EuroCloud AUSTRIA

EuroCloud.Austria

Leitfaden

Cloud Services Öffentliche Auftragsvergabe

ÖSTERREICH

02

Der Druck dieses Leitfadens wurde freundlicherweise durch Sponsoren der EuroCloud.Austria finanziert:

Inhaltsverzeichnis

1	Vorwort	4
2	Einleitung	6
3	Vergaberechtliches Projektmanagement bei der Ausschreibung von Cloud Computing-Leistungen	8
4	Auswahl geeigneter Unternehmen (Präqualifikation)	13
5	Umgang mit der Leistungserbringung im Ausland und innerhalb eines Konzerns	15
6	Vergaberechtliche Anforderungen an die Leistungsbeschreibung	17
7	Prüfung und Bewertung der Angebote	19
8	Berücksichtigung der Besonderheiten von Cloud Computing im Leistungsvertrag	22
9	Vorgehensweise für Anbieter von Cloud Computing-Leistungen	23
10	Checkliste Vertragselemente	25
11	Glossar Cloud Computing	31
12	Rechtlicher Hinweis	33
13	Autoren	35

Impressum

EuroCloud.Austria
Verein zur Förderung von Cloud Computing
Neubaugasse 11/9
1070 Wien

E-Mail: info@eurocloud.at
Web: http://www.eurocloud.at
Sitz des Vereins: Wien

Copyright: EuroCloud.Austria
Verein zur Förderung von Cloud Computing



Dr. Tobias Höllwarth
Vorstandsmitglied der EuroCloud.Austria
Arbeitsgruppe Zertifizierung und Recht

1 Vorwort

Liebe Leserinnen und Leser!

Es gibt wenige IT-Themen, die so kontrovers diskutiert werden wie Cloud Computing. Dies gilt für privatwirtschaftlich geführte Unternehmen ebenso wie für Unternehmen und Organisationseinheiten der öffentlichen Hand. Auf der einen Seite locken Einsparungen durch Konsolidierung, Standardisierung und Automatisierung der IT, die eine flexible Nutzung von IT-Services über Self-Service Portale prognostiziert. Auf der anderen Seite stellen die technische Sicherheit, strengere gesetzliche Vorgaben, geänderte Zugänge zu Servicelevel Agreements, Fragen der Schnittstellen und Interoperabilität eine besondere Herausforderung dar, für den Cloud-Nutzer ebenso wie für den Cloud-Anbieter.

Mittlerweile steht außer Streit, dass Cloud-Services ein Bestandteil zukünftiger IT-Planungen praktisch jeder Organisation sind. Diese sind fortlaufend gezwungen, über die Ökonomisierung ihrer IT nachzudenken und zwischen der traditionellen Eigenerrichtung, dem klassischen IT-Outsourcing (womöglich sogar non-shared) oder dem Zukauf von IT-Services aus der Cloud zu wählen. In vielen Fällen wird es letztlich ein hybrides Modell sein.

Faktum ist jedoch, dass sich die Geschäftsführung jedes Unternehmens, egal welcher IT-Größenordnung, in den kommenden Monaten ernsthaft mit der Frage beschäftigen wird müssen, ob Teile der erforderlichen IT-Services aus der Cloud bezogen werden sollen. Und spätestens zu diesem Zeitpunkt wird deutlich, wie groß die mit dieser Frage verbundenen Risken – insbesonders hinsichtlich des Datenschutzes – sind.

Der folgende Leitfaden soll Informationen zu rechtlichen Aspekten des Cloud Computings im Zusammenhang mit öffentlichen Auftragsvergaben bieten. Die Arbeitsgruppe „Law“ der EuroCloud.Austria hat diesen Leitfaden initiiert. Ich danke den Fachleuten der Rechtsanwaltskanzlei Heid Schiefer Rechtsanwälte OG für dessen Erstellung.

EuroCloud ist eine Non-Profit-Organisation, die in 28 europäischen Ländern vertreten ist. EuroCloud bietet einen europäischen Katalog an Qualitätskriterien zur Auditierung von Cloud-Anbietern, bei der neben den rechtlichen Aspekten auch die betriebliche Bereitstellung und die Serviceerbringung selbst durch unabhängige Experten geprüft wird.

Gerade mittelständische Unternehmen, die die eigene Wettbewerbsfähigkeit durch Einbindung von externen Serviceangeboten erhalten und ausbauen wollen, verfügen oftmals nicht über die Ressourcen zur individuellen Prüfung von externen Anbietern. EuroCloud-zertifizierte Cloudserviceanbieter weisen mit diesem Gütesiegel nach, dass sie ihr Service nach höchsten Qualitätsansprüchen abwickeln.

Wien, April 2012

Dr. Tobias Höllwarth
Vorstand EuroCloud.Austria

2 Einleitung

Cloud Computing ist für öffentliche Auftraggeber ebenso eine attraktive Option wie für private Unternehmen, da die Vielfalt der möglichen Einsatzgebiete für Cloud Computing auch im öffentlichen Bereich nahezu unbegrenzt ist (vgl Höllwarth [Hrsg.], Der Weg in die Cloud [2011] 45). Wie bei anderen IT-Outsourcingprojekten stellt auch die Ausschreibung und Vergabe von Cloud Computing-Leistungen eine Herausforderung für den öffentlichen Auftraggeber dar: Zur Komplexität der auszuschreibenden Leistungen gesellt sich die Komplexität der einzuhaltenden vergaberechtlichen Normen:

- Das Vergaberecht ist vor allem durch die laufende Rechtsfortbildung durch den Europäischen Gerichtshof, die Überarbeitung der EU-Vergaberichtlinien und die regelmäßigen Novellierungen des Bundesvergabegesetzes von einer besonderen Dynamik geprägt. Diese Dynamik stellt gerade bei komplexen Ausschreibungsprojekten öffentliche Auftraggeber und Bieter vor besondere Herausforderungen.
- Wesentlich für ein erfolgreiches Ausschreibungsprojekt ist weiters die Kenntnis des Marktes. Ohne Kenntnis der Möglichkeiten und Grenzen der IT-Dienstleister geht eine Ausschreibung am Markt vorbei und bietet keine Grundlage für gute Angebote.

Öffentliche Auftraggeber sollten daher entweder selbst über Know-how in den Bereichen Cloud Computing und IT-Ausschreibungen verfügen oder sich durch entsprechende Berater verstärken.

Die vornehmlichen Ziele des Vergaberechtes sind die Sicherstellung eines freien und lauteren Wettbewerbs, die Gleichbehandlung aller Bewerber bzw. Bieter und die Vergleichbarkeit der Angebote. Die meisten vergaberechtlichen Verfahrensregeln zielen darauf ab, das Erreichen dieser Ziele zu gewährleisten, um in weiterer Folge ein optimales Preis-Leistungsverhältnis des geschlossenen Cloud-Leistungsvertrages sicherzustellen. Darüber hinaus trägt die Einhaltung dieser Verfahrensregeln noch dazu bei, dass der Beschaffungsprozess im Geiste eines partnerschaftlichen Miteinanders von Auftraggeber und Bietern stattfindet, was das Risiko vergaberechtlicher Auseinandersetzungen minimiert.

Das Vergaberecht stellt dem öffentlichen Auftraggeber somit ein gutes Instrumentarium für die marktkonforme Ausschreibung und Vergabe von Cloud Computing-Leistungen zur Verfügung. Nicht zuletzt spart – wie die Berichte der Rechnungshöfe regelmäßig zeigen – die professionelle Abwicklung der Vergabeverfahren und Einhaltung der vergaberechtlichen Normen viel Geld.

Ziel dieses Leifadens ist die kompakte Darstellung der wesentlichen vergaberechtlichen Fragen bei der Ausschreibung und Vergabe von Cloud Computing-Leistungen aus der Sicht der öffentlichen Auftraggeber und der Bieter. Dieser Leitfaden basiert auf dem Bundesvergabegesetz (in der Folge „BVergG“), BGBl I 2006/17 unter Berücksichtigung der Änderungen durch die BVergG-Novelle 2012, BGBl I 2012/10, die am 1.4.2012 in Kraft tritt.

