INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

zeppelin universität

zwischen
Wirtschaft Kultur Politik

Prof. Dr. Dirk Heckmann
Prof. Dr. Jörn von Lucke
Thorsten Hennrich
Michael Marc Maisch

C³ COMPLIANT COMMUNITY CLOUD

Sicheres IT-Outsourcing für Kommunen

STUDIE

Vorwort

Cloud Computing ist in aller Munde. Nicht nur Unternehmen, auch Verbraucher (iCloud, Windows 365) nutzen die „Datenwolke“ zur Verwaltung ihrer Datenbestände oder für den Zugriff auf aktuelle Applikationen. Für die öffentliche Verwaltung, nicht zuletzt die Kommunalverwaltung, stellt sich die Frage, ob sich Cloud Services „lohnen“ – in wirtschaftlicher oder organisatorischer Hinsicht. Sie sind aber auch verunsichert wegen der vielbeschworenen Risiken und Unwägbarkeiten, vor allem im Hinblick auf Datenschutz und Datensicherheit. Dürfen Kommunen überhaupt Cloud Computing nutzen? Diese Rechtsunsicherheit verhindert eine sachliche Auseinandersetzung mit den Chancen und Risiken solcher Innovationen, dem technischen Fortschritt, organisatorischen Weichenstellungen und zeitgemäßen Geschäftsmodellen.

Das Projekt C^3 (Compliant Community Cloud) soll Licht in das Dunkel der „Behördencloud“ bringen. Was versteht man überhaupt unter Cloud Computing? Wie unterscheidet sich dieses gegenüber dem herkömmlichen IT-Outsourcing? Welche Vorteile bietet es, mit welchen Nachteilen muss man rechnen? Welche Gestaltungsmöglichkeiten ergeben sich für Kommunen vor dem Hintergrund verfassungsrechtlicher und einfachgesetzlicher Grenzen und Restriktionen?

Die Ausführungen richten sich an Behördenleiter aller kommunalen Ebenen, die eine Inanspruchnahme von Diensten des Cloud Computing in Betracht ziehen. Ihr Ziel ist es, ein Grundverständnis und das notwendige Hintergrundwissen zu vermitteln, um die richtigen Fragen zu stellen und die richtigen Schritte einzuleiten. Ungeachtet ob man sich für oder gegen kommunales Cloud Computing entscheiden sollte: Es darf jedenfalls nicht willkürlich, zufällig oder irrtumsbehaftet sein.

Der hierzu separat erstellte Praxisleitfaden dient bewusst einer schnellen Orien-tierung und legt Wert auf eine verständliche Darstellung. Die damit einhergehende Vereinfachung ist gewollt. Der Praxisleitfaden wird daher durch diese stärker juristisch geprägte Begleitstudie ergänzt, die als „Langfassung“ zahlreiche Details und Hinweise auch für kleine Kommunen enthält. Beides zusammen genommen soll dazu beitragen, dass sich rechtskonforme kommunale Cloud Lösungen etablieren können: als „Compliant Community Cloud“ (C^3).

Das Projekt C^3 wurde von der Bayerischen Innovationsstiftung gefördert. Unter der Leitung von Professor Dr. Dirk Heckmann haben Wissenschaftler des Deutsche Telekom Institute for Connected Cities TICC an der Zeppelin Universität Friedrichshafen die rechtlichen, technischen, organisatorischen und ökonomischen Aspekte des kommunalen Cloud Computing erforscht. Diese Erkenntnisse sind unmittelbar in die Begleitstudie und den hieraus hervorgegangenen Praxisleitfaden eingeflossen. Durch mehrere Workshops und weitere Interaktionen mit den Kommunalen Spitzenverbänden in Bayern sowie einer empirischen Erhebung bei über 100 bayerischen Gemeinden, Landkreisen und Bezirken wurde den Bedürfnissen und Interessen der kommunalen Verwaltungspraxis Rechnung getragen.

Friedrichshafen und Passau, im März 2013

Prof. Dr. Dirk Heckmann (Projektleiter)

Inhaltsverzeichnis

1. Was ist überhaupt „dieses Cloud Computing“?

a) Entstehung und Bedeutung eines schillernden Begriffs

Cloud Computing – Kaum ein anderer Begriff aus der IT-Sprache erzielt eine solche Resonanz: 85 Millionen Treffer in Google, davon 145.000 im Bereich der „Nachrichten“ – und das bisher allein im Jahr 2012. *„Die Cloud verändert alles“* war das Credo auf der Cebit 2012 in Hannover. *„How the cloud changes everything“* titelte Matt Welsh seinen Vortrag auf der Konferenz „The Future of Computation in Science“ Anfang 2012 an der Harvard University, wo der Informatikprofessor früher lehrte.

Offenbar kommt man beim Cloud Computing nicht ohne Superlative aus. So wird eine **neue Ära** ausgerufen (Microsofts Chief Software Architect Ray Ozzie) und das Potenzial des Cloud Computing mit den Auswirkungen der industriellen Revolution des späten 18. und frühen 19. Jahrhunderts verglichen (Gartner-Analyst Daryl Plummer).

Auch die EU-Kommissarin Neelie Kroes sprach im Juni 2012 von einer **Revolution** und ergänzte: "In einem Land wie Deutschland könnte das Cloud Computing nach verschiedenen Schätzungen über fünf Jahre mehr als 200 Milliarden Euro einbringen." Deshalb legte die EU-Kommission im September 2012 eine einheitliche Strategie zum Cloud Computing vor, um Rechtssicherheit und Datenschutz zu gewährleisten.

Das alles nur für einen **Hype**? Nein, meinte das führende Marktforschungsunternehmen für IT, Gartner, in seinem Hype Cycle Report 2009: Cloud Computing sei kein Hype, sondern ein Super-Hype. Und dieser hat eine rasante Geschichte, seit der Begriff im Jahr 2007 einer breiten Öffentlichkeit bekannt geworden ist. IBM hatte da gerade die Initiative „Blue Cloud“ angekündigt.

Was Marktstrategen oder die Medien (vielleicht auch eigensinnig oder im Sinne einer selbsterfüllenden Prophezeiung) als Hype bezeichnen, ist streng genommen

nichts anderes als eine andere Art der Auftragsdatenverarbeitung, **IT-Outsourcing**. Also die Verlagerung von Daten auf externe Server, die sich als sog. Datenwolke über einen oder mehrere Standorte erstrecken kann. Im Detail mag es Unterschiede, Varianten und Weiterungen geben, die man berücksichtigen muss (hierzu im Anschluss auf S. 10 ff.). Das hinderte allerdings nicht die Marketing-Abteilungen großer IT-Unternehmen wie Microsoft, Amazon, Dell oder der Deutschen Telekom, ihre neuen Angebote und Geschäftsmodelle mit einer ebenso wolkigen wie griffigen Bezeichnung zu garnieren. IT-Outsourcing klingt dagegen scheinbar spröde und weniger innovativ. Und dennoch muss ein nüchterner Blick auf die technischen, organisatorischen, wirtschaftlichen und rechtlichen Aspekte dieser Art von IT-Einsatz beim IT-Outsourcing beginnen. Wenn in der Folge dennoch immer wieder vom „Cloud Computing“ oder von „Cloud Services“ die Rede ist, dann deshalb, weil diese Begriffe ihre Berechtigung auch im öffentlichen Sektor erlangen können, wenn man sie nur richtig versteht – und nicht etwa pauschal mit einer US-Cloud assoziiert. Auch hierzu dient die vorliegende Studie.

b) Cloud ist nicht gleich Cloud: Varianten des IT-Outsourcing

Definition des Cloud Computing

Cloud ist nicht gleich Cloud. Dies zeigt sich vor allem in begrifflicher Hinsicht. In der weltweiten IT-Branche konnte sich gegenwärtig noch keine einheitliche Begriffsdefinition für **„Cloud Computing“** herausbilden.

Das US-amerikanische National Institute for Standards and Technology (NIST) hat Cloud Computing als ein Modell definiert, ***„das es erlaubt, bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z.B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Service-Provider-Interaktion zur Verfügung gestellt werden können.“*** (Übersetzung nach BSI, Eckpunktepapier, Sicherheitsempfehlungen für Cloud Computing Anbieter, S. 14)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat, auf der NIST-Definition aufbauend, der eigenen Definition einen etwas allgemeineren Ansatz zugrundegelegt und Cloud Computing wie folgt definiert:

„Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z.B. Rechenleistung, Speicherplatz), Plattformen und Software."

(BSI, Eckpunktepapier, Sicherheitsempfehlungen für Cloud Computing Anbieter, S. 15 f.)

Der enthaltene Verweis auf das komplette Spektrum der Informationstechnik verdeutlicht dabei anschaulich die faktischen Schwierigkeiten, die mit einer einheitlichen Begriffsfindung zwangsläufig bestehen müssen. Vereinfacht ausgedrückt ist Cloud Computing nämlich nichts anderes als **„IT as a Service"** – also Software und Hardwareressourcen als Dienstleistung. Der Gedanke von „XaaS – Everything as a Service" zeigt, dass bei Cloud Computing grundsätzlich alles möglich sein soll. Bei Cloud Computing handelt es sich daher in erster Linie um einen Oberbegriff für flexible und bedarfsgerechte Bereitstellungs- und Nutzungsszenarien von sämtlichen am Markt angebotenen IT-Leistungen. Die in der Praxis gängige – und auch von dem BSI vorgenommene – Untergliederung nach Infrastruktur, Plattformen und Software „as a service" (näheres hierzu sogleich) trägt insoweit besonders praxisrelevanten Einsatzszenarien Rechnung. Weitere Unterteilungen und begriffliche Spezifizierungen sind hierdurch nicht ausgeschlossen und in der Praxis auch wiederzufinden.

Unterschied zu „klassischem IT-Outsourcing"

Mit dem Begriff IT-Outsourcing sind verschiedene Formen der Ausgliederung von IT-Dienstleistungen verbunden. Ein solches IT-Outsourcing liegt z.B. dann vor,

wenn Administration, Betrieb und Wartung von Arbeitsplatzrechnern oder Serversystemen von einem anderen Unternehmen übernommen werden. Um dabei die mit Cloud Computing verbundenen Innovationen (wie vor allem flexible und gemeinsam nutzbare Ausformungen) anschaulicher präsentieren zu können, werden bisherige IT-Outsourcing-Szenarien, die vor allem noch durch den Einsatz von dedizierter Hardware gekennzeichnet sind, dagegen häufig als „klassisches IT-Outsourcing" bezeichnet. Insoweit soll vor allem das Merkmal „as a Service" – ein fertiges Standardangebot aus der Wolke bzw. aus dem Netz bzw. aus der Netzsteckdose – das Cloud Computing von dem bisher bekannten IT-Outsourcing abheben: Webserver/Rechenkapazitäten as a Service, Applikationen as a Service, Virenschutz as a Service, Firewall as a Service, Storage as a Service (z.B. iCloud, Dropbox) und vieles mehr.

Hinzu kommen beim Cloud Computing besondere **Virtualisierungseffekte**. Diese ermöglichen es, die Hardware-Ebene von sämtlichen darüber liegenden Ebenen zu entkoppeln. Hierdurch können Laufzeitumgebungen abstrahiert von der zugrundeliegenden Hardware zur Verfügung gestellt werden – mit anderen Worten: die genutzten Hardware-Ressourcen werden durch eine Software „simuliert" und sind daher losgelöst von den in einem Rechnergehäuse enthaltenen Ressourcen zu betrachten. Die Hardware kann dadurch von mehreren Nutzern gleichzeitig genutzt werden (sog. „Multimandantenfähigkeit"). Der Einsatz virtualisierter Systeme ermöglicht es Anbietern (im Unterschied zu dem Einsatz dedizierter IT-Systeme), Hardware-Ressourcen deutlich besser auszulasten. Dies erhöht vor allem die Wirtschaftlichkeit und Effektivität.

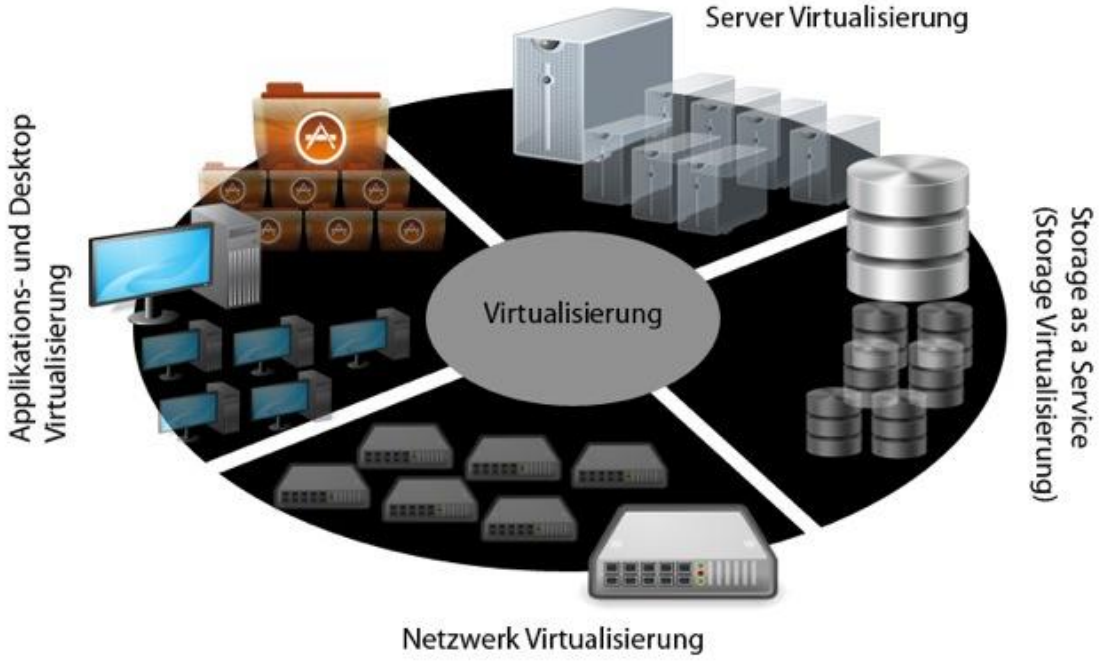


Abbildung 1: Virtualisierung

Daneben kennzeichnen gerade nutzungsbasierte Abrechnungsmodelle und flexible Vertragslaufzeiten „Cloud Computing" in seiner Idealform. Indem Anbieter Leistungen flexibel und bedarfsgerecht zur Verfügung stellen („pay per use"), können Kommunen mit anderen Vertragslaufzeiten und Kosten kalkulieren, als dies in klassischen IT-Outsourcing-Szenarien mit regelmäßig sehr langen Vertragslaufzeiten noch der Fall war.

Fließender Übergang und unklare Konturen in der Praxis

Der zuvor gewählte Begriff einer Idealform lässt bereits erahnen, dass auch solche Clouds existieren, die diesem Idealtypus nicht vollumfänglich entsprechen. Insofern ist jedoch zu berücksichtigen, dass der Übergang vom „klassischen IT-Outsourcing" zu einer flexiblen Cloud-Nutzung gerade erst begonnen hat. So weisen verschiedene Leistungen zwar in technischer Hinsicht bereits Elemente einer Cloud auf. Zugleich können aber längere Vertragslaufzeiten einem wirklich **flexi-**

blen Einsatz in der Praxis (teilweise) noch entgegenstehen. Welche Maßstäbe für eine flexible Nutzung insoweit anzulegen sind, wird wiederum von den unterschiedlichen Einsatzszenarien und Interessen abhängen und kann dementsprechend variieren. Bei einem Einsatz durch staatliche Stellen sowie im privatwirtschaftlichen Umfeld wird eine Flexibilität bei der tatsächlichen Inanspruchnahme (**pay-per-use-Basis)** dabei immer auch im Kontext von gesetzlichen und regulatorischen Anforderungen zu betrachten sein. Diese können insoweit zu Einschränkungen führen (bei Anbieterwahl, Vertragslaufzeiten bei hochspezifischen Lösungen, u.a.m.). Gerade die öffentliche Verwaltung wird bei der Haushaltsaufstellung meist fest kalkulierbare Beträge bevorzugen. Variable Nutzungsszenarien könnten insoweit von einer zu vereinbarenden Obergrenze abhängen.

Zugleich kann hier auch ein Bedürfnis nach einem wiederkehrenden **Grundbedarf** bestehen, der lediglich um bestimmte Leistungen bedarfsgerecht ergänzt wird. Bedarfsgerecht bedeutet, dass z.B. einer Kommune als Cloud-Kunde mit nur einem Mausklick mehr Speicherplatz, eine weitere Arbeitsplatzlizenz einer Software oder ein Update zur Verfügung gestellt wird, um Engpässe abzudecken. Die Bereitstellung von IT-Dienstleistungen richtet sich insoweit nach dem individuellen Bedarf.

Weiterhin ist zu berücksichtigen, dass vor allem die im geschäftlichen Umfeld wiederzufindenden „Private Clouds“ nicht mit den für die allgemeine Öffentlichkeit bestimmten „Public Clouds“ vergleichbar sind. Es existieren also sehr **unterschiedliche Grundformen** von Cloud Computing. Daneben ist zu beachten, dass der Begriff Cloud in der Praxis oftmals aus reinen Marketing-Gesichtspunkten verwendet wird. Dies hat teilweise zu einer weiteren Verwässerung der Konturen von Cloud Computing geführt. Auch deshalb ist es wichtig, dass Kommunen bedarfsgerechte Lösungen für IT-Outsourcing bzw. Cloud Computing finden, die ihrem Status als öffentlich-rechtliche Körperschaften gerecht werden.

Service-Modelle

Bei Cloud Services kann grundsätzlich zwischen der Bereitstellung von Infrastruktur, Plattformen und Software „als Dienst“ unterschieden werden. Auf der untersten Ebene der IT-Systemarchitektur umfasst das Servicemodell **„Infrastructure as a Service“** (IaaS) die **bedarfsbasierte Bereitstellung skalierbarer IT-Ressourcen**. In der Praxis stehen hierbei vor allem Rechenleistung, Speicherplatz, Datennetze und andere Netzwerkkomponenten im Vordergrund. Auf der nächsthöheren Ebene beinhaltet **„Plattform as a Service“** (PaaS) die Bereitstellung von Laufzeitumgebungen oder Entwicklungsplattformen. **„Software as a Service“** (SaaS) steht schließlich für die flexible Bereitstellung von jeglicher Form an Software und Anwendungen. Im kommunalen Sektor existiert dieser Service für bestimmte Fachanwendungen, etwa im Bereich Meldewesen oder Personalverwaltung. Im privaten Sektor (z.B. „Office 365“ von Microsoft) werden cloud-basierte Softwareanwendungen für Textverarbeitung, Tabellenkalkulation und andere Bürokommunikationsdienste bereits von mittelständischen und großen Unternehmen sowie Verbrauchern genutzt.

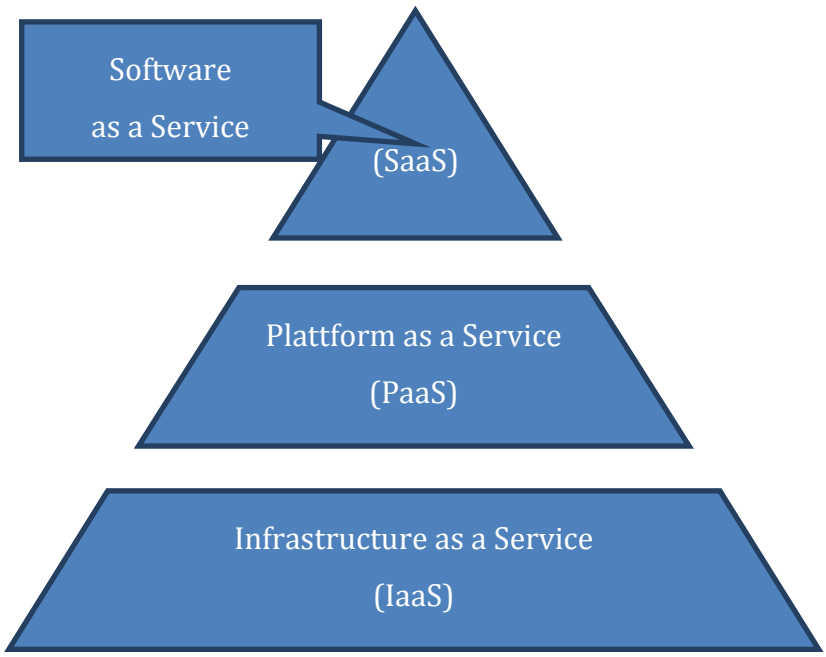


Abbildung 2: Ebenen der Service-Modelle

Bereitstellungsformen

Dienste aller Service-Modelle können grundsätzlich in zwei Formen bereitgestellt werden.

Als **Public Cloud** wird eine Cloud-Umgebung bezeichnet, die einer unbestimmten Allgemeinheit über das Internet zugänglich ist. Jedermann kann sich als Kunde registrieren. Public Clouds sind vor allem bei einer Vielzahl an Ressourcen hochskalierbar und in der Regel durch einen (sehr) hohen Standardisierungsgrad gekennzeichnet. **Hochskalierbar** bedeutet, dass zusätzliche Ressourcen (aufgrund der oftmals immensen Dimensionierung der zugrundeliegenden Infrastruktur) selbst in einem größeren Umfang ad hoc bereitgestellt werden können. Als bekannte Beispiele für Public Cloud Dienste wird regelmäßig auf die allgemein über das Internet zugänglichen Dienste von Google, Microsoft oder Amazon Web Services verwiesen, da diese Anbieter die Entwicklung von Cloud Services maßgeblich vorangetrieben haben. Public Clouds werden jedoch auch von vielen deutschen und europäischen Unternehmen (mit Infrastruktur in Deutschland bzw. im EU-/EWR-Raum) betrieben.

Private Clouds sind dagegen geschlossene Cloud-Umgebungen, die ausschließlich für ein Unternehmen oder für eine Organisation betrieben werden. Aufgrund des insoweit eingeschränkten Nutzerkreises sind sie der Öffentlichkeit gerade nicht allgemein zugänglich. Private Clouds weisen regelmäßig cloud-spezifische Elemente (wie etwa hardwareseitig eine Virtualisierung) auf. Auf der Infrastruktur-Ebene sind sie klassischen IT-Outsourcing-Szenarien allerdings sehr ähnlich. Die Hardware-Ressourcen werden allein für den jeweiligen Nutzer oder Nutzerkreis betrieben und sind daher – im Unterschied zu Public Clouds – regelmäßig kleiner dimensioniert. Private Clouds sind daher nur in Bezug auf die zugrundeliegenden Ressourcen skalierbar und folglich weniger flexibel im Einsatz.

Ausgehend von dieser grundsätzlichen Unterscheidung wird die Kombination von Public und Private Clouds als **Hybrid Cloud** bezeichnet.

Für Cloud-Umgebungen, die wiederum ausschließlich von Unternehmen oder Organisationen mit vergleichbaren (sicherheitstechnischen) Interessen und Anfor-

derungen gemeinsam genutzt werden, hat sich der Begriff **Community Cloud** durchgesetzt. Dies bietet sich auch für den kommunalen Sektor an, weil die Kommunen, die gemeinsame Cloud-Strukturen nutzen bzw. entsprechende IT-Outsourcing-Angebote in Anspruch nehmen, gleichermaßen Rechtsbindungen, Sicherheitsanforderungen oder haushaltsmäßige Grenzen beachten müssen.

Abbildung 3: Bereitstellungsformen

Zur Vertiefung:

Zu den genannten, nicht-abschließenden Bereitstellungsformen tritt zunehmend die **Human Cloud.** Menschen werden dabei freiwillig über das Netz dazu eingebunden, bestimmte Aufgaben zu übernehmen. Dieser Ansatz entspricht dem Crowdsourcing (Schwarmauslagerung: Crowd plus Outsourcing), also der Auslagerung von ursprünglich innerhalb einer Organisation ausgeübten Arbeiten und Leistungen auf die Intelligenz und Arbeitskraft einer unbestimmt großen, heterogenen Masse meist unentgeltlich tätiger Freizeitaktivisten (Crowd) im Internet. Erforderlich sind Aufrufe zur Mitwirkung, die motivieren und insgesamt attraktiv genug wirken. Initiatoren versprechen sich von der kollektiven Intelligenz und Arbeitskraft hochwertige Ergebnisse. Mittlerweile gibt es Plattformen, über welche Interessierte direkt angesprochen werden können, und Crowdrecruiter, die von sich aus Interessenten für Jobs anbieten. Erfolgsentscheidend für diese „People Services“ und „Human Cloud Services“ wird es sein,

verlässliche Plattformen mit attraktiven Experten, engagierten Bürgern und versierten Crowdmanagern zusammenzustellen.

Vertiefungshinweise:

Lucke, v., Open Government Collaboration, 25.20.2012, Kap 2.5, S. 3, http://www.zu.de/deutsch/lehrstuehle/ticc/JvL-121025-OpenGovernmentCollaboration-V1.pdf

Hammon/Hippner, Crowdsourcing, Wirtschaftsinformatik, 54. Jahrgang, Heft 3, Wiesbaden 2012, S. 165-168.

Hoßfeld/Hirth/Tran-Gia, Crowdsourcing, in: Informatik-Spektrum, 35. Jahrgang, Heft 3, Heidelberg 2012, S. 204-208.

Das begriffliche Verständnis von Cloud Computing in der C^3-Studie

In der vorliegenden Studie werden die Begriffsdefinition des BSI und die dargestellte, grundsätzliche Unterscheidung zwischen verschiedenen Service-Modellen und Bereitstellungsformen zugrunde gelegt. Das Merkmal einer flexiblen Bereitstellung wird jedoch nicht streng, sondern in einer abgeschwächten Form verstanden. Hierdurch sollen vor allem Private Clouds begrifflich einbezogen werden. Diese enthalten nämlich verschiedene cloud-typische Elemente. Allerdings weisen sie in der Regel nicht das hohe Maß an Flexibilität oder Skalierbarkeit auf, wie dies große Public Clouds kennzeichnet. Der Einsatzbereich der insofern weniger flexiblen Private Clouds ist aber gegenwärtig gerade dort wiederzufinden, wo vor allem auch Sicherheitsanforderungen von zentraler Bedeutung sind: nämlich in IT-Outsourcing-Szenarien von Unternehmen und der öffentlichen Hand. Hochflexible Bereitstellungsmodelle stellen demgegenüber aus Sicht der Cloud Anbieter den Idealfall von Cloud Computing dar.

Typologie in Bezug auf Kontroll- und Sicherheitsanforderungen

Ausgehend von den Bereitstellungsformen lassen sich Cloud-Umgebungen in Bezug auf Kontroll- und Sicherheitsanforderungen anhand des Grades der Kontrollaufgabe sowie der gleichzeitigen Nutzungsmöglichkeiten typisieren.

Private Clouds in Eigenregie (auch internal/insourced cloud) verbleiben vollständig im Kontrollbereich einer verantwortlichen Stelle. Da keinerlei Auslagerung erfolgt, stellen sie grundsätzlich die **sicherste Lösung** dar. Die Datenwolke geht – bildlich gesprochen – nicht über den organisationsinternen Horizont hinaus, den die zugrundeliegende, meist virtualisierte Hardware zur Verfügung stellt. Dem stehen aus wirtschaftlicher und technischer Sicht jedoch vor allem hohe Anschaffungs- und Wartungskosten sowie eine geringe, lediglich auf die jeweilige Hardware beschränkte Skalierbarkeit entgegen.

Private Clouds, die von einem **externen Anbieter** bereitgestellt werden (outsourced private cloud), sind als geschlossene Umgebungen nur einem bestimmten Nutzerkreis zugänglich. Grundsätzlich sind sie mit „klassischen IT-Outsourcing"-Szenarien vergleichbar und hardwareseitig oftmals lediglich um Virtualisierungstechniken ergänzt. Die virtualisierte Hardware kann dabei von einem Nutzer grundsätzlich selbst in ein Rechenzentrum eingebracht werden. Meistens wird sie aber von einem externen Anbieter im Paket mit den Rechenzentrums-Leistungen bereitgestellt. Die Sicherheit der Leistungen eines externen Anbieters ist anhand der auf den jeweiligen Ebenen einer IT-Sicherheitsarchitektur in Betracht zu ziehenden Maßnahmen zu beurteilen.

Von externen Anbietern bereitgestellte, der allgemeinen Öffentlichkeit zugängliche **Public Clouds** werden hohen Sicherheitsanforderungen dagegen am wenigsten genügen. Die Gründe hierfür liegen vor allem in der allgemeinen Zugangsmöglichkeit sowie der gleichzeitigen Nutzung durch mehrere, nicht bekannte Nutzer. In wirtschaftlicher und technischer Hinsicht bieten sie jedoch die meisten Vorteile (v.a. Skalierbarkeit, Elastizität).

Hybrid und **Community Clouds** liegen in Bezug auf Kontroll- und Sicherheitsanforderungen **zwischen Private und Public Clouds**. Bei hybriden Cloud-

Umgebungen wird vor allem der jeweilige Anteil von Private oder Public Cloud zu berücksichtigen sein. Eine sicherheitsspezifische Typisierung von Community Clouds muss demgegenüber vor allem die Anzahl der gemeinsamen, interessengleichen Nutzer sowie die allgemeine Zugänglichkeit der Beurteilung zugrunde liegen. Insoweit können sich sowohl Elemente einer Public Cloud als auch einer Private Cloud wiederfinden.

Aktionsradius des kommunalen Cloud Computing

Cloud Computing im kommunalen Umfeld fasst verschiedene Aktivitäten zur Auslagerung von Leistungen und IT-Leistungen auf einen externen Dienstleister zusammen. Dazu zählen zum Beispiel:

- die Auslagerung kompletter elektronischer Fachverfahren
- die Auslagerung lokaler IT-Dienstleistungen der kommunalen IT-Abteilung
- die Auslagerung ausgewählter kompletter papierbasierter Verfahren in ein kommunales Dienstleistungszentrum (Shared Service Center)
- die Auslagerung ganzer Abteilungen und deren Leistungsspektren in ein kommunales Dienstleistungszentrum (Shared Service Center)
- der Aufbau neuartiger interaktiver Angebote der Verwaltung im Web 2.0 und
- die Nutzung vorhandener interaktiver Angebote Dritter im Web 2.0.

c) Exkurs: Die Cloud-Strategie der EU-Kommission (September 2012)

Mit der am 27.09.2012 veröffentlichten **Strategie** zum Cloud Computing in Europa, KOM(2012) 529 endg., bekennt sich die **EU-Kommission** klar zur Unverzichtbarkeit dieses Geschäftsmodells. Unbegrenzte Leistung, die über das Internet genutzt werden kann, ermögliche sogar den kleinsten Unternehmen, neue, größere Märkte zu erreichen. Die öffentliche Verwaltung werde in die Lage versetzt, ihre Dienste attraktiver und effizienter zu gestalten und dabei gleichzeitig Kosten einzusparen. Die EU-Kommission strebt daher eine rasche Verbreitung von Cloud

Computing in allen Bereichen der Wirtschaft an, wo Kosten für Informationstechnologie eingespart und in Verbindung mit neuen digitalen Geschäftsmodellen Produktivität, Wachstum und die Entstehung von Arbeitsplätzen gefördert werden kann.

Dazu hat die EU-Kommission eine umfangreiche Untersuchung und Befragung der beteiligten Akteure unternommen, um die erforderlichen Handlungsschritte und Hürden zu identifizieren. Die Cloud Strategie solle als politisches Bekenntnis der Kommission, aber auch als Aufruf aller Akteure zur Beteiligung bei diesem Vorhaben verstanden werden. Im Jahr 2020 könnte im Bereich von Cloud Computing ein Umsatz von weiteren 45 Milliarden Euro erwirtschaftet werden. Zugleich könnten 3,8 Millionen Arbeitsplätze geschaffen werden. Zu den Zielen der EU-Kommission gehört auch die Schaffung eines harmonisierten europäischen Binnenmarktes für Cloud Dienstleistungen. **Cloud Computing in der öffentlichen Verwaltung** könne interne Datenverarbeitungsanlagen, Rechenzentren oder entsprechende Abteilungen reduzieren. Gerade öffentliche Stellen sollen aufgrund des wirtschaftlichen Potentials einer Leistungsvergabe bei der Schaffung eines sicheren Cloud-Computing-Umfelds in Europa eine zentrale Rolle einnehmen. Zugleich kann die Nutzung von sicheren Cloud-Lösungen durch die öffentliche Verwaltung dazu beitragen, dass sich gerade auch kleine und mittelständische Unternehmen dazu ermutigt fühlen, auf derartige Leistungen zurückzugreifen.

Nach Auffassung der EU-Kommission sind folgende Hürden zu überwinden:

- Die **Zersplitterung des „digitalen Binnenmarktes“**, der durch divergierendes nationales Recht und Rechtsunsicherheit bei der Anwendung von Gesetzen herbeigeführt wurde, gehöre zu den bedeutsamsten Hürden des Cloud Computings aus der Sicht der Cloud-Kunden und -Provider.
- **Vertragsrechtliche Hürden** seien Unsicherheiten bei der Verfügbarkeit, Portabilität, Berichtigung/Kontrolle und Nutzungsberechtigung. Ein „Dschungel“ an Standards trage zur Verunsicherung bei und verhindere ein angemessenes Niveau an Interoperabilität zur Herstellung von Portabilität.

- **Datenschutzrechtlich** sei unklar, welche (technischen und vertraglichen) Sicherungsmaßnahmen getroffen werden müssten, wie mit Datenschutzverstößen und Schutz vor Angriffen durch Dritte umgegangen werden soll.

Die EU-Kommission betont, dass mit der Cloud Strategie zwar keine Schaffung einer „Europäischen Super-Cloud" angedacht wird, die den öffentlichen Sektor beliefert. Dennoch sollen **öffentlich zugängliche Cloud Dienste (Public Cloud)** eingerichtet werden, die nicht nur im Einklang mit europäischem Recht stehen, sondern auch im Wettbewerb stehen und dabei offen und sicher sein sollen. Vorstöße der öffentlichen Verwaltung zur Einrichtung von Private Clouds blieben davon unberührt.

Cloud Computing im öffentlichen Sektor sollte – soweit dies möglich ist –

- dem Wettbewerb zugänglich sein und gleichzeitig
- den Anforderungen der IT-Compliance und
- weiterer objektiver (Schutz-) Ziele gerecht werden.

Im Rahmen der **Digitalen Agenda** strebt die EU-Kommission ferner eine Vereinfachung der urheberrechtlichen Fragestellungen, Freistellungen und grenzübergreifende Lizensierung an. Cloud Provider müssten einfach und flexibel Lizenzen für Software erwerben können, die sowohl für die Cloud als auch für Content-Plattformen genutzt werden kann. Die Nutzung von Inhalten solle auch für Verbraucher EU-weit vereinfacht werden, wobei eine Privilegierung von Privatkopien, die bei Cloud Diensten, die die Synchronisation mehrerer Endgeräte über einen Storage-Dienst vereinfachen, grundlegend erforscht werden müsse.

Die Frage der Zersplitterung des Rechts werde bereits von der EU-Kommission im Rahmen der **EU-Datenschutzgrundverordnung** thematisiert. Der Entwurf der Datenschutzgrundverordnung adressiere cloud-spezifische Fragen, beende Rechtsunsicherheiten und schaffe eine einheitliche Rechtsordnung in Europa sowie Transparenz in der Datenverarbeitung. Nach Einschätzung der EU-Kommission werde die EU-Datenschutzgrundverordnung die nötigen Bedingungen für Regelungen und Standards im Cloud Computing schaffen. Die erhebliche Hürde datenschutzrechtlicher Unsicherheiten könne daher durch diesen legislativen

Vorstoß gegebenenfalls bereits im Jahr 2013 überwunden werden. In Bezug auf die Anwendung der geltenden Datenschutzrichtline 95/46/EG verweist die Kommission auf die Stellungnahme WP 196 der Art.-29-Datenschutzgruppe. Diese Stellungnahme wird als gute Ausgangsbasis für die künftige europäische Datenschutzgesetzgebung dienen und die Arbeit der nationalen Aufsichtsbehörden leiten.

Im Kern sieht die EU-Kommission drei **Schlüsselmaßnahmen zur weiteren Vorgehensweise** vor:

- Das **Regelungsgewirr bei Standards** (und Definitionen) müsse beendet werden.
- Es bedarf **sicherer und fairer Vertragsbedingungen.**
- Förderung der Innovation im öffentlichen Sektor durch eine **Europäische Cloud Partnerschaft (ECP).**

Mit der ECP soll ein neuer Rahmen für die Förderung von Cloud Computing Programmen und Projekten geschaffen werden. Dabei soll vor allem Fachwissen aus der Industrie und aus dem öffentlichen Sektor zusammengebracht werden.

