz sowie die wachsende Nutzung von Cloud Computing in Unternehmen und der Verwaltung entstehen weitreichende Abhängigkeiten und Vernetzungen. Deren fehlerfreies Funktionieren ist für diese sowie für einen Privatanwender von existentieller Bedeutung. Hierdurch erlangt Cloud Computing den Stellenwert vergleichbar einer kritischen Infrastruktur (wie z. B. Strom- und Wasserversorgung). Parallel dazu findet aufgrund der extremen Skalierbarkeit von Cloud Systemen eine Konsolidierung und somit eine Konzentration im Cloud-Computing-Markt auf einige Unternehmen statt, die zu schwer revidierbaren Marktstrukturen führt.

Cloud Computing ist das Thema eine Vielzahl von Initiativen der öffentlichen Hand, wie z. B. die Trusted Cloud Initiative des BMWi, aber auch der Wissenschaft und Wirtschaft²⁶. Diese Initiativen sind in erster Linie technologieorientiert und auf einzelne Unternehmen ausgerichtet. Solche einzelnen, punktuellen Maßnahmen bringen Verbesserungen mit sich, jedoch ist ein breiter angelegter Rahmen notwendig, um die Nutzung von Cloud Computing in Unternehmen, Verwaltung und Gesellschaft zu fördern, zu begünstigen und nachhaltig zu verankern.²⁷

Orchestrierung aller Beteiligten der deutschen Cloud-Computing-Wertschöpfungskette

Mit einer Initiative zur Orchestrierung aller Beteiligten der deutschen Cloud-Computing-Wertschöpfungskette unter Einbeziehung der relevanten Wissenschaften könnte Basis für die Entstehung und Entfaltung von Anbietern und Wettbewerb im Cloud-Umfeld verbreitert werden. Erst hierdurch kann sich ein geeigneter Innovationsrahmen entwickeln, der als Grundlage für die Entstehung und Entfaltung von Anbietern und Wettbewerb künftiger Cloud-Märkte in Deutschland und Europa dient. Wegen der Dimension dieser Initiative und der Heterogenität der Teilnehmer ist die Initiative und Moderation der Politik unerlässlich.

²⁵ Das aktuelle Technologieprogramm Trusted Cloud des BMWi (www.trusted-cloud.de) liefert hierfür ein gutes Vorbild, sind doch zahlreiche IT-Anbieter, Cloud-Anwender und Forschungsinstitute in die Entwicklung sicherer Cloud-Services involviert. In Arbeitsgruppen werden dabei zentrale Querschnittsthemen, wie Recht, Standardisierung und Geschäftsmodelle erarbeitet.

²⁶ Direkte Bezüge gibt es auch zum Theseus-Projekt, die systematisch erschlossen werden sollten.

²⁷ In das Kapitel 3.3 sind Überlegungen einer Gruppe von Wissenschaftlern eingeflossen, vgl. „Denk ich an Clouds in der Nacht – Nachhaltige Cloudstrategie für Europa“. Memorandum Harmonized EU Clouds. 25.10.2011. Autoren: Helmut Krcmar, Claudia Eckert, Arnold Picot, Dieter Klumpp, Nico Gro-ve, Tiziana Margaria, Volker Markl, Michael Pauly, Daniel Veit

Agenda

Initiative zur Orchestrierung aller Beteiligten der deutschen Cloud-Computing-Wertschöpfungskette bilden.

Forschung für eine integrierte Sicht auf Cloud-Services intensivieren

Um die Zukunftsfähigkeit des Industrie- und Dienstleistungsstandortes Deutschland zu sichern, ist es notwendig, technologische, wirtschaftliche, soziologische und rechtliche Aspekte des Cloud Computing zu betrachten. Wichtige Fragestellungen in diesem Bereich sind Organisation und Verwaltung von Clouds und den darin gespeicherten großen Datenmengen sowie Diensten im Hinblick auf Sicherheit, Programmierung, Skalierbarkeit, Kompatibilität, Datenschutz, Wirtschaftlichkeit und Nachhaltigkeit. Daher sollte die Forschung intensiviert werden, die eine integrierte und ganzheitliche Sichtweise auf Cloud-Services entwickelt. Dabei ist auch

der wachsende Bereich der Cyber-Physical Systems zu berücksichtigen („Industrie 4.0“) – sie werden Teil einer zukünftig vernetzten Welt sein und großen Einfluss auf Cloud-Services haben.

