



INNOVATIONSSTIFTUNG
BAYERISCHE KOMMUNE

zeppelin universität

zwischen
Wirtschaft Kultur Politik

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



Sicheres IT-Outsourcing für Kommunen

PRAXISLEITFADEN

Executive Summary

Cloud Computing ist mehr als ein Hype. Es ist die wolkige, aber assoziationsreiche Kurzformel für den durchgreifenden Trend, IT-Outsourcing an die neuen technischen Möglichkeiten in verteilten Netzen und an neue maßgeschneiderte Geschäftsmodelle anzupassen. Dass dieser Trend nun auch die öffentliche Verwaltung erreicht, ist nicht nur naheliegend, sondern auch begrüßenswert. Im Kontext einer notwendigen Verwaltungsmodernisierung und unter der Last knapper öffentlicher Kassen sind insbesondere die Kommunen gehalten, Möglichkeiten auszuloten, ihre vielfältigen öffentlichen Aufgaben effizient und zukunftsorientiert zu erfüllen.

Kommunale Cloud Lösungen können und sollen in diesem Sinne als Weiterentwicklung der bereits jetzt vielfach stattfindenden Auftragsdatenverarbeitung durch spezialisierte IT-Dienstleister und Rechenzentren genutzt werden. Das entspricht auch der Cloud Strategie der EU-Kommission vom September 2012 und nationalen Aktionsplänen, die den sensiblen öffentlichen Sektor ausdrücklich einbeziehen.

Cloud Computing bietet nämlich viele Vorteile, insbesondere die Steigerung der Qualität der Datenverarbeitung und des Sicherheitsniveaus, die Senkung des Wartungsaufwands und eine Erhöhung der Verwaltungseffizienz. Den Risiken einer Auslagerung von Daten und Werkzeugen in eine Cloud (in organisatorischer Hinsicht etwa die Anbieterabhängigkeit, in technischer Hinsicht die Verwundbarkeit der Cloud-Technologie) muss, kann aber auch begegnet werden. Dies fordert auch die (datenschutz-) rechtliche Verantwortung der Hoheitsträger, die wie bei jeder Auftragsdatenverarbeitung beim Auftraggeber verbleibt.

Solche rechtlichen Anforderungen sind aber kein K.-O.-Kriterium für die kommunale Nutzung von Cloud Services, sondern mahnen lediglich zu sorgfältiger Auswahl der Cloud Anbieter (hierzu Art. 6 Abs. 2 Satz BayDSG i.V.m. Nr. 1 VollzBekBayDSG) und umsichtiger Durchführung des Auslagerungsprozesses. Kommunen dürfen Cloud Services nutzen. Bei bestimmten sensiblen Datenbeständen (wie Steuerdaten, Sozialdaten, Meldedaten oder Personenstandsdaten) muss die Datenverarbeitung im Hoheitsbereich verbleiben (Art. 33 Abs. 4 GG). Außerdem bestehen grundlegende Bedenken gegenüber einer Übermittlung bzw. Speicherung von Verwaltungsdaten außerhalb der EU. Deshalb ist generell eine sog. Private Cloud oder Community Cloud mit einer klaren Zuordnung der Server und Prozesse und Begrenzung der Akteure vorzugswürdig.

Im Übrigen kommt es auf die Ausgestaltung des konkreten Cloud Services im Einzelfall an. Unter Beachtung von vergabe- und haushaltsrechtlichen Bindungen sowie fachkundigen Wirtschaftlichkeitsberechnungen sind entsprechende Angebote sorgfältig zu prüfen. Der notwendige schriftliche Cloud Vertrag stellt die Bedarfsdeckung und Erfüllung gesetzlicher Anforderungen sicher und klärt insbesondere Gewährleistungs- und Haftungsfragen. Dabei ist eine juristische Beratung genauso empfehlenswert wie es begleitende akzeptanzstiftende Maßnahmen bei den Bediensteten sind, auf deren Arbeitsumfeld sich die neuen IT-Strukturen auswirken.