Insgesamt zeigt das Cloud Strategie Papier der EU-Kommission den Weg zur Umsetzung von Cloud Computing in der EU auf. Diese Stellungnahme wird auch von der Bayerischen Staatsregierung begrüßt. Die Justiz- und Verbraucherschutzministerin Beate Merk gab jedoch zu bedenken, dass Verbraucher bei Storage-as-a-Service-Diensten besser abgesichert sein müssen:

„Auch über den Wolken darf die Freiheit nicht grenzenlos sein“, mahnte Merk. „Es kann deshalb nicht nur darum gehen, Cloud Computing zu fördern, sondern es dürfen auch die Nutzer nicht aus den Augen verloren werden.“ Der Datenspeicher in der Wolke werfe für den Verbraucher drängende Fragen auf: Wer garantiert mir, dass meine Daten vor dem Zugriff Unbefugter geschützt werden? Wie gut sind die Schutzvorkehrungen der Cloud-Anbieter? Sind die bisherigen Angebote nicht zu nebulös? „Auf all diese Fragen muss eine Strategie eine Antwort bieten“, machte Beate Merk deutlich.

Zur Vertiefung:

EU-Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Freisetzung des Cloud-Computing-Potentials in Europa, KOM(2012) 529 endg., http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf

Art.-29-Datenschutzgruppe, WP 196, Opinion 05/2012 on Cloud Computing, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

Hullen, EU-Kommission stellt Weichen für europaweite Förderung des Cloud Computings, jurisPR-ITR 18/2012 Anm. 2.

Maisch, Die Cloud-Strategie der EU-Kommission – Unter Bezugnahme auf die Datenschutz-Grundverordnung und § 203 StGB, jurisAnwZert ITR 23/2012, Anm. 3.

d) Fazit: Cloud Computing – Evolution statt Revolution

Gehen Kommunen in die Cloud, so bedeutet dies zunächst nichts anderes, als dass IT-Leistungen von einem externen Anbieter bezogen werden (ausgenommen ist der vollständige Eigenbetrieb einer Private Cloud). Es liegt insoweit ein IT-Outsourcing der öffentlichen Hand vor. Das gibt es in der kommunalen Praxis im Prinzip schon seit vielen Jahren und zwar in rechtskonformer und wirtschaftlich vernünftiger Weise.

Vertiefungshinweise:

Umfassend hierzu *Heckmann*, IT-Outsourcing der Öffentlichen Hand, in: Bräutigam (Hrsg.), IT-Outsourcing. Eine Darstellung aus rechtlicher, technischer, wirtschaftlicher und vertraglicher Sicht, 2. Aufl. 2009 (3. Aufl. 2013 i. Vorb.), S. 647-725.

Die innovativen Möglichkeiten eines Cloud Computing sind damit aber nicht ausgeschöpft. Cloud Computing in dem vorstehend dargestellten Sinne und Umfang kann als adäquate Antwort auf die Herausforderungen der **Verwaltungsmodernisierung** im IT-Zeitalter angesehen werden. Es ist damit eine Weiterentwicklung (Evolution) der technisch-organisatorischen Möglichkeiten kommunaler Aufgabenerledigung und Verwaltungsführung – und keine Revolution. Dafür müssen allerdings die Vorteile und Chancen genutzt, die Risiken minimiert und notwendige Sicherheitsmaßnahmen ergriffen werden. Dies wird nunmehr auch von der EU-Kommission in ihrer vorstehend skizzierten Cloud Strategie vom 27.09.2012 so gesehen.

2. Brauchen Kommunen „dieses Cloud Computing“?

Cloud Computing gehört zu jenen Begriffen einer Techniksprache, die schon wegen der heterogenen Motive ihrer Protagonisten (Marketing und Vertrieb der Cloud Anbieter, Datenschützer, Medien u.a.m.) sehr uneinheitlich, verunklarend und interessensgeleitet verwendet werden. Solchen „Vor-Urteilen“ gilt es mit einem ganz nüchternen Blick auf die Fakten zu kontern: Was sind die Vorteile und Chancen, was die Nachteile und Risiken des IT-Outsourcing in der Form von Cloud Computing?

a) Die wichtigsten Vorteile „auf einen Blick“

Die Komplexität der auf kommunaler Seite zu erfüllenden Aufgaben nimmt ständig zu. Zugleich werden die zur Erfüllung von Aufgaben zur Verfügung stehenden Mittel ständig reduziert. Ein erfolgreicher und effizienter Einsatz von IT kann somit maßgeblich zum Erhalt und zur weiteren **Steigerung der Leistungsfähigkeit der öffentlichen Hand** beitragen.

- Durch Cloud Computing können die Qualität der Datenverarbeitung und das Sicherheitsniveau gesteigert werden, wenn auf einen diesbezüglich spezialisierten Dienstleister zurückgegriffen wird. Selbst hohe Sicherheitsstandards können gewahrt werden, sofern ein Anbieter auf derartige Lösungen spezialisiert ist. Dies vermag auch ein wenig den Fachkräftemangel auszugleichen.

  Kleine Kommunen *profitieren insbesondere von einer Steigerung der Qualität und Verfügbarkeit der Anwendungen sowie von einer Verbesserung des Datenschutzes. Dies betrifft vor allem die Auslagerung von technisch anspruchsvollen Fachverfahren (Standesamt, Finanzen, Einwohnerwesen etc.).*

- Der **Wartungsaufwand** für Soft- und Hardware kann gesenkt werden.
- Ein Rückgriff auf das **Know-how spezialisierter Anbieter** kann zu Personaleinsparungen führen.

- Cloud Computing ermöglicht es ferner, einen projektbezogenen Bezug von IT-Serviceleistungen herzustellen und das **Betriebsrisiko zu vermindern**.
- Wirtschaftliche Vorteile bestehen darin, IT-Infrastrukturen bedarfsorientiert, flexibel und damit kostensparend beziehen zu können. Während in dem wiederkehrenden Kernbereich der Verwaltungstätigkeit (v.a. bei Fachanwendungen, Arbeitsplatzlizenzen) meist ein gleichbleibender Bedarf vorliegen wird, können flexible Nutzungsmodelle gerade in Randbereichen der Verwaltungstätigkeit zu wirtschaftlichen Vorteilen führen.
- Durch den Rückgriff auf einen spezialisierten Anbieter können **Investitions- und Betriebskosten gesenkt** werden (im Vergleich zu einer „in house"-Lösung der Kommune).
- **Fixkosten** können **in variable Kosten** gewandelt werden.
- Durch die **Nutzung verteilter Ressourcen** kann zugleich die Redundanz und Verfügbarkeit und damit die Qualität der Datenverarbeitung erhöht werden.

Richtig und effektiv eingesetztes Cloud Computing kann im kommunalen Sektor als Chance zur Verwirklichung effizienter und bürgerfreundlicher E-Government-Konzepte verstanden werden. Gerade für kleine Kommunen kann sich hierbei mitunter auch eine interkommunale Zusammenarbeit anbieten.

b) Die meistgenannten Risiken

Jede Form von IT-Outsourcing enthält verschiedene Risiken. Zu den klassischen Risiken können dabei sog. **cloud-spezifische Risiken** hinzutreten. Es werden drei Kategorien differenziert: Die Auslagerung von Daten und Diensten kann vor allem durch rechtliche, organisatorische und technische Risiken beeinträchtigt werden.

Zur Vertiefung:

Nach diesen Kriterien differenziert auch die Europäische Agentur für Netz- und Informationssicherheit (ENISA) in einem Leitfaden zu Cloud Computing („Cloud

Computing, Benefits, risks and recommendations for information security, S. 26 ff.). Cloud-spezifische Risiken werden ferner im BSI-Leitfaden „Sicherheitsempfehlungen für Cloud Computing Anbieter" aus dem Jahr 2011 ausgeführt. Rechtliche Empfehlungen finden sich beispielsweise in einem Leitfaden des Branchenverbandes EuroCloud Deutschland_eco e.V. „Leitfaden Cloud Computing: Recht, Datenschutz & Compliance" aus dem Jahr 2010.

Vertiefungshinweise:

ENISA, Cloud Computing, Benefits, risks and recommendations for information security (2009), http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

EuroCloud Deutschland_eco e.V. , „Leitfaden Cloud Computing: Recht, Datenschutz & Compliance" (2010)

- **Rechtliche Risiken** sind vor allem mit Fragen des **Datenschutzes** und der **Datensicherheit** verbunden. Aspekte der Datensicherheit beziehen sich vor allem auf die Gewährleistung der **Vertraulichkeit**, **Verfügbarkeit** und **Integrität** von Daten. Vor allem die Virtualisierung von IT-Systemen gefährdet dabei das Schutzziel der Vertraulichkeit. Nach derzeitiger Rechtslage gibt es keine konkreten Vorschriften, die den Besonderheiten von Cloud Computing insoweit Rechnung tragen (allerdings auch keine Rechtsvorschriften, die Cloud Computing dezidiert verbieten). Zu den rechtlichen Risiken zählen auch **legale Zugriffsmöglichkeiten von Sicherheitsbehörden in Drittstaaten**. Dies betrifft besonders den Patriot Act in den USA, der US-amerikanischen Sicherheitsbehörden Zugriffsmöglichkeiten selbst auf Cloud-Inhalte US-amerikanischer Unternehmen außerhalb der USA eröffnen kann, soweit diese im Kontext mit einer terroristischen Gefahr stehen oder dies in Betracht gezogen wird.

- Zu den **organisatorischen Risiken** zählt die **Anbieterabhängigkeit** (sog. Vendor-Lock-in). Hierunter wird die faktische Abhängigkeit eines Nutzers von den Dienstleistungen eines Cloud-Anbieters verstanden. Die Leistung ist meist derart spezifisch (und erfüllt keine anerkannten Standards), dass vergleichbare Dienste am Markt (fast) nicht existieren. Eine derartige Abhängigkeit kann von Relevanz sein, wenn etwa große Datenbestände aus der Sphäre des Anbieters exportiert oder kündigungsbedingt auf einen anderen Dienstleister im Rahmen eines Anbieterwechsels übertragen werden sollen. Organisatorische Risiken können i.Ü. durch **missverständliche Datensicherheitskonzepte** und Service Level Agreements verursacht werden.

- Unter **technischen Risiken** werden von der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) u.a. die **Erschöpfung der IT-Ressourcen** und die **Verwundbarkeit der Cloud-Technologie** angeführt. Außerdem spielt auch die Verlässlichkeit der Netzinfrastruktur im Allgemeinen eine zentrale Rolle. Ein Cloud-Provider wird in der Regel automatisierte Verfahren nutzen, um die IT-Ressourcen seiner Kunden zu verwalten. Verfügbarkeitsengpässe oder Schwachstellen bei Sicherheitssystemen sind nicht ausgeschlossen, wenn der IT-Diensteanbieter keine ausreichenden Maßnahmen zur Gewährleistung der Datensicherheit vornimmt. Durch den Einsatz virtueller Maschinen entstehen neue Angriffsvektoren, u.a. im Kontext mit der Multimandantenfähigkeit. Eine Zusammenstellung der wichtigsten technischen Risiken, die im Kontext von Cloud Computing in Betracht zu ziehen sind (wie Verfügbarkeit von Cloud-Umgebung oder Netzwerk, Ausfallrisiken, allgemeine Aspekte der Datensicherheit), findet sich auf Seite 74 ff.

Die hier skizzierten Risiken müssen von der Kommune ernstgenommen und frühzeitig berücksichtigt werden. Daher muss darauf geachtet werden, dass im Rahmen der Beschreibung der technischen und organisatorischen Maßnahmen in

einem Auftrag auf diese Risiken Bezug genommen wird und konkrete Lösungen im Rahmen eines IT-Sicherheitskonzepts gefordert werden.

c) Fazit: Abwägung von Chancen und Risiken

Cloud Computing enthält, wie dargelegt, diverse Risiken, die den Vorteilen und Chancen gegenüberstehen. Die Entscheidung, ob und in welchem Umfang Cloud Services zum Einsatz gelangen können, sollte daher anhand einer vordefinierten Herangehensweise (Compliance Management) unter Zugrundelegung eines **Informationssicherheitsmanagementsystems** (ISMS) erfolgen. In diesem Rahmen sind vor allem die gesetzlichen und organisationsinternen Anforderungen zu ermitteln und mit einer Bedarfs-, Wirtschaftlichkeits-, Sicherheits- und Risikoanalyse zu verknüpfen. Dabei ist es erforderlich, dass sämtliche Phasen eines IT-Outsourcings (Planung, Migration in die Cloud, Betriebsphase, Beendigung/Exit) Berücksichtigung finden. Die Bestimmung der Sicherheitsanforderungen hat vor allem die jeweiligen Datenkategorien zu berücksichtigen, die Gegenstand des kommunalen IT-Outsourcings sind. In dem vorliegenden Leitfaden finden sich vor allem im Rahmen der Anbieterauswahl (siehe S. 45 ff.) und bei den nach Vertragsabschluss zu berücksichtigenden Aspekten (siehe S. 72 ff.) wichtige Hinweise, die von einer Kommune auf dem Weg in die Cloud insoweit zu beachten sind. Die Besonderheiten eines jeden einzelnen Cloud Services sind jedoch stets zu berücksichtigen. Insoweit kann der Rat eines auf (Rechts-) Fragen von Cloud Computing spezialisierten Experten einzuholen sein.

Zur Klarstellung ist hervorzuheben, dass es nicht darum gehen kann, sämtliche Risiken vollständig auszuschließen (dies ist weder praktisch möglich noch rechtlich geboten), sondern die Risiken in Abwägung mit den Chancen im Kontext der rechtlichen, technischen und ökonomischen Bedingungen zu minimieren. Für Datenschutz und Datensicherheit gilt das **Prinzip der Angemessenheit** (Art. 7 Abs. 1 Satz 2 BayDSG).

Hilfreich ist insoweit auch eine sog. SWOT-Analyse (unterschieden nach Strengths (Stärken), Weaknesses (Schwächen), Opportunities (Chancen) und Threats (Risiken).

Stärken	Schwächen
• Steigerung der Qualität der Datenverarbeitung • Senkung der Wartungskosten • Nutzung verteilter Ressourcen	• Rechtslage teilweise nicht geklärt • Kosten für Vertragsverhandlungen • Koordinierungsaufwand und -kosten • Überwachung der Vertragserfüllung • Zusätzliche Transaktionskosten
Chancen	**Risiken**
• Wirtschaftliche Vorteile • Senkung der Investitionskosten • Betriebsrisikominderung • Rückgriff auf Spezialisten • Schub für das E-Government	• Anbieterabhängigkeit • Erschöpfung der IT-Ressourcen • Technische Verwundbarkeit • Verstöße gegen den Datenschutz • Verstöße gegen die Datensicherheit

Tabelle 1: Kompaktanalyse zum Cloud Computing

3. Dürfen Kommunen überhaupt Cloud-Services nutzen?

Als eine der wesentlichen Hürden für Cloud Computing im Allgemeinen und die Nutzung von Cloud Services durch die öffentliche Verwaltung im Besonderen werden immer wieder rechtliche Bedenken genannt. Insbesondere im Hinblick auf Datenschutz und Datensicherheit werden die rechtlichen Anforderungen so eingestuft, dass etwa kommunales Cloud Computing eigentlich nicht in Betracht gezogen werden würde. Dürfen Kommunen überhaupt Cloud Services nutzen? Diese Frage muss beantwortet werden, bevor man sich Gedanken über die Gestaltung macht. Sie kann aber wiederum gar nicht abschließend beantwortet werden, ohne die konkrete Gestaltung zugrunde zu legen. Denn das sei vorab gesagt: Rechtskonformes Cloud Computing ist keine Frage des „Ob“, sondern eine Frage des „Wie“.

a) Verfassungsrechtliche Grenzen

Verfassungsrechtliche Grenzen ergeben sich für Cloud-Dienste zunächst dort, wo auch IT-Outsourcing eingeschränkt ist, nämlich bei der Beauftragung privater Cloud-Anbieter. Ein derartiger Rückgriff ist zwar nicht grundsätzlich verboten, unterliegt jedoch den **Grenzen des Art. 33 Abs. 4 GG**.

Nach Art. 33 Abs. 4 GG ist „die Ausübung hoheitsrechtlicher Befugnisse ... als ständige Aufgabe in der Regel Angehörigen des öffentlichen Dienstes zu übertragen, die in einem öffentlich-rechtlichen Dienst- und Treueverhältnis stehen“. Dieser Funktionsvorbehalt setzt auch einem IT-Outsourcing an private IT-Dienstleister Grenzen. Dies gilt etwa für die Verlagerung solcher Datenverarbeitungsvorgänge, die eine besondere Grundrechtsrelevanz haben oder unmittelbar hoheitliche Entscheidungen bewirken. Erlaubt ist umgekehrt eine Auftragsdatenverarbeitung, soweit diese auf die Erbringung technischer Hilfeleistungen gerichtet ist. Solche

Hilfeleistungen müssen in Bezug auf die Verwaltungsaufgabe von ausschließlich dienender und untergeordneter Art sein und dürfen keine besondere Gefährdungslage schaffen.

Gemäß Art. 33 Abs. 4 GG dürfen den Beamten vorbehaltene Aufgaben mithin nicht aus dem staatlichen **Organisationszusammenhang** gerissen und auf private Stellen ausgelagert werden. Von der hoheitlichen Aufgabenwahrnehmung ist allerdings die aus verfassungsrechtlicher Sicht zulässige Wahrnehmung bloßer technischer Hilfsfunktionen zu unterscheiden. Für die Abgrenzung ist dabei maßgeblich auf die Möglichkeit abzustellen, eine hoheitliche Entscheidung zu treffen (dann handelt es sich um eine privatisierungsfeindliche hoheitliche Aufgabenwahrnehmung). Für die Zulässigkeit des IT-Outsourcings durch Cloud-Services im öffentlichen Sektor kommt es demnach vor allem darauf an, inwieweit die **Entscheidungsbefugnis** über die Datenverarbeitung und diesbezügliche Weisungsrechte bei der öffentlichen Hand verbleiben.

Im Rahmen der Einbindung von Cloud-Services in den Verwaltungsalltag stellt sich weiterhin die Frage, ob mittels der Schaffung einer technisch-organisatorischen Verflechtung gegen das **Verbot der Mischverwaltung** verstoßen wird. Dieses Verbot folgt aus der Feststellung, dass die verfassungsrechtliche Verteilung der Verwaltungskompetenzen nicht zur Disposition der Beteiligten steht. Vielmehr handelt es sich um „eine zwingende Ordnung, die gerade nicht durch informelle Vereinbarungen oder einfachgesetzliche, von der Grundstruktur des GG abweichende Regelungen abbedungen werden kann."

Ein Verstoß kommt insbesondere dann in Betracht, wenn nicht lediglich die IT eines einzelnen Trägers der öffentlichen Verwaltung virtualisiert wird, sondern vielmehr eine ebenenübergreifende Realisierung von Cloud Computing angestrebt wird. Derartige IT-Kooperationen stehen im Verdacht, gegen das Verbot der Mischverwaltung zu verstoßen. Insoweit ist allerdings zu berücksichtigen, dass das Verbot der Mischverwaltung vor allem eine Preisgabe von Entscheidungskompetenzen verhindern und eine eigenverantwortliche Aufgabenwahrnehmung gewährleisten möchte. Die Kompetenzordnung der Art. 83 ff. GG betrifft primär den Gesetzesvollzug und mithin die Erledigung von Sachaufgaben. Sofern eine Auswir-

kung des IT-Outsourcings auf den Gesetzesvollzug ausgeschlossen werden kann, sind diesbezügliche Kooperationsformen verfassungsrechtlich zulässig. Nach bislang herrschender Auffassung ist damit der Aufbau und Betrieb gemeinsamer IT-Infrastrukturen unter Verwendung von Cloud-Lösungen möglich, wenn nicht bei wirtschaftlicher Betrachtung eventuell sogar erforderlich.

Eine weitere verfassungsrechtliche Schranke für Cloud Computing im öffentlichen Sektor ergibt sich aus dem sog. **IT-Grundrecht** (Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme). Dieses schützt nicht nur das Interesse des IT-Verwenders, der möchte, dass die von ihm mittels eines IT-Systems erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Vielmehr sind dem IT-Grundrecht über seine Abwehrfunktion hinaus auch weitergehende **Schutzpflichten** des Staates zu entnehmen, die allerdings auch Vorkehrungen zur Reduzierung derjenigen Gefährdungen umfassen, die außerhalb des Bereichs staatlicher Eingriffsmaßnahmen verortet werden können.

Der Staat hat folglich **Maßnahmen** zu ergreifen, die darauf abzielen, die Infiltration, Manipulation und Ausforschung informationstechnischer Systeme zu verhindern, mittels derer Daten verarbeitet werden, die einem Grundrechtsträger zugeordnet werden können. Diese Gefahr liegt im Rahmen des Einsatzes von Cloud Computing-Lösungen nicht fern. Gerade bei multimandantenfähigen Public Clouds (oder Community Clouds) stellt sich die Frage, wie die öffentliche Hand sicherstellen kann, dass die Integrität der genutzten IT-Ressourcen gewährleistet wird und der Schutzanspruch jedes einzelnen Bürgers auf Gewährleistung der Vertraulichkeit seiner Daten nicht verletzt wird.

Insgesamt sind es die **rechtsstaatlichen Anforderungen** der Gesetzmäßigkeit der Verwaltung gem. Art. 20 Abs. 3 GG und des notwendigen Grundrechtsschutzes zugunsten der Bürger und Unternehmen, die dem Einsatz innovativer Technologien verfassungsrechtliche Grenzen setzen. Weitere Grenzen, die jede Behörde beim IT-Outsourcing beachten muss, können sich aus dem Haushalts- und Vergaberecht ergeben (insbesondere die Wirtschaftlichkeitsbetrachtung nach Art. 7 Abs. 2 BayHO oder die Pflicht zur öffentlichen Ausschreibung nach Art. 55 BayHO i.V.m. Vergaberecht; zu letzterem siehe auch auf S. 47). Cloud Computing darf auch

insoweit kein abenteuerliches IT-Projekt darstellen, sondern muss auf solider Grundlage geplant und durchgeführt werden. Die Verwaltung muss handlungsfähig und vertrauenswürdig sein. Deshalb ist IT-Sicherheit im Sinne der Verfügbarkeit und Vertraulichkeit der Datenverarbeitung (ob mit oder ohne Cloud) zu gewährleisten. Bei deren Beachtung steht umgekehrt das Verfassungsrecht einem Cloud Computing im öffentlichen – und dabei insbesondere im kommunalen – Sektor nicht im Wege.

b) Gesetzliche Vorgaben

Die Nutzung von Cloud Services kann aber auch eine **Vielzahl an gesetzlichen Bestimmungen** (etwa aus dem Vertragsrecht, Datenschutzrecht, Datensicherheit oder Urheberrecht) berühren. Die Ermittlung der für ein konkretes IT-Outsourcing-Szenario einer Kommune insgesamt in Betracht kommenden Vorschriften muss insoweit grundsätzlich anhand einer einzelfallbezogenen Betrachtung erfolgen.

Zur Vertiefung:

Die juristische Literatur verweist auf verschiedenste Fragestellungen, die bei Cloud Computing auf Gesetzesebene zu berücksichtigen sein können. Cloud Computing enthält hiernach vor allem neue Herausforderungen in vertrags- und datenschutzrechtlicher Hinsicht sowie an die allgemeinen Grundsätze der Daten- und Informationssicherheit. Daneben kann das Rechnen in der Wolke aber beispielsweise auch Fragen des Urheberrechts, des Straf- und Strafprozessrechts oder des Bilanz- und Steuerrechts – sowie zahlreiche bereichsspezifische Sondervorschriften (datenschutzrechtlich sei insofern vor allem auf die Bestimmungen des TMG oder des TKG verwiesen) – betreffen.

Vertiefungshinweise:

Niemann/Paul, Kommunikation & Recht (K&R), 2009, 444 ff. (Überblick)

Pohle/Ammann, Computer & Recht (CR) 2009, 273 ff. (Überblick)

Bierekoven, IT-Rechtsberater (ITRB) 2010, 42 ff. (zu Urheberrecht)

Bisges, MultiMedia und Recht (MMR) 2012, 574 ff. (zu Urheberrecht)

Gercke, Computer & Recht (CR) 2010, 345 ff. (zu Straf-/Strafprozessrecht)

Die Frage, ob eine Kommune einen bestimmten Cloud Service nutzen darf, wird jedoch vor allem anhand von Aspekten des Datenschutzes und der Datensicherheit zu beantworten sein. Dementsprechend steht der datenschutzrechtliche Rechtsrahmen daher auch im Fokus der nachstehenden Darstellung.

Der gesetzliche Rechtsrahmen für Datenschutz

Der Datenschutz ist sowohl in Bundesgesetzen als auch in Landesgesetzen geregelt. Für nicht-öffentliche Stellen sowie für **öffentliche Stellen des Bundes** richtet sich die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach dem BDSG. Bayerische **öffentliche Stellen** unterliegen hingegen dem **BayDSG**. Datenschutzrechtliche Regelungen finden sich überdies in einer Vielzahl an bereichsspezifischen Regelwerken (auf Bundesebene v.a. § 11 ff. TMG [Telemediengesetz], §§ 91 ff. TKG [Telekommunikationsgesetz], § 80 SGB X, § 146 Abs. 2, Abs. 2a AO [Abgabenordnung]; auf Landesebene etwa Art. 33 BayMeldeG [Bay. Gesetz über das Meldewesen]) wieder. Da die Frage der Nutzung von Cloud Services durch eine bayerische Kommune anhand des BayDSG zu beantworten ist, wird im Folgenden allein auf die dort enthaltenen Regelungen eingegangen.

Der Personenbezug von Daten

Das BayDSG ist nur bei **personenbezogenen Daten** anwendbar (Art. 4 BayDSG). Dies sind Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen (Betroffene). Derartige bestimmte Einzelangaben sind unzweifelhaft vor allem in Meldedaten, Personenstandsdaten (Standesamt), Personaldaten (Gehaltsabrechnung, Lohnbuchhaltung), Steuerdaten oder in Sozialdaten enthalten.

Die hohe Praxisrelevanz der Datenkategorie „personenbezogener Daten“ ergibt sich aber vor allem aus dem Tatbestandsmerkmal der **Bestimmbarkeit**. Eine Bestimmbarkeit liegt vor, wenn sich anhand der in einem Datensatz enthaltenen Informationen die Verbindung zu einer natürlichen Person herstellen lässt. Zur Bejahung einer solchen Verknüpfungsmöglichkeit ist – nach dem gegenwärtigen Verständnis – nicht allein auf die Kenntnisse und Möglichkeiten einer Kommune als verantwortlicher Stelle abzustellen. Allgemein bestehende Verknüpfungsmöglichkeiten – vor allem unter Zuhilfenahme der Kenntnisse von Dritten – reichen aus, um eine Bestimmbarkeit zu bejahen. In der Praxis bedeutet dies, dass Daten, die auf den ersten Blick datenschutzrechtlich neutral aussehen, dennoch ein personenbezogenes Datum darstellen können. Vor allem bei IP-Adressen ist insoweit von einem Personenbezug auszugehen. Zugleich bestehen aber auch Abgrenzungsschwierigkeiten. Sind etwa Geodaten – die auf den ersten Blick als bloße Sachdaten erscheinen – auch personenbezogene Daten? Sofern derartige Datensätze zugleich Referenzierungen enthalten (sog. Georeferenzdaten), die eine Profilbildung ermöglichen, wird auch hier von einem Personenbezug auszugehen sein. Als Faustregel gilt daher, dass die Bestimmbarkeit grundsätzlich sehr weit zu verstehen und im Zweifel zu unterstellen ist.

Zur Vertiefung:

Als **„bestimmt“** sind Einzelangaben einer natürlichen Person anzusehen, die eine unmittelbare Zuordnung ermöglichen (v.a. Name, Adresse, E-Mail-Adresse, Personalausweisnummer, Steuer-ID). Wie dargelegt, sind derartige Angaben vor allem in Meldedaten, Personenstandsdaten, Sozialdaten und in den für die Lohn- und Gehaltsabrechnung erforderlichen Personaldaten wiederzufinden.

Die Alternative der **„Bestimmbarkeit“** ist im Rahmen des „Personenbezugs von Daten“ jedoch ein in Rechtsprechung und juristischer Literatur seit langem umstrittenes und lebhaft diskutiertes Thema.

Nach der **objektiven Theorie des absoluten Personenbezugs** reicht hiernach jede theoretische Möglichkeit, anhand derer eine Verbindung zu einer Person hergestellt werden kann. Zur Bejahung eines Personenbezugs kommt es demnach

nicht bloß auf die Möglichkeiten oder das bei einer verantwortlichen Stelle vorhandene Zusatzwissen an. Auch das Wissen Dritter ist zu berücksichtigen. Hiernach stellen beispielsweise IP-Adressen ein personenbezogenes Datum dar. Eine Zuordnung zu einer natürlichen Person ist insofern nämlich unter Einbeziehung der Kenntnisse des jeweiligen Access-Providers möglich.

Die **Theorie der Relativität des Personenbezugs** zieht in ihre Betrachtung die Kenntnisse Dritter nicht mit ein. Sie stellt im Hinblick auf die Bestimmbarkeit vielmehr allein auf die Kenntnisse und Zuordnungsmöglichkeiten der datenverarbeitenden Stelle ab. Bei der zuvor beispielhaft angeführten IP-Adresse ist hiernach ein Personenbezug zu verneinen, da das Wissen des Access-Providers (als Dritter) in die Betrachtung gerade nicht einzubeziehen ist. Verfügt eine datenverarbeitende Stelle jedoch selbst über ein entsprechendes Zusatzwissen, ist der Personenbezug nach dieser Ansicht zu bejahen. Ein derartiges Zusatzwissen kann vor allem bei Anbietern von großen Shop-Systemen oder sozialen Netzwerken regelmäßig unterstellt werden. Aufgrund der umfangreichen Datenbestände über einen Nutzer (v.a. aufgrund einer Registrierungspflicht, um den Dienst nutzen zu können) wird es diesen Anbietern regelmäßig möglich sein, Verbindungsdaten (IP-Adressen und Angaben über Beginn und Ende einer Nutzung) mit Bestandsdaten zu verknüpfen.

Die Theorie der Relativität des Personenbezugs galt lange Zeit als herrschend. Gerade in den letzten Jahren befindet sich jedoch die objektive Theorie des absoluten Personenbezugs zunehmend im Vordringen. Uneinheitliche Rechtsprechung zu der Frage der Personenbeziehbarkeit von IP-Adressen hat zur bestehenden Rechtsunsicherheit beitragen. In der Praxis ist daher davon auszugehen, dass die Bestimmbarkeit im Zweifel weit zu verstehen ist. In diese Richtung zielt auch der Entwurf zur EU-Datenschutzgrundverordnung der EU-Kommission, der in Zukunft das nationale Recht im Bereich der nicht-öffentlichen Stellen ersetzen wird.

Verbot mit Erlaubnisvorbehalt, Ermächtigungsgrundlage

Nach der gesetzlichen Systematik des BayDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit eine Erlaubnisnorm vorliegt oder ein Betroffener einwilligt (vgl. Art. 1, 15 BayDSG). Da in der behördlichen Praxis nicht für jede externe Datenverarbeitung die **Einwilligung** eines Betroffenen eingeholt werden kann, wird für die Datenübermittlung an einen Dritten regelmäßig eine Ermächtigungsgrundlage erforderlich sein. Eine derartige Erlaubnisnorm für die Datenübermittlung an öffentliche Stellen stellt Art. 18 BayDSG dar. Datenübermittlungen an nicht-öffentliche Stellen sind unter Einhaltung der Voraussetzungen von Art. 19 BayDSG zulässig. Datenübermittlungen an Stellen in das Ausland richten sich nach Art. 21 BayDSG. In den Fällen einer Datenübermittlung überträgt die verantwortliche Stelle zugleich ihre Verantwortung für Daten.

Auftragsdatenverarbeitung

Erfolgt der Rückgriff auf einen externen Dienstleister allerdings im Wege einer Auftragsdatenverarbeitung, so bleibt der Auftraggeber datenschutzrechtlich verantwortlich. Eine Datenverarbeitung im Auftrag setzt dabei voraus, dass auf Seiten eines Auftragnehmers kein weiteres Ausführungsermessen besteht. Im Anbieter-Nutzer-Verhältnis kann die standardisierte Bereitstellung von IaaS-, PaaS- oder SaaS-Leistungen (vgl. dazu S. 13) insoweit regelmäßig als eine klassische Konstellation einer Auftragsdatenverarbeitung angesehen werden. Meist wird schon aufgrund des hohen Standardisierungsgrades einer Cloud-Leistung von einem Ausführungsermessen auf Seiten eines Anbieters nicht auszugehen sein.

Beispiele hierfür sind etwa die standardisierte Bereitstellung von Rechenkapazität oder Speicherplatz, von Firewallsystemen, Antivirensoftware, Büroanwendungen oder Exchange-Postfächern.

Im Falle einer **Datenverarbeitung im Auftrag** werden Auftraggeber und Auftragnehmer rechtlich als Einheit betrachtet. Es liegt somit **keine Datenübermittlung** an einen Dritten vor. Die Datenweitergabe ist privilegiert und bedarf daher keiner Ermächtigungsgrundlage (Verbot mit Erlaubnisvorbehalt, vgl. zuvor). Es sind allein

die für eine Auftragsdatenverarbeitung geltenden formalen Bestimmungen von einem Auftraggeber zu beachten. Für bayerische Kommunen sind diese in Art. 6 und 7 BayDSG enthalten. Hiernach ist ein Auftragnehmer vor allem unter besonderer Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen auszuwählen. Zugleich bestehen hierzu korrespondierende Kontrollpflichten (vgl. unten S. 74).

Kommt es bei der Nutzung cloud-basierter Dienste, wie es regelmäßig der Fall sein wird, zur Verarbeitung personenbezogener Daten Art. 4 Abs. 1 BayDSG, so ist im Verhältnis des Anwenders zum Diensteanbieter von einer **Auftragsdatenverarbeitung i.S.d. Art. 6 Abs. 1 BayDSG** auszugehen, bei der der Auftraggeber als „Herr der Daten" datenschutzrechtlich verantwortlich bleibt. Art. 6 Abs. 1, 2 BayDSG regelt – anders als § 11 Abs. 2 BDSG – nicht im Detail, welche Anforderungen an einen IT-Outsourcing-Vertrag, also die Vereinbarung zur Auftragsdatenverarbeitung, zu stellen sind. Im schriftlichen Auftrag sind demnach (lediglich) Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen. Der Auftraggeber hat sich, soweit erforderlich, von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen (näher beschrieben in Art. 7 BayDSG) beim Auftragnehmer zu überzeugen. Man kann unterdessen davon ausgehen, dass der **Anforderungskatalog**, der auch erst kürzlich in § 11 Abs. 2 BDSG konkretisierend normiert wurde, in vergleichbarer Weise für die Auftragsdatenverarbeitung von bayerischen Behörden anzuwenden ist.

Vertiefungshinweise:

Heckmann, Cloud Computing im Zeitgeist. Juristische Hürden, rechtspolitische Unwägbarkeiten, unternehmerische Gestaltung, in: Festschrift für Thomas Würtenberger, hrsg. von Dirk Heckmann, Ralf Schenke und Gernot Sydow, 2013, S. 7 ff.

Maisch/Seidl, Cloud Government: Rechtliche Herausforderungen beim Cloud Computing in der öffentlichen Verwaltung, VBl BW 2012, 7 ff.

Niemann/Hennrich, Kontrollen in den Wolken? – Auftragsdatenverarbeitung in Zeiten des Cloud Computings, CR 2010, 686 ff.

Hennrich, Compliance in Clouds – Datenschutz und Datensicherheit in Datenwolken, CR 2011, 546 ff.

Bereichsspezifische Besonderheiten für eine Auftragsdatenverarbeitung

Sofern **bereichsspezifische Vorschriften** dem BDSG bzw. BayDSG vorrangig sind, sind die dort enthaltenen Regelungen zusätzlich zu beachten. Für die Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag ist insoweit etwa auf die weitergehenden Voraussetzungen von **§ 80 SGB X** zu verweisen. Die Auftragsdatenverarbeitung von Sozialdaten durch nichtöffentliche Stellen (bspw. private Unternehmen) ist nur zulässig, wenn beim Auftraggeber sonst Störungen im Betriebsablauf auftreten können, die Datenverarbeitung erheblich kostengünstiger ist und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst (vgl. § 80 Abs. 5 SGB X). Dagegen konkretisiert beispielsweise **Art. 33 BayMeldeG** die Modalitäten einer Datenspeicherung. Im Falle der Datenverarbeitung für mehrere Meldebehörden kann eine beauftragte Stelle hiernach die Daten eines Einwohners in einem Datensatz speichern, sofern sichergestellt wird, dass die jeweilige Meldebehörde auf diesen Datensatz nur im Rahmen ihrer Zuständigkeit zugreifen kann. Regelungen zum Datenschutz finden sich beispielsweise aber auch in **Art. 27 des Bayerischen Krankenhausgesetzes** für Patientendaten wieder. Das Spektrum an datenschutzrechtlichen Vorschriften auf Gesetzesebene ist daher sehr breit und muss einzelfallbezogen bewertet werden.