3 Vergaberechtliches Projektmanagement bei der Ausschreibung von Cloud Computing-Leistungen

3.1 Vorbemerkungen

Der Vorbereitung des Vergabeverfahrens kommt besondere Bedeutung zu.

Die Ausschreibung und Vergabe von Cloud Computing-Leistungen ist ein komplexes Projekt und ist daher professionell aufzusetzen. Bevor noch die Erstellung von Ausschreibungsunterlagen und die Schaltung einer Bekanntmachung in Angriff genommen wird, sollten folgende Parameter ermittelt werden:

- Bedarfserhebung: Welche Geschäftsprozesse bzw. Dienste kommen für die Auslagerung in die Cloud in Frage?
- Einholung von Marktinformationen: Welche Unternehmen kommen für die Erbringung der Cloud-Leistungen in Frage?
- Abklärung der für den Beschaffungsprozess erforderlichen Ressourcen: Ist im Haus ausreichend technisches und juristisches Know-how für das Projekt vorhanden?
- Festlegung des Projektteams: Wer ist wofür verantwortlich?
- Strategiedefinition: Was ist das Ziel des Projekts?
- Erstellung eines Projektplans: Welche Meilensteine sind bis wann zu erreichen?
- Unterstützung durch Entscheidungsträger: Steht die Geschäftsführung hinter dem Projekt?

Diese Parameter sind auch für die vergaberechtlichen Rahmenbedingungen – und damit für die Rechtssicherheit des Vergabeverfahrens – von Bedeutung.

3.2 Ausschreibungspflicht von Cloud Computing-Leistungen

Die Vergabe von Cloud Services fällt in den Vollanwendungsbereich des BVergG.

Cloud Computing-Leistungen sind in den meisten Fällen als Dienstleistungen zu qualifizieren und fallen dabei unter die Kategorie 7 „Datenverarbeitung und verbundene Tätigkeiten“ des Anhangs III BVergG, womit sie prioritäre Dienstleistungen sind. Die Vergabe dieser Leistungen fällt daher in den Vollanwendungsbereich des BVergG, was bedeutet, dass öffentliche Auftraggeber bei ihrer Vergabe alle einschlägigen vergaberechtlichen Regelungen zu beachten haben. Cloud Computing-Leistungen können in bestimmten Fällen aber auch als Lieferleistungen zu qualifizieren sein, und zwar vor allem dann, wenn sie als Miete von Cloud Services ausgestaltet sind.

In Einzelfällen kann die Vergabe von Cloud Computing-Leistungen unter eine Ausnahmebestimmung des BVergG fallen, was zur Folge hat, dass die Regelungen des BVergG nicht beachtet werden müssen. Dies kann z.B. bei geheimen oder sicherheitskritischen Beschaffungsvorgängen (§ 10 Z 1 BVergG) oder Inhouse-Vergaben (§ 10 Z 7 BVergG) der Fall sein. Nach dem BVergG ausschreibungsfrei kann eine Beschaffung weiters dann sein, wenn der öffentliche Auftraggeber bei einer zentralen Beschaffungsstelle einkauft – diese kann sich auch im Ausland befinden –, sofern die zentrale Beschaffungsstelle selbst in Übereinstimmung mit den EU-Vergaberichtlinien ausschreibt (siehe § 10 Z 19 und 20 BVergG).

Denkbar ist auch, dass bestimmte Leistungen aus technischen Gründen oder wegen bestehender Ausschließlichkeitsrechte EU-weit nur von einem bestimmten Unternehmen erbracht werden können, was die Durchführung eines Verhandlungsverfahrens ohne Bekanntmachung mit diesem Unternehmen ermöglichen würde (§ 30 Abs 2 Z 2 BVergG). Bei Cloud Computing-Leistungen wird dies jedoch nur selten der Fall sein. Generell ist zu diesen Ausnahmebestimmungen anzumerken, dass sie eng zu interpretieren sind und die Beweislast für ihr Vorliegen beim Auftraggeber liegt. Das Vorliegen dieser Voraussetzungen ist daher vor Einleitung des Beschaffungsvorhabens schriftlich zu dokumentieren.

3.3 Geschätzter Auftragswert und vergaberechtliche Schwellenwerte

Der Auftragswert ist unter Berücksichtigung aller Optionen und allfälliger Vertragsverlängerungen zu ermitteln.

Als nächster Schritt ist der geschätzte Auftragswert (exklusive USt) zu ermitteln; dieser ist ausschlaggebend dafür, welche Verfahrensarten zulässig sind, welche Bekanntmachungen geschaltet und welche Mindestfristen beachtet werden müssen.

Das BVergG fordert eine sorgfältige Schätzung des Auftragswerts unter Berücksichtigung aller Optionen und in Frage kommender Leistungen (auch Kosten für Leistungsanpassungen, Change Requests, Wartung und Betrieb usw). Bei unbefristeten Verträgen ist der vierfache Jahreswert anzusetzen. Ausgangspunkt für die Schätzung können z.B. in der Vergangenheit eingeholte Angebote, die Ergebnisse von Markterkundungen oder auch die Einschätzung eines IT-Sachverständigen sein.

Das „Splitten“ von technisch, sachlich und zeitlich zusammengehörigen Aufträgen (vor allem, wenn damit das Ziel verfolgt wird, die vergaberecht-

lichen Regelungen zu umgehen) ist unzulässig. Beim Cloud Computing könnte beispielsweise der zeitnahe Abschluss von Verträgen über einzelne Services beim selben Cloud Provider als unzulässiges Splitten qualifiziert werden.

Da sich die vergaberechtlichen Schwellenwerte laufend ändern, wird in diesem Leitfaden auf die Wiedergabe der aktuellen Schwellenwerte verzichtet. Als Faustregel kann jedoch davon ausgegangen werden, dass

- bis zu einem geschätzten Auftragswert von EUR 100.000,- eine Direktvergabe durchgeführt werden kann (nach Ablauf der derzeit noch gültigen Schwellenwertverordnung reduziert sich dieser Betrag jedoch auf EUR 50.000,-),
- bis zu einem geschätzten Auftragswert von ca. EUR 200.000,- ein Verfahren mit vorheriger österreichweiter Bekanntmachung durchzuführen ist und
- ab einem geschätzten Auftragswert von ca. EUR 200.000,- ein Verfahren mit vorheriger EU-weiter Bekanntmachung durchzuführen ist.

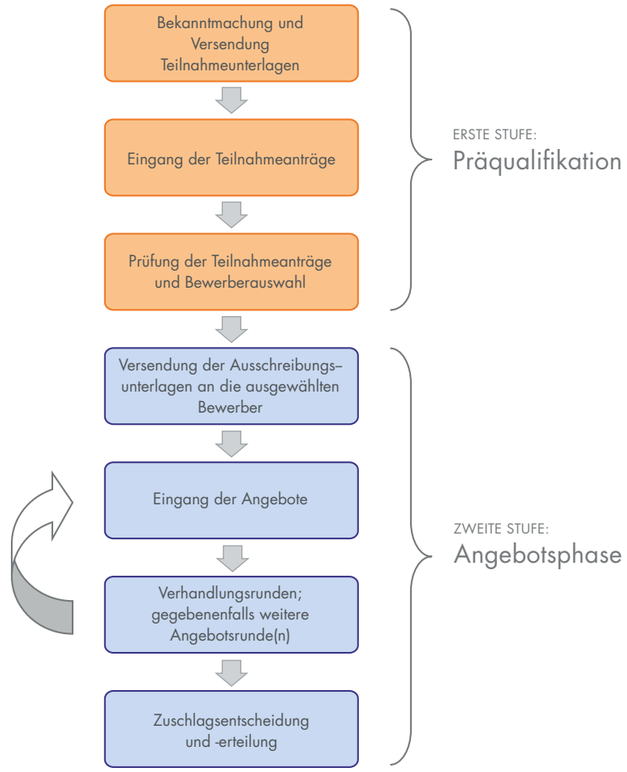
3.4 Wahl der Verfahrensart

Für die Vergabe von Cloud Services ist vor allem das Verhandlungsverfahren mit vorheriger Bekanntmachung geeignet.