Heute zögern viele Unternehmen mit der Nutzung von Cloud-Services, da das Verhalten des Cloud-Service-Anbieters außerhalb des Normalbetriebes unklar ist, beispielsweise ob, in welchem Umfang und mit welchem zeitlichen und finanziellen Aufwand Änderungen an einem Cloud-Service durchgeführt werden können. Daher sollte die Forschung zu Spezifikationsverfahren initiiert werden, die den gesamten Lebenszyklus von Cloud-Services abdecken.

Agenda

Zeitnahe Investitionen in Forschung und Entwicklung zur Intensivierung einer integrierten und ganzheitlichen Sicht auf Cloud Services zur Lösung wichtiger Fragestellungen im Bereich der Organisation, Verwaltung, Optimierung und Nutzung von Clouds.

Anhang: Cloud Computing – Revolution im Business, Chancen, Herausforderungen

■ Begriffsbestimmung Cloud Computing

Cloud Computing wird definiert als eine Form der bedarfsgerechten und flexiblen Nutzung von IT-Leistungen. Diese werden in Echtzeit als Service über das Internet bereitgestellt und nach Nutzung abgerechnet. Damit ermöglicht Cloud Computing den Nutzern eine Umverteilung von Investitions- zu Betriebsaufwand. Die IT-Leistungen können sich auf Anwendungen, Plattformen für Anwendungsentwicklungen und -betrieb oder Basisinfrastruktur beziehen.²⁸

■ Bedeutung von Cloud Computing für Anwender-Unternehmen

Cloud Computing bietet Unternehmen aller Größenklassen vielfältige Chancen:

- Kleine und neugegründete Unternehmen profitieren von dem sich ständig weiter entwickelnden Lösungsangebot. Die Unternehmen können ihre Ideen schnell und professionell via Internet realisieren und ihren Kunden präsentieren. Zusätzlich können sie schnell (virtuelle) Unternehmensverbände gründen und auflösen, um stärker am Markt aufzutreten. Die zugrundeliegende IT in der Cloud unterstützt sie dabei dynamisch und ohne große Vorabinvestitionen.
- Mittelständische Unternehmen profitieren von der Effizienz und Geschwindigkeit im Marktzugang (Time-to-Market), die ihnen Cloud Computing ermöglicht. Sie können sich stärker im globalen Wettbewerb engagieren. Diese Unternehmen können dynamische

IT-Lösungen einsetzen, die bisher größeren Unternehmen mit entsprechenden IT-Abteilungen vorbehalten waren. Sie nutzen die in der Praxis erprobten Angebote des globalen Marktes.

- Für große Unternehmen bietet Cloud Computing eine Verbesserung von Agilität und Flexibilität und somit eine Erhöhung der Unternehmensperformanz.

Während es heute noch undenkbar erscheinen mag, dass Unternehmen ohne hausinterne IT- und Rechenzentren auskommen, so könnte das in wenigen Jahren vielleicht schon Normalität sein. Zumindest ergänzend werden fast alle Unternehmen Cloud Computing nutzen.²⁹

■ Industriestandort Deutschland – ein Cloud-Thema

Für den Standort Deutschland sind auch die Auswirkungen von Cloud Computing auf die traditionell starken Anwenderbranchen wie Maschinen- und Anlagenbau, Automobilindustrie, Energiewirtschaft und Logistik besonders wichtig. Auf der Grundlage von Cloud-Technologien werden Business-Plattformen entwickelt, mit denen Wertschöpfungsketten wesentlich effizienter und umfassender als bislang organisiert werden können. Traditionelle ERP-Datensilos in den Unternehmen werden integriert, die Cloud wird zum Organisationsprinzip von Innovationsnetzwerken und Wertschöpfungsketten („Business Web“). Das „Internet der Dinge“ lässt insbesondere das produzierende Gewerbe zu einem Hauptnutzer von Cloud-Plattformen werden.