So kann es aufgrund spezieller Anforderungen im Einzelfall auch zu einem **Privatisierungsverbot** kommen, was ein IT-Outsourcing und damit auch Cloud Computing Dienste von vorneherein ausschließt. So kann zum Beispiel die **Personenstandsdatenverarbeitung** (als „Ganzes“) nicht als technisch-administrative Hilfeleistung, sondern muss als Hauptleistung angesehen werden, die im Kern Hoheitsverwaltung ist und damit nicht von Privaten erledigt werden darf. Im Personenstandswesen ist die Erhebung und Verarbeitung der Daten primäre, praktisch einzige Aufgabe der Verwaltung; sie ist nicht Mittel zum Zweck, sondern der Zweck selbst. Der gesamte Verwaltungsvorgang spielt sich mittlerweile in den

Fachverfahren und in der Registerführung ab. Überträgt man dessen Grundlage, die Erfassung, Speicherung und Verarbeitung der Personenstandsdaten, in private Hände, ist nicht mehr der Dienstleister verlängerter Arm der Behörde, sondern der behördliche Sachbearbeiter eine Art Stenotypist des IT-Dienstleisters, unter dessen Regie die eigentliche Datenverarbeitung stattfindet. Eine Datenherrschaft der Standesämter wäre, selbst wenn man die Rollenverteilung von Auftraggeber und Auftragnehmer datenschutzkonform in Outsourcing-Verträgen festlegt, illusorisch, eine reine Fiktion.

Es gibt deshalb eine besondere staatliche Pflicht zum Schutz identitätsprägender Bürgerdaten, aufgrund dessen die Personenstandsdatenverarbeitung öffentlich-rechtlich ausgestaltet werden muss. Art. 33 Abs. 4 GG begründet den Funktionsvorbehalt hoheitlicher Verwaltung auch damit, dass eine „Privatisierung" solcher Verwaltungsleistungen ausscheidet, in denen Grundrechte der Bürger besonders gefährdet sind. Dies gilt auch und besonders für das Recht auf informationelle Selbstbestimmung. Insofern ist zu beachten, dass Personenstandsdaten in besonderem Maße sensibel und kontextsensitiv sind.

Der bayerische Gesetzgeber hat aufgrund dieser verfassungsrechtlichen Anforderungen die Personenstandsdatenverarbeitung hoheitlich ausgerichtet. Dies gilt nicht nur für das Abrufverfahren (Art. 7 Abs. 1 PStG), sondern auch für den Betrieb der Personenstandsregister (Art. 7 Abs. 2 PStG). Diese klare Zuordnung zum hoheitlichen Bereich unterscheidet die Personenstandsdatenverarbeitung von anderen Verwaltungsbereichen, in denen die Erbringung technischer Hilfsleistungen durch Private als tendenziell unproblematisch angesehen wird, was wiederum durch Art. 6 BayDSG auch gerechtfertigt werden kann. Dies sind aus rechtlicher Sicht etwa Büroanwendungen, Geoinformationssysteme, Presseregister oder der Betrieb von Internetseiten.

Die Verarbeitung von Personenstandsdaten mit ihren identitätsprägenden Informationen gehört zur verwaltungstechnischen und notariellen Grundversorgung eines Gemeinwesens, für die nur die demokratisch legitimierten Repräsentanten der Bürger die Verantwortung übernehmen können. Eine Auftragsdatenverarbeitung durch private IT-Dienstleister scheidet aus. Staatliche Datenherrschaft

setzt zumindest in Teilen der öffentlichen Verwaltung eine „eigenhändige" Datenverarbeitung öffentlicher Stellen voraus, damit das entsprechende KnowHow nicht mittelfristig verloren geht und dann eine mit dem Schutz- und Gestaltungsauftrag des Staates unvereinbare strukturelle Abhängigkeit von privaten IT-Dienstleistern entstünde.

Internationale Datentransfers

Internationale Datentransfers sind – im Falle eines Personenbezugs von Daten oder bei anderen sensiblen Datenkategorien – mit teilweise äußerst komplexen Fragen und Herausforderungen an einen wirksamen Datenschutz und an eine ausreichende Datensicherheit verbunden. Im Rahmen von IT-Outsourcing-Szenarien der öffentlichen Verwaltung wird die Nutzung von im außereuropäischen Ausland belegenden Datenwolken daher grundsätzlich nicht in Betracht kommen. Der für internationale Datentransfers geltende Rechtsrahmen soll daher auch nicht vertieft behandelt werden.

Zur Vertiefung:

Art. 21 BayDSG regelt die Übermittlung personenbezogener Daten an Destinationen im Ausland. Neben den allgemeinen Voraussetzungen einer Ermächtigungsgrundlage für die Datenermittlung bedarf es eines angemessenen Schutzniveaus in dem Empfängerstaat (vgl. Art. 21 Abs. 2 Satz 2 BayDSG).

Die **Angemessenheit des Datenschutzniveaus** ist grundsätzlich von der verantwortlichen Stelle anhand sämtlicher Umstände einer Datenübermittlung zu beurteilen. Hierzu zählen vor allem die jeweiligen Begebenheiten in einem Empfängerstaat. Von der EU-Kommission wurde ein angemessenes Schutzniveau für mehrere Staaten, unter anderem für Argentinien, Kanada und die Schweiz, verbindlich festgestellt. Ein angemessenes Schutzniveau kann daneben auch durch den Einsatz von Vertragsklauseln als ausreichende Garantien (vgl. Art. 21 Abs. 2 Satz 4 Nr. 7 BayDSG) individuell hergestellt werden. Die in der Praxis gerade für internationale Konzernunternehmen bestehende Möglichkeit der freiwilligen

Selbstverpflichtung durch „verbindliche Unternehmensregelungen“ (vgl. § 4c Abs. 2 BDSG) stellt jedoch vielmehr ein Instrument für nicht-öffentliche Stellen dar.

Mit der sog. **Safe-Harbor-Vereinbarung** existiert überdies eine praxisrelevante Sonderregelung für die USA, für die von der EU-Kommission kein angemessenes Datenschutzniveau festgestellt wurde. Die Relevanz dieser Vereinbarung zeigt sich bei Cloud Computing allein daran, dass viele marktführende Cloud-Anbieter Rechenzentrumsstandorte in den USA unterhalten. Vor allem aufgrund einer fehlenden Kontrolle dieser faktischen Selbstzertifizierung durch US-amerikanische Unternehmen wird das Safe-Harbor-Abkommen allerdings regelmäßig kritisiert. Datenschutzbehörden verweisen regelmäßig darauf, dass das Abkommen europäischen Anforderungen an einen wirksamen Datenschutz nicht genügt. Nach einem Beschluss des sog. Düsseldorfer Kreises aus dem April 2010, einem Zusammenschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, bestehen bei Safe Harbor für Unternehmen verschiedene Prüfungs- und Nachweisverpflichtungen, die erst recht für Datenverarbeitung durch öffentliche Stellen gelten.

Die Sicherstellung eines angemessenen Datenschutzniveaus wird bei Cloud Computing vor allem dann Schwierigkeiten bereiten, wenn die einer Datenwolke zugrundeliegende Infrastruktur (einschließlich eingeschalteter Sub-Unternehmer) sich nicht ausschließlich in einem Drittstaat befindet. Oftmals sind mangels fehlender Anbieterinformationen die genauen Standorte einer Datenverarbeitung bereits gar nicht ohne weiteres ersichtlich.

Insgesamt werden vor allem die traditionell sehr restriktiven Ansichten der Aufsichtsbehörden für den Datenschutz, die gerade bei öffentlichen Stellen Datentransfers meist nur innerhalb von EU und EWR für zulässig erachten, internationalen Datentransfers durch öffentliche Stellen regelmäßig entgegenstehen.

Vertiefungshinweise:

Düsseldorfer Kreis, Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29.4.2010 in Hannover (überarbeitete Fassung vom 23.8.2010)

Hennrich/Maisch, Cloud Computing und Safe Harbor: Wolken über dem sicheren Hafen?, Juris Anwaltszertifikat IT-Recht (AnwZert ITR) 15/2011

c) Fazit: Es kommt auf den Einzelfall an...

Sowohl die verfassungsrechtlichen als auch die einfachgesetzlichen Anforderungen zeigen deutlich, dass Cloud Computing im kommunalen Sektor weder per se rechtlich unzulässig noch stets zulässig ist. Es kommt auf den jeweiligen Einzelfall an.

*Auch bei **kleinen Kommunen** gilt: Je sensibler die Daten sind, die vom IT-Outsourcing betroffen sind, desto mehr Maßnahmen sind zur Gewährleistung der Datensicherheit zu treffen. Schutzmaßnahmen können auch für die Kommune Aufwand und Kosten verursachen.*

Soweit diese Maßnahmen vor Ort nicht zu akzeptablen wirtschaftlichen Bedingungen getroffen werden können, ist ein rechtskonformes Outsourcing zu einem verlässlichen IT-Dienstleister eine sehr empfehlenswerte Option.

Unzulässig ist kommunales Cloud Computing daher in allen Fällen, in denen eine Kommune den bestehenden Anforderungen nicht nachkommen kann. Sofern Anbieter Leistungen lediglich auf Grundlage von Standardverträgen erbringen, die datenschutzrechtlichen Anforderungen nicht genügen und zugleich auch keine Beschreibungen zu einem implementierten Datensicherheitskonzept enthalten, wird eine Kommune diese Leistung nicht nutzen dürfen. Bleiben die konkreten Standorte der verteilten Infrastruktur im Unklaren oder bestehen diesbezügliche Zweifel, wird eine derartige Intransparenz einer Leistungsinanspruchnahme ebenso entgegenstehen, da eine Kommune nicht einmal in der Lage ist, technisch-organisatorische Sicherheitskonzepte zu überprüfen.

Im Übrigen kommt es auf die **konkrete Ausgestaltung des Auftragsverhältnisses** an. Dabei spielen – neben der sorgfältigen Auswahl des IT-Dienstleisters, der von diesem angebotenen Cloud-Infrastruktur und Aspekten der Sicherheitsgewährleistung – auch Art und Inhalt der zu verarbeitenden Daten eine wesentliche Rolle. Im Rahmen der Risikoabwägung steigen bzw. sinken die Anforderungen an ein adäquates Sicherheitsniveau in Abhängigkeit von der Sensibilität und

Schutzbedürftigkeit der Daten. So wären etwa Personenstandsregisterdaten, Sozialdaten, Steuerdaten oder Waffenregisterdaten generell sehr streng zu behandeln. Das gilt auch für komplette Meldedatenbestände. Hier zieht Art. 33 Abs. 4 GG einem IT-Outsourcing und damit auch einer entsprechender Auslagerung „in eine Cloud“ Grenzen, wonach etwa keine privaten Cloud Anbieter beauftragt werden dürfen. Umgekehrt werden die Anforderungen zum Beispiel an Geodaten, auch wenn diese einen Personenbezug haben, oder an Daten um Rahmen von Kfz-Zulassungen geringer sein. Soweit es nur um untergeordnete technische Hilfsleistungen geht, dürfen dort auch private Cloud-Lösungen in Betracht gezogen werden. Für die Akteure im sicheren kommunalen IT-Outsourcing bietet dies die Chance, die jeweilige Cloud Lösung individuell anzupassen, so dass rechtliche, wirtschaftliche und technische Aspekte angemessen berücksichtigt werden.

Die Prüfung solcher Eckdaten und Nutzungsbedingungen muss bereits vor dem Abschluss eines Cloud-Vertrages erfolgen.

4. Was muss *vor* Abschluss eines Cloud-Vertrags beachtet werden?

a) Sorgfältige Auswahl eines zuverlässigen Cloud-Anbieters

Die Auswahl eines Cloud-Anbieters muss sorgfältig erfolgen. Im Auswahlprozess sind bestehende Gesetze und Vorgaben zu berücksichtigen. Mit Blick auf die auszulagernde Tätigkeiten oder IT-Dienste sollte im Vorfeld eine **Marktsondierung** vorgenommen werden, um zu beurteilen, ob es für eine Auslagerung überhaupt geeignete Anbieter gibt. Erst wenn die Gewissheit besteht, dass es für die Auslagerung einen oder mehrere geeignete Anbieter gibt, sollte der eigentliche Auswahlprozess angestoßen werden.

Will eine bayerische öffentliche Stelle Datenverarbeitungsanlagen oder Anwendungen an einen externen Auftragnehmer auslagern, hat sie diesen gem. **Art. 6 Abs. 2 Satz 1 BayDSG** „unter besonderer Berücksichtigung der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen".

Die Eignungsprüfung eines Auftragnehmers stellt in jedem Fall des Outsourcings eine wichtige Etappe dar. Erforderlich ist eine sorgfältige Prüfung unter Berücksichtigung der hier genannten Aspekte.

- Die **Eignungsprüfung** des Auftragnehmers **entfällt**, soweit das **Landesamt für Statistik und Datenverarbeitung** oder **die Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB)** im Wettbewerb beauftragt werden. Weitere Nachforschungen und besondere Maßnahmen müssen in diesem Fall nicht unternommen werden, da es sich bei diesen Stellen um öffentliche Stellen handelt, die entsprechend zuverlässig sind (vgl. Nr. 1 VollzBekBayDSG).
- **Sonstige öffentliche Stellen** (sowie sämtliche privatwirtschaftliche Unternehmen) sind von diesem Ausnahmetatbestand nicht umfasst. Soll ein IT-

Outsourcing an diese Stellen erfolgen, muss stets eine Eignungsprüfung durchgeführt werden.

- Eine **sorgfältige Auswahl** erfordert die Einholung einer Auskunft vom Auftragnehmer über die getroffenen technischen und organisatorischen Maßnahmen (Datensicherheitskonzept). Der Auftraggeber muss sich Gewissheit verschaffen, dass diese Maßnahmen dem Schutzbedarf der Daten entsprechen und eingehalten werden (zu den insoweit zu berücksichtigenden Gefahren und Risiken sowie den in Betracht zu ziehenden Maßnahmen vgl. auch auf S. 74).
    - Im Rahmen dieser Auskunft sind Referenzen anzufordern.
    - Auskünfte können u.a. von einem Branchenverband (z.B. BITKOM, EuroCloud Deutschland_eco e.V.) oder von gemeinnützigen eingetragenen Datenschutzvereinen eingeholt werden.
    - Ferner können Prüfberichte, Gutachten und Zertifikate (bspw. ISO 27001) eingefordert werden.

*Zur Beurteilung eines Datensicherheitskonzepts sind ein Abgleich mit der „Orientierungshilfe für erforderliche Maßnahmen der technischen und organisatorischen Sicherheit“ des **Landesbeauftragten für den Datenschutz** empfehlenswert.*

http://www.datenschutz-bayern.de/technik/orient/grunds.pdf

Zur Vertiefung:

Zur Beauftragung des Landesamtes für Statistik und Datenverarbeitung oder der Anstalt für Kommunalen Datenverarbeitung in Bayern vgl. auch Wilde/Ehmann/Niese/Knoblauch, BayDSG, Art. 6, 16. EL, Rn.18, 21. Bei diesen genügt lediglich die allgemeine vertragliche Verpflichtung, die erforderlichen und geeigneten Maßnahmen zu treffen.

Im Falle des Rückgriffs auf Datenverarbeitungsanlagen in den USA – für Kommunen wird dies im Anwendungsbereich des Datenschutzrechts (wie zuvor bereits erläutert, vgl. S.41) grundsätzlich nicht in Betracht kommen – kann ggf. auch ein Nachweis einer gültigen Safe-Harbor-Zertifizierung verlangt werden.

- Eine **Vor-Ort-Kontrolle** der technischen und organisatorischen Maßnahmen durch den behördlichen Datenschutzbeauftragten wird vom **Landesbeauftragten für den Datenschutz** empfohlen, obgleich das Gesetz keine ausdrückliche Pflicht enthält.
- **Faustregel:** Der Auftraggeber muss vom Auftragnehmer die Vornahme von Schutzmaßnahmen verlangen, die er treffen müsste, sofern er die Daten selbst verarbeiten würde. Zu weitgehende Anforderungen sind jedoch nicht einzufordern.

Der Auftraggeber bleibt auch nach der Auftragsvergabe datenschutzrechtlich in der Verantwortung. Die sorgfältige Auswahl des Auftragnehmers ist daher nicht nur für den Abschluss eines Auftragsdatenverhältnisses von Bedeutung, sondern auch für die Abwehr von Schadensersatzansprüchen.

b) Eventuell: Öffentliche Ausschreibung des Cloud-Auftrags

Ob eine nationale oder EU-weite Vergabe durchzuführen ist, hängt von der Höhe des geschätzten Ausgangswertes ab. Für Liefer- und Dienstleistungsaufträge liegt dieser Schwellenwert seit dem 01.01.2012 bei 200.000,- EUR. Bei komplexen, umfangreichen IT-Outsourcing-Maßnahmen kann diese Schwelle überschritten werden. In diesem Fall sind staatliche Stellen verpflichtet, die Nutzung von Cloud-Diensten auszuschreiben (§ 99 Abs. 1 GWB), soweit es sich nicht um hoheitliche Tätigkeit handelt, die einem Outsourcing-Verbot unterliegt (Art. 33 Abs. 4 GG); dies wiederum hängt davon ab, welche Daten und Verfahren ausgelagert werden sollen und welche Rechte, Befugnisse oder Zugriffsmöglichkeiten dem Dienstleister übertragen werden sollen.

*Bei der Auslagerung von Bürokommunikationsdiensten wird bei **kleinen Kommunen** diese Schwelle im Regelfall nicht überschritten.*

Das hat zur Folge, dass der Zuschlag grundsätzlich dem **wirtschaftlichsten Angebot** erteilt werden muss. Zudem dürfen **gleichwertige Lösungen** nicht von vorne herein aus dem Vergabeverfahren ausgeschlossen werden. Es muss also berücksichtigt werden, dass im Rahmen von Cloud-Ausschreibungen ggf. auch

Angebote über klassische IT-Leistungen zugelassen werden müssen. Dieser Grundsatz gilt natürlich auch umgekehrt für die Beschaffung klassischer IT-Leistungen, die sich nicht a priori gegenüber einer Cloud-Lösung verschließen darf.

Angesichts der Komplexität eines Vergabeverfahrens und der Besonderheiten von Cloud Computing kann sich bereits die Erstellung einer **sachgerechten Leistungsbeschreibung** als Herausforderung erweisen. Die frühzeitige Einbindung externer Sachverständiger kann somit sinnvoll sein. Aber auch dann wird die Beantwortung der Frage, welche konkreten IT-Systemlösungen gewünscht werden, oftmals nicht auf den ersten Blick ersichtlich. Dies muss vielmehr schrittweise im Rahmen einer kooperativen Zusammenarbeit mit den IT-Dienstleistern erarbeitet werden. Eine Möglichkeit zur Problemlösung kann insoweit der **wettbewerbliche Dialog** darstellen.

Soweit die strengen Vorgaben des EU-Vergaberechts nicht gelten, weil die Vergabeschwellen nicht überschritten werden (was bei kleineren Aufträgen im kommunalen Bereich nicht selten ist), ist die Auftragsvergabe an einen Cloud Anbieter zumindest durch das Haushaltsrecht begrenzt. So müssen in der Regel 3 Vergleichsangebote eingeholt werden, um Hinweise zur Wirtschaftlichkeit des geplanten Auftrags zu erhalten und den Wettbewerb nicht ganz auszuschließen. So heißt es unter Punkt 1.2.1 der Bekanntmachung des Bayerischen Staatsministeriums des Innern zur Vergabe von Aufträgen im kommunalen Bereich vom 14. Oktober 2005 Az.: IB3-1512.4-138, zuletzt geändert durch Bekanntmachung vom 12. Dezember 2012 (StAnz Nr. 51/52):

„In der Regel ist mindestens ein Bewerber, ab einem Auftragswert von 75.000 € ohne Umsatzsteuer sind mindestens drei Bewerber aufzufordern, die ihre Niederlassung nicht im eigenen Landkreis des kommunalen Auftraggebers bzw. bei kreisfreien Städten im eigenen Stadtgebiet haben; die Bewerber sind regelmäßig zu wechseln“.

c) Fachkundige Wirtschaftlichkeitsberechnung des Cloud-Angebots

Cloud Computing kann für Kommunen **finanzielle Vorteile** bieten. Je nach Vertragsgegenstand und Vertragsausgestaltung können solche Dienste aber auch nachteilig sein. Deshalb ist eine fachkundige Wirtschaftlichkeitsberechnung unerlässlich, wie dies auch das Haushaltsrecht fordert. Zu beachten ist: Die haushaltsrechtliche Verpflichtung zur Wirtschaftlichkeitsberechnung gilt für jede finanzwirksame Maßnahme und damit für jedes IT-Projekt, auch wenn es „im eigenen Hause" durchgeführt wird. Die Prüfung aller ökonomischen Faktoren kann auch zu dem Ergebnis führen, dass ein IT-Outsourcing bzw. Cloud-Angebot sogar wirtschaftlicher ist als die „eigene" IT-Lösung. Dies wiederum ist u.a. abhängig von der Dimensionierung des IT-Bedarfs.

Unter Berücksichtigung von Wirtschaftlichkeitserwägungen (Anhang: Aspekte der wirtschaftlichen Vorteilhaftigkeit im Überblick:) ist jedem IT-Outsourcing durch Cloud-Services im öffentlichen Sektor ein **Beschaffungsvorlauf** voranzustellen. Im Zuge dieses Beschaffungsvorlaufs sind die Bedarfslage und die Wirtschaftlichkeit des Vorhabens zu ermitteln. Nur wenn eine Abwägung für die Wirtschaftlichkeit des Vorhabens ausfällt, kann mit seiner Realisierung begonnen werden.

Zudem muss bereits zu diesem frühen Zeitpunkt darüber nachgedacht werden, wie die Outsourcing-Aktivitäten ggf. rückabgewickelt werden können. Die öffentliche Hand darf sich nicht in eine Abhängigkeit vom Cloud-Anbieter begeben (vgl. oben zu Anbieterabhängigkeit, S. 25 ff.). Ein funktionierendes **Exit-Management** ist beim Cloud Computing daher unerlässlich und sollte daher schon vor der Auslagerung in die Cloud im Rahmen der Auswahlentscheidung Berücksichtigung finden.

*Bei **kleinen Kommunen** kann Outsourcing eine Verbesserung des Sicherheitsniveaus bedeuten. Um ein bestimmtes Niveau an Daten- und IT-Sicherheit zu erreichen, sind die hierfür erforderlichen Aufwendungen in der Betrachtung zu berücksichtigen.*

Zur Beurteilung der Wirtschaftlichkeit einer Cloud-Anwendung im kommunalen Umfeld eignet sich auch der Ansatz der **Wirtschaftlichkeitsbetrachtungen des Bundes**, in dem die wesentlichen Beurteilungskriterien zusammengefasst sind. Im

Allgemeinen hängt eine Beurteilung von den Entwicklungskosten und dem Entwicklungsnutzen sowie von den Betriebskosten und dem Betriebsnutzen ab. Cloud-Diensteanbieter profitieren vom Ressourcenpooling, der Mandantenfähigkeit und der Skalierbarkeit durch die verwendeten Virtualisierungslösungen sowie vom Selbstbedienungsangebot. Die Auftraggeber können ihr Produkt- und Dienstleistungsportfolio ausweiten, ihre Gebühren und Preise dank anderer Rahmenbedingungen neu kalkulieren und ihr Personal nun anders einsetzen. Letztendlich profitieren davon auch die Bürger und Unternehmen als Nutznießer dieser Cloud-Angebote.

Nichtwirtschaftliche Kriterien finden sich in der Dringlichkeit, vorhandene Altsysteme abzulösen und in der Einhaltung von Gesetzen und Verwaltungsvorschriften.

Hinzu kommen **qualitative Kriterien** und **Effekte** mit Mehrwerten für die Bürger als Anwender. Cloud-Dienste eröffnen der Kommunalverwaltung zusätzliche Flexibilität und vereinfachen den Umgang mit vorhandenen Risiken. Zugleich sollten sie zum Datenschutz, zur IT-Sicherheit und im Sinne von Green-IT zu einem wirtschaftlichen wie ökologischen Betrieb beitragen können, sobald die erforderlichen Breitbandanschlüsse in der Kommunalverwaltung vorhanden sind.

Zu den Mindestanforderungen an die Sicherheit von Cloud Computing im kommunalen Sektor wird auf die ausführlichen Hinweise in der ISPRAT-Studie „Cloud-Computing für die öffentliche Verwaltung“, S. 111 ff., zurückgegriffen werden.

http://www.fokus.fraunhofer.de/de/elan/_docs/_studien_broschueren/isprat_cloud_studie_20110106.pdf

In Entsprechung mit dem Aufbau der **Grundschutzkataloge des BSI** muss sich eine Kommune für einen verstärkten Einsatz von Cloud-Anwendungen mit den Zielen, Gefährdungen und Maßnahmen zum Datenschutz und zur Datensicherheit auseinander setzen, wie sie im Falle des klassischen IT-Outsourcings zum Tragen kommen. Im Rahmen der ISPRAT-Studie zu Cloud Computing für die öffentliche Verwaltung haben die Autoren sämtliche zu berücksichtigende Gefährdungen und Maßnahmen akribisch zusammengetragen. Aus diesen Vorgaben zum IT-Outsourcing leiten sich jene erforderlichen **Kenntnisse und Fähigkeiten des Personals** ab, die in der Kommunalverwaltung künftig bei der Inanspruchnahme von Cloud-Diensten vorausgesetzt

werden. Dazu zählen Markt- und Angebotskenntnisse, Kenntnisse zur Auswahl, Vertragsgestaltung, zum sicheren Betrieb, zur Migration und zur Notfallvorsorge. Allerdings stehen Kenntnisse und Fähigkeiten in einer starken Abhängigkeit von den ausgewählten Cloud-Diensten und deren angestrebten Umfang im kommunalen Einsatz.

Zur Wirtschaftlichkeitsbetrachtung zählen auch **künftig ersparte Aufwendungen**. Durch die Inanspruchnahme von Cloud-Diensten entfällt für Kommunen auf technischer Seite die Notwendigkeit zu Systeminstallationen, zur Bereitstellung und Wartung von Serverhardware und Software, zur Systembetreuung und zur Systemadministration. In Abhängigkeit der gewählten Cloud-Dienste und ihres Umfangs ergeben sich weitere Einsparpotentiale im administrativen Aufgabenbereich der Kommunalverwaltung. Durch den Wegfall einzelner oder zentraler Aufgaben entfallen einzelne Stellen, falls dies nicht durch zusätzliche Aufgaben kompensiert werden kann. Allerdings können keine pauschalen Aussagen zu Personaleinsparungen durch Cloud-Dienste gemacht werden. Einsparungen bei den Personalkosten eröffnen sich vor allem bei der Planung und Entwicklung, bei der Systemeinführung, beim Betrieb und bei der Migration.

*Das Ersparnis von Aufwendungen trifft auf **kleine Kommunen** nur teilweise zu. Weiterhin besteht vor allem der Bedarf an sachverständigem Personal zur Systemadministration und an Schulungen der Mitarbeiter im Umgang mit den Anwendungen.*

Ob und wie diese **Personaleinsparungen** realisiert werden sollen, ist eine personalpolitisch zu beantwortende Frage, die jede Kommune separat mit Blick auf die Zukunft ihrer kommunalen IT-Abteilung und die ausgewählten Cloud-Diensteanbieter zu treffen hat. Soll langfristig der Weg zur Inanspruchnahme von Cloud-Diensten beschritten werden, ohne der kommunalen IT-Abteilung noch eine große Zukunft einzuräumen, muss dies überzeugend und nachhaltig begründet sowie mit einem tragfähigen Umsetzungskonzept realisiert werden. Zum Erhalt von **Arbeitsfrieden und Zufriedenheit** der qualifizierten Beschäftigten sollte auf jeden Fall den betroffenen Mitarbeitern und

*Die Einsparung von Personal kann für **große Kommunen** bedeutsam sein, die über eine eigene Abteilung zur Systemadministration verfügen oder ein eigenes Rechenzentrum betreiben.*

Führungskräften eine echte Perspektive geboten werden. Hierzu zählen Fortbildungsmaßnahmen zur Qualifizierung für neue Aufgaben, das Controlling von Dienstleistungsvereinbarungen (Service Level Agreements) mit den Cloud-Anbietern und weiterführende Personalentwicklungskonzepte. Andererseits kann die verstärkte Nutzung von Cloud-Diensten neue Freiräume für weitere IT-Vorhaben und dringend vorgesehene Modernisierungsprojekte eröffnen, für deren Umsetzung bisher nicht ausreichende Kapazitäten zur Verfügung stehen. Die Gefahr, dass sich im Falle eines drohenden Personalabbaus leistungsstarke Kräfte der IT-Abteilung auf dem Arbeitsmarkt nach Alternativen umsehen und abgeworben werden könnten, während leistungsschwächere Arbeitskräfte der IT-Abteilung der Kommune auch weiter auf Dauer erhalten bleiben, kann allerdings nicht ausgeschlossen werden.

Zur Vertiefung:

Eine einführende Übersicht zu den zu berücksichtigenden Posten einer Wirtschaftlichkeitsberechnung auf Grundlage der Vorgaben des Bundesministeriums des Innern findet sich im Anhang.

BSI, IT-Grundschutz-Kataloge,
https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/kataloge.html

d) Hinzuziehung von Rechtsexperten für den Cloud-Vertrag

Schon die vorstehenden Ausführungen haben gezeigt, wie anspruchsvoll die rechtliche Ausgestaltung eines Cloud-Vertrags sein kann. Dies gilt erst recht, wenn man alle weiteren rechtlichen Risiken einbezieht, die teilweise auch zu erheblichen Haftungsfolgen führen können. Die Hinzuziehung von **Rechtsexperten** ist bei der Vorbereitung und Durchführung eines **komplexen oder weitreichenden IT-Outsourcing-Projekts** daher zu empfehlen.

Hierfür sprechen nicht nur praktische Erwägungen einer vernünftigen **Projektabwicklung**, sondern auch rechtliche Anforderungen. Eine Haftung für sorgloses

Verhalten durch die Unterlassung, rechtliche Beratung in Anspruch zu nehmen, kann jedenfalls im Ausnahmefall nicht ausgeschlossen werden.

e) Akzeptanzstiftende Maßnahmen für die Betroffenen

Selbst wenn ein Cloud-Vertrag rechtskonform angebahnt und vollzogen wird, ist der Projekterfolg dadurch noch nicht garantiert. Gerade mit der Einführung von Cloud-Services werden regelmäßig **organisatorische Änderungen in der Kommune** notwendig. Bestimmte Stellen mögen kurz- oder mittelfristig wegfallen, andere ein neues **Anforderungsprofil** erhalten. Oftmals sind auch Qualifizierungsmaßnahmen erforderlich. Mit all dem kann eine Belegschaft nicht einfach konfrontiert werden. Vielmehr bedarf es eines **Change Managements**, mit dessen Hilfe die Bediensteten auf die neuen Verhältnisse vorbereitet und eingestellt werden.

Akzeptanzstiftende Maßnahmen können in diesem Kontext sein:

- Allgemeine Sensibilisierung zum Thema Cloud/IT-Outsourcing
- Geeignete Fortbildungsmaßnahmen und Qualifizierungsmaßnahmen
- Information über die neuen Herausforderungen (z.B. zur Datensicherheit)
- Information über diejenigen technischen und organisatorischen Maßnahmen, die gegenwärtig als erforderlich angesehen werden
- Information über die kurz- und mittelfristigen Veränderungen in der Personal- und Aufgabenstruktur der Kommune
- Information über die erwarteten Vorteile und Chancen

Sonstige Aspekte eines Change Managements in der öffentlichen Verwaltung betreffen Coaching, Motivation, Kommunikation und Kontrolle.

Zur Vertiefung:

Zusätzliche Kenntnisse, Fähigkeiten und Tätigkeiten, die auf Seiten des Personals benötigt werden können, sind in Anhang 3 tabellarisch dargestellt. Diese Zusammenstellung richtet sich v.a. an große Kommunen.

f) Eventuell: Beteiligung des Personalrats

Der **Personalrat** ist (soweit vorhanden) zu beteiligen, wenn eine **Mitbestimmungspflicht** besteht. Im Zuge einer IT-Outsourcing-Maßnahme kann eine solche Pflicht in Betracht kommen, wenn Beschäftigte einer Dienststelle eingestellt, versetzt oder umgesetzt werden sollen (Art. 75 Abs. 1 Nr. 1, Nr. 6 BayPVG). Sollte die Auslagerung von IT eine Kündigung von Beschäftigten oder die Auflösung, Verlegung oder Zusammenlegung von Dienststellen oder Teilen davon zur Folge haben, hat der Personalrat gem. Art. 77 BayPVG bzw. Art. 76 Abs. 2 Nr. 4 BayPVG mitzuwirken. Technische und organisatorische Veränderungen in der Dienststelle sind lediglich dann mitbestimmungspflichtig, soweit es sich um sogenannte Organisationsmaßnahmen zur Personalverwaltung gem. Art. 75a BayPVG handelt. Wird bspw. die Personalverwaltungssoftware in die Cloud ausgelagert, muss jedenfalls der Personalrat beteiligt werden. Die Einführung einer Software zur automatisierten Personalverwaltung unterliegt ferner gem. Art. 75a Abs. 1 Nr. 2 BayPVG der Mitbestimmung des Personalrats. Ein Personalrat ist (auch) bei der Nutzung von Cloud-Leistungen stets dann zu beteiligten, wenn ein Tatbestand der Mitbestimmung betroffen ist oder zumindest nicht ausgeschlossen werden kann, dass das Outsourcing sonstige Auswirkungen für Beschäftigte hat.

*Dies gilt nur für **Kommunen**, die einen gewählten Personalrat haben.*

Zur Vertiefung:

Allgemeine Übersicht von Maßnahmen, die im Rahmen eines Outsourcings (unabhängig von einer Cloud) auf kommunaler Seite zur Datensicherheit in Betracht zu ziehen sind:

(M x.xx entspricht der Maßnahme in den IT-Grundschutz-Katalogen des BSI)

- Rechtzeitige Beteiligung des Personal-/Betriebsrates, M 2.40
- Änderungsmanagement, M 2.221

- Regelungen für den Einsatz von Fremdpersonal, M 2.226
- Strategische Planung des Outsourcing-Vorhabens, M 2.250
- Definition der wesentlichen Sicherheitsanforderungen, M 2.251
- Auswahl des Outsourcing-Dienstleisters, M 2.252
- Vertragsgestaltung mit dem Outsourcing-Dienstleister, M 2.253
- Erstellung eines IT-Sicherheitskonzepts für ausgelagerten IT-Verbund, M 2.254, M 2.83
- Sichere Migration, M 2.255
- Planung und Sicherstellung des laufenden Betriebs, M 2.256
- Sicherheitsüberprüfung von Mitarbeitern, M 3.33
- Vereinbarung über die Anbindung an Netze Dritter, M 5.87
- Vereinbarung über Datenaustausch mit Dritten, M 5.88
- Geordnete Beendigung eines Outsourcing-Dienstleistungsverhältnisses, M 2.307
- Notfallvorsorge beim Outsourcing, M 6.83
- Notfallplan für den Ausfall eines VPNs, M 6.109

Allgemeine Übersicht von Maßnahmen, die im Rahmen eines Outsourcings (unabhängig von einer Cloud) auf kommunaler Seite zur Datenschutz in Betracht zu ziehen sind:

(M x.xx entspricht der Maßnahme in den IT-Grundschutz-Katalogen des BSI)

- Datenschutzmanagement, M 7.1

- Regelung der Verantwortlichkeiten im Bereich Datenschutz, M 7.2
- Aspekte eines Datenschutzkonzeptes, M 7.3
- Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten, M 7.4
- Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten, M 7.5
- Verpflichtung/Unterrichtung der Mitarbeiter bei der Verarbeitung personenbezogener Daten, M 7.6
- Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten, M 7.7
- Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten bei der Verarbeitung personenbezogener Daten, M 7.8
- Datenschutzrechtliche Freigabe, M 7.9
- Meldung und Regelung von Abrufverfahren bei der Verarbeitung personenbezogener Daten, M 7.10
- Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten, M 7.11
  Regelung der Verknüpfung und Verwendung von Daten bei der Verarbeitung personenbezogener Daten, M 7.12
- Dokumentation der datenschutzrechtlichen Zulässigkeit, M 7.13
- Aufrechterhaltung des Datenschutzes im laufenden Betrieb, M 7.14
- Datenschutzaspekte bei der Protokollierung, M 2.110
- Datenschutzgerechte Löschung bzw. Vernichtung, M 7.15

Quellen und Vertiefungshinweise:

Deussen/Strick/Peters, Computing für die öffentliche Verwaltung, ISPRAT-Studie, Fraunhofer Institut FOKUS, Berlin 2010, http://www.fokus.fraunhofer.de/de/elan/_docs/_studien_broschueren/isprat_cloud_studie_20110106.pdf.