Für die Vergabe komplexer Cloud Computing-Leistungen bietet sich an erster Stelle das Verhandlungsverfahren mit Bekanntmachung an. Dieses Verfahren ist insbesondere immer dann zulässig, wenn es die Komplexität der zu vergebenden Leistungen nicht erlaubt, das Leistungsbild vorab so abschließend zu definieren, dass ein offenes oder nicht offenes Vergabeverfahren durchgeführt werden kann. Das Vorliegen der Voraussetzungen für das Verhandlungsverfahren sollte vor seiner Einleitung in einem Vergabevermerk dokumentiert werden.

Das Verhandlungsverfahren mit vorheriger Bekanntmachung gliedert sich in die Präqualifikationsphase (erste Stufe) und die Angebots- bzw. Verhandlungsphase (zweite Stufe). In der Präqualifikationsphase trifft der Auftraggeber unter den Unternehmen, die sich für die Teilnahme am Vergabeverfahren bewerben, eine Vorauswahl. In der zweiten Phase werden dann die ausgewählten Unternehmen zur Angebotslegung aufgefordert und wird über den gesamten Auftrag verhandelt. Das Verhandlungsverfahren ermöglicht es, das Know-how der Bieter in die Definition der Leistungen einzubeziehen und die Leistungsbeschreibung im Zuge des Verfahrens nachzuschärfen, um ein optimales Preis-Leistungsverhältnis zu erzielen.

Ein Verhandlungsverfahren mit vorheriger Bekanntmachung läuf wie folgt ab:



Bei der Vergabe standardisierter Cloud Computing-Leistungen, an die auftraggeberseitig keine speziellen Anforderungen gestellt werden, kommt auch das offene oder nicht offene Verfahren in Frage. In beiden Verfahren sind Verhandlungen verboten; sie unterscheiden sich dadurch, dass beim offenen Verfahren jeder interessierte Unternehmer anbieten kann, wohingegen beim nicht offenen Verfahren zuvor eine Präqualifikationsphase wie im Verhandlungsverfahren durchgeführt wird.

Der Abschluss von Rahmenvereinbarungen erleichtert den flexiblen Abruf der Cloud Services.

Steht der konkrete Bedarf des Auftraggebers an Cloud Computing-Leistungen noch nicht fest, kommt der Abschluss von Rahmenvereinbarungen in Betracht. Rahmenvereinbarungen sind Vereinbarungen ohne Abnahmeverpflichtung für den Auftraggeber, die grundsätzlich auf maximal drei Jahre abgeschlossen werden dürfen. Die Partner einer Rahmenvereinbarung werden in einem der zuvor beschriebenen Verfahren ermittelt; während ihrer Laufzeit ist dann ein rascher Abruf entweder direkt aus der Rahmenvereinbarung oder nach erneutem Aufruf zum Wettbewerb möglich. Rahmenvereinbarungen sind auch deshalb für Cloud Services interessant, weil sie die Grundlage für eine flexible Inanspruchnahme diversester Cloud Services bieten können.

Als mögliche Verfahrensart zu erwähnen ist schließlich noch der wettbewerbliche Dialog. Hier werden nach einer Präqualifikationsphase die technischen und rechtlichen Auftragsbedingungen von Auftraggeber und Bietern in Einzelgesprächen gemeinsam erarbeitet. Die Bieter werden dann aufgefordert, auf Basis der so erarbeiteten Lösungsvorschläge Angebote zu legen, wobei in dieser Phase keine Verhandlungen mehr zulässig sind. Diese Verfahrensart ermöglicht somit die Definition der Cloud-Leistungen mit den Bietern, lässt jedoch ab der Angebotslegung keine Optimierung des Leistungsbildes oder der Vertragsbedingungen mehr zu.

4 Auswahl geeigneter Unternehmen (Präqualifikation)

Mit den Eignungskriterien definiert der Auftraggeber Mindestanforderungen an die Bewerber.

Vor allem im Verhandlungsverfahren ist es erforderlich, die Anzahl der Bieter, die zur Angebotslegung aufgefordert werden sollen, einzugrenzen, da der Verfahrensaufwand ansonsten enorm wäre. Dafür sieht das Vergaberecht das Präqualifikationsverfahren vor, in dem

- Mindestanforderungen definiert werden, die jedes Unternehmen erfüllen muss, das für die Teilnahme am Verfahren in Frage kommen soll (Eignungskriterien),
- und in weiterer Folge von den Unternehmen, welche die Mindestanforderungen erfüllen, die besten auf Grundlage von Auswahlkriterien ausgewählt werden.

Diese Kriterien sind in der Bekanntmachung bzw. in den Teilnahmeunterlagen transparent festzulegen.

Für Cloud Computing-Leistungen kommen insbesondere folgende Eignungskriterien in Frage:

- Nachweis einer IT-Infrastruktur, welche die vom Auftraggeber geforderten Verfügbarkeiten gewährleisten kann unter Angabe der Standorte, der technischen Ausstattung etc.;
- Nachweis von Referenzprojekten im Bereich Cloud Providing (hier ist es wesentlich, die konkreten Mindestanforderungen an die Referenzprojekte wie z.B. Leistungsinhalte, Dauer und Auftragsvolumen zu definieren);
- Nachweis von Schlüsselpersonen, die Erfahrung mit Cloud Computing-Projekten vorweisen können (auch hier sind konkrete Mindestanforderungen festzulegen);
- Nachweis von Zertifizierungen, wobei hier sowohl allgemeine Zertifizierungen im Bereich IT und Sicherheit als auch Zertifizierungen im Bereich Cloud Computing (z.B. EuroCloud SaaS-Gütesiegel) in Frage kommen.

Mittels der Auswahlkriterien wählt der Auftraggeber aus den Bewerbern, welche die Mindestanforderungen erfüllen, die besten aus.

Die Auswahl der besten Bewerber kann z.B. auf Basis weiterer, über die Mindestanforderungen hinausgehender Referenzprojekte und/oder Qualifikationen des Schlüsselpersonals erfolgen.

Wesentlich ist im Präqualifikationsverfahren, dass der Auftraggeber zwischen Eignungs- und Auswahlkriterien eine klare Trennung vornimmt und sich genau an die Vorgaben hält, die er in den Teilnahmeunterlagen definiert hat. Ein nachträgliches Abgehen von diesen Vorgaben (z.B. die Einladung eines Cloud Providers zur Angebotslegung, der eine geforderte Zertifizierung nicht aufweist) wäre rechtswidrig.

5 Umgang mit der Leistungserbringung im Ausland und innerhalb eines Konzerns

Es liegt in der Natur von Cloud Computing, dass die genauen Orte, an denen die Daten verarbeitet werden, unbestimmt sein können. Je mehr Spielraum der Auftraggeber dem Cloud Provider diesbezüglich lässt, desto günstiger kann tendenziell die Leistung angeboten werden. Öffentliche Auftraggeber haben jedoch zu berücksichtigen, dass sie im Falle der Verarbeitung personenbezogener Daten in der Cloud auch datenschutzrechtliche Auftraggeber sind und sich daraus Einschränkungen im Hinblick auf die zulässigen Orte der Datenverarbeitung ergeben können (siehe EuroCloud. Austria, Leitfaden Cloud Computing – Recht, Datenschutz & Compliance [2011]).

Vergaberechtlich sind diese Verpflichtungen in den Ausschreibungsunterlagen durch entsprechende Regelungen im Hinblick auf die Orte der Leistungserbringung sowie den Einsatz von Subunternehmern zu berücksichtigen (siehe dazu auch unten die Abschnitte „Compliance“ bzw. „Überbindung auf Subunternehmer“ der Checkliste Vertragselemente).