1. Was ist überhaupt „dieses Cloud Computing“?

a) 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 Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert Cloud Computing eher allgemein:

„Cloud Computing ist 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 Spannweite 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.“

Virtualisierung bedeutet, dass die Rechenleistung von Computern über die „Grenze“ der Server-Gehäuse hinaus zusammengefasst wird. Dies ermöglicht eine verteilte Verarbeitung von Daten.

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 um einen Oberbegriff für flexible und bedarfsgerechte Bereitstellungs- und Nutzungsszenarien von sämtlichen am Markt angebotenen IT-Leistungen.

Damit hat Cloud Computing viel mit **IT-Outsourcing**, der Ausgliederung von IT-Dienstleistungen, Administration, Betrieb und Wartung von Arbeitsplatzrechnern

oder Serversystemen zu tun. 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.

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.

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.

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 regelmäßig kleiner als im Unterschied zu Public Clouds 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 Anforderungen 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.

b) Kommunales Cloud Computing: eine Empfehlung

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. 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.

Mit der am 27.09.2012 veröffentlichten **Strategie** zum Cloud Computing in Europa, COM(2012) 529, 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 bei gleichzeitiger Einsparung von Kosten zu gestalten. Die EU-Kommission strebt daher eine rasche Verbreitung des 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.

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 staatlicher 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 kann die **Qualität der Datenverarbeitung und das Sicherheitsniveau** gesteigert werden, wenn auf einen diesbezüglich spezialisierten Dienstleister zurückgegriffen wird.
- 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. **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.

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.

*Durch den Rückgriff auf spezialisierte Diensteanbieter können **kleine Kommunen** v.a. die Qualität und Sicherheit der Datenverarbeitung steigern. Die Einsparung von Kosten kommt meist erst ab einer bestimmten Anzahl an Arbeitsplatzlizenzen in Betracht (abhängig je Anbieter).*

- **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.
- Zu den **organisatorischen Risiken** zählt die faktische Abhängigkeit eines Nutzers von den Dienstleistungen eines Cloud-Anbieters (**Anbieterabhängigkeit**).
- 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.

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.

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. Rechtskonformes Cloud Computing ist aber keine Frage des „Ob“, sondern eine Frage des „Wie“.

a) Gesetzliche Vorgaben

Die Nutzung von Cloud Services kann 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 anhand einer einzelfallbezogenen Betrachtung erfolgen.

Die Frage, ob eine Kommune einen bestimmten Cloud Service nutzen darf, wird vor allem anhand von Aspekten des Datenschutzes und der Datensicherheit zu beantworten sein. Kommt es bei der Nutzung cloud-basierter Dienste - wie es regelmäßig der Fall sein wird - zur Verarbeitung personenbezogener Daten (vgl. 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. 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.

b) 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, insbesondere 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

*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.

der Daten. So wären etwa Personenstandsregisterdaten, Sozialdaten, Steuerdaten oder Waffenregisterdaten generell sehr „streng“ zu behandeln. Das gilt auch für komplette Meldedatenbestände. Umgekehrt werden die Anforderungen zum Beispiel an Geodaten, auch wenn diese einen Personenbezug haben, oder an Daten im Rahmen von Kfz-Zulassungen geringer sein. 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

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

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.

b) Eventuell: Öffentliche Ausschreibung des Cloud-Auftrags

Bei komplexen, umfangreichen IT-Outsourcing-Maßnahmen kann die Schwelle von 200.000,- EUR überschritten werden, so dass eine EU-weite Ausschreibung des Cloud Service Auftrags notwendig wird (§ 99 Abs. 1 GWB), was bei kleinen Kommunen eher selten vorkommt. 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.

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. Im Allgemeinen hängt diese 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.