Bundesministerium des Innern, Wirtschaftlichkeitsbetrachtungen (WiBe), Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT, Version 1.4, KBSt-Band 92, Berlin 2007, http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/wibe_fachkonzept_download.pdf.

5. Was sollte man zum Cloud-Vertrag wissen?

a) Formalia

Bei einem Cloud-Vertrag handelt es sich regelmäßig um einen Auftrag gem. Art. 6 BayDSG (bzw. § 11 BDSG). Bei einer Auftragsdatenverarbeitung bleibt **die Kommune als Auftraggeber datenschutzrechtlich in der Verantwortung**. Dies gilt sowohl gegenüber dem Betroffenen als auch gegenüber den Fachaufsichts- und Kontrollbehörden. Durch eine Auftragsdatenverarbeitung kann sich die Kommune nicht ihrer Pflichten und Verantwortlichkeiten entziehen.

Zur Vertiefung:

Die Kommune als öffentliche Stelle ist verpflichtet, den Datenschutz und die Datensicherheit der bei einem externen Diensteanbieter gespeicherten und verarbeiteten Daten sicherzustellen. Die Auslagerung der Datenverarbeitung im Rahmen der Auftragsdatenverarbeitung befreit ferner nicht von der Pflicht, Auskunfts-, Löschungs- und Berichtigungsansprüche der Betroffenen zu erfüllen und bei Vorliegen eines Schadens zu haften, vgl. Art. 14 BayDSG.

Neben der Regelung des wesentlichen Inhalts bedarf ein Auftrag der **Schriftform**. Die Schriftform für Verpflichtungsgeschäfte bspw. einer Kommune ergibt sich i.Ü. aus **Art. 38 Abs. 2 GO**. Der Vertrag muss also vom wirksam bestellten Vertreter einer öffentlichen Stelle eigenhändig unterzeichnet werden.

Die Unterzeichnung des Vertrags setzt die in Kap. 4 genannten Schritte zur Vorprüfung und die Einholung der erforderlichen Gremienbeschlüsse voraus.

b) Wesentlicher Inhalt

In einem Auftrag sind **bestimmte Vertragsinhalte ausdrücklich zu regeln**. Das Gesetz gibt in Art. 6 Abs. 2 S. 2 BayDSG nur allgemeine Hinweise. Eine konkretere Ausgestaltung enthält der (entsprechend anwendbare) **Katalog des § 11 Abs. 2 BDSG**, der die wichtigsten Regelungskomplexe einer Auftragsdatenverarbeitung umfasst. In Anlehnung an diese Vorschrift sollten in einem Auftrag daher drei Themenblöcke thematisiert werden.

> ***Kleine Kommunen*** *können den Mustervertrag zur Auftragsdatenverarbeitung des* ***Landesbeauftragten für den Datenschutz*** *heranziehen. Dieses Muster kann an die Umstände des Einzelfalls und die hier genannten Hinweise angepasst werden.*
>
> *http://www.datenschutz-bayern.de/technik/orient/m-vertr.htm*

Zunächst sind alle **schuldrechtlich relevanten Aspekte** zum Vertrag selbst zu regeln. Dazu zählen die Leistungsbeschreibung, die Gegenleistung (Gebühren/Tarife) die Vertragsdauer, die Eigentumsrechte an Soft- und Hardware, der Umgang mit Verstößen und Kündigungsmodalitäten.

> *Zu den Mindestanforderungen an die Sicherheit von Cloud Computing im kommunalen Sektor kann auf die ausführlichen Hinweise*
>
> - *in der* ***Studie****, Kapitel 6 b)*
> - *und in der ISPRAT-Studie „Cloud-Computing für die öffentliche Verwaltung“, S. 111 ff., zurückgegriffen werden.*
>
> *http://www.fokus.fraunhofer.de/de/elan/_docs/_studien_brochueren/isprat_cloud_studie_20110106.pdf*

In einem zweiten Themenblock sind die **datenschutzrelevanten Inhalte,** wie z.B. die Zweckbindung, die Bestimmung der betroffenen Benutzergruppen, Umfang, Grenzen und Ort der Datenverarbeitung sowie die Vorgehensweise bei Berichtigung und Löschung von Daten festzulegen.

Im dritten Themenblock werden die **Rechte und Pflichten der Parteien** u.a. im Hinblick auf die Durchführung von technischen und organisatorischen Schutzmaßnahmen sowie deren Kontrolle, Aufbewahrungspflichten, Gewährleistungsansprüche, Haftung und Vertragsstrafen geregelt. Da eine Kommune mit einem Auftrag gem. Art. 6 BayDSG die datenschutzrechtliche Verantwortung für eine

sonstige (ggf. nicht-öffentliche) Stelle übernimmt, hat der Entscheidungsträger sicherzustellen, dass beim Vertragsschluss keine Regelungslücken entstehen.

Zur Vertiefung:

Im Einzelnen sind folgende Regelungsaspekte zu beachten:

- Die **Beschreibung des Vertragsgegenstandes**: Der Vertragsgegenstand sollte im Auftrag enthalten sein. Anstatt dieser Beschreibung kann auch auf eine Leistungsvereinbarung bzw. auf ein **Service-Level-Agreement** als Anlage Bezug genommen werden, in denen der Leistungsgegenstand ausführlich beschrieben wird. Eine ausführliche Beschreibung schützt vor Missverständnissen und erleichtert die später durchzuführende Vertragsausführung und Umsetzung sowie die Kontrolle.
- Mit dem Vertragsgegenstand korrespondiert ferner eine Regelung, wonach der Auftragnehmer verpflichtet wird, dem Auftraggeber alle für die Erstellung und Führung eines Verfahrens- und Verarbeitungsverzeichnisses erforderlichen Informationen zur Verfügung zu stellen. Diese Informationen sind für den Datenschutzbeauftragten des Auftraggebers, z.B. des Bezirks, von essentieller Bedeutung.
- Die **Dauer des Auftrags**: Es sind die Laufzeit bzw. die einmalige oder unbefristete Ausführung und die Kündigungsmöglichkeit bei Vorliegen eines schwerwiegenden Verstoßes gegen die Regelungen des Auftrags näher zu bestimmen. Wird ein Auftrag langfristig vereinbart, ist insbesondere zu prüfen, ob und wie das anbieterseitig implementierte Sicherheitskonzept an die sich fortentwickelnden technischen Standards und Gefahrensituationen angepasst werden soll.
- Die **Art, der Umfang und der Zweck** der Datenerhebung, -verarbeitung oder -nutzung: Hierbei empfiehlt es sich, eine Regelung aufzunehmen, wonach die Übermittlung von Daten in ein Drittland nur dann erfolgen darf, wenn die besonderen Voraussetzungen des Art. 21 BayDSG bzw. der §§ 4b, 4c BDSG erfüllt sind.

- Die **Art der Daten**: Im Auftrag kann auf die Leistungsvereinbarung Bezug genommen werden, sofern die Art der verwendeten Daten dort genauer beschrieben ist.
- Der **Kreis der Betroffenen**: Um der Verantwortung gerecht zu werden, die eine Stelle als Auftraggeber hat, sollten präzise Angaben zu betroffenen Personengruppen gemacht werden. Diese Angabe erleichtert die Schutzbedarfsanalyse der zu verarbeitenden personenbezogenen Daten und die Abwicklung von Anträgen zur Auskunft gem. Art. 10 BayDSG.
- Das **Verbot der Nutzung der Daten zu anderen Zwecken** und der unerlaubten Weitergabe der Daten: Dieses Verbot sichert den im Datenschutzrecht unverzichtbaren Grundsatz der Zweckbindung ab. Der Auftraggeber stellt mit dieser Klausel sicher, dass der Auftragnehmer die Daten nicht über andere Zwecke weiterverarbeiten darf.
- Die **Berichtigung, Löschung und Sperrung von Daten**: Hier können ggf. bestimmte Vorgehensweisen geregelt oder zumindest skizziert werden, sodass sie auf der Ebene der Weisungen unter erleichterten Bedingungen kommuniziert werden können.
    - Löschen ist nicht gleich Löschen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat schutzbedarfsabhängige Maßnahmen zur sicheren Löschung von (personenbezogenen) Daten definiert und klargestellt, dass „einfache Löschkommandos der jeweiligen Betriebssysteme und auch die Formatierung“ nicht ausreichen, um Daten zu löschen, die dort gespeichert sind (vgl. M 2.167).
    - Während bei Papierdokumenten und Mikrofilm keine zuverlässige Lösch-Methode vorhanden ist (hier kommen nur Methoden zur Vernichtung mit entsprechend zugelassenen Aktenvernichtern nach DIN 32757-1 in Betracht; dazu M 2.435), empfiehlt das BSI bei magnetischen Speichermedien das Überschreiben mit handelsüblicher Software, sofern die Daten lediglich normalen Schutzbedarf aufweisen. Bei

Daten, die als Verschlusssachen eingestuft wurden, sind Löschprogramme zu benutzen, die für diesen Zweck zertifiziert sind (vgl. BSI-TL 03400). USB-Sticks, Flash-Karten, Flash-Disks und PCMCIA-Karten sind dreimal vollständig zu überschreiben.

- Die vom **Auftragnehmer einzuhaltenden technischen und organisatorischen Maßnahmen**: Maßnahmen zur Datensicherheit sind ein entscheidendes Kriterium sowohl bei der Auswahl eines Auftragnehmers als auch bei der regelmäßigen Überprüfung der Datensicherheit.
    - Eine **Beschreibung der organisatorischen, räumlichen und personellen Maßnahmen** zur Gewährleistung der Datensicherheit kann sich hier an der Anlage zu § 9 BDSG orientieren. Diese Informationen sind auch für den behördlichen Datenschutzbeauftragten zur Erstellung bzw. Führung eines Verfahrens- und Verarbeitungsverzeichnisses wichtig.
    - Nach der Empfehlung **des Bayerischen Landesdatenschutzbeauftragten** sollte bei einer Auftragsdatenverarbeitung, die sehr sensible Daten betrifft, der Auftragnehmer vertraglich dazu verpflichtet werden, das Personal namentlich zu benennen, das von ihm im Rahmen der Verarbeitung dieser Daten eingesetzt wird. Sensible Daten können besonders schutzwürdige Daten gem. § 3 Abs. 9 BDSG, aber auch VS-Daten sein.
- Die bestehenden Rechte und Pflichten des Auftraggebers, insbesondere die von ihm vorzunehmenden Kontrollen sowie die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers:
- Nach der Empfehlung des **Bayerischen Landesdatenschutzbeauftragten** sollte sich der Auftraggeber selbst von der Angemessenheit und Wirksamkeit der vom Auftragnehmer ergriffenen Sicherheitsmaßnahmen überzeugen. Eine Vor-Ort-Kontrolle könne „insbesondere bei konkreten Anlässen (z.B. Hinweisen auf Fehlverhalten des Auftragnehmers) rechtlich geboten sein“; vgl.

Bayerischer Landesbeauftragte für den Datenschutz, Orientierungshilfe Auftragsdatenverarbeitung v. 24.02.2011, S. 9 ff.

- Es ist daher ratsam – gerade auch für kleine Kommunen – eine Inaugenscheinnahme vor Ort zumindest vertraglich zu regeln. Je nach Umständen des Einzelfalls, insbesondere des Umfangs der Datenverarbeitung und die Sensibilität der Daten kann anstatt einer Vor-Ort-Kontrolle später auch auf Testate eines vertrauenswürdigen Dritten zurückgegriffen werden (vgl. dazu S. 63). Ein solches Testat könnte z.B. eine ISO 27001 Zertifizierung auf der Basis von BSI-Grundschutz sein.
- Die vom **Auftragnehmer zu beachtenden Pflichten**: Zu diesen zählt u.a. die Pflicht des Auftragnehmers, seine eigenen Beschäftigten gem. Art. 5 BayDSG (bzw. § 5 BDSG) zur Einhaltung des Datengeheimnisses zu verpflichten.
- Die **mitzuteilenden Verstöße** des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen: Hier sind entsprechende Regelungen zu treffen, die eine angemessene Verwaltung erlauben, bspw. könnte ein elektronisches Beschwerdemanagement genutzt werden.
- Die **Festlegung des Orts bzw. der Region der Datenverarbeitung**: Sobald personenbezogene Daten außerhalb von EU/EWR verarbeitet werden, stellt sich eine Fülle an Rechtsfragen und Risiken für den Datenschutz (vgl. S. 58). Zur Vermeidung dieser juristischen Minenfelder ist die Datenverarbeitung der öffentlichen Verwaltung von vornherein auf Deutschland, auf bestimmte EU/EWR-Staaten oder Drittstaaten mit einem europarechtlich anerkannten angemessenen Datenschutzniveau (z.B. Kanada, die Schweiz oder Argentinien) zu beschränken. Angaben zur jeweiligen Lage bestimmter Rechenzentrums-Standorte sollten ferner eingefordert werden.
- Die **Kündigungsmodalitäten** und weiteres Vorgehen: Bereits beim Abschluss des Vertrags bzw. in der Planungsphase sollte die künftige Möglichkeit einer Kündigung oder eines Anbieterwechsel bedacht werden. Um Schwierigkeiten

beim Export der Daten und die Abhängigkeit vom Diensteanbieter, sog. Vendor-Lock-in, zu vermeiden, sind entsprechende Regelungen zum Datenexport zu treffen. Datenexport-Möglichkeiten können auch außerhalb von Kündigungsfällen bedeutsam sein.

- Die **Eigentumsrechte** an Hard- und Software: Dieser Punkt ist insbesondere dann wichtig, wenn IT-Ressourcen in der räumlichen Sphäre der öffentlichen Stelle betrieben werden, wie dies bspw. bei einem IT-Outsourcing in eine Private Cloud möglich sein kann. Auch im Hinblick auf eine mögliche Kündigung ist es wichtig zu wissen, welcher Partei welche Hardware gehört.
- Die **Rückgabe** überlassener Datenträger und die Löschung der beim Auftragnehmer gespeicherten Daten nach Beendigung des Auftrags: Regelungsbedürftig sind insbesondere die Löschungsmethoden bei den zum Einsatz kommenden Datenträgern, z.B. die Überschreibung der Datenträger mit einem bestimmten Muster (vgl. M 4.32, Maßnahmenkatalog, BSI IT-Grundschutz-Kataloge). Hierbei ist entscheidend, ob es sich in der Bereitstellungsform um eine Private oder Public Cloud handelt.
- Die **System- und Benutzerdokumentation**: Technische Informationen, bspw. auch Konzepte zum Identitätsmanagement oder zu den eingesetzten Datenverarbeitungsanlagen, können hier beschrieben werden.
- Die **Aufbewahrungspflichten**: Die Aufbewahrungspflichten richten sich nach den gesetzlichen Vorschriften, die die rechtliche Grundlage eines Vorgangs bilden.
- Die **Gewährleistungsansprüche**: Die Gewährleistungsansprüche richten sich nach denen in der Leistungsbeschreibung bzw. im Service-Level-Agreement getroffenen Vereinbarungen.
- Die **Haftung** und ggf. die Höhe einer **Vertragsstrafe**.
- Der Umfang der **Weisungsbefugnisse**, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält.

- Die etwaige Berechtigung zur Begründung von **Unterauftragsverhältnissen**: Soweit möglich, **sollte der Unterauftragnehmer namentlich benannt** werden. Zumindest sollte der Auftraggeber eine Liste von möglichen Unterauftragnehmern, bspw. Infrastrukturbetreibern etc., auf die der Auftragnehmer zurückgreift, einfordern.
- Auf die **Empfehlung des Landesbeauftragten für den Datenschutz** sollten auch Klauseln aufgenommen werden, die den Schutz des Eigentums und der personenbezogenen Daten des Auftraggebers vor Zugriffen Dritter, bspw. in Bezug auf Pfändung, Beschlagnahme, Zwangsvollstreckung oder Insolvenz des Auftragnehmers dokumentieren. Der Auftragnehmer ist zu verpflichten, den Auftraggeber über den möglichen oder bevorstehenden Zugriff eines Dritten unverzüglich in Kenntnis zu setzen.

c) Gewährleistungs- und Haftungsfragen

Allgemeine Rechtsunsicherheiten bei IT-Verträgen

Haftungsfragen stellen sich bei vertraglichem oder außervertraglichem Fehlverhalten. Bei Störungen oder Mängeln sind im Rahmen eines laufenden Vertragsverhältnisses vor allem Fragen der Gewährleistung von zentraler Bedeutung. Enthält ein IT-Service-Vertrag hierfür keine (ausreichenden) Regelungen, so gelangen die gesetzlichen Vorschriften zur Anwendung. Allerdings finden sich im **Bürgerlichen Recht** für verschiedene Vertragstypen ganz unterschiedliche **Gewährleistungsregelungen** wieder. Welches gesetzliche Gewährleistungsregime daher im Falle einer Nicht- oder Schlechtleistung anzuwenden ist, hängt von der vertragstypologischen Klassifizierung des jeweiligen IT-Service-Vertrags ab. Diese rechtliche Einordnung kann aber gerade bei komplexen Verträgen – zu denen auch Cloud Service Agreements zählen können – Schwierigkeiten bereiten.

Zur Vertiefung:

Die vertragstypologische Klassifizierung eines IT-Service-Vertrages kann sich gerade bei verschiedenartigen vertraglichen Leistungen mitunter als schwierig herausstellen. Als neuartige Vertragsform sind derartige Verträge keinem gesetzlichen Vertragstyp eindeutig zuzuordnen. Eine Zuordnung wird dabei vor allem dadurch erschwert, da sich die gesetzlichen Vertragstypen in dem letzten Jahrhundert fast kaum verändert haben – und moderne Vertragstypen daher gar nicht kennen.

Werden Hard- und Software nur auf Zeit genutzt (kein Eigentumserwerb), wird in bestehenden, klassischen IT-Outsourcing-Szenarien regelmäßig ein Mietvertrag vorliegen. Vor allem die infrastrukturbezogenen Elemente eines IT-Service-Vertrags (Rechenzentrumsfläche, Servermiete, Webhosting) werden regelmäßig als Mietvertrag eingeordnet. Diese Einordnung wird regelmäßig gerade auch auf IaaS zu übertragen sein. Auch Leistungen im SaaS-Umfeld werden in der Regel als Mietvertrag zu qualifizieren sein. Bereits der SaaS-Vorgänger Application-as-a-Service (ASP) wurde diesem Vertragstyp vom BGH zugeordnet. Inwiefern die Form der Leistungsbereitstellung als Dienst insoweit zu Änderungen führen wird, bleibt abzuwarten. Verbleibende Rechtsunsicherheiten sind jedoch bei einem Cloud-Vertrag gerade im Hinblick auf Gewährleistungs- und Haftungsfragen zu berücksichtigen. Da auch Cloud-Verträge als sog. Cloud-Service-Agreements zahlreiche Merkmale von verschiedenen gesetzlichen Vertragstypen aufweisen können (v.a. Mietvertrag, ggf. auch Werk- oder Dienstvertrag), sind insoweit verbleibende Rechtsunsicherheiten von hoher Praxisrelevanz.

Vgl. *Grapentin*, in: Bräutigam, IT-Outsourcing, 2. Aufl. 2009, Teil 3, Rn. 13, 43, 56 ff.

Die schnellen und flexiblen Möglichkeiten einer **Leistungsinanspruchnahme** als Dienst („as a Service“) können dabei zusätzliche Herausforderungen an die Schwerpunktbestimmung enthalten. Werden unterschiedliche Leistungen je nach Bedarf in Anspruch genommen, können sich zuordnungsrelevante Leistungs-

elemente ggf. binnen kürzester Zeit ändern. Zugleich kann sich die Bereitstellung als Dienst auf anerkannte Zuordnungen (wie v.a. als Mietvertrag) auswirken.

Hinweise zur Gestaltung eines Cloud-Service-Agreements

Um den zuvor dargestellten Rechtsunsicherheiten zu begegnen, empfiehlt es sich in der IT-Vertragspraxis, möglichst detaillierte, den Bedürfnissen der Vertragsparteien entsprechende Gewährleistungs- und Haftungsregelungen in den IT-Service-Vertrag aufzunehmen. In umfangreicheren Vertragswerken geschieht dies meist im Rahmen eines sog. **Service Level Agreements** als eigenständigem Vertragsbestandteil.

Ein IT-Service-Vertrag über eine IaaS-, PaaS- oder SaaS-Leistung sollte zunächst die jeweiligen Verantwortlichkeiten abgrenzen und insoweit die Leistungspflichten zwischen den Vertragsparteien klar und eindeutig definieren.

Die Beschreibung der von einem Anbieter zu erbringenden Leistungen sollte sodann Festlegungen enthalten, aus denen die genauen Leistungsparameter, sog. Service Level, sowie die diesbezüglichen Mess- und Berechnungsmethoden klar und transparent hervorgehen. Für eine wirksame Kontrolle finden sich hierbei idealerweise etwa auch Ausführungen zu Aufzeichnungen oder einem Monitoring.

Detaillierte Regelungen sind für den Fall einer **Leistungsbeeinträchtigung** erforderlich. Als vertragliche Rechtsfolge für das Nicht-Erreichen eines Service Levels haben sich in der Praxis pauschale Gutschriften-Regelungen bewährt. Diese pauschalen Gutschriften, sog. Credits, sind in ihrer Höhe nach dem prozentualen Grad der Unterschreitung des vereinbarten Service Levels gestaffelt.

Andere Sanktionsregelungen und Kombinationsvarianten (etwa mit außerordentlichen Kündigungsrechten) sind jedoch auch möglich. Im Rahmen eines Vertrags zur Auftragsdatenverarbeitung empfiehlt sich vor allem eine Vertragsklausel, die den Auftraggeber zu einer **außerordentlichen Kündigung** berechtigt, wenn der Auftragnehmer trotz einer schriftlichen Aufforderung die vereinbarten Leistungen nicht ordnungsgemäß erbringt oder andere Vertragspflichten verletzt.

Ein besonderes Augenmerk sollte zugleich auf Regelungen zu einer schnellen Leistungswiederherstellung und diesbezüglich definierter Prozesse gelegt werden (Reaktionszeiten, Notfallmaßnahmen).

Zur Vertiefung:

Die Bedeutung derartiger Regelungen folgt vor allem daraus, dass sich das Interesse eines Cloud-Nutzers vor allem auch auf eine unverzügliche Wiederherstellung der Leistung richten wird. Neben der Bestimmung eines Ansprechpartners (in der Praxis wird dies der Help-Desk des Anbieters sein) sollten daher vor allem die **Reaktionszeiten** festgelegt sein (ggf. unter Staffelung für unterschiedlich kritische Ereignisse). Für den Fall, dass ein Service nicht innerhalb der Reaktionszeiten wiederhergestellt werden kann, sollten auch weitere **Notfallmaßnahmen**, sog. Escalation Procedures, festgelegt werden. Welche Maßnahmen und Regelungen dabei konkret in Betracht zu ziehen sind, wird von dem jeweiligen Cloud-Service abhängen und muss einzelfallbezogen betrachtet werden.

Sollte ein Anbieter lediglich einen **Standardvertrag** zur Verfügung stellen und sollte keine weitere Verhandlungsmöglichkeit bestehen, sind die Vertragsbestimmungen des Anbieters vor Vertragsabschluss in Bezug auf individuelle Verfügbarkeitserfordernisse und Haftungsinteressen sorgfältig zu bewerten. Spätestens bei dieser Phase sollte juristischer Rat und ggf. eine technische Begutachtung eingeholt werden.

Auch das anbieterseitige Interesse nach **Haftungsbeschränkungen** oder einem Haftungsausschluss ist zu berücksichtigen. Sofern gesetzlich zulässig (Grenzen bestehen etwa in den Allgemeinen Geschäftsbedingungen bei Haftungsausschlüssen für vorsätzliche oder grob fahrlässige Pflichtverletzungen), werden Anbieter in den Verträgen regelmäßig mittelbare Schäden oder einen entgangenen Gewinn ausschließen bzw. Haftungshöchstsummen vereinbaren. In der Praxis ist dabei vor allem zu beachten, dass Anbieter teilweise keine Haftung für den Verlust von Daten übernehmen wollen. Cloud-Nutzer sollten daher für bestimmte Schadensfälle gegebenenfalls eine zusätzliche Versicherung in Betracht ziehen.

d) Erinnerung und Empfehlung: Kein Cloud-Vertrag ohne juristische Beratung

> ***Kleinen Kommunen*** *kann der im Anhang beigefügte Mustervertrag zur Auftragsdatenverarbeitung des Landesbeauftragten für den Datenschutz unter Berücksichtigung der in dieser Begleitstudie hervorgehobenen Aspekte eine erste Hilfestellung bieten.*
>
> *Bei komplexen, langfristigen Outsourcing-Vorhaben, bspw. wichtigen Fachverfahren, unverzichtbaren Anwendungen oder einem besonders schutzwürdigen Bestand an (personenbezogenen) Daten, sollte juristische Beratung über die Landratsämter oder ggf. extern in Erwägung gezogen werden.*

Bei der Datenverarbeitung im Auftrag greift eine öffentliche Stelle auf einen externen Dritten zurück. Bereits bei einer einfachen IT-Outsourcing-Maßnahme lässt der Landesgesetzgeber die öffentliche Stelle im Stich: Art. 6 BayDSG enthält nur punktuelle und abstrakte Hinweise, welche Regelungen getroffen werden müssen, um eine zuverlässige und vertrauenswürdige Bindung zu einem externen Dienstanbieter einzugehen. Der Regelungskatalog des § 11 Abs. 2 BDSG lässt erahnen, welches Mindestmaß an Maßnahmen, Rechten und Pflichten zu berücksichtigten ist. Die C^3-Studie zeigt, dass deutlich mehr Leistungs- und Haftungsfragen bedacht werden müssen. Eine präzise Darstellung aller Regelungsaspekte kann von der vorliegenden Studie nicht geleistet werden. Der Erwerb von fachspezifischen Grundkenntnissen bewahrt den Behördenleiter daher nicht davor, in einem zweiten Schritt auf externes Know-how zurückzugreifen. Gerade bei komplexen Outsourcing-Vorhaben ist eine juristische Beratung zu empfehlen, die von einem technischen Gutachter unterstützt werden sollte, um die Prüfung der technischen und organisatorischen Schutzmaßnahmen erfolgreich durchzuführen.

Zur Vertiefung:

In der Stellungnahme 05/2012 vom 01.07.2012 (WP 196) hat die Art.-29-Datenschutzgruppe die datenschutzrechtlichen Herausforderungen von Cloud Computing einer aktuellen Analyse unterzogen. Diese Arbeitsgruppe ist mit den Leitern der nationalen Datenschutzbehörden besetzt und steht der EU-Kommission als unabhängiger Sachverständigenrat zur Seite. Die Stellungnahme setzt sich aus

einer Untersuchung und Schlussfolgerungen zusammen, die hier kurz dargestellt werden:

Cloud-Kunden aus Privatwirtschaft und aus dem öffentlichen Sektor wird die Vornahme einer Risikoanalyse empfohlen, bei der die Risiken der Datenverarbeitung, insbesondere der Verlust von Kontrolle und unzureichende Information in Bezugnahme auf die Art der Daten untersucht werden. Besondere Aufmerksamkeit solle auf die Betrachtung der datenschutzrechtlichen Risiken gerichtet werden. Für die Verarbeitung von besonders schutzwürdigen (sensitiven) Daten seien, unbeschadet des nationalen Rechts, spezielle vertraglich festgelegte Sicherungsmaßnahmen notwendig.

Dazu werden Leitlinien für das Vertragsverhältnis zwischen Cloud-Kunde und Cloud-Provider skizziert. Grundsätzlich sei der Cloud-Kunde für die Datenverarbeitung als Auftraggeber verantwortlich (vgl. Art. 17 Abs. 2 Richtlinie 95/46/EG; § 11 Abs. 1 BDSG). Ausnahmsweise käme auch eine Verantwortung des Cloud-Service-Providers in Frage, wenn dieser personenbezogene Daten für eigene Zwecke weiterverarbeitet. Dies ist nunmehr auch im Entwurf zur EU-Datenschutzgrundverordnung (EU-DSGVO-E) vorgesehen: Artikel 26 EU-DSGVO-E, der zum Teil auf Art. 17 Abs. 2 Richtlinie 95/46/EG gestützt ist, präzisiert Stellung und Pflichten des Auftragsdatenverarbeiters. So haftet er (ggf. gemeinsam mit dem Auftraggeber), soweit er über die Anweisungen des für die Verarbeitung Verantwortlichen hinaus Daten verarbeitet. Dieses Konzept der gemeinsamen Verantwortung ist neu und wirft Fragen auf, bspw. ob die Datenverarbeitung somit der Kontrolle bzw. die Möglichkeit der Weisungserteilung der ursprünglich verantwortlichen Stelle entziehen kann.

Den Regelfall bildet die Verantwortung des Cloud-Kunden für die Rechtmäßigkeit der Datenverarbeitung. Dieser sollte nach Ansicht der Art.-29-Datenschutzgruppe die Auswahl eines Cloud-Providers auf Diensteanbieter beschränken, die den Einklang ihrer Dienste mit europäischem Datenschutzrecht und die Aufnahme hinreichender vertragsrechtlicher Absicherungen garantieren. Zu diesen Absicherungen zählen die Bestimmungen für Unterauftragnehmer, deren Beauftragung

von der Einwilligung des Auftraggebers abhängen sollte. Diese Einwilligung könne auch generell erteilt werden, sofern der Provider verpflichtet wird, den Auftraggeber über alle Änderungen in Kenntnis zu setzen und die Möglichkeit einzuräumen, den Vertrag zu ändern. Der Cloud-Provider sollte ferner verpflichtet werden, alle Unterauftragnehmer zu benennen und mit ihnen Verträge zu schließen, die dem Cloud-Vertrag zwischen dem Auftraggeber und Verarbeiter Rechnung tragen. Der Cloud-Kunde müsste ferner über die Orte der Datenverarbeitung, auch bei Unterauftragnehmern, insbesondere wenn diese in Drittstaaten erfolgt, unterrichtet werden. Bei der Löschung von personenbezogenen Daten wird hervorgehoben, dass sichere Mechanismen vertraglich festgelegt werden sollten. Desweiteren werden Empfehlungen gegeben, welche Gegenstände im Cloud-Vertrag regelungsbedürftig sind (diese Empfehlungen bilden eine große Schnittmenge mit den bereits gem. § 11 BDSG Abs. 1, Abs.2 BDSG normierten Katalogtatbeständen). Ferner wird die Abgabe hinreichender Garantien in Bezug auf technische und organisatorische Sicherungsmaßnahmen sowie eine Spezifikation der konkret zum Einsatz kommenden Schutzmaßnahmen gefordert.

Ob der Cloud-Provider rechtmäßig Datentransfers in Drittländer vornehmen darf, sollte nach Auffassung der Art.-29-Datenschutzgruppe der Cloud-Kunde überprüfen. Eine unabhängige Prüfung kann ferner von einer vertrauenswürdigen, unabhängigen Stelle durchgeführt werden (WP 196, S. 22). Dieses Audit sollte von Cloud-Service-Providern dem Cloud-Kunden als Kopie ausgehändigt werden. Vom Cloud-Kunden individuell durchgeführte Audits bei einer Datenverarbeitung mit einer Vielzahl an Stellen, hält die Gruppe für technisch unmöglich. Die Integration von datenschutzfördernden Standards und die Förderung von Vertrauen sollten zentrale Aspekte in der Kunden-Provider-Beziehung darstellen.

Die Arbeitsgruppe kommt zu dem Ergebnis, dass Cloud Computing einen Grad an Komplexität erreicht hat, dem in der Stellungnahme mit Empfehlungen zu vertraglicher Absicherung nicht hinreichend Rechnung getragen werden kann. Die Stellungnahme schafft jedenfalls eine Ausgangsbasis für Vertragswerke und gibt Einblick in die Rechtsauffassung der europäischen Datenschutzbehörden.

6. Was muss *nach* Abschluss eines Cloud-Vertrags beachtet werden?

a) Beachtung gesetzlicher Anforderungen

Nach Abschluss eines Vertrags über eine IaaS-, PaaS- oder SaaS-Leistung hat eine Kommune nicht nur den vertraglich vereinbarten (Mitwirkungs-)Pflichten, sondern auch verschiedenen gesetzlichen Pflichten nachzukommen. Für den praxisrelevanten Fall der Verarbeitung personenbezogener Daten sind derartige Anforderungen in dem BayDSG vor allem im Rahmen der Auftragsdatenverarbeitung (Art. 6 BayDSG) wiederzufinden.

Auftragsdatenverarbeitung – Kontrollen der Kommune als Auftraggeber

Bei einer Auftragsdatenverarbeitung hat sich eine Kommune als Auftraggeber von der Einhaltung der im Vertrag vereinbarten und beim Cloud-Anbieter getroffenen technischen und organisatorischen Maßnahmen zu überzeugen (vgl. Art. 6 Abs. 2 Satz 3 BayDSG).

Gem. Art. 6 Abs. 2 Satz 3 BayDSG hat sich der Auftraggeber soweit erforderlich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen beim Auftragnehmer zu überzeugen.

Die Überprüfung des anbieterseitig implementierten, technisch-organisatorischen **Sicherheitskonzepts** kann dabei sowohl durch die Kommune selbst als auch durch einen Dritten (v.a. Datenschutzbeauftragte oder Sachverständige)

Die (Nach-)Prüfung korrespondiert mit der im Rahmen der sorgfältigen Auswahl eingeholten und im Vertrag vereinbarten Maßnahmen (Datensicherheitskonzept).

Bei Verstößen ist der Auftragnehmer zur Wiederherstellung des angemessenen, vereinbarten Niveaus an Datenschutz und Datensicherheit anzuweisen. Die Erfüllung dieser Weisung ist zu einem späteren Zeitpunkt erneut zu kontrollieren.

Alle Vorgänge müssen hinreichend dokumentiert werden.

erfolgen. Bei **Kontrollen** haben Zertifikate und Testate sonstiger Prüfstellen wie etwa TÜV-Siegel nur Hinweischarakter.

Nach der Empfehlung des **Landesbeauftragten für den Datenschutz** sollte sich der Auftraggeber selbst von der Angemessenheit und Wirksamkeit der vom Auftragnehmer ergriffenen Sicherheitsmaßnahmen überzeugen. Eine Vor-Ort-Kontrolle könne „insbesondere bei konkreten Anlässen (z.B. Hinweisen auf Fehlverhalten des Auftragnehmers) rechtlich geboten sein"; vgl. Der Bayerische Landesbeauftragte für den Datenschutz, Orientierungshilfe Auftragsdatenverarbeitung v. 24.02.2011, S. 9 ff.

Je nach den Umständen des Einzelfalls, insbesondere nach dem Umfang der Datenverarbeitung und der Sensibilität der Daten, kann anstatt einer Vor-Ort-Kontrolle durch den behördlichen Datenschutzbeauftragten auch auf Testate eines vertrauenswürdigen Dritten zurückgegriffen werden. Ein solcher Dritter kann ein entsprechend zertifizierter Sachverständiger sein, bspw. anerkannte ISO 27001-Auditoren für Audits auf der Basis von IT-Grundschutz (https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzZertifikat/Veroeffentlichungen/ISO27001Auditoren/iso27001auditoren_node.html).

Damit eine Kommune den Kontrollen auch wirksam nachkommen kann, sollten sämtliche Duldungs- und Mitwirkungsverpflichtungen des Auftragnehmers bereits in dem der Auftragsdatenverarbeitung zugrundeliegenden Vertrag hinreichend konkret festgehalten sein (vgl. S. 62). Das Ergebnis der Überzeugungsbildung sollte **dokumentiert** werden (entsprechend § 11 Abs. 2 Satz 5 BDSG).

Liegen der Datenwolke eines Anbieters **mehrere Standorte** zugrunde, so haben sich die Kontrollen grundsätzlich auf sämtliche Standorte zu erstrecken, an denen die Daten dauerhaft oder auch nur vorübergehend verarbeitet werden. In der globalen Dimension von Cloud Computing und einer Verteilung der Standorte über mehrere Länder kann eine effektive Kontrolle mit erheblichen praktischen Schwierigkeiten verbunden sein. Aufgrund gesetzlicher Anforderungen (insbesondere Datenschutz- und Datensicherheit) ist jedoch davon auszugehen, dass bayerische Kommunen auch für die Auslagerung von Datenverarbeitungsprozessen weiterhin auf die **Datenwolke eines verlässlichen Anbieters** zurückgreifen werden, dessen

Infrastruktur sich in Bayern, in Deutschland oder zumindest im EU- bzw. EWR-Raum befindet.