Eine örtliche Beschränkung der Datenverarbeitung auf Österreich ist vergaberechtlich bedenklich.

Die Gestaltung dieser Regelungen hängt eng mit der grundsätzlichen Frage zusammen, wie weit man als öffentlicher Auftraggeber bereit ist, die unmittelbare Kontrolle über die eigenen Daten und Dienste dem Cloud Provider anzuvertrauen. Vom geschlossenen Konzept einer Private Cloud, bei der alle Cloud-Services innerhalb des eigenen Rechenzentrums laufen, bis zum offenen Konzept der Public Cloud, bei der die eigenen Dienste gemeinsam mit den Diensten anderer Kunden beim Cloud Provider laufen, sind vergaberechtlich alle Lösungen möglich, sofern die Vorgaben des öffentlichen Auftraggebers einzelne Anbieter nicht unsachlich bevorzugen oder benachteiligen.

Die Vorgabe in den Ausschreibungsunterlagen, dass die Daten nur in Österreich verarbeitet werden dürfen, wird in den meisten Fällen im Hinblick auf das vergaberechtliche Verbot, Bieter aus dem EU-Ausland zu diskriminieren, vergaberechtlich problematisch sein, sofern nicht im Einzelfall sachliche Gründe eine derartige Beschränkung rechtfertigen. Hingegen wird die Vorgabe, die Verarbeitung der Daten örtlich auf die Europäische Union zu beschränken, vergaberechtlich zulässig sein.

Was die Einbindung von Subunternehmern angeht, ist vergaberechtlich zwischen dem Vergabeverfahren und der Vertragsabwicklung zu unterscheiden:

Im Vergabeverfahren kann die Einbeziehung von Subunternehmern nicht beschränkt werden.

- Im Vergabeverfahren darf der öffentliche Auftraggeber die Einbindung von Subunternehmern nicht beschränken. Er ist jedoch berechtigt, von den Bietern zu verlangen, jeden Subunternehmer namentlich zu nennen und für diese die vergaberechtlich geforderten Nachweise (vor allem Befugnis) vorzulegen.
- Für die Phase der Vertragsabwicklung kann der öffentliche Auftraggeber festlegen, dass der Auftragnehmer ohne Zustimmung des Auftraggebers keine zusätzlichen Subunternehmer einsetzen darf.

Im laufenden Vertragsverhältnis kann der Auftraggeber die Einbeziehung neuer Subunternehmer von seiner Zustimmung abhängig machen.

Besondere Herausforderungen kann die Leistungserbringung im Konzern mit sich bringen, und zwar wenn der Auftragnehmer im Ausland ansässige Schwester- oder Tochterunternehmen in die Leistungserbringung miteinbezieht. Durch die Bündelung gleichartiger Leistungen an bestimmten Standorten innerhalb des Konzerns können sich erhebliche Skaleneffekte und damit Kostenreduktionen ergeben. Vergaberechtlich ist bei der Gestaltung der Ausschreibungsunterlagen darauf zu achten, dies auch zu ermöglichen, um die damit einhergehenden Kostenvorteile lukrieren zu können. Es empfiehlt sich daher, festzulegen, unter welchen Voraussetzungen diese Konzernunternehmen als Subunternehmer zu qualifizieren und von den Bietern im Vergabeverfahren – bzw. im Projekt vom Auftragnehmer – namhaft zu machen sind. Die enge arbeitsteilige Zusammenarbeit im Konzern kann die vergaberechtliche Qualifizierung der Rolle der Konzernunternehmen im Rahmen des Projekts zu einer komplexen Aufgabe machen.

Der Auftraggebers sollte Regelungen über den Umgang mit der Leistungserbringung im Konzern vorsehen.

6 Vergaberechtliche Anforderungen an die Leistungsbeschreibung

Die Leistungsbeschreibung muss eindeutig, vollständig und neutral sein sowie die Vergleichbarkeit der Angebote ermöglichen.

Grundlage jedes erfolgreichen Vergabeprojekts ist eine gute Leistungsbeschreibung, die

- alle wesentlichen Anforderungen des Auftraggebers definiert (Vollständigkeit),
- keine Widersprüche und möglichst wenig Unklarheiten enthält (Eindeutigkeit), damit die Bieter ihre Angebotspreise ohne Übernahme unkalkulierbarer Risken kalkulieren können,
- einzelnen Bietern keine Wettbewerbsvorteile bringt (Neutralität) und
- die Vergleichbarkeit der Angebote sicherstellt.

Die Leistung kann vom Auftraggeber entweder konstruktiv über die Definition der Teilleistungen oder funktional über die Festlegung von Leistungs- und Funktionsanforderungen beschrieben werden. Bei der Beschreibung von Cloud Services wird idR nur die funktionale Leistungsbeschreibung in Frage kommen, bei der die zur Verfügung zu stellenden Services und die an sie gestellten Anforderungen (z.B. Verfügbarkeiten, Antwortzeiten) festgelegt werden.

Zunächst ist in der Leistungsbeschreibung klar zu definieren, auf welcher Serviceebene Cloud Computing in Anspruch genommen werden soll (Infrastructure as a Service, Platform as a Service, Software as a Service: Näheres zu diesen Serviceebenen findet sich unten im Glossar Cloud Computing). Weiters zeichnen sich Cloud Services durch charakteristische Eigenschaften aus, die bei der Erstellung der Leistungsbeschreibung zu berücksichtigen sind (siehe Höllwarth [Hrsg], Der Weg in die Cloud [2011] 36). Dazu gehören insbesondere die

- Virtualität der Ressourcen (für den Nutzer ist nicht erkennbar, wie die Dienste realisiert werden),
- Mandantenfähigkeit (die gemeinsam genutzte Umgebung wirft Anforderungen im Hinblick auf den Schutz und die Isolierung der einzelnen Mandanten auf),
- verbrauchsabhängige Bezahlung (die Abrechnung der erbrachten Leistungen muss für den Auftraggeber nachvollziehbar sein) und

» nutzergesteuerte Bereitstellung und Elastizität der Dienste (bis zu welchem Ausmaß müssen die Ressourcen skaliert werden).

Als Grundsatz für die Leistungsbeschreibung kann festgehalten werden, dass die Angebote tendenziell umso günstiger werden, je mehr sich die Leistungsbeschreibung an Standards – seien es Normen, seien es de facto im Markt etablierte standardisierte Leistungspakete – orientiert.

Soweit für die ausgeschriebenen Leistungen Normen oder standardisierte Leistungsbeschreibungen existieren, sind öffentliche Auftraggeber verpflichtet, diese heranzuziehen, wobei Europäische Normen Vorrang haben. Ein Abweichen von diesen Normen ist zwar in einzelnen Punkten möglich, muss jedoch sachlich begründet sein.

7 Prüfung und Bewertung der Angebote

Die Bewertung der Angebote steht unter den Anforderungen der Transparenz und Nachvollziehbarkeit.

Bei der Ausschreibung von Cloud Services hat der öffentliche Auftraggeber die Wahl, den Auftrag an den Bieter mit dem niedrigsten Preis (Billigstbieterprinzip) oder an den Bieter, der das wirtschaftlich und technisch günstigste Angebot gelegt hat (Bestbieterprinzip), zu vergeben. In beiden Fällen muss der öffentliche Auftraggeber die Zuschlagskriterien zuvor in der Bekanntmachung bzw. in den Ausschreibungsunterlagen definieren; diese Kriterien müssen transparent und die auf ihrer Grundlage vorgenommenen Bewertungen nachvollziehbar sein.