²⁸ Vgl.: „Cloud Computing - Evolution in der Technik, Revolution im Business“, BITKOM-Leitfaden, Berlin 2009, www.cloud-practice.de

²⁹ Vgl.: Cloud-Monitor Deutschland 2012. Studie von PAC im Auftrag von KPMG und in Zusammenarbeit mit BITKOM, Berlin, März 2012, www.cloud-practice.de

■ Bedeutung für IT-Anbieter

Cloud Computing ist ein Paradigma, das die gesamte Informationswirtschaft, ihre Technologien und ihr Geschäft nachhaltig verändert³¹. Um diese Technologie bilden sich neue Geschäftsmodelle, Wertschöpfungsketten und auch Marktsegmente³². Vom Cloud Computing bleibt wohl kaum ein Unternehmen dieser Branche verschont. Das Selbstverständnis der Unternehmen als unabhängiger Softwareanbieter, Consulting-Unternehmen oder Systemintegrator, Value Added Partner oder Value Added Reseller und Hostler bzw. IT-Dienstleister wird sich zügig wandeln – wie auch die Arbeitsteilung zwischen ihnen.

■ Bedeutung für die öffentliche Verwaltung und den Staat

Die öffentliche Verwaltung erhält mit dem Cloud Computing die Möglichkeit, erhebliche Skaleneffekte zu erzielen und so insgesamt ihre Effektivität deutlich zu erhöhen. Die stärkere Einführung standardisierter Verwaltungsprozesse, gepaart mit einem breiteren Einsatz von Cloud Computing, vermindert die Kosten und den Anteil von Routearbeiten. Auf diese Weise können die Folgen der demografischen Entwicklung abgefedert werden. Der Staat profitiert von einer gestiegenen Wachstumsdynamik als Folge von agileren Unternehmen, von Unternehmensneugründungen und zunehmender Beschäftigung. So werden in einer Studie für das World Economic Forum speziell für Deutschland folgende Einschätzungen gegeben³³:

- Sobald Cloud Computing auf breiter Basis eingesetzt wird, werden allein in Deutschland innerhalb von fünf Jahren bis zu 40.000 neue Unternehmen durch die Nutzung von Cloud Computing zusätzlich entstehen, wodurch insgesamt bis zu 160.000 neue, zusätzliche Arbeitsplätze geschaffen werden.

- Bezogen auf die Arbeitsmarktwirkung ist Deutschland damit innerhalb der EU nach Großbritannien (240.000) der zweitgrößte Profiteur vom Cloud Computing.
- Insgesamt werden bis zu 30% der IT-Fixkosten durch Cloud-Technologien variabilisiert und können somit produktiver genutzt werden. Die Gesamtwirkung auf das deutsche Bruttoinlandsprodukt wird konservativ auf 0,3% zusätzliches Wachstum geschätzt, was auf der Basis der Werte für 2010 einem jährlichen zusätzlichen BIP-Wachstum von rund 7,5 Mrd. Euro entspricht. 2015 werden 50% der IT-Investitionen in Cloud-Projekte fließen.

Die Kompetenz zur Entwicklung und Anwendung von Cloud Computing wird also zu einem bedeutenden Standort- und Wettbewerbsfaktor. Aus diesem Grund ist Cloud Computing nicht nur ein Aktionsfeld für das Business. Das Effektivitätspotenzial dieser Innovation muss zügig und auf breiter Basis erschlossen werden. Dafür sind fördernde Rahmenbedingungen erforderlich, die von der Politik im Zusammenwirken mit der Wirtschaft zu entwickeln sind. Bestehende Hindernisse für die wirtschaftlich sinnvolle Nutzung von Cloud Computing müssen kurzfristig überwunden werden. Wenn es gelingt, Deutschland stärker als international bevorzugten Standort für Cloud Computing ausprägen, so wird auch die Attraktivität des Landes für Investitionen weiter angehoben. Deutschland kann nicht nur Absatzmarkt für Cloud-Technologien, sondern muss ein bedeutender Anbieter auf internationalen Märkten sein. Die Voraussetzungen dafür sind gegeben:

- Zahlreiche große IT-Unternehmen unterhalten Entwicklungsstandorte in Deutschland.
- Die Forschungsinstitute haben einen hervorragenden Stand.
- Die Anwenderindustrien verfügen über international führende Prozesskompetenz.
- Das Zusammenwirken von Politik und Wirtschaft ist etabliert³⁴.

³¹ Vgl. „Cloud Computing – Was Entscheider wissen müssen“, Leitfaden, Januar 2011, herausgegeben vom BITKOM e.V.; vgl. auch www.cloud-practice.de.

³² Ein Beispiel sind weltweite Marktplätze für Daten, u.a. für Geodaten, Sportstatistiken, Gesundheitsdaten, Wetterdaten, Analysen über Kaufkraft nach Regionen, Sehenswürdigkeiten von Ländern oder Städten.