Auftragsdatenverarbeitung – Weisungsbefugnisse der Kommune

Ein Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen (Art. 6 Abs. 3 Satz 2 BayDSG). Eine Kommune hat daher sicherzustellen, dass sie ihren **Weisungsbefugnissen** jederzeit nachkommen kann. Weisungsrechte sollten daher bereits vertraglich festgelegt werden. Zugleich empfiehlt es sich bereits aus Beweis- und Dokumentationszwecken, Weisungen nicht nur mündlich, sondern zumindest in elektronischer Form zu erteilen.

Allgemeine Daten- und Informationssicherheit

Nach Vertragsschluss hat eine Kommune außerdem sicherzustellen, dass die **Grundsätze der allgemeinen Daten- und Informationssicherheit** eingehalten werden. Diese finden sich in Art. 7 BayDSG wieder. Diesbezügliche Kontrollmaßnahmen dienen der fortlaufenden Gewährleistung und Absicherung der Schutzziele von Verfügbarkeit, Vertraulichkeit und Integrität.

b) Umsetzung technischer und organisatorischer Anforderungen

Die auf Seiten eines Anbieters implementierten technischen und organisatorischen Maßnahmen sind der maßgebliche Bezugspunkt bei der Umsetzung von Kontroll- und Weisungsrechten (einschließlich diesbezüglicher Dokumentationsverpflichtungen) sowie bei der Einhaltung von allgemeinen Datensicherheitsanforderungen. Vor Vertragsabschluss können diese Maßnahmen bereits im Rahmen der Auswahl eines Anbieters oder bei vertraglichen Festlegungen entsprechend zu beachten sein.

Art. 7 Abs. 2 BayDSG enthält einen **Katalog an Maßnahmen** (Zugangs-, Datenträger-, Speicher-, Benutzer-, Zugriffs-, Übermittlungs-, Eingabe-, Auftrags- und

Transportkontrolle), die im Rahmen einer IT-Sicherheitsarchitektur zu beachten sind. Cloud Computing enthält jedoch zahlreiche neuartige Gefahren. Diesbezüglich implementierte technische und organisatorische Maßnahmen eines Anbieters sind zusätzlich zu berücksichtigen.

Eine ausführliche Erläuterung der Gefahrenlage beim Cloud Computing im kommunalen Sektor findet sich in der ISPRAT-Studie „Cloud-Computing für die öffentliche Verwaltung", S. 71 ff.

http://www.fokus.fraunhofer.de/de/elan/_docs/_studien_broschueren/isprat_cloud_studie_20110106.pdf

Risiken und Gefahren

Ein IT-Outsourcing in die Cloud begegnet typischerweise den folgenden Risiken und Gefahren:

- Kontrollverlust und Abhängigkeit von Anbietern (einschließlich eingeschalteter Subunternehmer)
- Schwierigkeiten bei dem Wechsel zu anderen Anbietern („vendor-lock-in"), Datenportabilität
- Sicherheitslücken bei dem Anbieter (v.a. Prozessmanagement, Fehlverhalten)
- Unzureichender Schutz von Datenverarbeitungsanlagen (Gebäudesicherheit)
- Sicherheitsmängel und Kompromittierungen der IaaS-, PaaS- oder SaaS-Lösung, Angriffe durch Schadsoftware
- Sicherheitsmängel auf den Übertragungswegen, Verschlüsselungsverfahren
- Sicherheitsmängel eines administrativen Webinterfaces
- Verfügbarkeit der IaaS-, PaaS- oder SaaS-Lösung bzw. der Übertragungswege; Wiederherstellungszeiten bei Ausfall
- Schnelles Kopieren von Daten (bspw. Snapshot einer virtuellen Maschine) unter Ausnutzung breitbandiger Datennetze
- Datenverarbeitungen in unterschiedlichen Jurisdiktionen; Zugriffsmöglichkeiten durch Geheimdienste oder andere staatliche Stellen in dem Drittland (US Patriot Act)

- Intransparenz auf Seiten von Anbietern über implementierte Maßnahmen
- Mehrmandantenfähigkeit (von virtuellen Umgebungen), Datentrennung, Fehler bei der Isolation
- Verschlüsselte Speicherung (bei Storage) / Verschlüsselung durch Anbieter
- Hoher Aufwand einer vollständigen Datenlöschung, technische Durchführbarkeit

Technische und organisatorische Maßnahmen

Um diesen Gefahren zu begegnen, sind im Rahmen der Kontrollen verschiedene Maßnahmen auf allen Ebenen einer IT-Sicherheitsarchitektur in Betracht zu ziehen. Diese gehen oftmals über klassische Sicherheitsmaßnahmen hinaus.

Infrastruktur-Ebene

Rechenzentrumsebene (Gebäude- und Betriebssicherheit)

Auf der untersten Ebene einer IT-Sicherheitsarchitektur sind geeignete Maßnahmen zur Gebäude- und Betriebssicherheit der Datenverarbeitungsanlage (Rechenzentrum) zu berücksichtigen. Im Falle einer insourced private cloud sind derartige Maßnahmen am jeweiligen Betriebsstandort der Kommune einzurichten. Zu treffende Maßnahmen sind aus klassischen IT-Outsourcing-Szenarien grundsätzlich bekannt und umfassen in der Regel:

- Allgemeine Gebäude- und Geländesicherheit, Zertifizierungen
- Zutrittskontrolle, Zugangsberechtigungen, Videoüberwachung
- Redundante Stromversorgung (USV etc.), Kühlung (inkl. Klimakontrolle), Datenleitungen
- Sicherheitsmaßnahmen auf den Datenetagen
- Datenleitungen: Redundante Zuführungen (im Gebäude, zum Gebäude)
- Brandschutz: Einteilung in Brandschutzabschnitte, Brandfrühwarnsysteme, Lösch- und Brandbekämpfungssysteme
- Aspekte der Standortredundanz (bei mehreren Rechenzentren)

Server-/IT-System-/Hardware-Ebene

Auch die einer Cloud-Umgebung zugrundeliegenden Hardware-Ressourcen sind durch geeignete Maßnahmen abzusichern. Diese beziehen sich im Wesentlichen auf:

- Zugangs-/Berechtigungsmanagement, Authentisierung
- Sichere Grundkonfiguration, Datensicherungen
  Kann diese durch verteiltes Speichern identischer Datensätze gewährleistet werden? Sind ggf. zusätzliche Datenbackups erforderlich?
- bei Speicherdiensten (Cloud Storage): Verschlüsselung / Verschlüsselungsmethode

Netzwerkebene

Zur Absicherung der Netzwerkebene können vor allem folgende Aspekte zu beachten sein:

- Firewalls, Intrusion Detection, DDoS-Protection
- Ausreichende Bandbreite, niedrige Latenzen
- Anbieter-Vielfalt als Aspekt der Ausfallsicherheit
- Sichere Übertragungswege (v.a. bei Remote-Administration)
- Segmentierte Netze, Redundanzaspekte
- Dedizierte oder öffentliche Leitungs-/Übertragungswege?
- Verschlüsselte Übertragung (+ Verschlüsselungsmethode)

Virtualisierungsebene

Gelangt virtualisierte Hardware zum Einsatz (insb. bei IaaS), ist ein Fokus auf den eingesetzten Hypervisor und die Sicherheit von Daten innerhalb der virtualisierten Umgebung zu legen. Folgende Aspekte sind daher besonders zu berücksichtigen:

- Hypervisor (Zertifizierung)
- Sichere Mandantenisolierung / kein Zugriff durch Dritte: dies ist gerade in Public Cloud-Umgebungen ein äußerst wichtiger Aspekt. Ob und wie

Anbieter dies (überhaupt) durchführen können, bedarf einer sorgfältigen Prüfung.

- Fragen der Sicherheit des der virtuellen Umgebung zugrundeliegenden (meist hochverfügbar ausgelegten Storage-Systems)
- Möglichkeit der Verschiebung von Daten / von ganzen sog. Snapshots virtueller Maschinen unter Berücksichtigung breitbandiger Übertragungswege

Software-/Anwendungs-/Plattform-Ebene

In Bezug auf Software, Anwendungen und Plattformen sind vielfältige Aspekte zu berücksichtigen. Exemplarisch hervorzuheben sind:

- Allgemeines Sicherheitskonzept des Anbieters/Subunternehmers
- Regelmäßige Überprüfung des Leistungsumfangs
- (Regelmäßiges) Update-/Patch-Management
- Rechtemanagement und -verwaltung
- ggf. Zustimmung bei anbieterseitigen Änderungen an der Funktionalität
- Maßnahmen gegen Schadsoftware
- Isolierung von PaaS- oder SaaS-Umgebungen

Weitere Instrumente und Aspekte zur Gewährleistung von Datensicherheit (ebenenübergreifend)

Zur Gewährleistung der Schutzziele der **Datensicherheit** können zudem verschiedene Maßnahmen oder organisatorische Aspekte auf allen Ebenen in Betracht zu ziehen sein. Bekannte Instrumente aus bestehenden IT-Outsourcing-Szenarien werden cloud-spezifisch etwa um Aspekte der Portabilität und Interoperabilität ergänzt (Einsatz von anerkannten Standards für eine schnelle Migration). Im Falle einer Insolvenz des IT-Dienstleisters besteht das Problem, dass der Zugang zu den Daten erschwert sein kann. Dies ist im Rahmen der Notfallplanung zu beachten.

Allgemein berücksichtigt werden sollte vor allem:

- Monitoring, Reports (zum Zweck der Kontrolle)
- Service-Level-Agreements (vgl. oben S. 59), Quality of Service (QoS)
  Definition von Escalation Procedures, Wiederherstellungszeiten
- Allgemeines Notfallmanagement des Anbieters/Subunternehmers
- Aspekte der sogenannten Business Continuity
  Ermittlung der Auswirkungen von anbieterseitigen Störungen
- Versicherung (Deckungssumme)
- Vollständige Löschung von Daten, Schwierigkeiten in virtualisierten Umgebungen / bei verteiltem Rechnen
- Anbieterabhängigkeit (Vendor-Lock-in),
  Auswirkungen bei Übernahme oder Insolvenz
- Portabilität / Interoperabilität, Migration
  (Standardisierungen, offene Standards, Schnittstellen)
- Vollständige Löschung von Daten, Schwierigkeiten in virtualisierten Umgebungen / bei verteiltem Rechnen
- Personalschulung / Mitarbeiter-Qualifizierung
  zur Vermeidung von fahrlässigem oder vorsätzlichem Fehlverhalten
- Behördliche Organisationsanweisungen
- Zertifizierungen, Prüfungen, Audits, Reports, Revisionsfähigkeit
- Maßnahmen zur vertrauensschaffenden Außenwirkung

c) Insbesondere: Anpassung des IT-Sicherheitskonzepts

Wird ein Cloud-Vertrag über einen längeren Zeitraum geschlossen, so ist ein besonderes Augenmerk darauf zu richten, ob und wie das anbieterseitig implementierte **Sicherheitskonzept** an die sich fortentwickelnden technischen Standards und Gefahrensituationen angepasst wird. Die zentrale Durchführung eines Patch- und Updatemanagements durch einen Anbieter kann gerade auf SaaS-Ebene einen großen Vorteil darstellen. Da sowohl die Software als auch die zugrundeliegende

Hardware von dem Anbieter administriert wird, kann dieser sehr zeitnah auf neue Gefahrensituationen reagieren.

Eine Kommune als Cloud-Service-Nutzer sollte zudem allgemein kontrollieren, ob das implementierte Sicherheitskonzept eines Anbieters (einschließlich eingeschalteter Subunternehmer) regelmäßigen Sicherheitstests, sog. Penetration Tests, unterzogen wird.

d) Insbesondere: Fortbildungsmaßnahmen

Fortbildungsmaßnahmen sind notwendig, wenn man bedenkt, wie komplex und nachhaltig Veränderungen sein mögen, die die Umstellung auf Cloud-Services notwendig machen. Solche Fortbildungsmaßnahmen sind ein Bestandteil des **Change Management** und der insoweit obligatorischen akzeptanzstiftenden Maßnahmen (siehe oben S. 53). Ein Anspruch auf Fortbildungsmaßnahmen der Beschäftigten besteht nicht.

*Eine Orientierungshilfe zu den Grundfragen der Auftragsdatenverarbeitung bietet auch der **Landesbeauftragte für den Datenschutz.***

http://www.datenschutz-bayern.de/technik/orient/oh_auftragsdatenverarbeitung.html

e) Die Rolle des Datenschutzbeauftragten

Öffentliche Stellen, die personenbezogene Daten mithilfe von automatisierten Verfahren verarbeiten, sind verpflichtet, einen Beauftragten für den Datenschutz zu bestellen. Bei **Kommunen**, Gemeindeverbänden und den sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts richtet sich die Bestellung des Datenschutzbeauftragten nach Art. 25 BayDSG.

Zur Vertiefung:

Bei öffentlichen Stellen des Bundes und privaten Unternehmen als nichtöffentlichen Stellen richtet sich die Bestellung nach § 4f BDSG. Öffentliche Stellen,

die personenbezogene Daten automatisiert verarbeiten, haben unabhängig von der Anzahl der hiermit beschäftigten Personen gem. § 4f Abs. 1 Satz 1 BDSG stets einen Beauftragten für den Datenschutz zu bestellen.

Gem. Art. 25 Abs. 2 Satz 2 BayDSG können mehrere öffentliche Stellen gemeinsam einen ihrer Beschäftigten als Datenschutzbeauftragten bestellen.

Automatisierte Verfahren bzw. Verarbeitung setzen voraus, dass neben der elektronischen Erhebung und Speicherung auch eine automatisierte Auswertung der Daten, d. h. die Nutzung der Daten ermöglicht wird (bspw. eine digitalisierte Videoaufzeichnung mit der Möglichkeit, bestimmte Personenaufnahmen herauszusuchen oder eine automatisierte Kontoabhebung, *Gola/Schomerus*, BDSG, 10. Auflage 2010, § 3, Rn. 15).

Bei **Staatsbehörden** ist das jeweils übergeordnete Staatsministerium für die Bestellung berechtigt. Beim Landratsamt als Staatsbehörde und Landkreisbehörde kann die Zuständigkeit aufgeteilt werden. Sofern es als Staatsbehörde handelt, ist das fachlich zuständige Staatsministerium verantwortlich. Handelt das Landratsamt als Landkreisbehörde, ist der Kreistag befugt. In **Staatsbehörden** ist der Behördenleiter für die Bestellung des Datenschutzbeauftragten zuständig. In **Kommunen** ist es das jeweilige Vertretungsorgan (Gemeinderat, Kreistag, Bezirkstag) oder ein beschließender Ausschuss, dem die Bestellung als Aufgabe übertragen wurde. Bei der Bestellung oder Abberufung eines behördlichen Datenschutzbeauftragten bedarf es keiner Mitbestimmung des Personalrats, es sei denn, es handelt sich um einen mitbestimmungspflichtigen Vorgang gem. Art. 75 ff. BayPVG, wie bspw. eine Einstellung, Versetzung oder Entlassung.

Durch die Geschäftsordnung kann die **Bestellungskompetenz** auch dem ersten Bürgermeister, dem Landrat oder dem Bezirkstagspräsidenten übertragen werden. Diese Zuständigkeiten gelten auch für die Abberufung des Datenschutzbeauftragten oder die Bestellung eines Vertreters für den Datenschutzbeauftragten. Mehrere behördliche Datenschutzbeauftragte dürfen hingegen gem. Art. 25 Abs. 2 Satz 1 BayDSG nicht für nur eine öffentliche Stelle bestellt werden. Im Unterschied zu § 4f BDSG ist die Schriftform bei der Bestellung zwar nicht verpflichtend vorge-

schrieben, zur Vorgangsdokumentation ist eine schriftliche Bestellung aber empfehlenswert (*Wilde/Ehmann/Niese/Knoblauch*, BayDSG, Art. 25, 16. AL, Rn. 15).

Die behördlichen Datenschutzbeauftragten sind gem. Art. 25 Abs. 3 BayDSG in dieser Eigenschaft der Leitung der öffentlichen Stelle oder deren ständigen Vertretung unmittelbar zu unterstellen.

Bei obersten Dienstbehörden können sie auch dem **Ministerialdirektor** (Amtschef) bzw. in Gemeinden einem berufsmäßigen Gemeinderatsmitglied unterstellt werden. Behördliche Datenschutzbeauftragte sind in ihrer Eigenschaft weisungsfrei, dürfen wegen der Erfüllung ihrer Aufgaben nicht diskriminiert werden und sind, soweit erforderlich, von der Erfüllung sonstiger dienstlicher Aufgaben freizustellen. Ferner sind die personellen, organisatorischen und verfahrensmäßigen Voraussetzungen zur Umsetzung eines effektiven Datenschutzes zu schaffen. Innerhalb der öffentlichen Stelle sind sie zudem Ansprechpartner in allen Angelegenheiten des Datenschutzes.

Bei der Personalauswahl ist zu beachten, dass nur Beschäftige des öffentlichen Dienstes als Datenschutzbeauftragte bestellt werden dürfen. Behördliche Datenschutzbeauftragte müssen zudem über die ausreichende Fachkunde auf dem Gebiet des Datenschutzes und der Datensicherheit verfügen (vgl. Nr. 3 VollzBekBayDSG.)

Externe Personen, bspw. Rechtsanwälte, dürfen nicht als Datenschutzbeauftragte bestellt werden. Gemeinderatsmitglieder sind keine Beschäftigten der Gemeinde und kommen daher nicht in Betracht. Zur Gewährleistung der Unabhängigkeit sollten Beschäftigte benannt werden, die keine offensichtlichen Interessenskonflikte erkennen lassen, wie bspw. ein Behördenleiter oder der Leiter der IT-Abteilung. Die Unabhängigkeit ist jedoch nur ein Gebot – das Gesetz enthält dazu keine konkrete Regelung. Da im Regelfall die überwiegende Anzahl an Beschäftigten in einer öffentlichen Stelle elektronische Datenverarbeitung nutzt, werden Interessenskonflikte nicht vollständig auszuschließen sein.

Vertiefungshinweise:

Wilde/Ehmann/Niese/Knoblauch, BayDSG, Art. 25, 16. AL, Rn. 18.

Gemäß Nr. 3 VollzBekBayDSG sollen nur Bedienstete zu behördlichen Datenschutzbeauftragten bestellt werden, die die notwendige **Fachkenntnis** in Fragen des Datenschutzes und der Datensicherung haben. Den Datenschutzbeauftragten sind nach Maßgabe der verfügbaren Haushaltsmittel die erforderlichen Schulungsmaßnahmen zu ermöglichen. Das Maß der erforderlichen Fachkunde bestimmt sich insbesondere nach dem Umfang der Datenverarbeitung der verantwortlichen Stelle und dem Schutzbedarf der personenbezogenen Daten, die die verantwortliche Stelle erhebt oder verwendet.

Erste Anhaltspunkte, welche Kenntnisse dabei erforderlich sind, lassen sich anhand der Aufgaben eines Datenschutzbeauftragten bestimmen, die in dem Katalog des Art. 25 Abs. 5 BayDSG geregelt sind. Die **juristische Kompetenz** des Datenschutzbeauftragten im Kontext der Datenverarbeitungstechnik nimmt dabei den höchsten Stellenwert ein. Ferner sind **Grundkenntnisse zur elektronischen Datenverarbeitung und zur Datenverarbeitung** und Vorgangsbearbeitung in der öffentlichen Stelle erforderlich. **Betriebswirtschaftliche Grundkenntnisse** können im Hinblick auf die Vergabe von Aufträgen zur Auftragsdatenverarbeitung hilfreich sein.

Vertiefungshinweise:

Albrecht/Dienst, JurPC Web-Dok. 19/2011, Abs. 11 ff.

Der behördliche Datenschutzbeauftragte hat die gesetzlich geregelten Aufgaben zu erfüllen. Dazu zählt, auf die **Einhaltung des Datenschutzes** in der öffentlichen Stelle **hinzuwirken** und diese zu **überwachen**.

- Im Kontext einer geplanten IT-Outsourcing-Maßnahme kann der behördliche Datenschutzbeauftragte den Behördenleiter und bspw. den Leiter der IT-Abteilung **beratend** unterstützen. Der Beauftragte könnte den zustän-

digen Entscheidungsträgern einer öffentlichen Stelle die terminologischen, wirtschaftlichen, rechtlichen und technischen Hintergründe eines IT-Outsourcings sowie die Besonderheiten von Cloud Computing vermitteln und diesbezüglich als Ansprechpartner fungieren.

- Auch bei der Erfüllung der **Sorgfaltspflicht** bei der Auswahl eines IT-Diensteanbieters gem. Art. 6 Abs. 2 Satz 1 BayDSG kann der Beauftragte beratend und prüfend tätig werden. Die Prüfung, ob eine sorgfältige Auswahl vorgenommen wird, kann – wie gesehen (oben Seite 40) – entfallen, Nr. 1 VollzBekBayDSG.
- Der Datenschutzbeauftragte kann in der **Orientierungs-, Planungs- und Gestaltungsphase** auf datenschutzrechtliche Fragen aufmerksam machen und die datenschutzrechtliche Zulässigkeit bestimmter Verfahren prüfen. Im Vorfeld eines IT-Outsourcings prüft der Datenschutzbeauftragte auch die Zulässigkeit der Auftragsdatenverarbeitung anhand der Vorgaben des Art. 6 BayDSG (bzw. ergänzend anhand des § 11 BDSG). Datenschutzrechtliche Vorgaben können auf diese Weise bei der Auftragsvergabe und bei der technischen Umsetzung – ggf. durch technische und organisatorische Maßnahmen – frühzeitig berücksichtigt werden und zu einem effizienten Datenschutz beitragen.
- Zu den Aufgaben des Datenschutzbeauftragten zählt auch die **Freigabe automatisierter Verfahren**, sofern sie nicht bereits vom fachlich zuständigen Staatsministerium oder von der von ihm ermächtigten öffentlichen Stelle für den landesweiten Einsatz erteilt worden ist.

Zur Vertiefung:

- Dies gilt auch für das **IT-Outsourcing**: Sofern die öffentliche Stelle personenbezogene Daten im Auftrag durch Dritte verarbeiten lässt, muss die datenschutzrechtliche Freigabe der zum Einsatz kommenden automatisierten Verfahren von der öffentlichen Stelle erteilt werden.

- Ausnahmen vom Freigabeerfordernis bilden:
    - Automatisierte Verfahren, die bereits vom Vorstand der **Anstalt für Kommunale Datenverarbeitung in Bayern** datenschutzrechtlich freigegeben worden sind und unverändert übernommen werden (vgl. Art. 26 Abs. 1 Satz 2 BayDSG) und
    - Verfahren, die gem. § 2 Bayerische Datenschutzverordnung von der Freigabeprüfung ausgenommen sind, bspw. Textverarbeitungsprogramme oder elektronische Aktenverzeichnisse. Diese Verfahren sind auch von der Aufnahme in das Verfahrensverzeichnis gem. Art. 27 BayDSG befreit.
- Die **Unterlassung eines erforderlichen Freigabeverfahrens** hat nicht die Rechtswidrigkeit der Datenverarbeitung zur Folge, da es sich bei Art. 26 BayDSG nur um eine Ordnungsvorschrift handelt, deren Nichteinhaltung von den vorgesetzten Behörden gem. Art. 31 BayDSG beanstandet werden kann.
- Eine datenschutzrechtliche Freigabe ist von der **Mitbestimmung des Personalrats unabhängig**.
- Darüber hinaus hat der behördliche Datenschutzbeauftragte ein sog. **Verfahrensverzeichnis** zu führen.
    - Es handelt sich um ein Verzeichnis, in dem die bei der Stelle eingesetzten und datenschutzrechtlich freigegebenen automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, dokumentiert werden.
    - Das Verfahrensverzeichnis darf grundsätzlich gem. Art. 27 Abs. 3 Satz 1 BayDSG von Betroffenen eingesehen werden.
    - Der **Behördenleiter** bzw. in Kommunen das jeweilige Vertretungsorgan hat dem Datenschutzbeauftragten die zur Füh-

rung des Verfahrensverzeichnisses erforderlichen Daten und Beschreibungen der Datenverarbeitungsverfahren der Stelle zur Verfügung zu stellen (vgl. Art. 26 Abs. 3 BayDSG).

Nach den Vorgaben der Art. 7, 8 BayDSG ist ferner ein **schriftliches Verarbeitungsverzeichnis** zu führen, das die Zulässigkeit automatisierter Abrufverfahren gem. Art. 8 BayDSG dokumentiert.

Vertiefende Hinweise zum Zeitpunkt der Freigabeprüfung:

Gem. Nr. 4 VollzBekBayDSG soll die Freigabeprüfung vor dem erstmaligen Einsatz eines automatisierten Verfahrens erfolgen. Es soll insbesondere die datenschutzrechtliche Zulässigkeit des Verfahrens geprüft werden. Sie ist daher so frühzeitig durchzuführen, dass erforderliche Änderungen noch ohne Schwierigkeiten berücksichtigt werden können.

Auch Verfahren, für die das Zehnte Buch des Sozialgesetzbuches (SGB X) gilt, sind datenschutzrechtlich freizugeben. Dies gilt nicht für Verfahren der Sozialversicherungsträger und ihrer Verbände. Neben Errichtungsanordnungen nach Art. 47 Abs. 1 PAG, Art. 9 Abs. 1 BayVSG und § 490 StPO sind keine datenschutzrechtlichen Freigaben nach Art. 26 BayDSG erforderlich, da dieser durch die bereichsspezifischen Regelungen verdrängt wird (Art. 2 Abs. 7 BayDSG, Art. 49 PAG, Art. 10 BayVSG).

Auszug von § 2 BayDatenschutzVO:

Keine Freigabe nach Art. 26 BayDSG und keine Aufnahme in das Verfahrensverzeichnis nach Art. 27 BayDSG sind für automatisierte Verfahren erforderlich,

- die ausschließlich Zwecken der Datensicherung und Datenschutzkontrolle dienen, oder
- deren einziger Zweck das Führen eines Registers ist, das auf Grund einer Rechtsvorschrift zur Information der Öffentlichkeit bestimmt

ist oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht.

Das Gleiche gilt für folgende, dem internen Verwaltungsablauf dienende Verfahren:

1. Verfahren, die ausschließlich der Erstellung von Texten dienen und bei denen die personenbezogenen Daten gelöscht werden, sobald sie für diesen Zweck nicht mehr benötigt werden,
2. Verfahren, die ausschließlich dem Auffinden von Vorgängen, Anträgen oder Akten dienen (Registraturverfahren),
3. Verfahren zur Überwachung von Terminen und Fristen (Termin- und Fristenkalender),
4. Telefon-, Telefax- und sonstige Kommunikations- und Teilnehmerverzeichnisse,
5. Zimmer-, Inventar- und Softwareverzeichnisse,
6. Bibliothekskataloge und Fundstellenverzeichnisse sowie
7. Anschriftenverzeichnisse für die Versendung von Informationen an Betroffene.

- Der behördliche Datenschutzbeauftragte kann ferner die Bediensteten mit den Datenschutzvorschriften vertraut machen und **Schulungen** durchführen, bei denen die technischen Risiken einer IT-Outsourcing-Maßnahme aus Anwendersicht Beachtung finden.

Der behördliche Datenschutzbeauftragte nimmt eine wichtige Rolle innerhalb einer öffentlichen Stelle ein. Insbesondere bei der Vorbereitung einer IT-Outsourcing-Maßnahme, bspw. der Auslagerung von Fachverfahren an einen externen Cloud-Provider, kann der behördliche Datenschutzbeauftragte nicht nur die Prüfung der datenschutzrechtlichen Anforderungen übernehmen, sondern auch als Berater und Ansprechpartner für Bedienstete oder IT-Dienstleister tätig werden.

7. Was man vielleicht sonst zum Cloud Computing wissen möchte: FAQ

Handelt es sich bei Cloud Computing um eine neue Technologie?

Nein. Hinter Cloud Computing stehen verschiedene bekannte Technologien und IT-Konzepte. Diese wurden vor allem um flexible und bedarfsgerechte Nutzungselemente ergänzt.

Ist Cloud Computing für öffentliche Stellen eine Revolution?

Im Zusammenhang mit Cloud Computing werden, wie eingangs dargelegt, immer wieder verschiedene Superlative genannt (teilweise auch aus bloßen Verkaufsinteressen). Cloud Computing steht in seinem flexiblen Ansatz jedenfalls für eine Abkehr von bisherigen Nutzungsszenarien. Insoweit liegt zumindest eine Evolution vor. Die Abkehr zur standardmäßigen Nutzung von IT aus Datenwolken wird den Alltag in den nächsten Jahren prägen und zu deutlich veränderten Nutzungsformen führen. Auch öffentliche Stellen können hiervon grundsätzlich profitieren. Da die Berücksichtigung sensibler Datenkategorien jedoch bereits die Anbieterwahl einschränken wird und zugleich meist Auswirkungen auf die Bereitstellungsform (Private Cloud, Community Cloud) hat, sind die insoweit in Betracht kommenden Cloud Lösungen aber gerade nicht vergleichbar mit den wirtschaftlichen Vorteilen von Public Clouds, die oftmals pauschal mit Cloud Computing assoziiert werden. Die Auswirkungen für öffentliche Stellen können daher sehr unterschiedlich sein. Virtualisierte Ressourcen und flexible Vertragslaufzeiten stellen jedenfalls eine deutliche Fortentwicklung gegenüber klassischen IT-Outsourcing-Szenarien dar. Vor allem Thin-Clients und SaaS-Lösungen haben aber das Potential, die alltägliche IT-Nutzung in einer Behörde vor Ort nachhaltig zu verändern.

Wie sicher ist Cloud Computing?

Sicherheitsfragen sind immer einzelfallbezogen zu beurteilen! Die gesamte Bandbreite an möglichen Cloud Services wird bereits durch die unterschiedlichen Servicemodelle (IaaS, PaaS, SaaS) und Bereitstellungsformen (Public Cloud, Private Cloud) verdeutlicht. Genauso vielfältig sind die jeweiligen Gefahren und Risiken, denen durch entsprechende technisch-organisatorische Maßnahmen zu begegnen ist. Dies lässt keine pauschalen Wertungen zu. Der vorliegende Leitfaden berücksichtigt insoweit speziell die Bedürfnisse eines öffentlichen Auftraggebers. Cloud Computing ist so wenig hundertprozentig sicher wie andere technische Lösungen oder soziale Prozesse. Ein erforderliches und angemessenes Sicherheitsniveau kann aber bei Beachtung der in dieser Studie genannten Anforderungen erreicht werden.

Welche Bereitstellungsform ist die sicherste für öffentliche Stellen?

Mit Blick auf die gesetzlichen Anforderungen (v.a. bei der Datenkategorie personenbezogener Daten) kann für öffentliche Stellen in den meisten Fällen nur eine Private Cloud bzw. eine Community Cloud, die nur öffentlichen Stellen zugänglich ist, in Betracht kommen. Die Empfehlung einer Private Cloud deckt sich mit den gegenwärtigen Empfehlungen an Unternehmen aus der Privatwirtschaft bei hohen gesetzlichen und regulatorischen Anforderungen. Es bedarf aber auch hierbei stets einer Bewertung im Einzelfall.

Gibt es neben Art. 6 BayDSG bzw. § 11 BDSG Sonderregelungen bei der Auftragsdatenverarbeitung?

Bei Daten, die dem Sozialgeheimnis gem. § 35 SGB I unterliegen, ist bei der Auftragsdatenverarbeitung ergänzend § 80 Abs. 2 bis 5 SGB X neben Art. 6 BayDSG anzuwenden. Praxisrelevant sind diese Vorschriften insbesondere, wenn kreisfreie Gemeinden, Landkreise oder Bezirke als örtliche oder überörtliche Träger der Sozialhilfe Sozialdaten im Auftrag verarbeiten lassen. Spezialvorschriften sind

auch bei der Auftragsdatenverarbeitung von Patientendaten aus Krankenhäusern zu beachten (Art. 27 Abs. 4, Satz 5-6 BayKrG).

Welche Vorteile bieten IT-Dienstleistungen aus der Cloud für eine Kommune?

Die Kommune kann IT-Dienstleistungen, die weder im Zusammenhang mit den kommunalen Kernaufgaben noch mit den hoheitlichen Aufgaben stehen, auf IT-Dienstleistungszentren auslagern. Diese Anbieter haben sich vielfach auf diese Aufgaben spezialisiert und können sie der Kommune zu erheblich günstigeren Kosten anbieten. Für die Kommune fallen so nicht mehr Fixkosten, sondern variable Kosten nach Inanspruchnahme an. Das bisher gebundene IT-Personal kann für andere, teils höherwertige Aufgaben in der Kommune eingesetzt werden.

Wie kommen Preisvorteile seitens eines Dienstanbieters zustande?

Dienstanbieter profitieren vom Ressourcenpooling und der Virtualisierung. Sie beziehen die bereitgestellte Infrastruktur, Server, Speicher und Software zu günstigen Konditionen und bieten diese im Rahmen eines Cloud-Angebots mit ergänzenden Dienstleistungen gleich mehreren Kommunen an. Durch diese Bündelung von Angebot und Nachfrage sind preiswerte Angebote möglich.

Warum ist das IT-Outsourcing in eine Public Cloud problematisch?

Ein IT-Outsourcing in eine Public Cloud ist im Kontext von frei zugänglichen Daten (Presse- und Öffentlichkeitsarbeit, Webportale, Open Data-Katalog, Informationsregister, Aufbau einer Datenallmende) eine realistische Option. Sobald jedoch personenbezogene Daten, Betriebs- und Geschäftsgeheimnisse oder nicht für die Öffentlichkeit bestimmte Dokumente ausgelagert werden sollen, erweist sich eine Public Cloud auf Grund der gesetzlichen Vorgaben als ungeeignet. Die erforderliche Vertraulichkeit im Umgang mit diesen Daten und Dokumenten kann bei einem frei zugänglichen Angebot im Internet nur sehr begrenzt gewährleistet werden.

Bedeutet Cloud Computing die Aufgabe oder den Verlust von Datenherrschaft und -kontrolle?

Die Kommune ist weiterhin für den gesetzeskonformen Umgang mit den Daten, Informationen und Informationssystemen verantwortlich. Beim Cloud Computing nutzt die Kommune jedoch Anwendungen und Ressourcen externer IT-Dienstleistungserbringer. Damit die Kommune die Herrschaft über die Daten nicht aufgibt und auch die Kontrolle nicht verliert, sind entsprechende vertragliche Regelungen mit dem Dienstleister erforderlich (insbesondere im Falle einer Auftragsdatenverarbeitung zu den im Rahmen dieser Studie dargestellten vertraglichen Aspekten eines Cloud Vertrags).

An welchen Orten werden die Daten in der Cloud gespeichert? „Zirkulieren" diese gar weltweit?

Daten „zirkulieren" nicht in einer weltweiten Cloud, sondern werden in den Rechenzentren gespeichert, die der jeweiligen Cloud des Anbieters zugrunde liegen und von dem Anbieter in dem Vertrag für Speicherung und Verarbeitung auch benannt sind. Anbieter von Cloud-Lösungen entscheiden grundsätzlich eigenverantwortlich, welche ihrer Rechenzentren sie (ggf. weltweit) für welche Aufgaben dabei einsetzen. Sofern Subanbieter zur Datenverarbeitung eingeschaltet werden, sind auch deren Datenverarbeitungsstandorte zu berücksichtigen. Möchten Cloud-Anbieter bayerische Kommunen als Kunden gewinnen, sollten sie wissen, dass die Rechenzentren in Bayern, Deutschland oder zumindest innerhalb des europäischen Wirtschaftsraums liegen sollten, damit die Kommune ihren datenschutzrechtlichen Verpflichtungen nachkommen kann. Die Speicherung replizierter Datensätze (als Sicherheitskopie) in einem zweiten, räumlich getrennten und sicheren Rechenzentrum ist aus Gründen der Ausfallsicherheit und der Fehlertoleranz sinnvoll. Eine über Europa hinausgehende verteilte Speicherung von Daten sollte vertraglich ausgeschlossen werden.

Können Daten in der Cloud verloren gehen?

Sollten gerade die Vorgaben der IT-Grundschutz-Kataloge des BSI von einem Cloud-Anbieter nicht eingehalten werden, kann die Gefahr eines Datenverlustes bestehen. Der Nachweis eines IT-Sicherheitskonzeptes sollte daher von dem Cloud-Anbieter vor Vertragsabschluss erbracht und seitens der Kommune durch unvorhergesehene Kontrollen regelmäßig überprüft werden. An einem Datenverlust hat keiner der Vertragspartner ein Interesse.

Was spricht dafür bzw. dagegen, alles in die Cloud auszulagern?

Wirtschaftlichkeit und Sparsamkeit, vor allem aber personelle und finanzielle Engpässe in den IT-Abteilungen sprechen mittel- und langfristig für eine Verlagerung von IT-Diensten in die Cloud. Die Auswahl ist aber abhängig vom Leistungsportfolio des Anbieters und von den von ihm hierfür veranschlagten Kosten. Der Anbieter muss die Entscheidungsträger im Wettbewerb mit einem attraktiven Angebot zu akzeptablen Konditionen im Rahmen einer Vergabe überzeugen.