In beiden Fällen stellt sich die zentrale Frage, wie die Kosten ermittelt werden, die zur Angebotsbewertung herangezogen werden. Wenn der öffentliche Auftraggeber den Umfang der benötigten Cloud Services genau kennt, kann es sinnvoll sein, von den Bietern das auftraggeberseitig definierte Leistungspaket zu Pauschalpreisen anbieten zu lassen. Die Stärke von Cloud Computing liegt aber gerade in ihrer Flexibilität, der Möglichkeit, die genutzten Ressourcen nach Bedarf zu skalieren und auf Kundenseite zusätzliche Services selbständig zu nutzen. Damit diese Flexibilität auch auf der Kostenseite Vorteile bringt, bietet es sich an, von den Bietern ein Portfolio von Leistungen auspreisen zu lassen, die vom Auftraggeber voraussichtlich benötigt werden. Diesbezüglich kann es ein gangbarer Weg sein, sich an die von Cloud Providern angebotenen Abrechnungsmodelle anzulehnen, um die Marktkonformität der Vorgaben sicherzustellen.

Grundlage der Bewertung sollten realistische Mengengerüste bilden.

Bei den Konzepten „Infrastructure as a Service“ und „Platform as a Service“ sind zumeist genutzter Speicherplatz und bereitgestellte CPU-Leistung Parameter für die Abrechnung; bei „Software as a Service“ wird meist nach der Anzahl der Nutzer, der Transaktionen oder auf Grundlage von Datendurchsatz und Datenbeständen verrechnet (siehe dazu auch Höllwarth [Hrsg], Der Weg in die Cloud [2011] 205).

Dabei ist jedoch besonders darauf zu achten, dass die Neutralität der Ausschreibungsvorgaben gewahrt bleibt: Legt ein öffentlicher Auftraggeber der Ausschreibung das Abrechnungsmodell eines bestimmten Bieters zugrunde, so kann dies zu einer vergaberechtlich unzulässigen Bevorzugung führen.

Eine wesentliche Voraussetzung für eine realistische Ermittlung der zu erwartenden Kosten ist – insbesondere dann, wenn die Bieter ein Leistungsportfolio anbieten sollen, aus dem flexibel abgerufen wird – die Ermittlung eines Mengengerüsts. Auf Basis der zu erwartenden Nutzerzahlen und der

Bei der Bestbieterermittlung ist die Berücksichtigung der gesamten Lebenszykluskosten zweckmäßig.

von den Cloud Services abzubildenden bzw. zu unterstützenden Geschäftsprozesse erstellte Mengengerüste können eine gute Grundlage für die Ermittlung der zu erwartenden Kosten bieten.

Bei Vergaben nach dem Bestbieterprinzip sind zusätzlich zum Preis noch weitere, qualitative Zuschlagskriterien zu definieren. Beispielsweise können Soll-Kriterien definiert werden, deren Erfüllung leicht feststellbar ist (z.B. Überschreitung der geforderten Mindestverfügbarkeit, Unterschreitung der definierten maximalen Fehlerbehebungszeit bei Störungen) und zu einer besseren Bewertung des Angebotes führt. Wesentlich dabei ist die richtige Gewichtung dieser Kriterien gegenüber dem Preis: Es ist abzuschätzen, wieviel die Erfüllung eines solchen Kriteriums dem Auftraggeber tatsächlich wert ist. Sind die qualitativen Zuschlagskriterien zu hoch gewichtet, so kann dies die Angebotsbewertung verzerren, z.B. wenn sich nachträglich herausstellt, dass aufgrund eines überbewerteten Qualitätskriteriums ein preislich weitaus günstigeres und insgesamt attraktiveres Angebot nicht zum Zuge kommt.

Neben den Kosten, die sich durch die an den Auftragnehmer zu zahlenden Entgelte ergeben, sollten bei der Bestbieterermittlung aber auch die weiteren mit den Cloud Services und dem Vertragsverhältnis insgesamt zusammenhängenden Kosten berücksichtigt werden. Hier spricht man von der Ermittlung der Lebenszykluskosten bzw. der „Total Cost of Ownership“ (TCO). Je umfassender man die gesamten Lebenszykluskosten bei der Bestbieterermittlung berücksichtigt, desto höher ist die Wahrscheinlichkeit, dass der Zuschlagsempfänger auch über die gesamte Vertragslaufzeit gesehen der günstigste Partner ist. Bei Cloud Services können dabei insbesondere folgende Aspekte wesentlich sein:

- Im Zusammenhang mit dem Initialprojekt – also bis zur Aufnahme des Echtbetriebs – können durch die erforderlichen Mitwirkungsleistungen beim Auftraggeber erhebliche Kosten auflaufen. Generell stellt die Migration von Alt- in Neusysteme einen erheblichen (und oft unterschätzten) Kostenfaktor dar. Ein Bieter, der diesen Aufwand beim Auftraggeber durch gute Projektorganisation minimiert, kann die Lebenszykluskosten erheblich senken.
- Kommunikationsprobleme stellen erhebliche „Kostentreiber“ in IT-Projekten vor der Abnahme wie auch im Echtbetrieb dar. Ein Bieter, der effektive Vorkehrungen trifft, Reibungs- und Informationsverluste zu minimieren, senkt ebenso die Lebenszykluskosten.
- Ein wesentlicher Kostenfaktor im Betrieb kann weiters das mögliche Erfordernis von Backups außerhalb der Cloud-Infrastruktur des Providers sein. Hier stellt sich die Frage, welche Schnittstellen die Cloud Services dem Auftraggeber bieten, neben der von Cloud Providern innerhalb der Cloud üblicherweise implementierten redundanten Datenhaltung effektiv selbst regelmäßige Backups der Datenbestände anzufertigen.
- Im Sinne eines ganzheitlichen TCO-Ansatzes sollten auch die externen Kosten – also die Kosten, die weder beim Auftraggeber noch beim Auftragnehmer unmittelbar anfallen, aber von der Allgemeinheit zu tragen sind – berücksichtigt werden. Das BVergG ermöglicht es beispielsweise ausdrücklich, ökologische Aspekte im Rahmen von Zuschlagskriterien zu bewerten. Es ist daher zulässig, im Rahmen der Zuschlagskriterien Parameter wie die Energieeffizienz der Rechenzentren der Bieter bzw. mögliche Zertifizierungen in diesem Bereich zu bewerten.
- Am Ende des Lebenszyklus der Cloud Services steht die wesentliche Frage, in welchem Umfang der Cloud Provider bei der Migration der Daten des Auftraggebers aus seinem System heraus mitzuwirken hat. Einerseits gilt es zu vermeiden, dass der Auftraggeber in ein Abhängigkeitsverhältnis zum Cloud Provider gerät („Customer Lock-in“), weil er keine effektive Möglichkeit mehr hat, wieder Herr über die eigenen Daten zu werden, andererseits sind auch die am Ende des Vertragsverhältnisses auflaufenden Kosten der Migration zu berücksichtigen.

Lassen sich bestimmte, für die Lebenszykluskosten maßgebliche Aspekte nur ungenügend in Zahlen abbilden, können sie auch im Rahmen der qualitativen Zuschlagskriterien bewertet werden.

8 Berücksichtigung der Besonderheiten von Cloud Computing im Leistungsvertrag

Bei komplexen IT-Projekten bieten sich partnerschaftlich orientierte Vertragsmodelle an.

Beim Leistungsvertrag stellt sich die Situation ähnlich dar wie in der Leistungsbeschreibung: Einerseits liegt es im Interesse des Auftraggebers, dass die Bieter in ihren Angeboten die eigenen Vorgaben und Wünsche vollständig zu erfüllen haben, andererseits sind Cloud Services gerade wegen der möglichen Kostenvorteile interessant. Diese Kostenvorteile sind jedoch zu einem wesentlichen Teil darauf zurückzuführen, dass die Cloud Provider ihren Kunden standardisierte Services zur Verfügung stellen, die auf Basis standardisierter Geschäftsbedingungen kalkuliert wurden. Vom Auftraggeber formulierte Leistungsverträge führen daher tendenziell dazu, dass die Bieter in ihren Angeboten Risikoaufschläge kalkulieren und die Services teurer werden. Da aber die Akzeptanz der Allgemeinen Geschäftsbedingungen (AGB) der Bieter im Vergabeverfahren nicht in Frage kommt (diese Vorgehensweise würde aufgrund der unterschiedlichen AGB zur Unvergleichbarkeit der Angebote führen), gilt es, den Leistungsvertrag maßvoll zu formulieren, damit die Interessen des Auftraggebers gewahrt und die Vergleichbarkeit der Angebote sichergestellt, gleichzeitig aber die Risikoaufschläge der Bieter in Grenzen gehalten werden.