Zur Wirtschaftlichkeitsbetrachtung zählen auch **künftig ersparte Aufwendungen**. Durch die Inanspruchnahme von Cloud-Diensten entfällt für Kommunen auf technischer Seite die Notwendigkeit zu Softwareeigenentwicklungen und Systeminstallationen, zur Bereitstellung und Wartung von Serverhardware und Software, zur Systembetreuung und zur Systemadministration.

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.

f) Eventuell: Beteiligung des Personalrats

Soweit ein **Personalrat** besteht, ist dieser 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.

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**.

Neben der Regelung des wesentlichen Inhalts bedarf ein Auftrag der **Schriftform**. Die Schriftform für Verpflichtungsgeschäfte ergibt sich auch aus **Art. 38 Abs. 2 GO** bzw. **Art. 35 Abs. 2 LKrO**. Der Vertrag muss also vom wirksam bestellten Vertreter einer öffentlichen Stelle eigenhändig unterzeichnet werden.

Eine juristische Beratung bei der Vertragserstellung ist empfehlenswert.

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 **Katalog des § 11 Abs. 2 BDSG**, der die wichtigsten Regelungskomplexe einer Auftragsdatenverarbeitung umfasst (schuldrechtlich und datenschutzrelevante Inhalte, Rechte und Pflichten der Parteien).

c) Gewährleistungs- und Haftungsfragen

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.

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.

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.

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

a) Beachtung gesetzlicher Anforderungen

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 S. 3 BayDSG). 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) erfolgen. Nach Auffassung des **Bayerischen Landesbeauftragten für den Datenschutz** sind **unangemeldete Vor-Ort-Kontrollen** bei den Einrichtungen des Auftragnehmers empfehlenswert und rechtlich dann geboten, wenn konkrete Anlässe, bspw. ein Fehlverhalten des Auftragnehmers, gegeben sind. Der Ablauf und die Ergebnisse der Kontrollen sind zu dokumentieren.

b) 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.

c) Insbesondere: Fortbildungsmaßnahmen

Fortbildungsmaßnahmen sind notwendig, wenn man bedenkt, wie komplex und nachhaltig Veränderungen sein mögen, die die Umstellung auf Cloud-Services notwendig machen. Sie sind ein Bestandteil des Change Management und der insoweit obligatorischen akzeptanzstiftenden Maßnahmen.

d) Die Rolle des Datenschutzbeauftragten

Öffentliche Stellen, die personenbezogene Daten mithilfe von automatisierten Verfahren verarbeiten, sind verpflichtet, einen Beauftragten für den Datenschutz zu bestellen (vgl. Art. 25 BayDSG). Im Kontext einer geplanten IT-Outsourcing-Maßnahme kann dieser den Behördenleiter oder den Leiter der IT-Abteilung **beratend** unterstützen, z.B. bei der Prüfung der Zulässigkeit der Auftragsdatenverarbeitung anhand der Vorgaben des Art. 6 BayDSG. Zu seinen Aufgaben 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.

7. Ausblick

Cloud Computing ist nützlich, politisch erwünscht und rechtskonform umsetzbar. Für Kommunen eröffnen sich neue Chancen, wenn sie eine angemessene und ihrem Bedarf entsprechende Variante des IT-Outsourcing wählen. Sich diesen Aussichten aus Sorge vor rechtlichen oder technischen Risiken ganz zu verschließen, ist nicht empfehlenswert:

Die meisten Anforderungen an die Kommunen stellen sich mit und ohne Cloud Computing. Gewährleistung von IT-Sicherheit und IT-Compliance, datenschutzkonforme Umsetzung elektronischer Geschäftsprozesse, ressourcenschonende IT-Verfahren: All dies und mehr kann über Cloud Computing sogar besser gelingen. Ein Argument wie „Das haben wir noch nie gemacht. Wo kommen wir denn da hin?“ kann sich schnell als Bumerang erweisen. Rechtliche und technische Risiken ergeben sich auch bei lokaler Datenverarbeitung.