Gibt es Cloud-Lösungen, die nicht unter dem Begriff Cloud bzw. Cloud Computing beworben werden?

Cloud und Cloud Computing sind verkaufsfördernde Marketingslogans, die gerne zur Verbildlichung und zur Generierung von Umsätzen eingesetzt werden. Obwohl es sich auch um Angebote aus der Public oder Private Cloud handelt, verbindet man Cloud Computing eigentlich weder mit Facebook und Twitter noch mit dem Ausländerzentralregister oder dem Schengener Informationssystem. Viele Angebote der kommunalen IT-Rechenzentren können im eigentlichen Sinne zu Cloud-Diensten gezählt werden.

Welche Auswirkungen hat es, wenn ein Dienstanbieter virtualisierte IT-Ressourcen verwendet? Was ändert sich für eine Kommune als Kunden?

Der Dienstanbieter stellt bei dem Einsatz von virtualisierten IT-Ressourcen den zugrundeliegenden Ressourcen-Pool mehreren Kunden zur gleichzeitigen Nutzung zur Verfügung. Durch den Rückgriff auf einen virtuellen Server können die Serverkosten pro Kunde (im Vergleich zu dedizierten, physischen IT-Systemen) signifikant gesenkt werden können. Der Anbieter hat zugleich sicherzustellen, dass jeder Kunde nur auf seinen Serverbereich zugreifen kann. Hiervon bekommt ein Kunde eigentlich nichts mit. Vielmehr wird er von all denjenigen technischen Betriebsaufgaben entlastet, die auf den Dienstanbieter übergehen.

Wieso kann Cloud Computing das Betriebsrisiko von IT senken?

Auch die interne IT einer Kommune ist einer Vielzahl an Risiken unterworfen, der sie mit einem eigenen IT-Sicherheitskonzept bereits heute angemessen Rechnung trägt. Durch die Auslagerung von Aufgaben an andere professionelle IT-Dienstleister werden auch die damit verbundenen Betriebsrisiken ausgelagert. Konsequenz ist die Reduzierung des eigenen Betriebsrisikos, zugleich aber auch eine erhöhte Pflicht, die Eintrittswahrscheinlichkeit von Risiken beim beauftragten IT-Dienstleistungsanbieter so gering wie möglich zu halten.

Cloud-basierte Dienstleitungen bergen organisatorische, technische und rechtliche Risiken. Wieso ist ein Rückgriff auf die Cloud trotzdem empfehlenswert?

Ein Rückgriff auf Cloud-Dienste macht Sinn, wenn die damit verbundenen Risiken nach Abwägung als beherrschbar und akzeptabel eingestuft werden und Chancen wie Nutzen weiterhin in der Meinungsbildung überwiegen. Mit den zahlreichen Vorgaben der IT-Grundschutz-Kataloge zum IT-Outsourcing soll gerade sichergestellt werden, dass die Eintrittswahrscheinlichkeit von Risiken äußerst begrenzt ist.

Was passiert bei Insolvenz des Anbieters?

Es sollten im Cloud-Vertrag Regeln vereinbart werden, wie im Falle der Insolvenz des Anbieters der laufende Betrieb fortgesetzt werden und wie gegebenenfalls eine Migration des Gesamtdatenbestandes und der Anwendungen zurück an die Kommune erfolgen kann. Sämtliche Fallgestaltungen einer Anbieter-Insolvenz sind in der Praxis allerdings risikobehaftet.

Anhang 1: Kriterien der Wirtschaftlichkeit

Aspekte der wirtschaftlichen Vorteilhaftigkeit im Überblick:

Wirtschaftliche Vorteilhaftigkeit für Betreiber (Diensteanbieter, Lieferant)

- Ressourcenpooling (Virtualisierung): Standards, Systeme, Anwendungen
  - Komplexitätsreduzierung durch Bildung größerer Einheiten
  - Komplexitätsreduzierung durch Bildung einer verringerten Anzahl von Einheiten
  - Komplexitätsreduzierung durch Verlagerung zu Experten und Spezialisten
  - Speicher-und Datenkonsolidierung durch zentrale Systeme
  - Stromkostensenkung für Betrieb und Kühlung
  - Rechenzentrumskonsolidierung
  - Automatisierte Verbrauchsabrechnung
- Mandantenfähigkeit
- Skalierbarkeit durch Virtualisierungslösungen
  - Bedarfsabhängige Skalierung von Ressourcen
  - Flexible Leistungsanpassung bei zunehmender Nachfrage
- Entwicklungskosten und Entwicklungsnutzen-Kriterien (WiBe 4.1)
- Betriebskosten- und Betriebsnutzen-Kriterien (WiBe 4.2)
  - Laufende Sachkosten/ Sachkosteneinsparungen
  - Laufenden Personalkosten / Personalkosteneinsparungen
  - Laufenden Kosten/ Einsparungen bei Wartung/Systempflege
  - Laufenden sonstige Kosten und Einsparungen
- Dringlichkeits-Kriterien (WiBe 4.3)
- Qualitativ-strategische Kriterien (WiBe 4.4)
- Externe Effekte (WiBe 4.5)
- Selbstbedienung – Besteller übernehmen die Inanspruchnahme
- Verschiedene Betriebsmodelle denkbar

Wirtschaftliche Vorteilhaftigkeit für Kunden (Auftraggeber, Besteller)

- Produkt- und Dienstleistungspolitik
  - Leistungsadäquanz:
    Aufgabenergebnis und Aufgabendurchführung gewährleistet

  - Service Level Agreements: Standardisierte Verträge und Verfügbarkeit
    - Steigerung der Verlässlichkeit und der Leistung
  - Dienstüberwachung: Monitoring
    - Messbare Dienstqualität
    - Protokollierungsmechanismen zur Spurensicherung
    - Vereinfachte Audits
  - Dienstmanagement: effektives Controlling, verkürzte Reaktionszeiten
  - Interoperabilität und Portabilität von Daten und Anwendungen
  - Komplexitätsreduzierung durch Bildung größerer Einheiten
  - Komplexitätsreduzierung durch Bildung einer verringerten Anzahl von Einheiten
  - Kurzfristige Kapazitätsanpassung
    - Nutzer kann selbst neue Server und Speicher aufsetzen
  - Jederzeitige Migrationsmöglichkeit
  - Professionalisierung
    - Hohe Spezialisierung und einheitliche Qualitätsstandards
    - Qualifizierte Systembetreuung durch Spezialisten
- Preispolitik
  - Senkung der Transaktionskosten (durch größere Einheiten)
  - Pay-per-Use-Modelle statt Lizenzen:
    Mieten mit bedarfsabhängiger Abrechnung
    - Rechenleistung
    - Nutzungsdauer
    - Datentransfervolumen
    - Datenspeichervolumen
    - Anwendungen
  - dynamische Erweiterung
  - kürzere Vertragslaufzeiten
  - keine Investitionskosten
  - bedarfsgerechter Rückbau
  - Kostenoptimierung: Kostenvorteile ggü. konventionellen Systemen
    - Lokale Ressourcen (Software/Hardware) lassen sich einsparen
    - Nutzer müssen Server und Softwarelösungen nicht selbst beschaffen
    - ⇨ Kamerale Effizienz:
      Auswirkung auf den Haushalt einer Institution
- Distributionspolitik:Vertrieb über geschlossene Netzwerke oder das Internet
- Entwicklungskosten und Entwicklungsnutzen-Kriterien (WiBe 4.1)
- Betriebskosten- und Betriebsnutzen-Kriterien (WiBe 4.2)
- Dringlichkeits-Kriterien (WiBe 4.3)
- Qualitativ-strategische Kriterien (WiBe 4.4)

  - Priorität der IT-Maßnahme
  - Qualitätszuwachs bei der Erledigung von Fachaufgaben
  - Informationssteuerung der administrativ-politischen Ebene
  - Mitarbeiterbezogene Effekte
  - Verlagerung des Investitionsrisikos bzw. Vermeidung von eigenen Investitionen
- Externe Effekte (WiBe 4.5)
  - Qualitäts- und Leistungssteigerungen: geringe Fehler, rasche Durchlaufzeiten
- Personalpolitik
  - Antwort auf demographischen Fachkräftemangel im IT-Fachkräfte-Arbeitsmarkt
  - Sinkender Bedarf an eigener technischer Infrastruktur-Expertise
  - Reduzierung der eigenen Personalkapazitäten

Wirtschaftliche Vorteilhaftigkeit für die Nutzer der Kunden (Anwender)

- Günstige Angebotspakete
- Senkung der Transaktions- und Verwaltungsgebühren
- Externe Effekte (WiBe 4.5)
  - Ablösedringlichkeit aus Perspektive der Anwender
  - Benutzerfreundlichkeit aus Anwendersicht
  - Wirtschaftliche Effekte bei den Anwendern
  - Qualitäts- und Leistungssteigerungen: geringe Fehler, hohe Durchlaufzeiten
  - Synergien

Quellen und Vertiefungshinweise:

Deussen/Strick/Peters, Computing für die öffentliche Verwaltung, ISPRAT-Studie, Fraunhofer Institut FOKUS, Berlin 2010, http://www.fokus.fraunhofer.de/de/elan/_docs/_studien_broschueren/isprat_cloud_studie_20110106.pdf.

Bundesministerium des Innern, Wirtschaftlichkeitsbetrachtungen (WiBe), Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT, Version 1.4, KBSt-Band 92, Berlin 2007,

http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/wibe_fachkonzept_download.pdf.

Bundesministeriums des Innern, Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung, Bonn 2007, http://www.orghandbuch.de/cln_236/nn_414290/OrganisationsHandbuch/DE/ohb__pdf,templateId=raw,property=publicationFile.pdf/ohb_pdf.pdf

Kriterien für die Wirtschaftlichkeit einer Cloud-Anwendung:

Allgemein: Entwicklungskosten und Entwicklungsnutzen (WiBe 4.1)

- Entwicklungskosten für die neue Cloud Computing-Maßnahme
  - Planungs- und Entwicklungskosten
    - Personalkosten (eigenes Personal)
    - Kosten externer Beratung
    - Kosten der Entwicklungsumgebung
    - Sonstige Kosten für Sach-/Hilfsmittel
    - Reisekosten (eigenes Personal)
  - Systemkosten
    - Hardwarekosten (falls verbuchbar)
      - Cloud, Host/Server, Netzbetrieb
      - Arbeitsplatzrechner
    - Softwarekosten (falls verbuchbar)
      - Kosten für die Entwicklung bzw. Beschaffung von Software
      - Kosten für die Anpassung von Software und/oder Schnittstellen
      - Kosten für die Evaluierung, Zertifizierung, Qualitätssicherung v. Software
    - Installationskosten
      - Bauseitige Kosten
      - Verlegung technischer Infrastruktur
      - Büro-/Raumausstattung, Zubehör
      - Personalkosten der Systeminstallation
  - Kosten der Systemeinführung
    - System- und Integrationstest(s)
    - Übernahme von Datenbeständen
    - Erstschulung Anwender und IT-Fachpersonal
    - Einarbeitungskosten Anwender und IT-Fachpersonal
  - Sonstige Umstellungskosten
- Entwicklungsnutzen aus Ablösung des alten Verfahrens
  - Einmalige Kosteneinsparungen
    - Vermeidung von Erhaltungs-/Erweiterungskosten am Altsystem
  - Einmalige Erlöse
    - Verwertung des Altsystems

Allgemein: Betriebskosten und Betriebsnutzen (WiBe 4.2)

Zu berücksichtigen sind dabei sowohl die Betriebskosten der neuen IT-Maßnahme wie auch der Nutzen aus dem Wegfall der alten IT-Maßnahme. Diesbezügliche Bezugspunkte sind vor allem:

- Laufende Sachkosten/Sachkosteneinsparungen
  - (Anteilige) Leitungs-/Kommunikationskosten
  - (Anteilige) Cloud-, Host-, Server- und Netzkosten
  - (Anteilige) Kosten für Arbeitsplatzrechner
  - Verbrauchsmaterial zur Hardware
  - Energie- und Raumkosten
- Laufende Personalkosten/Personalkosteneinsparungen
  - Personalkosten aus Systembenutzung
  - Kosten/Nutzen aus Dienstposten-Umstufung
  - Systembetreuung und -administration
  - Laufende Schulung/Fortbildung
- Laufende Kosten/Einsparungen bei Wartung/Systempflege
  - Wartung/Pflege der Hardware
  - Wartung/Update der Software
  - Ersatz-/Ergänzungskosten
- Sonstige Laufende Kosten und Einsparungen
  - Datenschutz-/Datensicherungskosten
  - Kosten begleitender externer Beratung
  - Versicherungen u.ä.
  - Sonstige laufende Kosten und Nutzen

Weitere relevante Kriterien für Cloud-Anwendungen:

Dringlichkeits-Kriterien (WiBe 4.3)

- Ablösedringlichkeit Altsystem
- Einhaltung von Verwaltungsvorschriften und Gesetzen
    - Rechtliche Zulässigkeit oder Verpflichtung
    - Gesetzliche Grundlage, die zu einer Auslagerung in eine Cloudlösung verpflichtet

Qualitativ-strategische Kriterien (WiBe 4.4)

- Priorität der IT-Maßnahme
- Qualitätszuwachs bei der Erledigung von Fachaufgaben
    - Qualitäts- und Leistungssteigerungen:
      geringe Fehler, rasche Durchlaufzeiten
- Steuerbarkeit: Informationssteuerung der administrativ-politischen Ebene
    - Ergebnissteuerung: Steuerung der Qualität der Aufgabenerfüllung
    - Durchführungssteuerung:
      Einhaltung spezifischer Vorgaben während Durchführung
    - Übergreifende Steuerung: Aufgabenunabhängige Steuerung
- Mitarbeiterbezogene Effekte
    - Antwort auf demographischen Fachkräftemangel
      im IT-Fachkräfte-Arbeitsmarkt
- Planungssicherheit für Haushalts- und Finanzplanung
- Verlagerung des Investitionsrisikos bzw. Vermeidung von eigenen Investitionen

Externe Effekte (WiBe 4.5)

- Ablösedringlichkeit aus Perspektive der Anwender
- Benutzerfreundlichkeit aus Anwendersicht
- Wirtschaftliche Effekte bei den Anwendern
- Qualitäts- und Leistungssteigerungen: geringe Fehler, rasche Durchlaufzeiten
- Synergien

Flexibilität

- Multiple Standorte – Erhöhte Redundanz
- Verteilte Datenhaltung
- Sofortige und adaptive Ressourcenskalierung

Risikobeherrschbarkeit

- Risikomanagement
    - Risikobewertung nach ENISA 2009
    - Rechtsrisiko: rechtsunsichere Ergebnisse, z. B. Verfahrensfehler
    - Effizienzrisiko:
      Wirtschaftliche Verbesserungseffekte kommen nicht zum Tragen
    - Abhängigkeitsrisiko:
        - Kompetenzverluste
        - Probleme beim Partnerwechsel
        - Missbrauch
    - Zeitnahe Aufdeckung und Beseitigung von Schwachstellen
- Mehr Sicherheit in und durch die Cloud
    - Skaleneffekte
        - Multiple Standorte, Erhöhte Redundanz, Verteilte Datenhaltung
    - Sicherheit als Marktfaktor
        - Sofortige und adaptive Ressourcenskalierung bei Angriffen
    - Security as a Service:
      Sicherheitsmanagement und Sicherheitsarchitektur
    - Bedrohungsmanagement

Hochwertiger Datenschutz

Datenschutz: Kontrollziele, Gefährdungen und Maßnahmen

- Vermeidung einer Auftragsdatenverarbeitung in Drittstaaten

Hochwertige Datensicherheit und Auftragsdatenverarbeitung

IT-Grundschutz (BSI): Ziele, Gefährdungen und Maßnahmen

- Vermeidung von Übernahme virtueller Maschinen durch Dritte
- Vermeidung von „Session Riding and Hijacking“
- Vermeidung von unsicherer oder obsoleter Kryptographie
- Vermeidung von unzureichenden Kontrollen in virtualisierten Netzwerken
- Vermeidung von unzureichenden Schlüsselmanagement-Prozeduren
- Nichtautorisierter Zugang zu Managementschnittstellen
- Netzwerkschwachstellen
- Datenwiedergewinnung:
  Unbefugte Wiedergewinnung von Daten anderer Benutzer
- Manipulation von Abrechnungen

Green IT - Wirtschaftlicher und ökologischer Betrieb

- Erfüllung geltender Umweltstandards
- Energiesparlösungen: Verwendung von energieeffizienteren IKT-Produkten
- Senkung des Energieverbrauchs und damit der Energiekosten der IT
- Nachhaltigkeit: langfristige Maßnahme zur Erhaltung der Umwelt
- Innovative Kühlkonzepte für Server- und Speichersysteme.
- Rechenzentrumskonsolidierung

Transparenz

- Offenlegung von Systemen, Hardware, Software
- Gesamtüberblick über ausgelagerte Datenbestände
- Markttransparenz

Anbieterzertifizierung und -aufsicht zur Marktselbstregulierung

- Zertifizierungsstellen führen Zertifizierungen in bestimmten Bereichen durch
- Erteilen Siegel, Zertifikate oder Prüfplaketten als Nachweise der Überprüfung

Gemeinwohl

- Orientierung am konkreten Nutzen der Cloud-Lösung für das Gemeinwesen

Quellen und Vertiefungshinweise:

Deussen/Strick/Peters, Computing für die öffentliche Verwaltung, ISPRAT-Studie, Fraunhofer Institut FOKUS, Berlin 2010, http://www.fokus.fraunhofer.de/de/elan/_docs/_studien_broschueren/isprat_cloud_studie_20110106.pdf.

Bundesministerium des Innern, Wirtschaftlichkeitsbetrachtungen (WiBe), Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT, Version 1.4, KBSt-Band 92, Berlin 2007, http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/wibe_fachkonzept_download.pdf.

Bundesministeriums des Innern, Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung, Bonn 2007, http://www.orghandbuch.de/cln_236/nn_414290/OrganisationsHandbuch/DE/ohb__pdf,templateId=raw,property=publicationFile.pdf/ohb_pdf.pdf.

Anhang 2: Beispiel eines Mustervertrags zur Auftragsdatenverarbeitung

Quelle: Der Bayerische Landesbeauftragte für den Datenschutz

Datenschutz; Stand: 24.04.2008

Nachfolgend wurde ein Mustervertrag für die Verarbeitung personenbezogener Daten im Auftrag entworfen, der allerdings möglichst universell gehalten ist und insbesondere an den verschiedenen, besonders gekennzeichneten Stellen noch aufgabenspezifisch anzupassen ist. Der Mustervertrag erhebt keinen Anspruch auf Vollständigkeit.

Die kursiv gehaltenen Texte enthalten nähere Erläuterungen zu den einzelnen Punkten und/oder sind durch eigene Angaben zu ersetzen.

Vereinbarung

zwischen .....

(Name der Behörde)

- nachstehend Auftraggeber genannt -

und .....

(Name der beauftragten Stelle)

- nachstehend Auftragnehmer genannt –

§ 1 Gegenstand der Vereinbarung

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers.

Der Auftrag umfasst folgende Arbeiten:

(*Genaue Definition der Aufgaben und der vom Auftragnehmer zu erbringenden Leistungen*)

für folgende Zwecke:

(detaillierte Beschreibung der Zwecke der Auftragsdatenverarbeitung)

§ 2 Rechte und Pflichten des Auftraggebers

1. Für die
   - Beurteilung der Zulässigkeit der Datenverarbeitung,
   - die Wahrung der Rechte der Betroffenen,
   - die datenschutzrechtliche Freigabe,
   - die Führung des Verfahrensverzeichnisses und
   - die Einhaltung der sonstigen gesetzlichen Datenschutzvorschriften

   ist allein der Auftraggeber verantwortlich. Er wird dabei vom Auftragnehmer auf Verlangen unterstützt.

2. Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich.
3. Der Auftraggeber legt die technischen und organisatorischen Maßnahmen nach Art. 7 BayDSG fest, die im Rahmen der Auftragsdatenverarbeitung einzuhalten sind. Generell ist
   1. Unbefugten der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),
   2. zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
   3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),
   4. zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),
   5. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),
   6. zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogenen Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle),
   7. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogene Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
   8. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
   9. zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),
   10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

*Dabei sind insbesondere folgende Maßnahmen zu ergreifen: (Anmerkung: Eine **detaillierte** Beschreibung der zu ergreifenden technisch-organisatorischen Datenschutz- und Datensicherheitsmaßnahmen kann sowohl hier erfolgen als auch in einer Anlage beigefügt werden)*

- ausschließliche Verwendung ausgetesteter und datenschutzrechtlich freigegebener DV-Programme
- Ergreifung von Maßnahmen zur Vollständigkeitskontrolle
- Einsatz von Sicherheitsmaßnahmen nach dem Stand der Technik
- zugriffssichere Speicherung und Aufbewahrung der Daten
- Maßnahmen zur Identifizierung und Authentifizierung
- Sicherheitsmaßnahmen im Rahmen einer Datenübertragung (z. B. Call-back-Verfahren, Verschlüsselung)
- Protokollierung und Auswertung von Protokolldaten insbesondere hinsichtlich von Sicherheitsverletzungen
- Maßnahmen zur Katastrophenvorsorge

4. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
5. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

§ 3 Pflichten des Auftragnehmers

1. Der Auftragnehmer verpflichtet sich, die ihm im Rahmen der Auftragsdatenverarbeitung bekannt gewordenen personenbezogenen Daten des Auftraggebers geheim zu halten und alle in §2 vereinbarten Sicherheitsmaßnahmen zu ergreifen.
2. Die dabei im Einzelnen ergriffenen bzw. zu ergreifenden Maßnahmen werden in einem Sicherheitskonzept festgelegt, das dem Auftraggeber zur Verfügung gestellt wird. Dieses Sicherheitskonzept wird laufend überprüft und (dem technischen Fortschritt) angepasst.
3. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber jederzeit dazu berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der von ihm getroffenen Weisungen zu überprüfen. Dies gilt auch für die Betretung einer Privatwohnung im Falle der Telearbeit. Der Auftragnehmer gewährleistet das für die Durchführung der Kontrollen erforderliche Betretungsrecht, die Einsichtnahme in diesbezügliche Unterlagen, die Vorführung der im Rahmen der Auftragsdatenverarbeitung betrieblichen Abläufe und unterstützt das mit der Durchführung der Kontrolle beauftragte Personal hinsichtlich ihrer Tätigkeit.
4. Der Auftragnehmer setzt für die auftragsgemäße Verarbeitung personenbezogener Daten nur Personal ein, das
   - auf das Datengeheimnis nach § 5 BDSG und nach dem Verpflichtungsgesetz verpflichtet wurde,
   - über die Regelungen der Datenschutzgesetze sowie sonstigen datenschutzrechtlichen Vorgaben angemessen und der Aufgabensituation entsprechend belehrt und geschult wurde und
   - über genügend Sachkunde für die ordnungsgemäße Abwicklung der Aufgaben verfügt.

5. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich nach den Weisungen des Auftraggebers. Er verwendet die zur Datenverarbeitung überlassenen Daten nicht für andere Zwecke und bewahrt sie nicht länger auf, als es der Auftraggeber bestimmt.
6. Der Auftragnehmer gewährleistet - soweit gewünscht - eine Protokollierung der Aktivitäten.
7. Anfallendes Test- und Ausschussmaterial wird vom Auftragnehmer unter Verschluss gehalten, bis es entweder vom Auftragnehmer datenschutzgerecht vernichtet oder dem Auftraggeber übergeben wird. Nicht mehr benötigte Unterlagen mit personenbezogenen Daten dürfen erst nach Weisung durch den Auftraggeber datenschutzgerecht vernichtet werden. Entsprechende Löschprotokolle sind dem Auftraggeber auf Verlangen auszuhändigen.
8. Nach der Beendigung seiner diesbezüglichen Tätigkeit hat der Auftragnehmer alle Daten und überlassene Datenträger (einschließlich etwaig angefertigter Kopien) an den Auftraggeber heraus- bzw. zurückzugeben oder auf dessen Verlangen datenschutzgerecht zu löschen.
9. Die Verarbeitung von personenbezogenen Daten in Privatwohnungen ist nur mit Zustimmung des Auftraggebers im Einzelfall gestattet.
10. Eventuelle Aufträge an Subunternehmer (auch zu Zwecken der Wartung bzw. Fernwartung) dürfen nur nach vorheriger schriftlicher Genehmigung durch den Auftraggeber vergeben werden. Bei der Einschaltung von Subunternehmen gelten für diese die gleichen Pflichten wie für den Auftragnehmer. Dieser hat die Einhaltung der Pflichten regelmäßig zu überprüfen.
    Ein Vertrag mit einem Subunternehmer ist ebenfalls schriftlich zu fixieren. Der entsprechende Vertrag ist dem Auftraggeber vorzulegen.
11. Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei Prüfungen durch die Datenschutzaufsichtsbehörde, schwer wiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers.
12. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich darüber, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis der Auftraggeber eine Entscheidung darüber getroffen hat.
13. Verlangt ein Dritter die Herausgabe bzw. Bekanntgabe von Daten, die im Rahmen der Auftragsdatenverarbeitung erhoben, verarbeitet oder genutzt werden, leitet der Auftragnehmer das diesbezügliche Begehren an den Auftraggeber weiter.

§ 4 Vertragsdauer

1. Der Vertrag

    beginnt am .....

    und endet

    - am .....
    - mit Auftragserledigung

    und wird auf unbestimmte Zeit geschlossen.

    Er ist mit einer Frist von ..... Monaten zum Quartalsende kündbar.

2. Der Auftraggeber ist zu einer außerordentlichen Kündigung des Vertrags berechtigt, wenn der Auftragnehmer trotz schriftlicher Aufforderung die vereinbarten Leistungen nach § 1 nicht ordnungsgemäß erbringt oder seine Pflichten nach § 3 verletzt.

§ 5 Vergütung und Kostenerstattung

Abmachungen über die Vergütung und Zahlungsweise sowie Aufteilung der Kosten zwischen Auftraggeber und Auftragnehmer

§ 6 Haftung

Treten fehlerhafte Arbeiten auf, so kann der Auftraggeber die kostenlose Berichtigung der Arbeiten verlangen. Der Anspruch auf kostenlose Berichtigung setzt voraus, dass der Auftraggeber die fehlerhaften Arbeiten innerhalb von..... Monaten nach Auslieferung schriftlich unter Beifügung der für eine Berichtigung notwendigen Unterlagen beanstandet.

Bei Programmierarbeiten gilt eine Gewährleistungszeit für die Behebung von Programmfehlern von..... Monaten. Danach auftretende Fehler werden im Rahmen der Wartung zu den üblichen Vergütungssätzen behoben.

§ 7 Schadensersatz

Bei Verstoß gegen die Abmachungen dieses Vertrages, insbesondere gegen die Einhaltung des Datenschutzes, wird eine Vertragsstrafe von ..... Euro *(etwa bis 20 Prozent des Auftragswertes)* vereinbart.

§ 8 Nichterfüllung der Leistung

1. Bei Nichterfüllung der Auftragsleistung durch den Auftragnehmer ist der Auftraggeber berechtigt, soweit er nicht von seinem Kündigungsrecht nach § 4 Gebrauch macht, im Benehmen mit dem Auftragnehmer ein anderes Dienstleistungsunternehmen zu beauftragen. Die dabei entstehenden Mehrkosten gehen zu Lasten des Auftragnehmers.
2. Kann der Auftragnehmer die vereinbarte Leistung wegen höherer Gewalt, Krieg, Aufruhr, Streik, Aussperrung oder Stromausfall nicht rechtzeitig erfüllen, so ist er von der Leistung frei. Die Beweislast hierfür obliegt jedoch dem Auftragnehmer. Der Auftraggeber hat in diesem Falle keinen Anspruch auf Schadenersatz. Er hat jedoch das Recht, ein anderes Dienstleistungsunternehmen mit der Auftragsausführung zu beauftragen.

§ 9 Sonstiges

1. Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, etwa durch Pfändung, durch ein Konkurs- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Alle Kundendaten sind in diesem Zusammenhang rechtzeitig vor Eintritt dieser Maßnahmen von den betroffenen DV-Komponenten zu entfernen.
2. Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
3. Sonstige wichtige aufgabenspezifische Regularien: .....

4. Ansprechpartner des Auftraggebers sind:

   .....
   (Name, Funktion, Erreichbarkeit)

   Ansprechpartner beim Auftragnehmer sind:

   .....
   (Name, Funktion, Erreichbarkeit)

   Bei einem Wechsel oder einer längerfristigen Verhinderung eines Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen.

5. Änderungen und Ergänzungen dieses Vertrages bedürfen einer schriftlichen Vereinbarung.

§ 10 Gerichtsstand und Schlussbestimmungen

(Vertragsspezifische Besonderheiten; Gerichtsstand)

_____ _____

(Ort, Datum) (Unterschrift Auftraggeber)

_____ _____

(Ort, Datum) (Unterschrift Auftragnehmer)

Anhang 3: Kenntnisse, Fähigkeiten und Tätigkeiten des Personals

<u>Zur Vertiefung</u>:

Zusätzliche Kenntnisse, Fähigkeiten und Tätigkeiten, die auf Seiten des Personals benötigt werden können:

(M x.xx entspricht der Maßnahme in den IT-Grundschutz-Katalogen des BSI)

Maßnahmen zur Datensicherheit auf kommunaler Seite

- Markt- und Angebotskenntnisse
- Kenntnisse zur Auswahl des Outsourcing-Dienstleisters, M 2.252
- Kenntnisse zur Vertragsgestaltung mit Outsourcing-Dienstleister, M 2.253
- Kenntnisse zur Erstellung eines IT-Sicherheitskonzepts für den ausgelagerten IT-Verbund, M 2.254, M 2.83
- Fähigkeiten zur sicheren Migration, M 2.255
- Kenntnisse zur Planung und Sicherstellung des laufenden Betriebs, M 2.256
- Kenntnisse zur geordneten Beendigung eines Outsourcing-Dienstleistungsverhältnisses, M 2.307
- Kenntnisse zur Notfallvorsorge beim Outsourcing, M 6.83
- Kenntnisse zum Notfallplan für den Ausfall eines VPNs, M 6.109

Maßnahmen zum Datenschutz auf kommunaler Seite

- Fähigkeiten zum Datenschutzmanagement, M 7.1
- Fähigkeiten zur Festlegung von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik bei der Verarbeitung personenbezogener Daten, M 7.5

- Fähigkeiten zur Aufrechterhaltung des Datenschutzes im laufenden Betrieb, M 7.14
- Revision: Aneignung von Wissen über die neuen Aktivitäten

Weitere Fähigkeiten stehen in einer starken Abhängigkeit von den ausgewählten Cloud-Diensten.

Quellen und Vertiefungshinweise:

Deussen/Strick/Peters, Computing für die öffentliche Verwaltung, ISPRAT-Studie, Fraunhofer Institut FOKUS, Berlin 2010, http://www.fokus.fraunhofer.de/de/elan/_docs/_studien_broschueren/isprat_cloud_studie_20110106.pdf.

Bundesministerium des Innern, Wirtschaftlichkeitsbetrachtungen (WiBe), Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT, Version 1.4, KBSt-Band 92, Berlin 2007, http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/wibe_fachkonzept_download.pdf.

Bundesministeriums des Innern, Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung, Bonn 2007, http://www.orghandbuch.de/cln_236/nn_414290/OrganisationsHandbuch/DE/ohb__pdf,templateId=raw,property=publicationFile.pdf/ohb_pdf.pdf.

Welche Tätigkeiten von Mitarbeitern werden zukünftig weniger benötigt?

Durch die Inanspruchnahme von externen Cloud-Diensten und der dazugehörigen Infrastruktur müssen bestimmte Aufgaben nicht mehr in der Behörde selbst wahrgenommen werden. Durch den Verzicht auf eine Vorhaltung dieser Kapazitäten eröffnen sich für Behörden an anderer Stelle ganz neue Gestaltungsmöglichkeiten durch zusätzliches Personal, finanzielle Mittel und freie Räumlichkeiten.

Fähigkeiten Tätigkeiten der Mitarbeiter in der kommunalen IT-Abteilung

- Systeminstallation
- Hardwarebereitstellung (Server vor Ort)
- Softwarebereitstellung
- Softwarewartung
- Systembetreuung und -administration
- Verwaltungsaufwand von Hard- und Softwarebereitstellung
- Schulung/Fortbildung
- Begleitende externer Beratung

Weitere Fähigkeiten in starker Abhängigkeit von den ausgewählten Cloud-Diensten.

Tätigkeiten der nicht-technischen Mitarbeiter in der kommunalen Verwaltung

- Tätigkeiten in den Sekretariaten (Schriftverkehr, Termine, Dienstreisen)
- Tätigkeiten in der Poststelle
- Administrative papierbasierte Tätigkeiten um Einstellungsverfahren
- Administrative papierbasierte Tätigkeiten um das Vergabeverfahren
- Administrative papierbasierte Tätigkeiten in der Bauverwaltung
- Administrative papierbasierte Tätigkeiten in der Schulverwaltung
- Administrative papierbasierte Tätigkeiten in der Finanzverwaltung
- Administrative papierbasierte Tätigkeiten in der Bibliothek

Weitere Fähigkeiten in starker Abhängigkeit von den ausgewählten Cloud-Diensten.

Tätigkeiten der technischen Mitarbeiter in der kommunalen Verwaltung

Lokale Systembetreuung und -administration innerhalb der technischen Abteilungen

Weitere Fähigkeiten in starker Abhängigkeit von den ausgewählten Cloud-Diensten.

Unter welchen Voraussetzungen / in welchem Umfang sind Personaleinsparungen möglich?

Pauschale Aussagen zu Personaleinsparungen lassen sich kaum treffen, denn diese hängen im Umfang immer vom Einzelfall, vom Cloud-Angebot und der bisherigen Situation in der Kommune ab. Ein Blick auf die Prozesskosten lässt zusätzliche Potentiale erkennen, die in einer vorbereitenden Analyse konkret zu beziffern sind.

Konkrete Personaleinsparungen durch Cloud-Dienste wären vorstellbar bei:

- Personalkosten bei Planung- und Entwicklung
    - Personalkosten für Planung und Entwicklung (eigenes Personal)
    - Personalkosten der Systeminstallation
- Personalkosten bei der Systemeinführung
    - Personalkosten der System- und Integrationstest(s)
- Betriebskosten: Laufende Personalkosten/Personalkosteneinsparungen
    - Kosten/Nutzen aus Dienstposten-Umstufung
    - Systembetreuung und –administration
- Personalkosten bei der finalen Migration – Systemablösung
    - Personalkosten der Migration

Gründe für einen Abbau von Dienstposten (Fixkostenreduzierung)

Tätigkeitsbereich des Mitarbeiters entfällt durch ausgewählte Cloud-Dienste

Zentrale Aufgaben im Tätigkeitsbereich entfallen durch Cloud-Dienst ersatzlos

- durch Verzicht auf eigene Softwareentwicklung und -wartung
- durch Verzicht auf den Betrieb im eigenen Rechenzentrum

Personal in einer internen Auffangorganisation andere Aufgaben zuweisen

Gründe für eine Schaffung neuer Dienstposten

- Neue niederwertige Tätigkeitsbereiche für Mitarbeiter durch Cloud-Dienste
- Neue gleichwertige Tätigkeitsbereiche für Mitarbeiters durch Cloud-Dienste
- Neue höherwertige Tätigkeitsbereiche für Mitarbeiters durch Cloud-Dienste

Gründe für eine Dienstposten-Umstufung

Tätigkeitsbereich des Mitarbeiters wird durch Cloud-Dienste niederwertig

- Einzelne/Zentrale Aufgaben im Tätigkeitsbereich entfallen ersatzlos
    - durch Verzicht auf eigene Softwareentwicklung und -wartung
    - durch Optimierung der Prozesse (Medienbrüche, Doppelarbeiten, Liegezeiten)
    - durch Kollaboration unterstützende Dienste (Soziale Netzwerke, Etherpads, virtuelle Arbeitsräume)
    - durch Meinungsbildung unterstützende Dienste (Portale, Liquid Feedback, E-Konsultation, Debatepedia)

  Dies führt zu einer Reduzierung der Bearbeitungskosten je Vorgang.
- Einzelne/Zentrale Aufgaben im Tätigkeitsbereich werden vereinfacht
    - durch Optimierung der Prozesse (Zeiteinsparungen, automatische Absprachen, Parallelarbeiten)

- durch Kollaboration unterstützende Dienste
- durch Meinungsbildung unterstützende Dienste

Dies führt zu einer Reduzierung der Bearbeitungskosten je Vorgang

Tätigkeitsbereich des Mitarbeiters wird durch Cloud-Dienste höherwertig:

- Einzelne Aufgaben im Tätigkeitsbereich werden neu geschaffen
- Zentrale Aufgaben im Tätigkeitsbereich werden neu geschaffen
- Versetzung des Mitarbeiters auf eine höherwertige Position

Wichtige Rahmenbedingung: Personalabbau ohne betriebsbedingte Kündigungen

Die hohe Staatsverschuldung, die Schuldenbremse zur Reduzierung des Haushaltsdefizits sowie die demographische wie budgetäre Herausforderung der anstehenden Pensionierungswelle legen einen weiteren Personalabbau im öffentlichen Dienst mittelfristig nahe. Von einer abrupten Freisetzung des bestehenden Verwaltungspersonals mit der Einführung von Cloud-Diensten ist jedoch dringend abzuraten. Ein solcher Schritt erzeugt erhebliche Unruhe in der öffentlichen Verwaltung und würde den Betriebsfrieden zwischen Arbeitgebern und Arbeitnehmern nachhaltig stören. Zudem profitiert ein Großteil der Beamten und Beschäftigten von einem besonderen Kündigungsschutz. Ein Personalabbau sollte daher laufend über die im öffentlichen Dienste mögliche Personalfluktuation erfolgen, etwa bei Erreichen der Altersgrenze oder die von den Beschäftigten freiwillig selbst ausgesprochenen Kündigungen, so dass keine betriebsbedingten Kündigungen erforderlich sind.