Der Leistungsvertrag ist ein Kompromiss zwischen der Standardisierung der Cloud Services und den Interessen des Auftraggebers.

Der Leistungsvertrag sollte alle in der Checkliste der Vertragselemente (siehe dazu unten) angeführten Themen behandeln. Da Flexibilität gerade bei Cloud Services ein wichtiger Aspekt ist, sollte der Leistungsvertrag so ausgestaltet sein, dass es möglich ist, Dienste und Entgelte anzupassen, ohne dass dadurch eine vergaberechtliche Verpflichtung zur Neuausschreibung entsteht.

Bei komplexen IT-Projekten sollten innovative Vertragsmodelle, welche den Fokus auf die partnerschaftliche Zusammenarbeit von Auftraggeber und Auftragnehmer legen, in Betracht gezogen werden. Da bei derartigen Projekten die in üblichen Verträgen vorgenommene Abgrenzung der Verantwortlichkeiten nur eingeschränkt möglich ist, bietet es sich an, die Abrechnung nach dem open-book-Prinzip vorzunehmen und gemeinsame Kostenziele zu definieren, an welche die Bonus-Malus-Regelungen geknüpft werden, und eine gemeinsame Risikoübernahme vorzusehen (risk sharing).

9 Vorgehensweise für Anbieter von Cloud Computing-Leistungen

Bieter sollten Ausschreibungsunterlagen rasch prüfen und Fragen und Bedenken unverzüglich dem Auftraggeber kommunizieren.

Auf Bieterseite lauten die beiden wichtigsten Gebote im Vergabeverfahren „rasch agieren“ und „Kommunikation mit dem Auftraggeber“:

Agieren kann man als Bieter bereits im Vorfeld eines Vergabeverfahrens: Der Bekanntmachung eines Vergabeverfahrens gehen oft Markterkundungen oder sonstige Absichtsbekundungen des öffentlichen Auftraggebers voraus, welche die Ausschreibung ankündigen. Ein Bieter, der diese Vorzeichen wahrnimmt, kann einerseits den Auftraggeber durch die Zurverfügungstellung von Fachinformationen unterstützen (zu beachten ist dabei jedoch das vergaberechtliche Verbot der Einflussnahme auf den Inhalt der Ausschreibung – „Vorarbeitenproblematik“) und sich auf die Ausschreibung vorbereiten.

Ist die Bekanntmachung veröffentlicht, so sollte der Bieter diese einer raschen Überprüfung unterziehen und im Falle von Unklarheiten oder Rechtswidrigkeiten den Auftraggeber ohne Verzug informieren. Öffentliche Auftraggeber sehen meist formalisierte Verfahren vor, in welcher Form die Bieter Fragen stellen und Bedenken kommunizieren können (vor allem schriftliche Anfragenbeantwortungen und Hearings). Als Bieter hat man jedoch idR nur die Chance, vom Auftraggeber gehört zu werden, wenn man rechtzeitig Fragen stellt und Bedenken äußert. Wartet ein Bieter bis kurz vor dem Ende der Frist für den Eingang der Teilnahmeanträge oder Angebote zu, wird der Auftraggeber in den seltensten Fällen auf seine Bedenken eingehen, und zwar aus folgenden Gründen:

Werden Rechtswidrigkeiten nicht binnen der jeweiligen Präklusionsfrist angefochten, können sie später nicht mehr bekämpft werden.

- Eine Beantwortung von Fragen oder eine Änderung der Ausschreibungsunterlagen kurz vor Fristende macht oft eine Erstreckung der Teilnahme- oder Angebotsfrist notwendig und würde damit den Terminplan umstoßen.
- Das Vergaberecht enthält ein rigides System von Präklusionsfristen. Rechtswidrigkeiten, die nicht binnen einer (zumeist recht kurzen) Frist bei der zuständigen Vergabekontrollbehörde mittels Nachprüfungsantrag angefochten werden, werden „bestandsfest“ und können in weiterer Folge von den Bietern nicht mehr bekämpft werden. Ist die Anfechtungsfrist zum Zeitpunkt der Anfrage des Bieters bereits verstrichen, so muss der Auftraggeber keinen Nachprüfungsantrag mehr befürchten und hat schon aus diesem Grund weniger Veranlassung, dem Bieter entgegenzukommen.

Kommuniziert der Bieter hingegen seine Fragen, Wünsche und Bedenken frühzeitig dem Auftraggeber, hat dieser Zeit, darauf zu reagieren und ist in vielen Fällen auch dankbar, wenn Widersprüche und Unklarheiten aufgrund der Anfrage eines Bieters frühzeitig aufgeklärt und bereinigt werden können. Wie ein IT-Projekt ist auch ein Vergabeverfahren ein Vorhaben, das zu seinem Erfolg ein partnerschaftliches Miteinander von beiden Seiten voraussetzt.

10 Checkliste Vertragselemente

In Anlehnung an das EuroCloud SaaS-Gütesiegel werden die wichtigsten Fragen hinsichtlich der vertraglichen Ausgestaltung angeführt. Anbieter, die durch EuroCloud nach diesen Anforderungen geprüft wurden, erfüllen die Basisanforderungen für die Bereitstellung von Cloud-Diensten.

Es gibt heute schon eine Vielzahl von professionellen und sicheren Lösungen. Das Gütesiegel soll auch Anbietern eine wichtige Hilfestellung dabei liefern, das Vertrauen der Anwender zu angemessenen Konditionen zu gewinnen.

Es muss eine klare Abgrenzung zu den Anbietern geben, die ihr Angebot auf „Minimalspur“ fahren, denn der Anwender kann nur mit erheblichem Aufwand und schlimmstenfalls erst im Eskalationsfall die wirklichen Defizite erkennen.

Konkret werden im Gütesiegel folgende Kategorien erfasst:

- Anbieterprofil
- Vertrag und Compliance
- Sicherheit
- Betrieb der Infrastruktur
- Betriebsprozesse
- Anwendung
- Implementierung

Durch ein Punktesystem und die Vorgabe von Mindestkriterien kann ein Anbieter Gütestufen von ein bis fünf Sternen erreichen.

Im Unterschied zu anderen Initiativen, bei denen entweder nur Teilbereiche berücksichtigt werden oder die Angaben ohne Gegenkontrolle als freiwillige Selbstverpflichtung zu sehen sind, wird beim SaaS-Gütesiegel eine Validierung der Angaben durchgeführt und in vereinbarten Zeiträumen wiederholt, damit ein konkreter Nachweis der Angaben vorliegt. Zudem verpflichtet sich der Anbieter, signifikante Änderungen der Rahmenbedingungen (z.B. Ort der Leistungserbringung, Änderung der Subunternehmervereinbarungen) und kritische Vorfälle unverzüglich zu melden.



Das SaaS-Gütesiegel wird seit 2011 offiziell vergeben. Folgende Punkte sollten bei der Vertragsgestaltung entsprechend umgesetzt werden und werden im Rahmen der EuroCloud SaaS-Gütesiegel-Zertifizierung geprüft:

10.1 Vertragsabschluss und Vertragsgestaltung

» Wie wird der Vertrag geschlossen?
- online
- schriftlich
- Kann der Kunde auf einen schriftlichen Vertrag bestehen?

10.2 Überbindung auf Subunternehmer

» Hat der Auftragnehmer seine Subunternehmer an dieselben Verpflichtungen gebunden, die er gegenüber dem Auftraggeber eingeht?