³³ Etro, Federico, 2009, The Economic Impact of Cloud Computing on Business Creation, Employment and Output in the E.U., Review of Business and Economics, 54, 2, 179-208

³⁴ So arbeiten BITKOM, Fraunhofergesellschaft und VOICE im Aktionsprogramm Cloud Computing des BMWi zusammen.

Kurzprofile BITKOM und VOICE



Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) vertritt mehr als 1.700 Unternehmen, davon über 1.100 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software & IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein. Die Interessen der Cloud-Anbieter bündelt der Arbeitskreis Cloud Computing und Outsourcing.



VOICE – Verband der IT-Anwender e.V. wurde ins Leben gerufen, um als Dachorganisation die bestehenden Verbände cioforum, CIOcolloquium und CIO-Circle noch effizienter miteinander zu verbinden. VOICE bietet eine dynamische und kompetente Plattform für den fachlichen Austausch von IT-Verantwortlichen und Entscheidungsträgern am Markt. Gebündeltes Know-how für unterschiedliche Branchen und Unternehmensgrößen prägen den hohen Anspruch, der in VOICE eine erfolgreiche Umsetzung findet. VOICE steht für eine starke Interessenvertretung mit einem weit reichenden Netzwerk. Als Ansprechpartner für Politik, Medien und Gesellschaft gestalten wir aktiv den Dialog mit der Öffentlichkeit.

Autoren und Projektteam

Autoren dieser Empfehlungen sind:

- Ansgar Baums, Hewlett-Packard GmbH
- Tanja Böhm, Microsoft Deutschland GmbH
- Susanne Dehmel, BITKOM e.V.
- Peter Deider, Deutsche Telekom AG
- Norbert Franke, arvato systems GmbH
- Rudolf Berthold Gerhard, Datev eG
- Christoph Hecker, VOICE e.V.
- Dr. Ralph Jahnke, Accenture GmbH
- Bernd Klusmann, BITKOM e.V.
- Dieter Krißgau, Datev eG
- Dr. Jan Geert Meents, DLA Piper UK LLP
- Dr. Pablo Mentzini, BITKOM e.V.
- Gerald Münzl, House of IT e.V. (Projektkoordinator)
- Caroline Neufert, BearingPoint GmbH
- Dr. Jan-Peter Ohrtmann, PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft, Frankfurt am Main
- Dr. Michael Pauly, T-Systems International GmbH
- Christoph Schiefer, BearingPoint GmbH
- Dr. Katrin Schleife, Pierre Audoin Consultants (PAC) GmbH, Berlin
- Prof. Dr. Rainer Schmidt, Hochschule Aalen
- Paul Schwefer, VOICE e.V.
- Linda Strick, Fraunhofer – Institut für Offene Kommunikationssysteme
- Christian Wallat, BearingPoint GmbH
- Dr. Mathias Weber, BITKOM e.V.
- Monika Wojtowicz, TÜV Informationstechnik GmbH
- Dr. Hans Peter Wiesemann, DLA Piper UK LLP
- Special Interest Group „Daten- und Rechtssicherheit in der Cloud“ (VOICE)

Weiter arbeiteten folgende Experten mit:

- Frank Brüggemann, Materna GmbH Information & Communications
- Peter Eisermann, UFP Unternehmensberatung für Projektmanagement GmbH
- Bijan Eskandarafshar, Siemens AG
- Werner Feld, Compass Deutschland GmbH
- Bernd Gill, Hewlett-Packard GmbH
- Mark Glowienka, arvato systems Technologies GmbH
- Ulrike Goose, cqc corporate quality consulting GmbH
- Dr. Saskia Horsch, Amazon.de GmbH
- Claudia Mrotzek, Oracle Deutschland B.V. & Co. KG
- Prof. Dr. Sven M. Prüser, Hochschule für Technik und Wirtschaft (HTW Berlin)
- Dr. Andreas Tegge, SAP AG
- Wolfram Weber, VMware Global, Inc. Zweigniederlassung Deutschland



Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org



VOICE – Verband der IT-Anwender e.V.

Inselkammerstr. 10
82008 Unterhaching
Tel.: 089.8982797-15
Fax: 089.8982797-79
Info@voice-ev.org
www.voice-ev.org