Wie kann eine Entwicklung weg vom autonomen Betrieb hin zum Einsatz von Rechenzentrumsangeboten aus Sicht der Personalwirtschaft gestaltet werden?

Entscheidend für den erfolgreichen Einstieg in das Cloud Computing ist eine überzeugende und nachhaltige Begründung für die Aufgabenverlagerung. Dabei

sollten vorhandene Zeitfenster für Veränderungen wie etwa Umsetzungsfristen, die zunehmende Nachfrage oder anstehende Beförderungen Berücksichtigung finden. Folgende Argumente sollten die Begründung faktisch unterlegen:

- Erweiterung des Leistungsportfolios zu vertretbaren (Mehr-)Kosten
- Vertrauenswürdige Anbieter mit einer angemessenen Qualitätszusicherung Leistungsangebot, Wettbewerbsfähigkeit, Servicequalität, Ergebnisse
- Wirtschaftliche Vorteilhaftigkeit für die Kommune und für ihre Kunden
    - Professionalisierung
      durch hohe Spezialisierung und einheitliche Qualitätsstandards
    - Kosteneinsparungen
    - Stärkere Konzentration auf Kerngeschäft
- Personalwirtschaftliche Kosteneinsparungen

  (Zeitfenster: Pensionierungen)
    - Demographische Herausforderung durch Altersstruktur der IT-Abteilung
    - Zu erwartender Rentenschub bei gleichzeitig geringem Nachwuchs
    - Umwidmung von fixen Personalkosten zu variablen Personalkosten
    - Aufgabenkritik und Geschäftsprozessanalyse abgeschlossen
    - Personalbedarfsermittlung legt künftig einen Stellenabbau nahe
- Perspektive für die betroffenen Mitarbeiter und Führungskräfte vorhanden
    - Freiwerden von Personalkapazität für wichtige Kernaufgaben
    - Konzentration auf Fachaufgaben und Managementaufgaben
    - Personalentwicklungskonzepte für die betroffenen Mitarbeiter
    - Fortbildungsmaßnahmen zur Qualifizierung für neue Aufgaben

Überzeugendes und nachhaltiges Konzept für die Aufgabenverlagerung

- Rechtzeitige und partnerschaftliche Beteiligung des Personalrates
- Überzeugung der IT-Abteilungsleitung von der Aufgabenverlagerung
    - Aufgabenkritik unter Einbindung verwaltungsinterner Organisationsberater
- Übertragung der Cloud Computing-Konzeptentwicklung auf die IT-Leitung
    - Ist-Aufnahme: Erheben der Abläufe, Bearbeitungszeiten und Mengen unter Einbindung aller Organisationseinheiten und Hierarchie-ebenen, die in die Aufgabenerledigung bisher eingebunden sind
    - Konkrete Aufgabenkritik
    - Geschäftsprozessanalyse
    - Erarbeitung des Cloud Computing Konzeptes mit Geschäftsprozessoptimierung
    - Personalbedarfsermittlung
- Vorstellung des Cloud-Computing-Konzepts mit Personalbedarfsermittlung
- Gemeinsames ergebnisoffenes Gespräch zum Cloud-Computing-Konzept
- Beschluss der Behördenleitung/Kommune zum Cloud-Computing-Konzept
- Übertragung der Cloud-Computing-Umsetzung auf die IT-Abteilung
- Aushandlung von Dienstleistungsvereinbarungen
- Einrichtung und Inanspruchnahme der ausgewählten Cloud-Computing-Dienste
- Controlling der Dienstleistungsvereinbarungen (Service Level Agreements)

Überzeugende Perspektive für Führungskräfte der kommunalen IT-Abteilung

- Personalentwicklungskonzepte für die betroffenen Führungskräfte

- Fortbildungsmaßnahmen zur Qualifizierung für neue Aufgaben
- Controlling von Dienstleistungsvereinbarungen (Service Level Agreements)

Überzeugende Perspektive für die Mitarbeiter der kommunalen IT-Abteilung

- Vorschläge zur Personalreduktion stets mit Perspektiven für die Beschäftigten verbinden
- Personalentwicklungskonzepte für die betroffenen Mitarbeiter
- Fortbildungsmaßnahmen zur Qualifizierung für neue Aufgaben

Optionen zu Aufgabenverlagerungen für die kommunale IT-Abteilung

- Verhandlungen und Abstimmung mit den Cloud-Computing-Anbietern
- Qualitätskontrolle gegenüber den Cloud-Computing-Anbietern
- Zuweisung anderer Aufgaben aus dem Portfolio der kommunalen IT-Abteilung
- Wahrnehmung anderer IT-Dienstleistungen vor Ort
- IT-Schulungsaufgaben vor Ort
- IT-Beratungsaufgaben vor Ort (Reorganisation, Prozessoptimierung)

Optionen zum Abbau von Mitarbeitern in der kommunalen IT-Abteilung

- Überführung der Mitarbeiter in andere Bereiche der Verwaltung der Kommune (Organisation, Revision)
- Überführung der Mitarbeiter zum Cloud-Computing-Dienstleistungsanbieter

Ungeeignet: Betriebsbedingte Kündigung

Herausforderungen aus Sicht der Kommune und ihrer Mitarbeiter:

Der Einstieg in das Cloud Computing kann bei den betroffenen Mitarbeitern auch negative Reaktionen hervorrufen, wenn sie sich Sorgen um die Zukunft ihres Arbeitsplatzes machen müssen. Zwar ersetzen Cloud-Dienste nicht die IT-Betreuung in den Behörden vor Ort. Jedoch können Aufgabenverlagerungen in die Cloud auch zu Veränderungen in den Beschäftigungsstrukturen führen. Mitarbeiter werden nur begrenzt eine Bereitschaft verspüren, an personalabbaufördernden Maßnahmen mitzuwirken, falls die eigenen Tätigkeiten dadurch in Frage gestellt werden.

Grundsätzlich kann sich der Einstieg für die kommunale IT-Abteilung aber auch positiv auswirken, insbesondere wenn die Mitarbeiter in ihrer Arbeitsbelastung bereits über das belastbare Maß hinaus eingespannt sind und sich durch das Cloud Computing neue Freiräume für weitere Vorhaben und dringend vorgesehene Projekte eröffnen.

Bundesministerium des Innern, Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung, Bonn 2007, http://www.orghandbuch.de/cln_236/nn_414290/OrganisationsHandbuch/DE/ohb__pdf,templateId=raw,property=publicationFile.pdf/ohb_pdf.pdf.

Anhang 4: C3-Umfrageergebnisse

Die C3-Umfrage wurde gemeinsam mit der Bayerischen Innovationsstiftung entwickelt. Um die Anforderungen für eine rechtskonforme, den Bedürfnissen der kommunalen Verwaltung Rechnung tragende „Cloud"-Lösung formulieren zu können, sollte zunächst grundlegend geklärt werden, welchen Bedarf die Kommunen selbst sehen und welches Verständnis sie von „Cloud Computing" haben. Um diese Frage offen zu halten, wurde in dem Fragenkatalog von einem weiten Verständnis von Cloud Computing und jeglicher Art von Datenverarbeitung auf zentralen, externen Servern eines (privat oder öffentlich-rechtlich organisierten) Dritten ausgegangen. Dies allerdings mit der Einschränkung, dass die Datenverarbeitung im Regelfall innerhalb Deutschlands, in jedem Fall aber in einem EU-Mitgliedstaat stattfindet. Cloud Computing wurde insoweit als eine besondere Ausprägung des bereits praktizierten und anerkannten IT-Outsourcing verstanden.

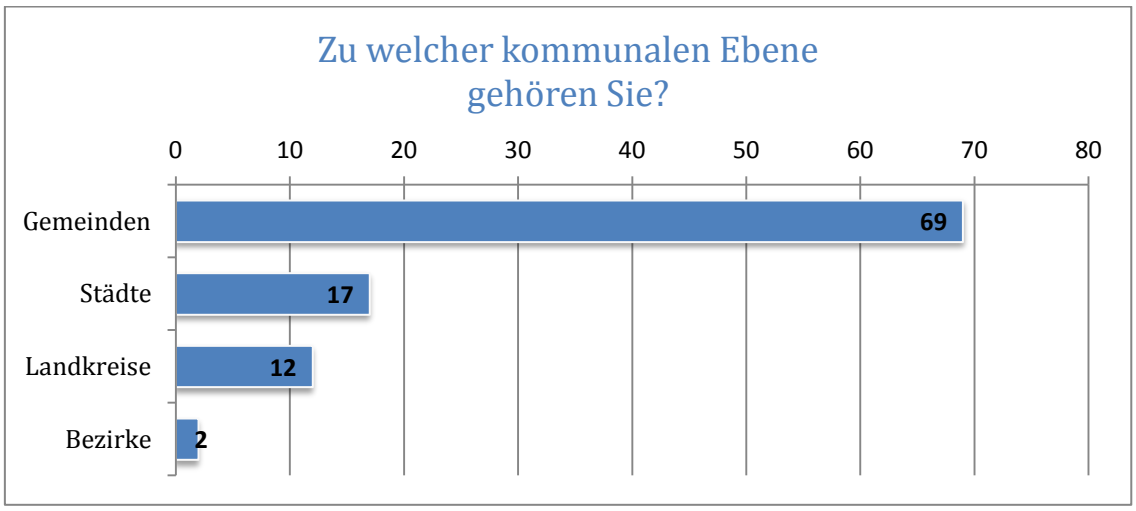
Der Fragenkatalog war allen bayerischen Gemeinden, Städten, Landkreisen und Bezirken auf einer speziell hierfür eingerichteten Webseite für vier Wochen zwischen Mitte April und Mitte Mai 2012 zugänglich.

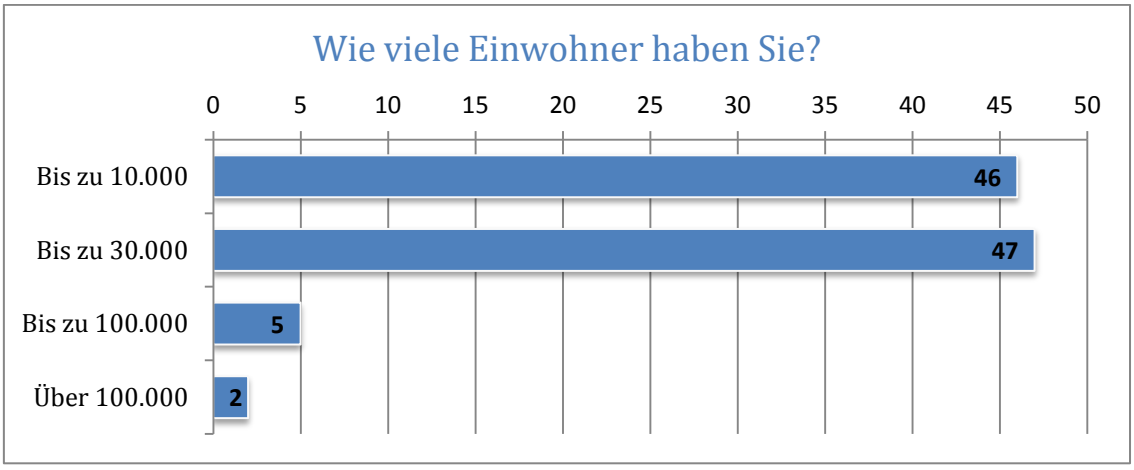
Die Auswertung der Umfrage erfolgte durch Mitarbeiter der der Zeppelin Universität Friedrichshafen. Insgesamt konnten 211 Antworten ausgewertet werden. Da bei den meisten Fragen eine Freitexteingabe möglich war, wurden ähnliche Antworten bei der Auswertung gruppiert und einem Thema/Oberbegriff zugeordnet.

Gesamtanzahl der ausgewerteten Antworten: **211**

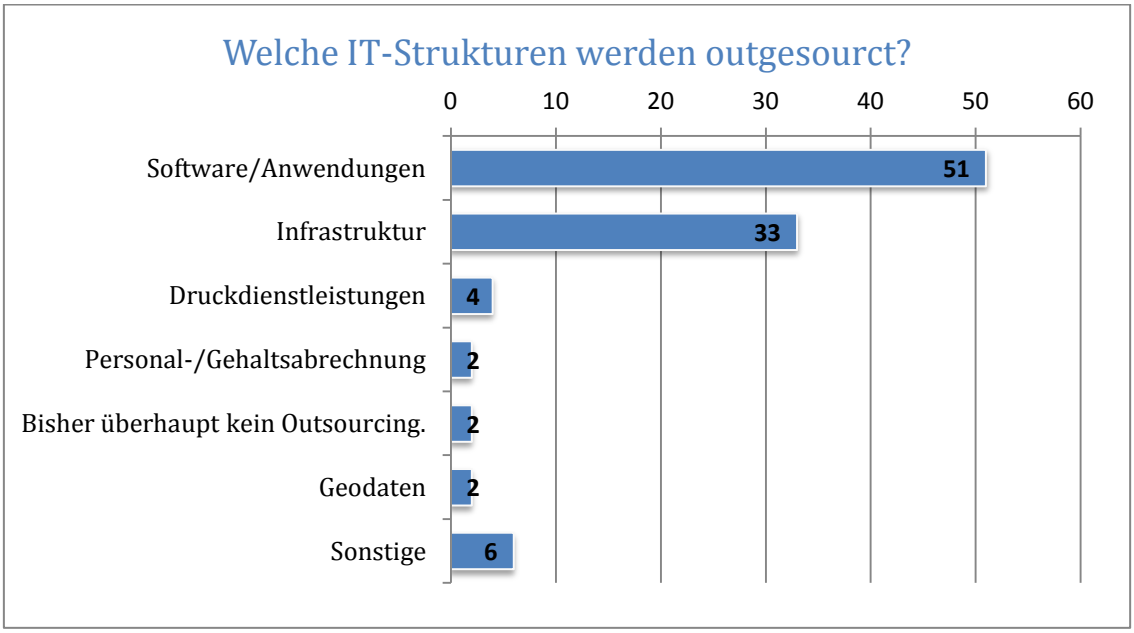
Alle Angaben in Prozent.

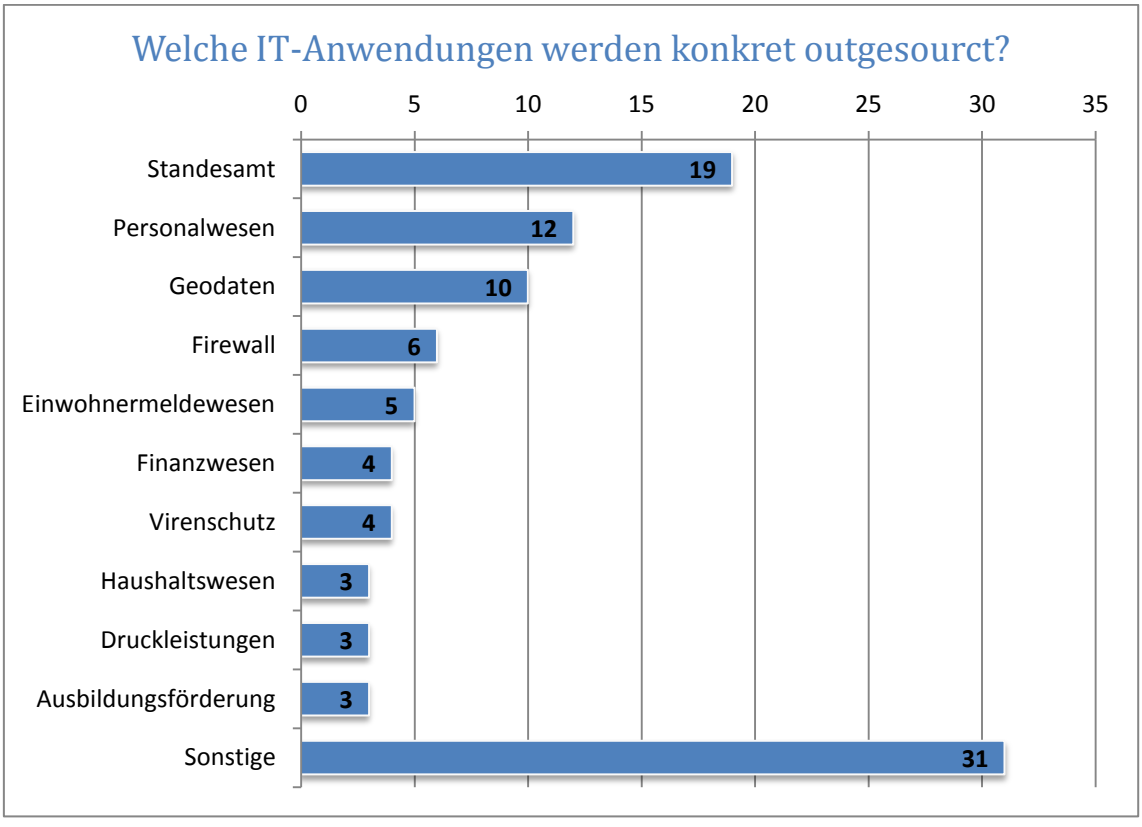
1) Statistische Angaben

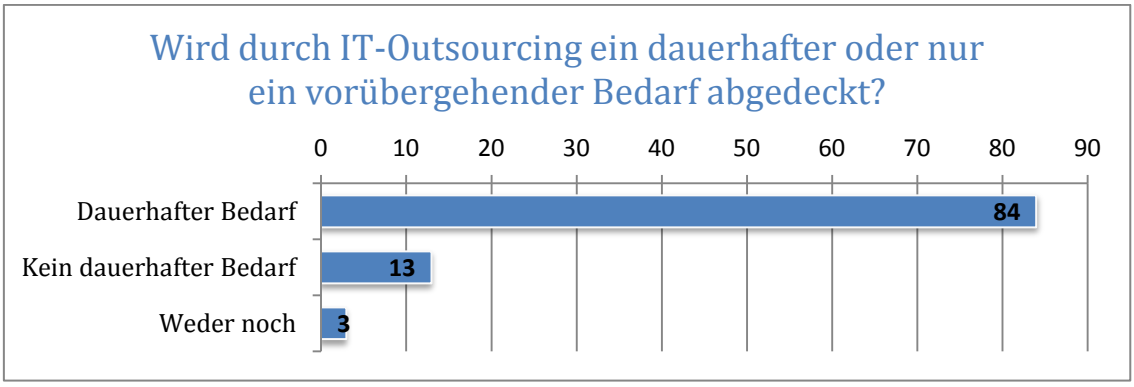


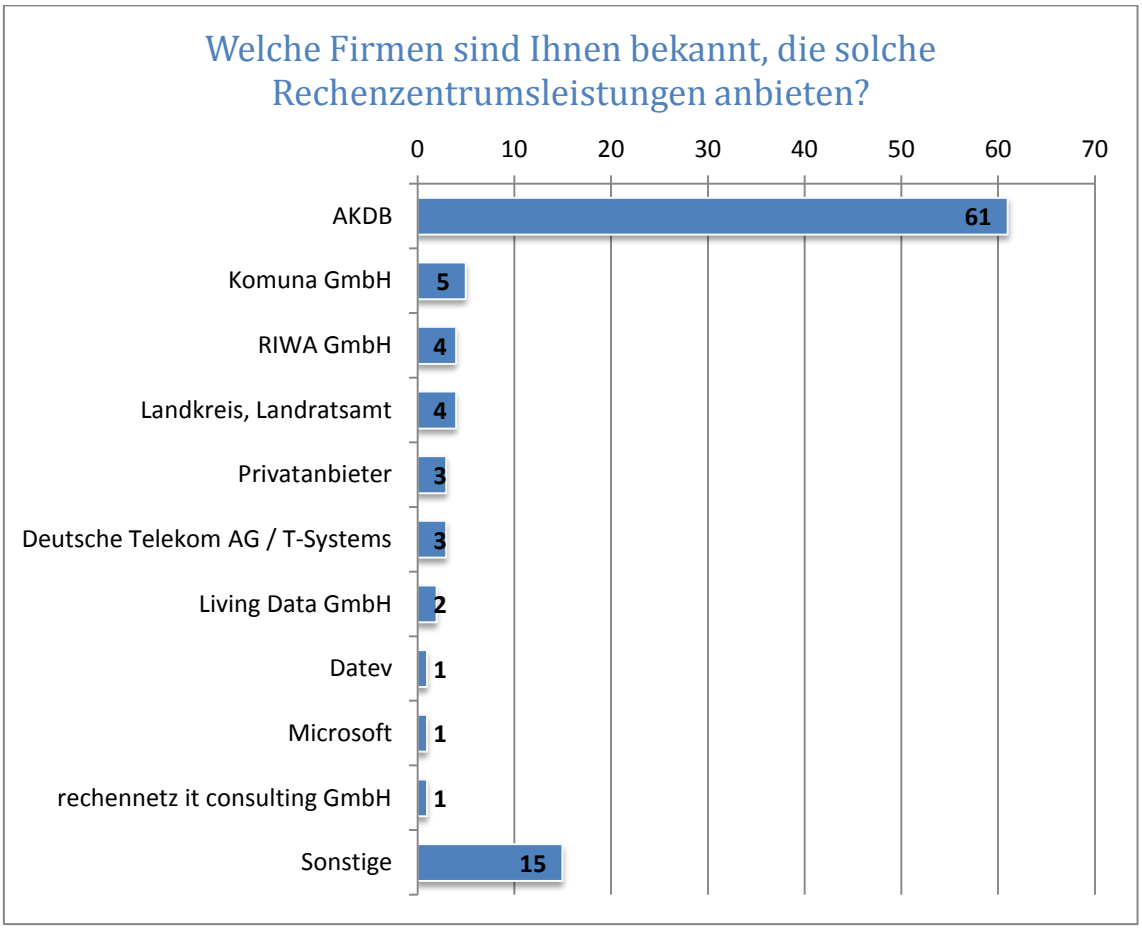


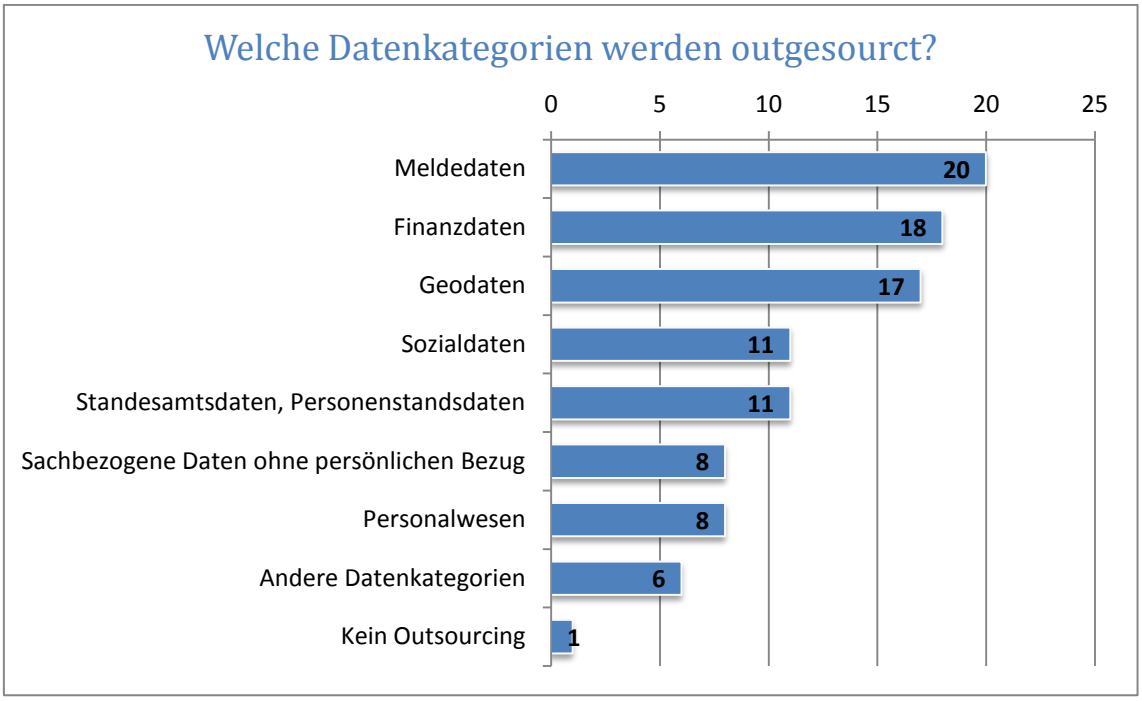
2) IT-Outsourcing – Status Quo – Stattfindendes Outsourcing





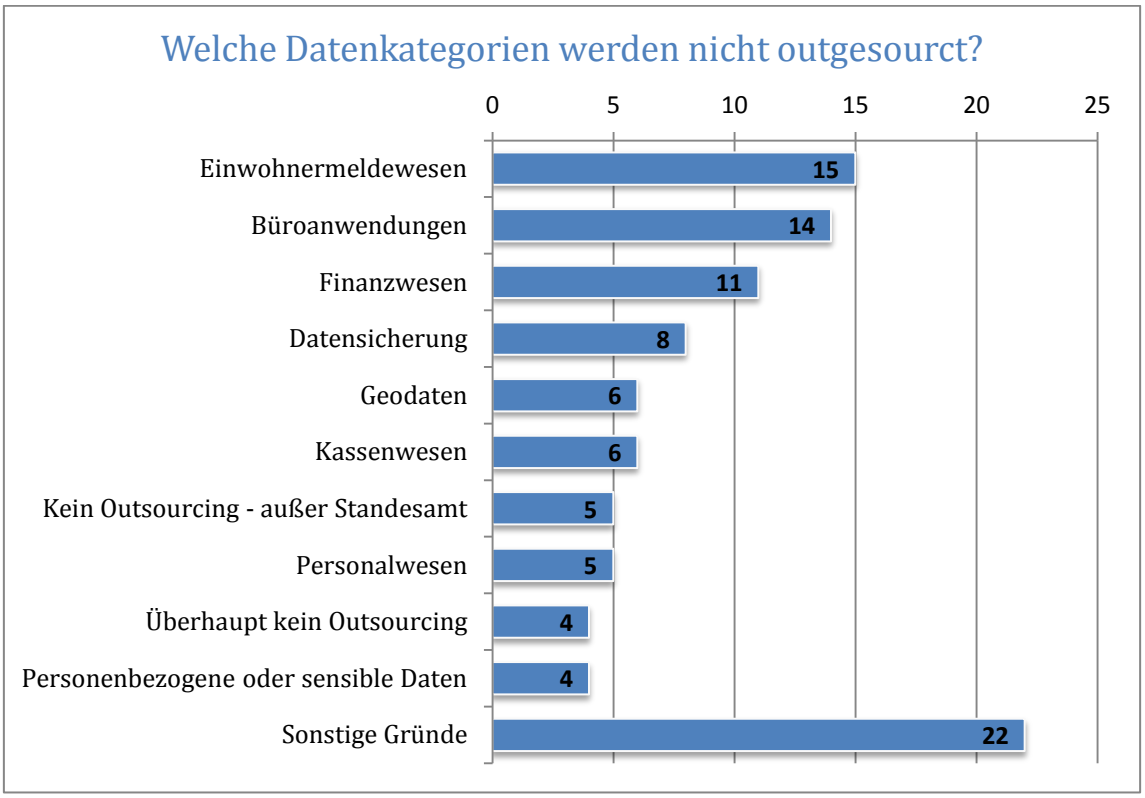

Wird durch IT-Outsourcing ein dauerhafter oder nur ein vorübergehender Bedarf abgedeckt?
0
10
20
30
40
50
60
70
80
90
Dauerhafter Bedarf
84
Kein dauerhafter Bedarf
13
Weder noch
3

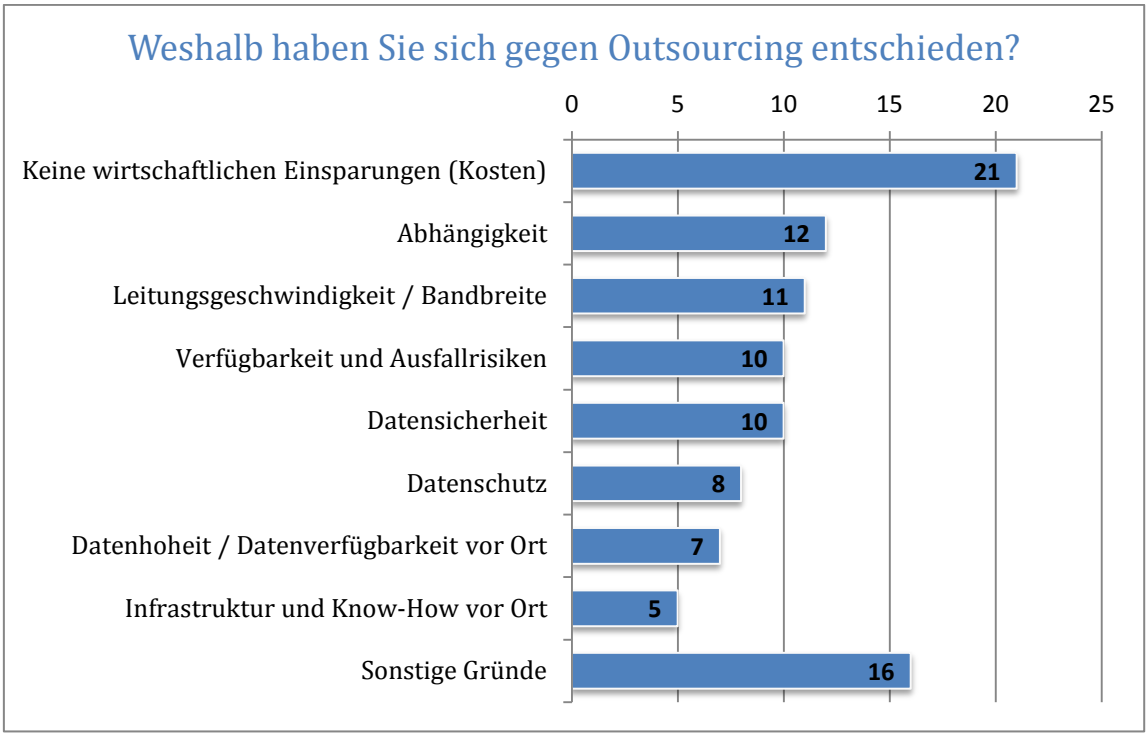

Welche Firmen sind Ihnen bekannt, die solche Rechenzentrumsleistungen anbieten?
0
10
20
30
40
50
60
70
AKDB
61
Komuna GmbH
5
RIWA GmbH
4
Landkreis, Landratsamt
4
Privatanbieter
3
Deutsche Telekom AG / T-Systems
3
Living Data GmbH
2
Datev
1
Microsoft
1
rechennetz it consulting GmbH
1
Sonstige
15

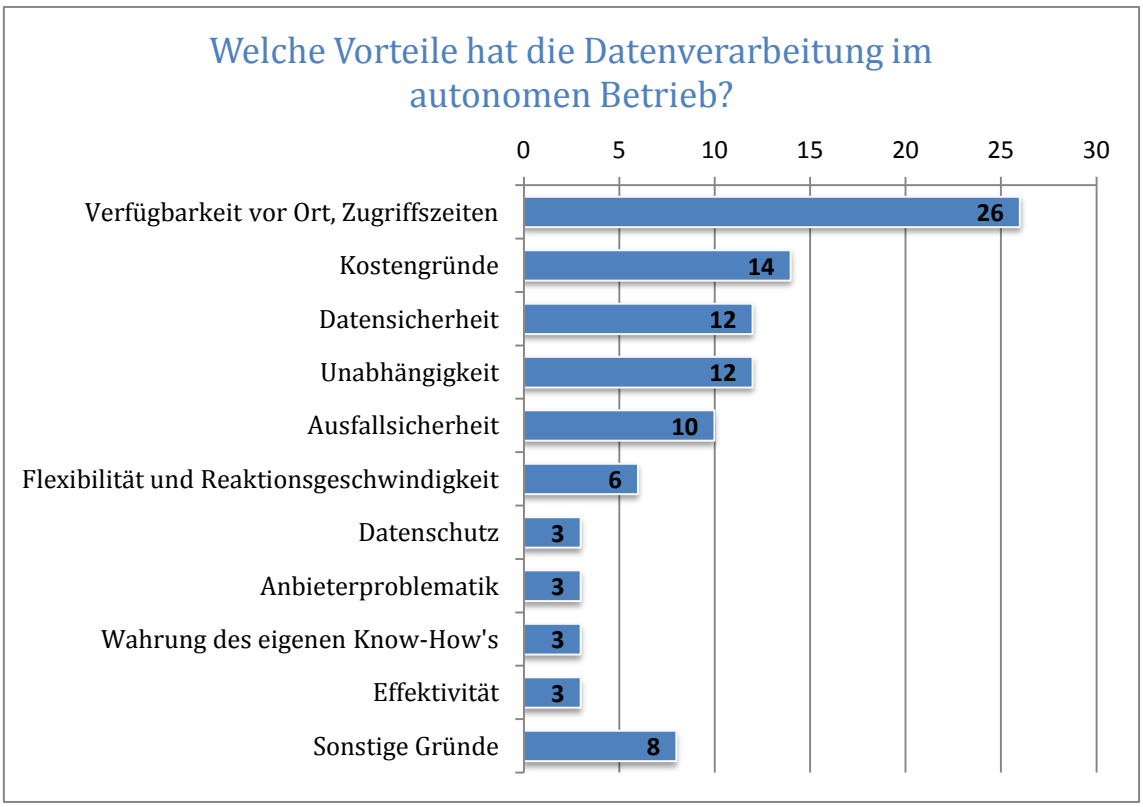

Welche Datenkategorien werden outgesourct?
0
5
10
15
20
25
Meldedaten
20
Finanzdaten
18
Geodaten
17
Sozialdaten
11
Standesamtsdaten, Personenstandsdaten
11
Sachbezogene Daten ohne persönlichen Bezug
8
Personalwesen
8
Andere Datenkategorien
6
Kein Outsourcing
1


Welche Gründe sprechen für Outsourcing?
0
2
4
6
8
10
12
14
16
18
20
Kosteneffizienz
19
Personaleinsparungen
13
Zeit- und Arbeitseinsparungen
9
Datensicherheit
9
Know How des Anbieters
7
Programmaktualisierungen
6
Gesetzliche Vorgaben
5
Mangelnde Hardwareausstattung (intern)
5
Sichere, dauerhaft verfügbare Abrufbarkeit
5
Keine Alternative
4
Sonstige Gründe
18

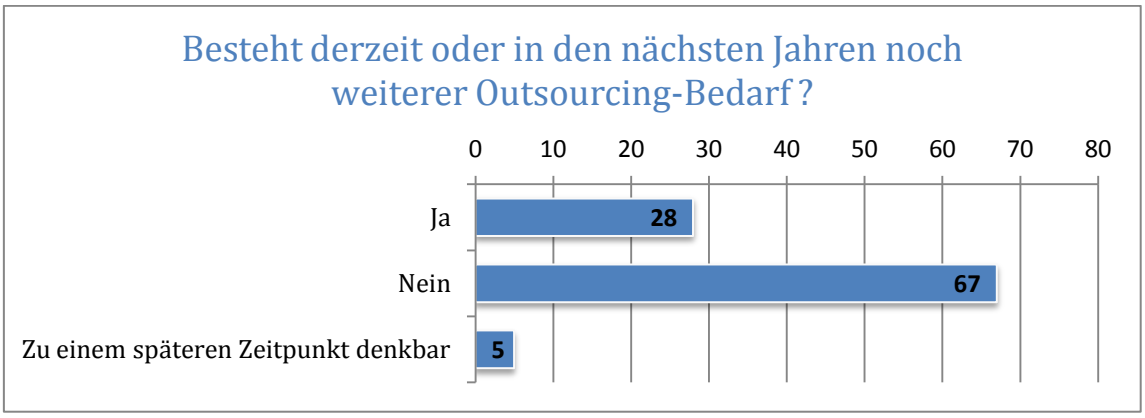
3) IT-Outsourcing – Status Quo – Unterbliebenes Outsourcing