Bedarf der Einsatz/Wechsel von Subunternehmern der Zustimmung des Auftraggebers?

10.3 Leistungsverrechnung

» Wird die Nutzung des Services pauschal zeitabhängig berechnet?

» Wird die Nutzung des Services nach Verbrauch berechnet?
- Existieren Mengenrabatte/unterschiedliche Tarife in Abhängigkeit von der abgenommenen Servicemenge?
- Kann der Auftragnehmer seinen Tarif bei signifikanter Änderung des Nutzungsumfangs ändern?
- Gibt es eine Best-Price-Option?

» Wird optional eine Flatrate oder per user-Flatrate angeboten?

» Gibt es extra zu verrechnende Sonderleistungen?

» Wenn ja, welche?

10.4 Leistungsstörungen

» Leistungsstörung beim Auftragnehmer oder dessen Unterauftragnehmern
- Bestehen Regelungen zum Schadenersatz bei Leistungsstörungen?

» Streit über Leistungserbringung/Zahlungsverzug
- Ist ein Zurückbehaltungsrecht an Daten des Auftraggebers oder ihm gegenüber zu erbringenden Leistungen vertraglich ausgeschlossen?
- Ist auch im Fall von Streitigkeiten zur Leistungserbringung oder bei Zahlungsverzug ausgeschlossen, dass der Auftragnehmer die Daten ohne Zustimmung des Auftraggebers löscht?

10.5 Vertragskündigung

» Welche Kündigungsfristen sind für den Auftraggeber und den Auftragnehmer definiert?

» Gibt es eine demonstrative Liste der möglichen (außerordentlichen) Kündigungsgründe?

» Wenn ja, für wen?
- Auftraggeber
- Auftragnehmer

» Ist eine Vorankündigung von Änderungen bei der Diensterbringung von Subunternehmern vertraglich geregelt?

» Existieren Regelungen zur Mitwirkung des Auftragnehmers bei der Datenbereitstellung nach einer Vertragskündigung?

10.6 Insolvenz des Auftragnehmers

» Existieren Regelungen zum Schutz der Daten des Auftraggebers und der Verfügbarkeit der Anwendung bei Insolvenz des Auftragnehmers?

» Existiert ein Source Code Deposit?

» Ist die Software an eine bestimmte Plattform gebunden?

» Wird dem Auftraggeber ein Recht auf Herausgabe der letzten Datensicherung und Dokumentation eingeräumt?

10.7 Compliance

» Datenarchivierung
- Es gibt eine Reihe von Sondernormen zu unternehmens- und steuerrechtlichen Aufbewahrungspflichten und Aufbewahrungsfristen bei der Verwendung von Datenträgern, so etwa die §§ 189, 190, 212 und

216 UGB sowie die §§ 131 und 132 BAO. Sowohl nach § 212 Abs. 1 UGB als auch nach § 132 Abs. 1 BAO beträgt die Aufbewahrungsfrist grundsätzlich 7 Jahre. Im Fall von SaaS muss somit bei elektronischer Verarbeitung und Archivierung beim SaaS-Anbieter sichergestellt sein, dass die betroffenen Daten (etwa elektronische Rechnungen, Bücher, Aufzeichnungen und sonstige Unterlagen) während der gesetzlichen Aufbewahrungsfristen sicher aufbewahrt werden und deren vollständige, geordnete und inhaltsgetreue Wiedergabe, auch an die Behörden, möglich ist. Weiters muss ein Prozess einer kontinuierlichen Rückübermittlung solcher Daten an den Auftraggeber gewährleistet sein.

» Datenschutzrelevanz
- Werden innerhalb der Anwendung personenbezogene Daten im Sinne des DSG verwendet?

Zu beachten ist, dass der Begriff der „personenbezogenen Daten" im Sinne des DSG sehr weit gefasst ist. Alle Daten, die einen Personenbezug haben oder bei denen der Auftraggeber, der Auftragnehmer oder ein Dritter einen Personenbezug herstellen könnte, gelten aus Sicht der Datenschutzbehörden als „personenbezogene Daten", und zwar sowohl bezüglich natürlicher als auch bezüglich juristischer Personen. In der Praxis wird es nur sehr wenige IT- und Cloud-Anwendungen geben, bei denen Daten verarbeitet werden, die nicht zumindest teilweise personenbezogen sind.

» Datenschutz-Organisation
- Ist die Datenverwendung – soweit erforderlich – beim Datenverarbeitungsregister (DVR) registriert?
- Sind die Mitarbeiter des Auftragnehmers nachweislich zur Einhaltung des Datengeheimnisses nach § 15 DSG verpflichtet?
- Ist geregelt, welche Seite gegenüber den Kunden des Auftraggebers den Ansprechpartner für den Datenschutz darstellt?
- Sind Regeln für die Berichtigung, Löschung und Sperrung von Daten auf Antrag eines Betroffenen definiert?

» Auswahl Auftragnehmer und Subunternehmer
- Bietet der Auftragnehmer genügend Informationen zu seinem Unternehmen und seinen Unterauftragnehmern, um dem Auftraggeber eine fundierte Auswahl des Auftragnehmers gemäß § 10 DSG zu ermöglichen?
- Werden die Unterauftragnehmer bekanntgegeben?

» Datenschutzniveau
- Ist – soweit einschlägig – auch außerhalb der EU (auch bei beteiligten Unterauftragnehmern) ein angemessenes Datenschutzniveau (z.B. über EU-Standardvertrag, Safe-Harbour-Regelung) hergestellt?
- Besteht die Möglichkeit, wenn aufgrund von gesetzlichen oder behördlichen Auflagen an den Auftraggeber erforderlich, die Orte der Datenhaltung auf Österreich oder die EU einzugrenzen?

» Beauftragung und Weisungsrecht
- Sind die Verantwortlichkeiten zwischen Auftraggeber (grundsätzliche datenschutzrechtliche Verantwortlichkeit) und Auftragnehmer (Umsetzung von Weisungen, technischen Schutzmaßnahmen etc.) sauber definiert?
- Ist der Umfang des Auftrags zur Datenverarbeitung hinreichend klar spezifiziert, insbesondere:
- Ist der Dienst grob beschrieben? Sind in der Beschreibung der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen dokumentiert?
- Sind die Dauer der Verarbeitung und die Löschung der Daten exakt definiert?
- Ist ein Entscheidungsspielraum des Dienstleisters zur Verarbeitung der Daten ausgeschlossen?
- Ist dokumentiert, ob und, wenn ja, wie sensible Daten im Sinne des § 4 Z 2 DSG erhoben, verarbeitet oder genutzt werden?
- Ist das Weisungsrecht des Auftraggebers eindeutig definiert?

» Kommunikation
- Ist eine Kommunikationsregel etabliert für den Fall, dass Weisungen des Auftraggebers nach Meinung des Auftragnehmers gegen den Datenschutz verstoßen?
- Sind Sachverhalte definiert, die als mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen dem Auftraggeber angezeigt werden müssen?

» Umsetzung technischer und organisatorischer Datenschutzmaßnahmen
- Existiert eine Dokumentation/ein Konzept, welche technischen und organisatorischen Maßnahmen umgesetzt werden, um die Vorgaben des Anhangs zu § 14 DSG zu erfüllen?
- Hat der Auftraggeber diesem Konzept (und Änderungen daran) zuzustimmen?

» Kontrollmöglichkeiten des Auftraggebers
- Existieren Regelungen zu Kontrollrechten des Auftraggebers und zu den entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers, insbesondere:
- Ist ein Kontrollrecht des Auftraggebers und/oder eines vom Auftraggeber beauftragten Dritten vor Ort beim Auftragnehmer oder seinen Subauftragnehmern ausdrücklich vereinbart?
- Existieren (kumulativ oder alternativ zu Kontrollen durch den Auftraggeber) regelmäßige Kontrollen/Audits und Zertifizierungen, die den Datenschutz beim Auftragnehmer und die Verpflichtungen gegenüber dem Auftraggeber kontrollieren und zertifizieren?
- Ist eine Regelung zur Mitwirkung des Auftragnehmers und zu den dadurch entstehenden Kosten getroffen?