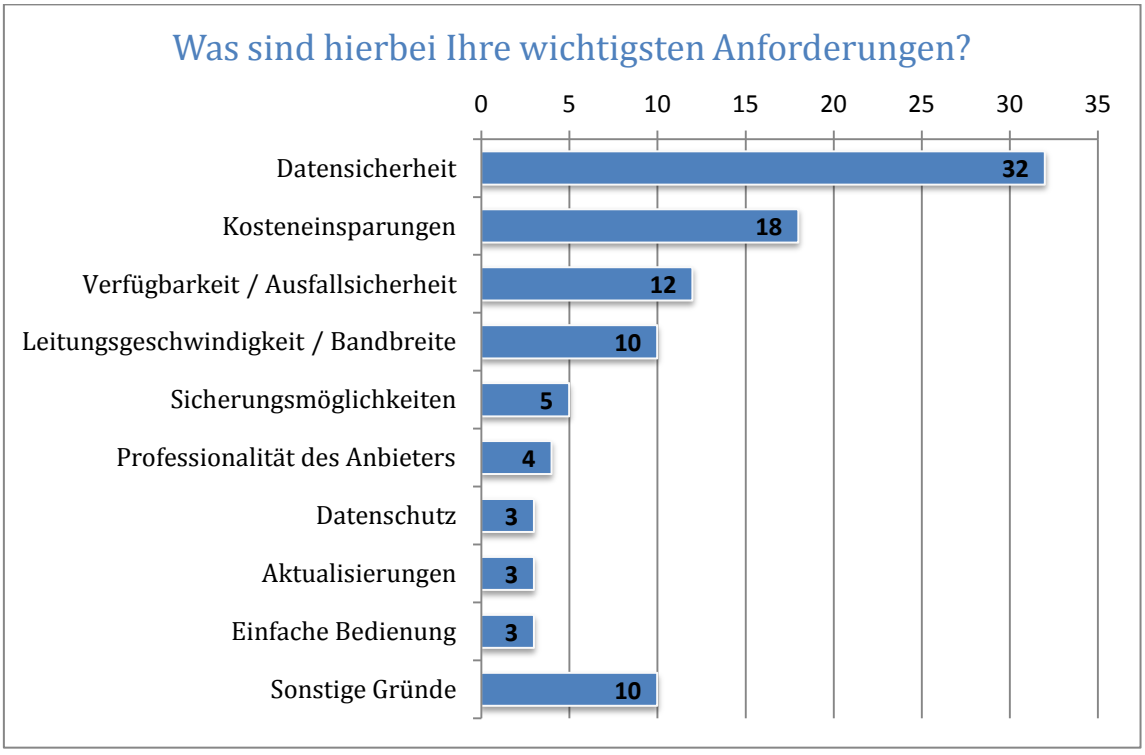


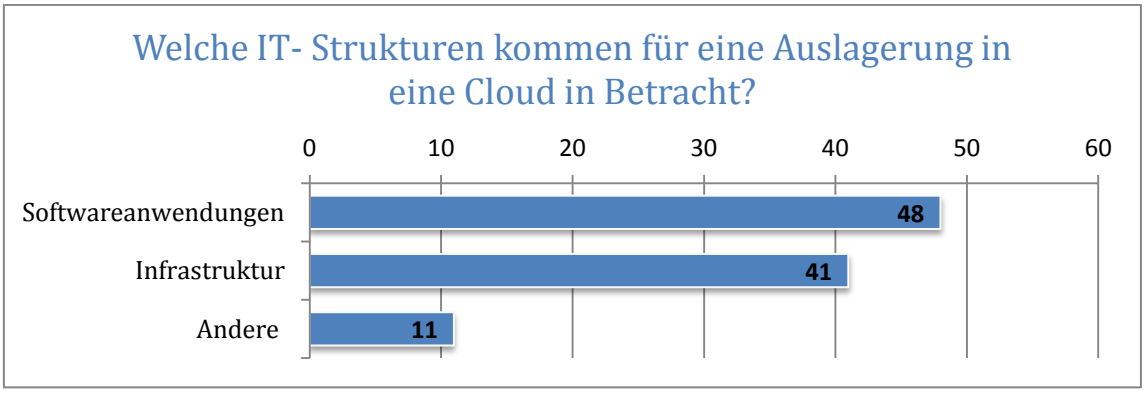

Weshalb haben Sie sich gegen Outsourcing entschieden?
0
5
10
15
20
25
Keine wirtschaftlichen Einsparungen (Kosten)
21
Abhängigkeit
12
Leitungsgeschwindigkeit / Bandbreite
11
Verfügbarkeit und Ausfallrisiken
10
Datensicherheit
10
Datenschutz
8
Datenhoheit / Datenverfügbarkeit vor Ort
7
Infrastruktur und Know-How vor Ort
5
Sonstige Gründe
16

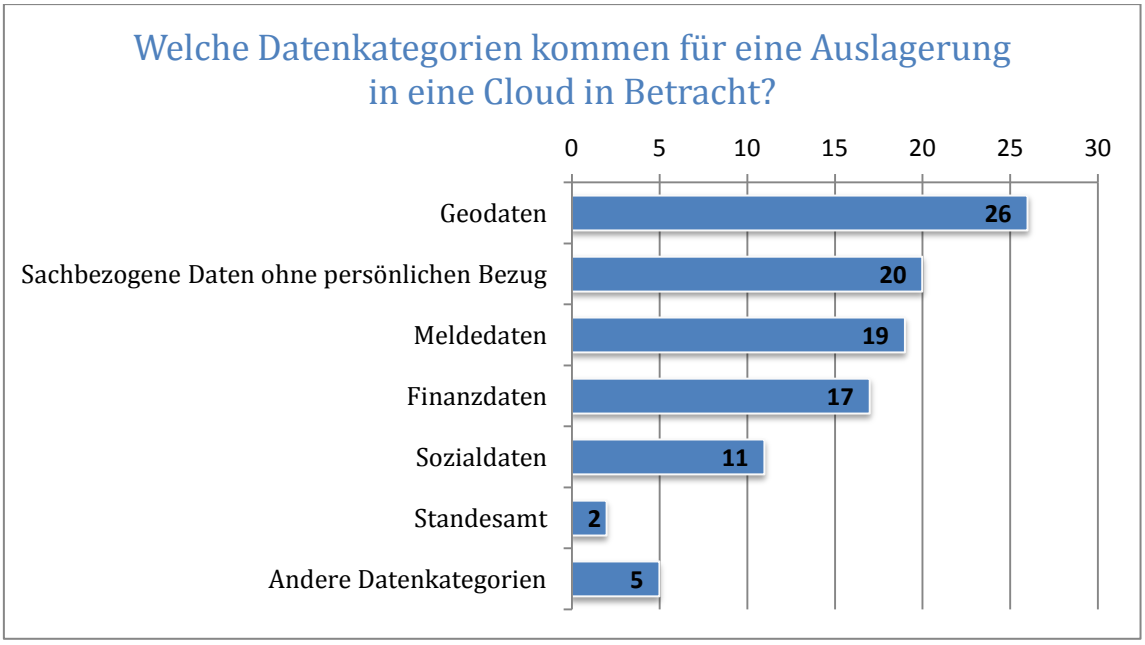

Welche Vorteile hat die Datenverarbeitung im autonomen Betrieb?
0
5
10
15
20
25
30
Verfügbarkeit vor Ort, Zugriffszeiten
26
Kostengründe
14
Datensicherheit
12
Unabhängigkeit
12
Ausfallsicherheit
10
Flexibilität und Reaktionsgeschwindigkeit
6
Datenschutz
3
Anbieterproblematik
3
Wahrung des eigenen Know-How's
3
Effektivität
3
Sonstige Gründe
8

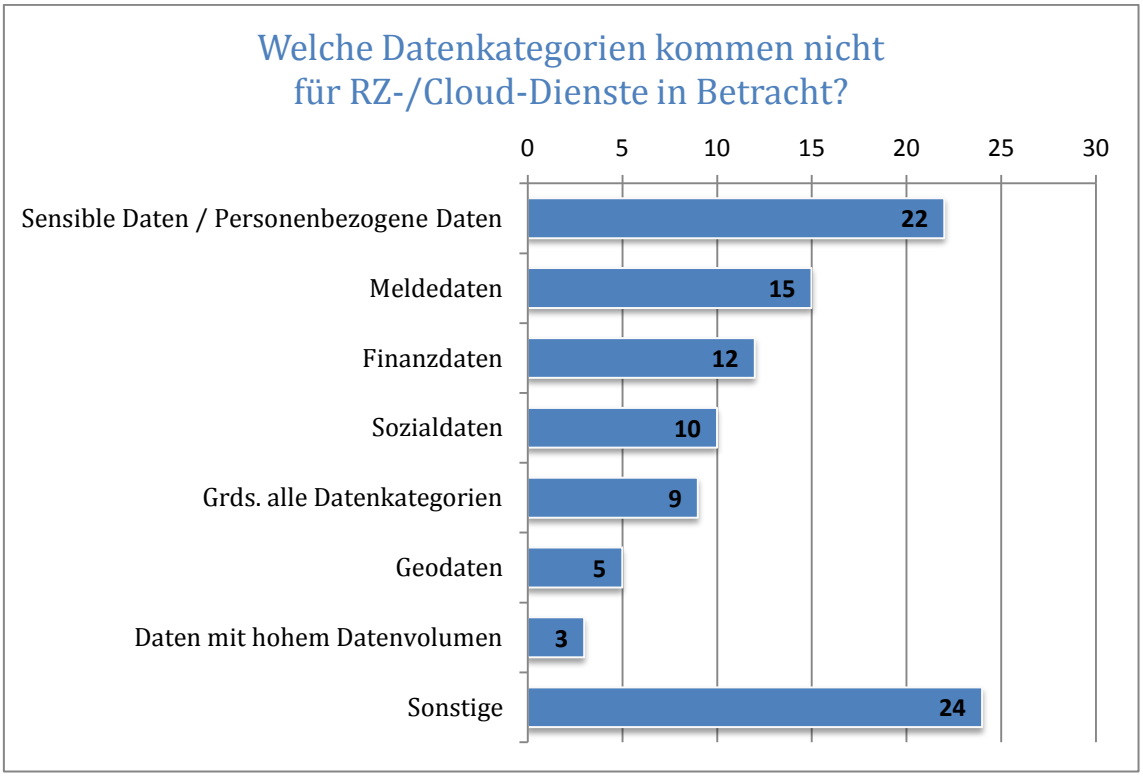
4) IT-Outsourcing – Zukünftige Cloud-/RZ-Szenarien

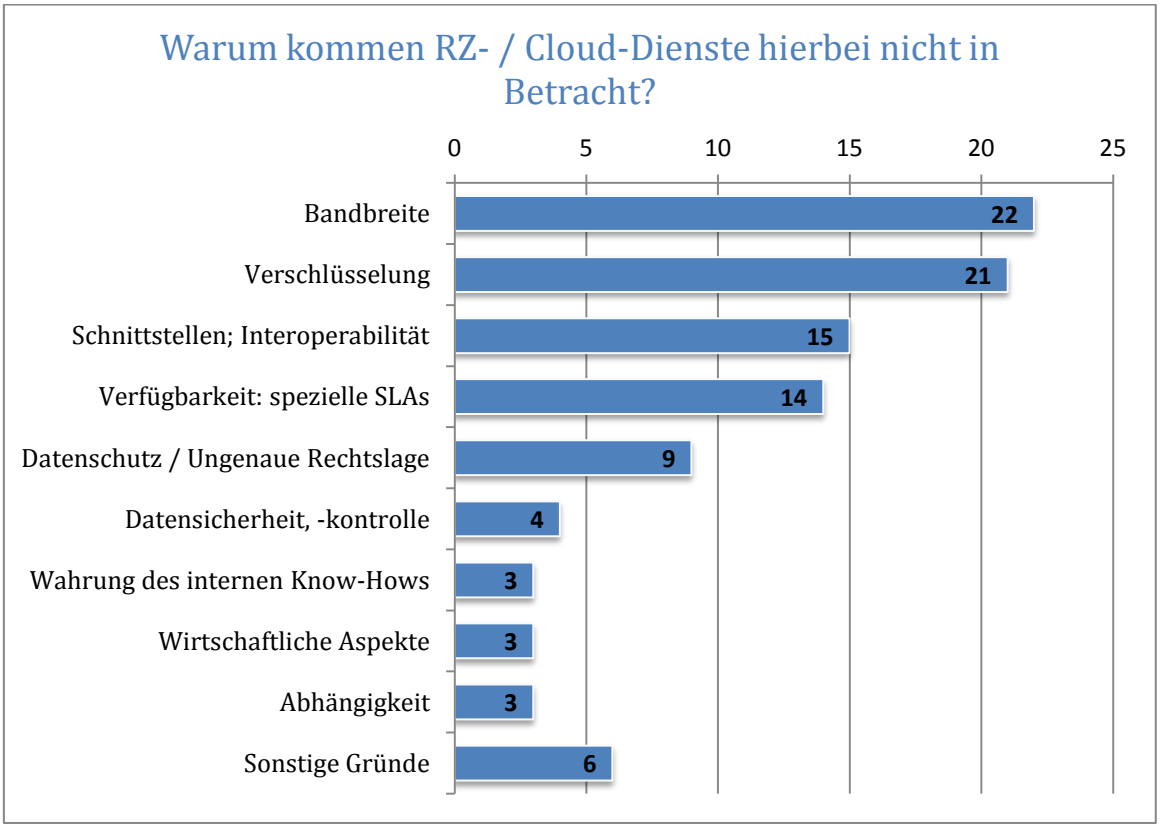


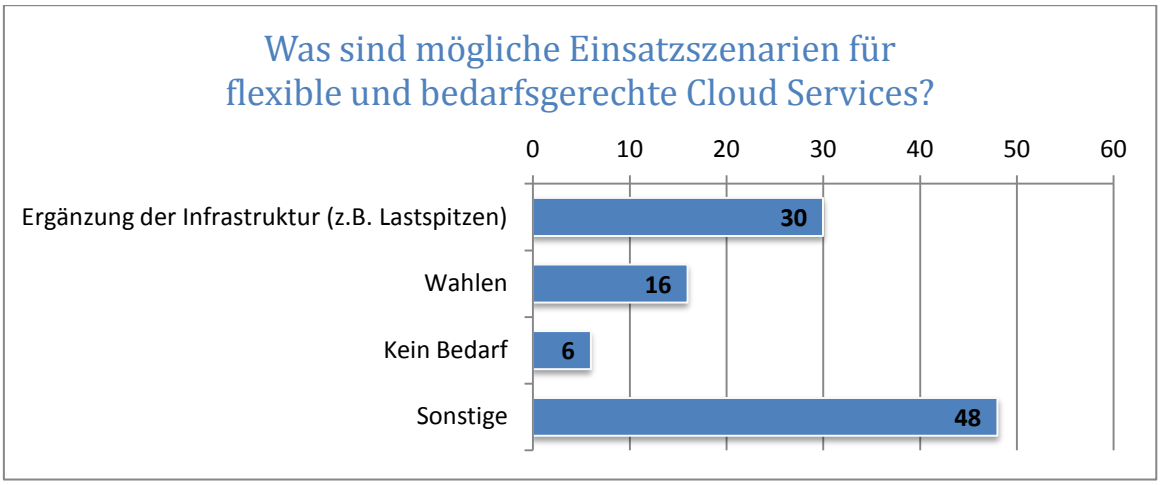


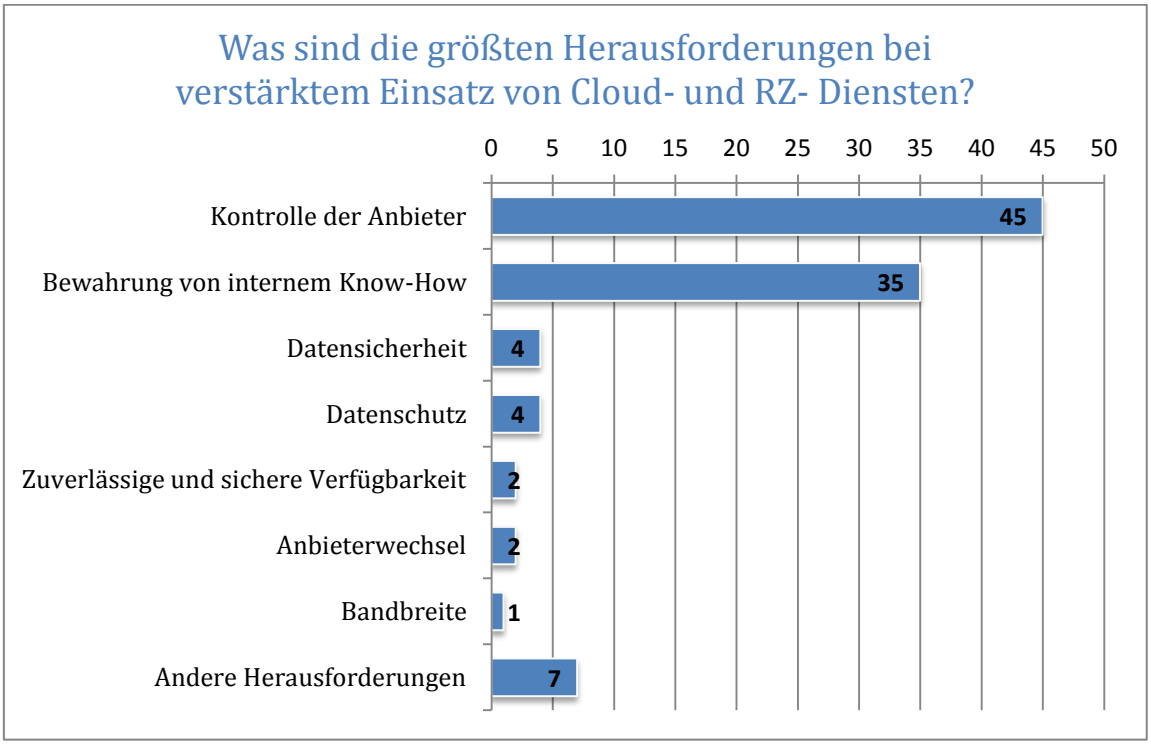

Welche IT- Strukturen kommen für eine Auslagerung in eine Cloud in Betracht?
0
10
20
30
40
50
60
Softwareanwendungen
48
Infrastruktur
41
Andere
11

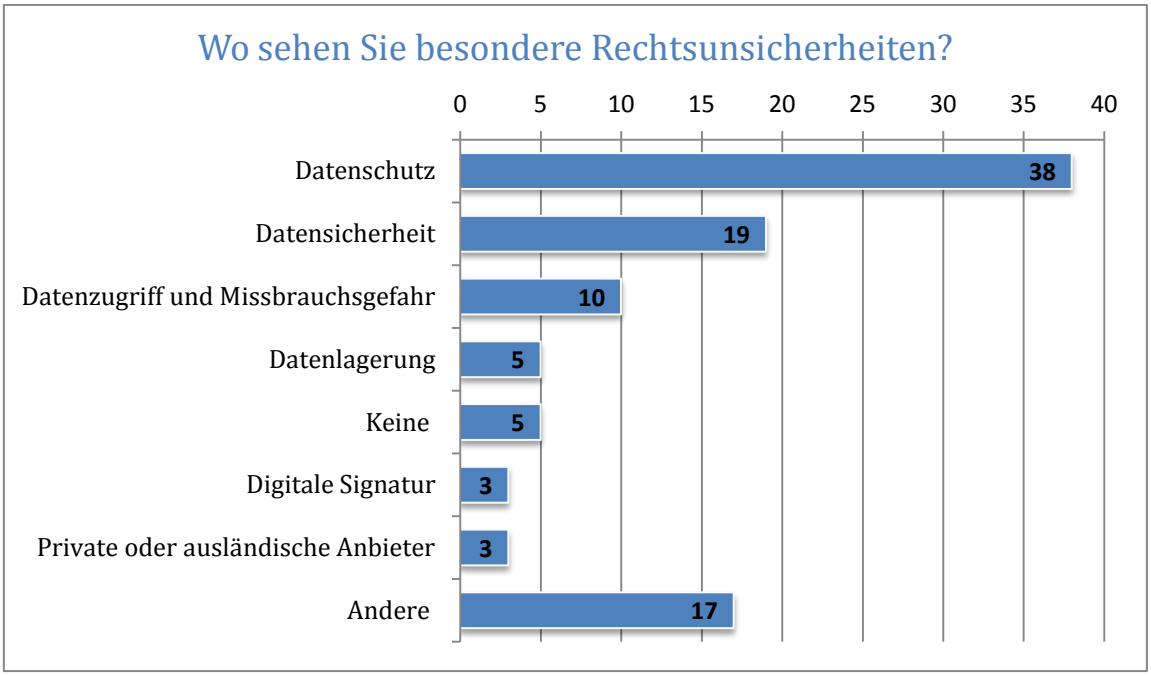

Welche Datenkategorien kommen für eine Auslagerung in eine Cloud in Betracht?
0
5
10
15
20
25
30
Geodaten
26
Sachbezogene Daten ohne persönlichen Bezug
20
Meldedaten
19
Finanzdaten
17
Sozialdaten
11
Standesamt
2
Andere Datenkategorien
5


Welche Datenkategorien kommen nicht für RZ-/Cloud-Dienste in Betracht?
0
5
10
15
20
25
30
Sensible Daten / Personenbezogene Daten
22
Meldedaten
15
Finanzdaten
12
Sozialdaten
10
Grds. alle Datenkategorien
9
Geodaten
5
Daten mit hohem Datenvolumen
3
Sonstige
24


Warum kommen RZ- / Cloud-Dienste hierbei nicht in Betracht?
0
5
10
15
20
25
Bandbreite
22
Verschlüsselung
21
Schnittstellen; Interoperabilität
15
Verfügbarkeit: spezielle SLAs
14
Datenschutz / Ungenaue Rechtslage
9
Datensicherheit, -kontrolle
4
Wahrung des internen Know-Hows
3
Wirtschaftliche Aspekte
3
Abhängigkeit
3
Sonstige Gründe
6


Was sind mögliche Einsatzszenarien für flexible und bedarfsgerechte Cloud Services?
0
10
20
30
40
50
60
Ergänzung der Infrastruktur (z.B. Lastspitzen)
30
Wahlen
16
Kein Bedarf
6
Sonstige
48


Was sind die größten Herausforderungen bei verstärktem Einsatz von Cloud- und RZ- Diensten?
0
5
10
15
20
25
30
35
40
45
50
Kontrolle der Anbieter
45
Bewahrung von internem Know-How
35
Datensicherheit
4
Datenschutz
4
Zuverlässige und sichere Verfügbarkeit
2
Anbieterwechsel
2
Bandbreite
1
Andere Herausforderungen
7


Wo sehen Sie besondere Rechtsunsicherheiten?
0
5
10
15
20
25
30
35
40
Datenschutz
38
Datensicherheit
19
Datenzugriff und Missbrauchsgefahr
10
Datenlagerung
5
Keine
5
Digitale Signatur
3
Private oder ausländische Anbieter
3
Andere
17

Anhang 5: Checklisten

Welches Verfahren/welche Anwendung soll an einen Dritten ausgelagert werden?
Firma des Dienstleisters
Ansprechpartner

Bleibt die Entscheidungsbefugnis über die Datenverarbeitung (insbes. Weisungsrechte, Kontrollrechte etc.) in der Hand der Kommune (Art. 33 Abs. 4 GG)?	
Ja	Nein
Die Form der Datenverarbeitung ist, soweit sie nicht gegen das Verbot der Mischverwaltung verstößt, verfassungsrechtlich unproblematisch. ➔ Zur Vorprüfung und zum Abschluss des Vertrags vgl. u.g. Checkliste.	Findet eine Übernahme der Verantwortung durch den externen Diensteanbieter statt, könnte dies gegen Art. 33 Abs. 4 GG verstoßen. Datenschutzrechtlich wäre eine Funktionsübertragung anzunehmen, auf die Art. 6 BayDSG (bzw. die Verarbeitung im Auftrag) keine Anwendung findet.

Ist von dem IT-Outsourcing die Datenverarbeitung personenbezogener Daten betroffen?	
Ja	Nein
➔ Zur Vorprüfung und zum Abschluss des Vertrags vgl. u.g. Checkliste.	In diesem Fall ist der Anwendungsbereich der Datenschutzgesetze nicht eröffnet.

➔ Dabei sind die in der Begleitstudie ausgeführten Hinweise zu beachten.	➔ Es ist zu prüfen, ob die Daten Geheimnisse oder Verschlusssachen enthalten, woraus eine Schutzbedürftigkeit abzuleiten wäre. Auch bereichsspezifische Sondervorschriften können zu beachten sein.

Werden Daten außerhalb von EU/ EWR verarbeitet oder an einen Empfänger in einem Drittstaat übermittelt?	
Ja	Nein
Internationale Datentransfers sind – im Falle eines Personenbezugs von Daten oder bei anderen sensiblen Datenkategorien – mit teilweise komplexen Fragen an einen wirksamen Datenschutz und an eine ausreichende Datensicherheit verbunden. Neben einer Ermächtigungsgrundlage sind vor allem die Regelungen für internationale Datentransfers zu berücksichtigen. Vor allem die sehr restriktiven Ansichten der Aufsichtsbehörden für den Datenschutz, die gerade bei öffentlichen Stellen Datentransfers meist nur innerhalb von EU und EWR für zulässig erachten, werden internationalen Datentransfers durch öffentliche Stellen regelmäßig entgegenstehen. ➔ Es ist vor allem zu klären, wo die Datenverarbeitung erfolgt. ➔ Es muss in dem Drittstaat, in dem die Datenverarbeitung erfolgt, ein angemessenes Datenschutzniveau vorliegen (ggf. von der EU-Kommission bereits festgestellt). ➔ Sonderfall USA: Safe-Harbor-Vereinbarung (v.a. Prüfung, ob Selbstzertifizierung überhaupt noch gültig ist. Kann zudem den von den Aufsichtsbehörden geforderten Nachweispflichten nachgekommen werden?).	➔ Zur Vorprüfung und zum Abschluss des Vertrags vgl. u.g. Checkliste.

Checkliste für den Vertragsschluss
(Wichtige Kontrollfragen bei der Verarbeitung personenbezogener Daten im Auftrag)

	Nr	Kontrollfragen	Ja Nein	Kap. der Studie	Anmerkung
Vorprüfung	1	Wurden im Hinblick auf das Outsourcing-Vorhaben verschiedene Angebote eingeholt? Bedarf es ggf. einer öffentlichen Ausschreibung?	☐ ☐	4a, 4b	
	2	Wurde eine Übersicht erstellt, welche Verfahren, Dienste, Anwendungen oder Infrastrukturkomponenten an einen Auftragnehmer ausgelagert werden sollen?	☐ ☐	4a, 6e	
	3	Wurde eine Risikoanalyse zur Ermittlung der Schutzbedürftigkeit der Daten, der Gefahren und Risiken sowie der zu ergreifenden, (wirtschaftlich) angemessenen Schutzmaßnahmen durchgeführt? Wurden die unterschiedlichen Phasen eines Projekts (wie Betriebsphase, Exit-Phase) entsprechend berücksichtigt?	☐ ☐	4a, 6b, 6e	
	4	Wurde eine Eignungsprüfung des Auftragnehmers vorgenommen (nicht erforderlich bei AKDB)?	☐ ☐	4a	
	5	Wurde von dem Anbieter eine Auskunft über technisch-organisatorische Schutzmaßnahmen eingeholt? Bestehen diesbezüglich auch Kontrollmöglichkeiten?	☐ ☐	4a, 6b	
	6	Wurde eine Wirtschaftlichkeitsberechnung durchgeführt?	☐ ☐	4c	
Vertragsschluss	7	Sind die Leistungsinhalte und die Gegenleistung (Schutz vor „Kostenexplosion“, Flatrate, transparente Tarifmodelle, Modalitäten einer „pay-per-use“-Nutzung) ausreichend beschrieben?	☐ ☐	5b, 5d	
	8	Ist der Ort der Datenverarbeitung (bei einem verteilten Rechnen über mehrere Standorte hat sich dies auf alle in Betracht kommenden Standorte zu erstrecken) bekannt und sind die	☐ ☐	6b, 6c	

		dort implementierten technisch-organisatorischen Maßnahmen ausreichend beschrieben? Kann das Sicherheitskonzept künftig angepasst werden?			
	9	Gibt es Unklarheiten, offene Rechtsfragen oder verweigert der Auftragnehmer die Vereinbarung bestimmter Klauseln?	☐ ☐	5d	
	10	Wurde ein Datensicherheitskonzept vereinbart, das der vorgenommen Risikoanalyse (vgl. Nr. 3) gerecht wird?	☐ ☐	5b	
	11	Sind die Pflichten des Auftragnehmers und die Weisungsbefugnisse der Kommune eindeutig geregelt?	☐ ☐	5b	
	12	Sind die Kontrollrechte der Kommune (insbesondere das Recht zur Inaugenscheinnahme vor Ort, die Art und Weise der Kontrolle, die Kontrolldichte, die Beauftragung eines Sachverständigen) und die korrespondierenden Duldungs- und Mitwirkungspflichten des Auftragnehmers klar geregelt? Sind die Prüfberichte von Zertifizierungen einsehbar?	☐ ☐	5b	
	13	Ist die Gewährleistung und die Haftung ausführlich, bspw. in Service Level Agreements, geregelt?	☐ ☐	5c	
	14	Sind die Verfügbarkeit, Reaktionszeiten und Notfallmaßnahmen sowie ein fester Ansprechpartner (Helpdesk) definiert?	☐ ☐	5c	
	15	Sind Unterauftragnehmer eingeschaltet und namentlich bekannt? Sind in dem Vertrag Regelungen zur Berechtigung von Unterauftragsverhältnissen enthalten? Kann der Anbieter die mit einem Unterauftragnehmer geschlossenen Verträge vorlegen? Wird das Schutzniveau hierdurch beeinträchtigt?	☐ ☐	5b	
	16	Ist die Vertragslaufzeit bekannt? Sind (flexible) Kündigungsrechte vereinbart?	☐ ☐	5b	
	17	Sind Verfahren des Exit-Managements (insbesondere mit Blick auf den Export der Daten, der Spezifikation der Schnittstellen, des Anbieterwechsels oder der Insolvenz des Anbieters) geklärt und geregelt?	☐ ☐	5b	

	18	Enthält der Vertrag Regelungen zu der Löschung von Daten, die dem Schutzbedarf der betroffenen Daten gerecht wird?	☐ ☐	5b	
	19	Wurde der Vertrag schriftlich abgeschlossen und sind die Unterlagen ausreichend dokumentiert?	☐ ☐	5a	
Anmerkungen					

Index

Literaturverzeichnis

Albrecht, Florian/Dienst, Sebastian	Fach- und Sachkunde der Beauftragten für den Datenschutz. Praktische Hinweise zu § 4f BDSG, JurPC Web-Dok. 19/2011 Abs. 1-36
Art.-29-Datenschutzgruppe	Working Paper 196, Stellungnahme zu Cloud Computing, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf;
Bierekoven, Christiane	Lizenzierung in der Cloud, ITRB 2010, 42-44
Bisges, Marcel	Urheberrechtliche Aspekte des Cloud Computing, MMR 2012, 574-578
Bräutigam, Peter	IT-Outsourcing – Eine Darstellung aus rechtlicher, technischer, wirtschaftlicher und vertraglicher Sicht, 2. Aufl., Berlin 2009
Bundesamt für Sicherheit in der Informationstechnik	Eckpunktepapier – Sicherheitsempfehlungen für Cloud Computing Anbieter (Mindestanforderungen in der Informationssicherheit) https://www.bsi.bund.de/DE/Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.html
Bundesamt für Sicherheit in der Informationstechnik	IT-Grundschutz-Kataloge, https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/kataloge.html
Bundesministerium des Innern	Wirtschaftlichkeitsbetrachtungen (WiBe), Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT, Version 1.4, KBSt-Band 92, Berlin 2007, http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/wibe_fachkonzept_download.pdf
Bundesministerium des Innern	Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung, Bonn 2007, http://www.orghandbuch.de/cln_236/nn_414290/OrganisationsHandbuch/DE/ohb__pdf,templateId=raw,property=publicationFile.pdf/ohb_pdf.pdf
Deussen, Peter H./Strick, Linda /Peters, Johannes	Computing für die öffentliche Verwaltung, ISPRAT-Studie, Fraunhofer Institut FOKUS, Berlin 2010, http://www.fokus.fraunhofer.de/de/elan/_docs/_studien_broschueren/isprat_cloud_studie_20110106.pdf

Düsseldorfer Kreis	Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29.4.2010 in Hannover (überarbeitete Fassung vom 23.8.2010)
EU-Kommission	Cloud Strategie Papier, Unleashing the Potential of Cloud Computing in Europe (Freisetzung des Cloud-Computing-Potentials in Europa), KOM(2012) 529 endg., http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf
EuroCloud Deutschland_eco e.V.	Leitfaden Cloud Computing: Recht, Datenschutz & Compliance, 2010, http://www.dmi.de/fileadmin/user_upload/PDF2012/Wissen/T_Cloud_Computing.pdf
European Network and Information Security Agency (ENISA)	Cloud Computing, Benefits, risks and recommendations for information security, 2009, http://www.enisa.europa.eu/
Gercke, Marco	Strafrechtliche und strafprozessuale Aspekte von Cloud Computing und Cloud Storage, CR 2010, 345-348
Gola, Peter/Schomerus, Rudolf	BDSG, 10. Aufl., München 2010
Grapentin, Sabine	in: Bräutigam, IT-Outsourcing, 2. Aufl., Berlin 2009
Hammon, Larissa/Hippner, Hajo	Crowdsourcing, Wirtschaftsinformatik, 54. Jahrgang, Heft 3, Wiesbaden 2012, S. 165-168
Heckmann, Dirk	IT-Outsourcing der Öffentlichen Hand, in: Bräutigam (Hrsg.), IT-Outsourcing. Eine Darstellung aus rechtlicher, technischer, wirtschaftlicher und vertraglicher Sicht, 2. Aufl., Berlin 2009
Heckmann, Dirk	Cloud Computing im Zeitgeist. Juristische Hürden, rechtspolitische Unwägbarkeiten, unternehmerische Gestaltung, in: Heckmann/Schenke/Sydow, Festschrift für Thomas Würtenberger, Berlin 2013
Hennrich, Thorsten	Compliance in Clouds – Datenschutz und Datensicherheit in Datenwolken, CR 2011, 546 ff.
Hennrich, Thorsten/Maisch, Michael Marc	Cloud Computing und Safe Harbor: Wolken über dem sicheren Hafen?, Juris Anwaltszertifikat IT-Recht 15/2011
Hoßfeld, Tobias/Hirth, Matthias/Tran-Gia, Phuoc	Crowdsourcing, Informatik-Spektrum, 35. Jahrgang, Heft 3, Heidelberg 2012, S. 204-208
Hullen, Nils	EU-Kommission stellt Weichen für europaweite Förderung des Cloud Computings, jurisPR-ITR 18/2012 Anm. 2.

Lucke, v. Jörn	Open Government Collaboration, 25.20.2012, http://www.zu.de/deutsch/lehrstuehle/ticc/JvL-121025-OpenGovernmentCollaboration-V1.pdf
Maisch, Michael Marc/Seidl, Alexander	Cloud Government: Rechtliche Herausforderungen beim Cloud Computing in der öffentlichen Verwaltung, VBl BW 2012, 7-12
Maisch, Michael Marc	Die Cloud-Strategie der EU-Kommission - Unter Bezugnahme auf die Datenschutz-Grundverordnung und § 203 StGB, jurisAnwZert ITR 23/2012, Anm. 3.
Merk, Beate	Pressemitteilung Nr. 248/12 v. 28.09.2012, http://www.justiz.bayern.de/ministerium/presse/archiv/2012/detail/248.php
Niemann, Fabian/Hennrich, Thorsten	Kontrollen in den Wolken? – Auftragsdatenverarbeitung in Zeiten des Cloud Computings, CR 2010, 686 ff.
Niemann, Fabian/Paul, Jörg-Alexander	Bewölkt oder wolkenlos- rechtliche Herausforderungen des Cloud Computings, K&R 2009, 444-452
Pohle, Jan/Ammann, Thorsten	Über den Wolken… - Chancen und Risiken des Cloud Computing, CR 2009, 273-278
Wilde, Christian Peter/Ehmann, Eugen/Niese, Marcus/Knoblauch, Anton	BayDSG, Loseblattsammlung, Hüthig-Jehle-Rehm, Heidelberg