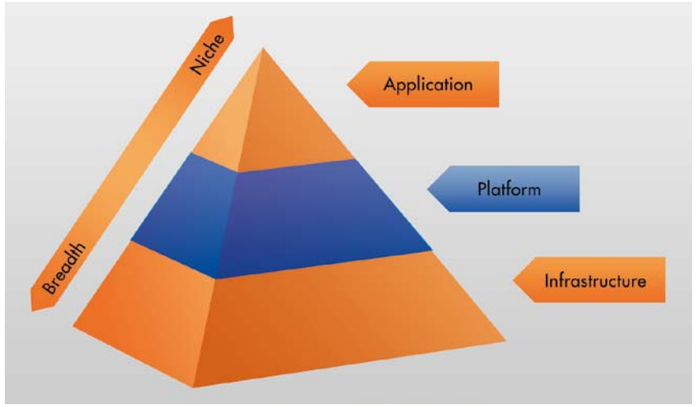
» Datenlöschung bei Vertragsende
- Existieren Regelungen zur Löschung der Daten und zur Rückgabe von Datenträgern nach Beendigung des Vertrags?
- Wird gewährleistet, dass die Daten auf Wunsch des Auftraggebers tatsächlich gelöscht werden?

11 Glossar Cloud Computing

Cloud Computing

„Cloud Computing ist ein Modell, das on-demand und online den Zugriff auf einen gemeinsamen Pool konfigurierbarer Computing-Ressourcen wie Netzwerke, Server, Speichersysteme, Anwendungen und Dienste ermöglicht. Diese können passgenau, schnell, kostengünstig und mit minimalem Verwaltungsaufwand bereitgestellt und abgerufen werden.“ *(Definition: NIST; National Institute of Standards and Technology, USA)*

Als Grundansatz für die Darstellung der verschiedenen Elemente des Cloud Computings wird oftmals das SPI-Modell herangezogen, welches die drei Serviceebenen – Infrastruktur, Plattform und Software – darstellt.



Hierbei werden die Ebenen aufeinander aufbauend dargestellt, wobei die jeweils unteren Ebenen auch unabhängig von der darüber liegenden Ebene genutzt werden können.

Public Cloud

IT-Dienstleistungen werden von einem Cloud-Anbieter bereitgestellt und können von jedem über das Internet genutzt werden.

Private Cloud

IT-Dienstleistungen werden aus den eigenen Rechenzentren bezogen. Alle Dienste und die Infrastruktur unterstehen einer Institution. Die Cloud kann durchaus von Dritten betrieben werden. Auf die Dienste wird entweder über das Intranet oder über VPN (Virtual Private Network) zugegriffen.

Hybride Cloud

ist eine Mischform bestehend aus einer Public Cloud und einer Private Cloud.

Föderierte Cloud

Hybride Cloud mit spezieller Sicherheitstechnik durch vertrauenswürdige Serviceanbieter im Bereich der Identifikation und Verschlüsselung.

IaaS: Infrastructure as a Service

Bereitstellung von Rechen- und Speicherkapazitäten als Service.

PaaS: Platform as a Service

Bereitstellung von „Middleware“ als Service.

SaaS: Software as a Service

Bereitstellung von Applikationen als Service.

XaaS: X as a Service

Bereitstellung von zusätzlichen Funktionen wie Geschäftsprozesse, Netzwerke, Kommunikation und weitere als Service.

12 Rechtlicher Hinweis

12.1 Allgemeines

Die in diesem Leitfaden zur Verfügung gestellten Informationen dienen der allgemeinen Darstellung spezieller rechtlicher Aspekte im Zusammenhang mit Cloud Computing, stellen keine Rechtsberatung dar und können auch keine Rechtsberatung ersetzen, da eine solche immer die Kenntnis aller Einzelumstände, insbesondere des konkreten Einzelfalls voraussetzt.

12.2 Inhalt des Leitfadens

Der Herausgeber/die Autoren übernehmen keine Gewähr für die Vollständigkeit, Richtigkeit oder Aktualität der bereitgestellten Informationen. Dies gilt insbesondere im Hinblick auf neueste Entwicklungen in der Rechtsprechung oder der Gesetzeslage. Haftungsansprüche gegen den Herausgeber/die Autoren, die sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen beziehungsweise durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen.

12.3 Verweise und Links

Bei direkten oder indirekten Verweisen auf fremde Inhalte (z.B. „Links”), die außerhalb des Verantwortungsbereichs des Herausgebers/der Autoren liegen, würde eine Haftungsverpflichtung ausschließlich in dem Fall in Kraft treten, in dem der Herausgeber/die Autoren von den Inhalten Kenntnis hatten und es ihnen technisch möglich und zumutbar wäre, die Nutzung im Falle rechtswidriger Inhalte zu verhindern. Der Herausgeber/die Autoren erklären hiermit ausdrücklich, dass zum Zeitpunkt der Linksetzung keine illegalen Inhalte auf den zu verlinkenden Seiten erkennbar waren. Auf die aktuelle und zukünftige Gestaltung, die Inhalte oder die Urheberschaft der verlinkten Seiten haben der Herausgeber/die Autoren keinen Einfluss. Sie distanzieren sich ausdrücklich von allen Inhalten aller verlinkten Seiten, die nach der Linksetzung verändert wurden. Für illegale, fehlerhafte oder unvollständige Inhalte und insbesondere für Schäden, die aus der Nutzung oder Nichtnutzung solcherart dargebotenen Informationen entstehen, haftet allein der Anbieter der Seite, auf welche verwiesen wurde, nicht derjenige, der über Links auf die jeweilige Veröffentlichung lediglich verweist.

12.4 Urheberrecht

Die in diesem Leitfaden dargestellten Inhalte wie Texte, Graphiken oder Bilder sind nach dem österreichischen Urhebergesetz urheberrechtlich geschützt. Jede urheberrechtlich nicht gestattete Verwertung bedarf der vorherigen schriftlichen Zustimmung des Herausgebers. Beiträge Dritter sind als solche gekennzeichnet. Dies gilt insbesondere für Vervielfältigung, Bearbeitung, Verarbeitung bzw. Wiedergabe von Inhalten in Datenbanken oder anderen elektronischen Medien. Die unerlaubte Vervielfältigung oder Weitergabe einzelner Teile oder des gesamten Leitfadens ist ausdrücklich nicht gestattet. Ausgenommen ist dabei der individuelle bzw. private Gebrauch, wobei die private Nutzung kein Recht zur Weitergabe an Dritte bein-haltet. Gleiches gilt für Veröffentlichungen oder sonstige Arbeiten.

12.5 Vergütung

Dieser Leitfaden wird den Adressaten/Empfängern kostenlos zur Verfügung gestellt.

13 Autoren

Die Autoren der Österreich-Version des Leitfadens, welche auf der Basis des deutschen Leitfadens der EuroCloud Deutschland _eco e.V. erstellt wurde, sind:



Rechtsanwalt Mag. Martin Schiefer
Heid Schiefer Rechtsanwälte, Wien
office@heid-schiefer.at



Rechtsanwalt Dr. Ralf Blaha LL.M.
Heid Schiefer Rechtsanwälte, Klagenfurt
office@heid-schiefer.at

HEID SCHIEFER
RECHTSANWÄLTE

Der Druck dieses Leitfadens wurde freundlicherweise durch Sponsoren der EuroCloud.Austria finanziert:

EuroCloud.Austria
Verein zur Förderung von Cloud Computing
Neubaugasse 11/9
1070 Wien

E-Mail: info@eurocloud.at
Web: http://www.eurocloud.at

Der Druck dieses Leitfadens wurde freundlicherweise durch Sponsoren der EuroCloud.Austria finanziert: