EuroCloud AUSTRIA

EuroCloud Austria e.V.

Leitfaden

Cloud Computing
Recht, Datenschutz & Compliance

ÖSTERREICH

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













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 e.V. 2011

1 Inhaltsverzeichnis

1	Vorwort	4
2	Einleitung	6
3	Rechtliche Anforderungen	7
4	Kernpunkte zur Auswahl des Cloud-Anbieters	8
5	Kernpunkte eines Vertrages aus datenschutzrechtlicher Sicht (sog. „Dienstleistervertrag“)	9
6	Produkt- und branchenspezifische Besonderheiten	17
7	Checkliste Vertragselemente	20
8	Glossar Cloud Computing	26
9	Rechtlicher Hinweis	28
10	Autoren	31



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

1 Vorwort

Liebe Leserinnen und Leser,

Es gibt wenige IT-Themen, die derzeit so kontrovers diskutiert werden wie Cloud Computing. Auf der einen Seite werden signifikante Einsparungen und eine flexible Nutzung von IT-Diensten prognostiziert, auf der anderen Seite sind die Bedenken zu Sicherheit, Datenschutz und der Ausgestaltung rechtlicher Anforderungen sehr ernst zu nehmen.

Mittlerweile lässt sich feststellen, dass Cloud Computing ein grundlegender Bestandteil zukünftiger IT-Planungen ist, da Unternehmen fortlaufend gezwungen sind, über die Ökonomisierung ihrer IT nachzudenken. Dabei kann zwischen der Eigenerrichtung, dem klassischen IT-Outsourcing oder dem Zukauf von IT-Services aus der Cloud gewählt werden. Vermutlich wird es sich letztlich um ein hybrides Modell handeln.

Fakt 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 wichtige Informationen zu rechtlichen Aspekten des Cloud Computing bereitstellen und für Anbieter und Anwender gleichermaßen hilfreich sein. Die Arbeitsgruppe Recht der EuroCloud Deutschland_eco e.V. hat einen Leitfaden Cloud Computing Recht und Datenschutz mit Unterstützung namhafter Rechtsexperten erstellt. EuroCloud Austria hat auf der Basis des deutschen Leitfadens den vorliegenden Leitfaden für Österreich erarbeitet.

EuroCloud bietet eine Auditierung von Cloud-Anbietern im Bereich „Software as a Service“ (SaaS), mit der neben den rechtlichen Aspekten auch die betriebliche Bereitstellung und die Serviceerbringung 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. Durch EuroCloud zertifizierte Cloudservice Anbieter weisen mit diesem Gütesiegel nach, dass sie ihr Service nach höchsten Qualitätsansprüchen abwickeln.

Ich danke den Fachleuten der Rechtsanwaltskanzlei andréewitch & simon, Wien dafür, dass sie die Österreich-Version dieses Leitfadens erstellt haben.

Wien, November 2011



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

2 Einleitung

Beim Cloud Computing stehen Sicherheit und Compliance als wichtigste Themen an erster Stelle. Mit dem Leitfaden *Recht & Datenschutz* bekommen sowohl Anbieter als auch Anwender eine Richtlinie in die Hand, die bei der Auswahl des Dienstleisters hilft und das richtige rechtliche Vorgehen unterstützt.

Der Leitfaden soll eine Grundlage für die richtige Einordnung rechtlicher Aspekte bilden. Dabei konzentriert er sich auf den Bereich „Software as a Service" als „Public Cloud"-Dienst und erörtert die besonderen Anforderungen hinsichtlich des Datenschutzes und bestimmte Aspekte im steuerrechtlichen Bereich.

Die Themenübersicht ist abgeleitet aus den Prüfkriterien des EuroCloud SaaS-Gütesiegels, das „Software as a Service"-Angebote in Bezug auf Serviceerbringung, Datensicherheit, Datenschutz, Vertragsgestaltung und Interoperabilität untersucht. Weitere rechtliche Leitfäden, insbesondere zu vertraglichen Aspekten, werden in den nächsten Monaten erstellt und zur Verfügung gestellt.

EuroCloud Austria engagiert sich seit 2010 als nationale Organisation des europäischen EuroCloud-Netzwerkes.

EuroCloud hat mit der Initiative SaaS-Gütesiegel und der grundlegenden Aufbereitung des rechtlichen Hintergrunds (Outsourcing von IT-Dienstleistungen und Auftragsdatenverarbeitung) wichtige Projekte gestartet, um die Rahmenbedingungen für einen erfolgreichen Einsatz von Cloud-Diensten aus den verschiedenen Bereichen (Software, Plattform und Infrastruktur) zu verbessern.

3 Rechtliche Anforderungen

Ein Schwerpunkt unter dem Aspekt „Recht und Datenschutz“ bei Cloud Computing ist der Datenschutz. Der Leitfaden befasst sich mit den Besonderheiten, die sich bei der Nutzung von Cloud Computing unter dem Gesichtspunkt der vertraglichen Vereinbarungen zwischen Nutzer und Anbieter ergeben.

Die datenschutzrechtlichen Vorgaben werden stets dann relevant, wenn personenbezogene Daten – z.B. Kundendaten oder Mitarbeiterdaten – betroffen sind. Zu beachten ist, dass der Begriff der „personenbezogenen Daten“ im Sinne des Datenschutzgesetzes (DSG) sehr weit gefasst ist. Alle Daten, die einen Personenbezug haben oder bei denen der Anbieter, der Nutzer oder ein Dritter einen Personenbezug herstellen könnte, gelten aus Sicht der Datenschutzbehörden als „personenbezogene Daten“. Zu beachten ist in diesem Zusammenhang, dass nach österreichischem Datenschutzrecht nicht nur eine natürliche Person „Betroffener“ sein und damit den Schutz des DSG in Anspruch nehmen kann, sondern auch juristische Personen, unternehmensrechtliche Personengesellschaften und sonstige Personengemeinschaften, deren Daten verwendet werden. In der Praxis wird es nur sehr wenige Cloud-Anwendungen geben, bei denen Daten verarbeitet werden, die nicht zumindest teilweise personenbezogen sind.

Die zivilrechtlichen Vertragsbestandteile über die zu erbringenden SaaS-Leistungen und Service Levels sowie die zivilrechtlichen flankierenden Regelungen über insbesondere die Haftung und Kündigung sind nicht Gegenstand der folgenden datenschutzrechtlichen Ausführungen.

Im Folgenden werden Hinweise zur Umsetzung der Anforderungen des Datenschutzes (§§ 10 f DSG) bei Verträgen zwischen Anbietern von SaaS bzw. Cloud Computing und deren Kunden gegeben. Der Leitfaden konzentriert sich auf die Darstellung spezifischer Datenschutzprobleme des Cloud Computings und zeigt, wie Fragen der datenschutzrechtlichen Dienstleisterstellung Cloud-spezifisch geregelt werden können.

Vorab ist Folgendes zu beachten:

Verantwortlich für die rechtmäßige Datenverarbeitung ist auch beim Cloud Computing der Nutzer, also der Auftraggeber (§ 6 Abs. 2 DSG).

- Der Nutzer bleibt auch bei der Nutzung von Cloud Computing im Rahmen der §§ 10 f DSG für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Er darf also auch mittels des Dienstes nur solche datenschutzrelevanten Verarbeitungen vornehmen lassen, die er auch selbst vornehmen dürfte.

Auch für einen reinen Test einer Cloud-Computing-Anwendung muss bereits ein Vertrag mit dem Anbieter abgeschlossen werden, wenn Echtdaten verarbeitet werden.

- Der Abschluss eines Vertrags über die Dienstleistung als datenschutzrechtliche Grundlage ist auch dann erforderlich, wenn der Einsatz der Cloud-Computing-Anwendung nur getestet werden soll. Um den Aufwand für den Abschluss eines solchen Vertrags zu vermeiden, bietet es sich an, Testzugänge ohne Echtdaten zu nutzen.

4 Kernpunkte zur Auswahl des Cloud-Anbieters

Der Auftraggeber ist gesetzlich verpflichtet, den Anbieter sorgfältig auszuwählen.

Der Auftraggeber (Nutzer) hat den Auftragnehmer (Anbieter) sorgfältig auszuwählen und sich auch vor Beginn der Datenverarbeitung (und sodann regelmäßig) von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Diese müssen eine ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten (§ 10 Abs. 1 DSG).

Nach Vertragsschluss muss der Auftraggeber regelmäßig prüfen, ob der Anbieter die erforderlichen technischen und organisatorischen Maßnahmen einhält.

In der Praxis bedeutet dies, dass der Nutzer sich von der Eignung des Anbieters vor dem Vertragsschluss „ein Bild machen“ muss, um seiner gesetzlichen Pflicht zur sorgfältigen Auswahl des Anbieters Rechnung zu tragen. Bereits diese Auswahl ist für den Nutzer erleichtert, wenn der Anbieter Standards eines Gütesiegels erfüllt oder über eine entsprechende Reputation verfügt.

5 Kernpunkte eines Vertrags aus datenschutzrechtlicher Sicht (sog. „Dienstleistervertrag")

5.1 Form

Der Vertrag bedarf für seine Wirksamkeit der Schriftform.

Zu beachten ist aber, dass die im DSG geregelten Pflichten des Dienstleisters schon kraft Gesetzes gelten, also grundsätzlich nicht eines schriftlichen Vertrags bedürfen. Für die Praxis bedeutet dies, dass entweder eine Vertragsurkunde handschriftlich durch den Nutzer und den Anbieter unterzeichnet wird oder qualifizierte elektronische Signaturen genutzt werden müssen.

Mögliches Vorgehen bei Online-Vertragsschluss, wenn dieser nicht den Anforderungen einer qualifizierten elektronischen Signatur genügt:

Der Kunde erhält auf Anfrage vom Anbieter unverzüglich ein schriftliches Vertragsangebot, welches von einer vertretungsberechtigten Person des Anbieters unterschrieben ist und inhaltsgleich mit den online geschlossenen Vertragsbedingungen ist. Hierbei kann klargestellt werden, dass die Rechte und Pflichten (z.B. zur Zahlung des Entgelts) aus dem Vertrag auch ohne schriftlichen Vertrag bestehen.

Der Vertrag bedarf der Schriftform, ein Online-Abschluss mit qualifizierter elektronischer Signatur ist möglich

5.2 Gegenstand des Auftrags

Der Gegenstand der erbrachten Leistung ist grob zu umschreiben. Soweit der Umgang mit personenbezogenen Daten betroffen ist, bedarf es detaillierter Beschreibungen (z.B. Hosting, Betrieb, Pflege und Zurverfügungstellen zum Online-Abruf einer bezeichneten Anwendung, Migration von Daten). Bei Parametrisierungen und kundenspezifischer Anpassung (Customizing) ist danach zu unterscheiden, ob dies vor dem „Einspielen" der Daten oder danach erfolgt.

Es kann auf deren Funktionsbeschreibung oder die Datenschutzhinweise des Anbieters verwiesen werden, sofern sich aus diesen Dokumenten ergibt, welche Daten im Rahmen der Anwendung auf welche Weise erhoben, verarbeitet und genutzt werden. Vorzugswürdig ist eine individuelle Beschreibung des Dienstes in Bezug auf den Umgang mit personenbezogenen Daten, wobei dies bei Cloud-Angeboten oft wenig problematisch ist. Ein bloßer Verweis auf die bestehende und eventuell durch den Kunden getestete Anwendung oder auf Online-Benutzerhandbücher genügt hingegen nicht,

Sind personenbezogene Daten betroffen, muss bei der Beschreibung der Auftrag spezifiziert werden: Hosting, Betrieb, Migration von Daten?

Customizing: Erfolgt dies vor oder nach der Übertragung personenbezogener Daten?

Werden personenbezogene Daten verarbeitet? Wenn ja, wie?

Welche Dritte haben darauf Zugriff?

Hinweis, dass Daten jederzeit auf Wunsch des Auftraggebers gelöscht werden können.

da diese einseitig vom Anbieter geändert werden können; dies gilt jedenfalls, sofern nicht ein Versionsstand explizit festgelegt und dokumentiert wird.

Auf folgende Aspekte sollte in jedem Fall näher eingegangen werden:

- Klarstellung, ob und gegebenenfalls in welcher Weise sensible Daten („besonders schutzwürdige Daten“) im Sinne des § 4 Z 2 DSG erhoben und/oder verwendet werden. Sensible Daten sind Daten natürlicher Personen über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Wenn solche Daten verarbeitet werden, ist fallspezifischer datenschutzrechtlicher Rat einzuholen.
- Erläuterung, welche Dritte Zugriff auf die Daten haben können (über Schnittstellen, als Wartungsunternehmen, Subunternehmer, etc.)
- Erläuterung, dass Daten jederzeit auf Wunsch des Auftraggebers gelöscht werden, und wie dies geschieht.

5.3 Auslandssachverhalte (einschließlich eingesetzter ausländischer Ressourcen und Subunternehmer)

Ohne weiteres ist Auftragsdatenverarbeitung nur mit Auftragnehmern mit Sitz in der EU oder im EWR möglich.

Bei Auftragnehmern in Drittländern müssen ergänzend besondere vertragliche Regelungen getroffen werden.

Das Datenschutzgesetz privilegiert Dienstleisterverhältnisse, indem es die Datenverarbeitung des Auftragnehmers dem Auftraggeber zurechnet und keine Erlaubnisnorm mehr für die Übermittlung an den Auftragnehmer fordert. Diese privilegierende Wirkung greift ohne weiteres jedoch nur bei einem Auftragnehmer, der seinen Sitz in der EU oder dem Europäischen Wirtschaftsraum (EWR) hat (§ 12 Abs. 1 DSG). Bei einer Beauftragung von Anbietern mit Sitz in einem Drittstaat – also außerhalb der EU und/oder des EWR – oder einer tatsächlichen Datenverarbeitung in einem solchen Drittstaat müssen zusätzliche Anforderungen erfüllt werden, damit eine Übertragung von Daten in einen solchen Drittstaat erfolgen darf.

Naheliegend ist, auf den von der Europäischen Union abgesegneten Standardvertrag zur „Auftragsdatenverarbeitung“ zurückzugreifen (sog. „Standard Contract Clauses“ für „Data Processing“).

Im Regelfall bedarf die Überlassung von Daten an einen Empfänger in einem Drittstaat der Genehmigung der österreichischen Datenschutzkommission (DSK). Zwar befreit der Abschluss dieses Standardvertrags nicht vom Erfordernis der Genehmigung des Datentransfers durch die DSK, doch kann er diese – in der Praxis – durchaus erleichtern.

5.4 Verantwortlichkeit

Im Interesse des Anbieters sollten die grundsätzlichen datenschutzrechtlichen Verantwortlichkeiten (der Anbieter ist nur Auftragnehmer, der Nutzer ist als Auftraggeber hauptverantwortlich wie bei Datenverarbeitung im eigenen Unternehmen) im Vertrag klarstellend geregelt und der Auftragnehmer dazu verpflichtet werden, nur datenschutzkonforme Nutzungen vorzunehmen. Dazu gehört insbesondere, dass die Daten ausschließlich im Rahmen der Aufträge des Auftraggebers verwendet werden und eine Übermittlung der verwendeten Daten ohne Auftrag des Auftraggebers verboten ist (§ 11 Abs. 1 Z 1 DSG).

Die datenschutzrechtlichen Verantwortlichkeiten müssen im Vertrag klar geregelt sein.

Im Interesse des Nutzers sollte vertraglich klargestellt werden, dass allein ihm die Außenkommunikation – auch bei Datenschutzpannen – obliegt, der Anbieter ihn aber unverzüglich über jeden Datenschutz- und/oder Sicherheitsverstoß – bzw. über den Verdacht von solchen – umfassend zu informieren hat.

Der Anbieter sollte den Nutzer dazu anhalten, dass dieser im Außenverhältnis zu den Betroffenen deutlich kommuniziert, dass allein der Nutzer für die Ansprüche der Betroffenen – insbesondere auf Auskunft, Berichtigung und Löschung – der Verantwortliche ist. Weiters ist es sinnvoll, im Vertrag klarzustellen, dass der Anbieter gegebenenfalls auf einen Verstoß gegen Vorschriften über den Datenschutz hinweist, er allerdings keine rechtliche Prüfung vornimmt und im Zweifel die Anweisung des Nutzers dennoch auszuführen hat. Erkennbar strafbare Weisungen darf der Anbieter aber in keinem Fall ausführen.

5.5 Kontrollrechte des Nutzers

Der Nutzer muss sich gegenüber dem Anbieter Kontrollrechte einräumen lassen (§ 11 Abs. 1 Z 6 DSG).

Der Auftraggeber muss sich gegenüber dem Auftragnehmer Kontrollrechte einräumen.

Das bedeutet, dass der Nutzer berechtigt sein muss, die Datenverarbeitung einschließlich der Schutzmaßnahmen beim Anbieter – auch vor Ort – kontrollieren zu dürfen oder durch Dritte kontrollieren zu lassen. Das muss sich auf alle Orte beziehen, an denen die Daten verarbeitet werden. Gerade bei vielen verschiedenen und/oder weit entfernten Orten bietet sich eine Kontrolle durch Dritte, etwa im Rahmen zertifizierter, gegebenenfalls standardisierter Audits, an. Allerdings fordern die Datenschutzbehörden (zumindest derzeit) wohl, dass der Nutzer zumindest das Recht hat, selbst die Kontrollen individuell vorzunehmen. Entsprechendes sollte daher im Vertrag auch geregelt werden.

Der Nutzer sollte neben diesem Kontrollrecht vor Ort auch die Pflicht des Anbieters regeln, dass der Anbieter die für eine Kontrolle erforderlichen Informationen bereitstellt und anderweitig angemessen mitwirkt. Die Kontrollen können für den Regelfall auf die Geschäftszeiten und auf eine Voranmeldung beschränkt werden. Typischerweise wird eine angemessene Kontrolle ohnehin nur unter diesen Voraussetzungen tatsächlich möglich sein.

Darüber hinaus sollten – soweit einschlägig – auch die Kontrollen durch Aufsichtsbehörden vertraglich geregelt werden. Dazu gehört auch, dass – allenfalls – auch die notwendigen technischen und organisatorischen Voraussetzungen geschaffen werden, um datenschutzrechtliche Auskunfts-, Richtigstellungs- und Löschungspflichten erfüllen zu können.

Da es sich hierbei um eine gesetzliche Pflicht zur Ausgestaltung der datenschutzrechtlichen Dienstleisterstellung handelt, ist es auch für Anbieter nicht sinnvoll, sich diesen Regelungen zu verschließen. Sie sollten vielmehr den Nutzern geeignete Standardverfahren anbieten. Das Gesetz fordert allerdings nicht, dass diese Unterstützung entgeltfrei erfolgen muss. Ein sinnvoller Interessensausgleich könnte darin bestehen, ab einem gewissen Aufwand eine Kostentragung des Nutzers zu regeln.

5.6 Technisch-organisatorische Maßnahmen

Gesetzliche Anforderung an den Inhalt eines Dienstleistervertrags ist die Verpflichtung, technisch-organisatorische Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten, also alle erforderlichen Datenschutzmaßnahmen, zu treffen. Diese sind in § 14 DSG näher geregelt.

Es muss ein konkretes, den tatsächlichen Gegebenheiten entsprechendes Sicherheitskonzept vertraglich als Leistungspflicht des Anbieters festgelegt werden. Abstrakte oder pauschale Beschreibungen genügen dieser Vorgabe nicht, sondern sie müssen so konkret sein, dass klar ist, welche Maßnahmen ergriffen sind. Diese Maßnahmen müssen ein angemessenes Schutzniveau sicherstellen, sodass es für die Bewertung der Schutzmaßnahmen auf die verarbeiteten personenbezogenen Daten ankommt.

In der Praxis bietet es sich an, dass der Anbieter ein Sicherheitskonzept für seine Dienstleistung erstellt, das durch den Nutzer geprüft und dann als vertragliche Anforderung festgelegt wird. Dabei ist allerdings klar, dass bei standardisierten SaaS- oder Cloud-Angeboten eine Prüfung durch den Nutzer nicht bedeuten kann, dass auf individuelle Wünsche des Nutzers eingegangen werden kann. Der Nutzer ist aber dazu verpflichtet, zu überprüfen, ob das Sicherheitskonzept den datenschutzrechtlichen Anforderungen genügt und der Sensibilität der involvierten Daten gerecht wird, bevor er die Daten auslagert.

Das Sicherheitskonzept muss entsprechend der technischen Entwicklung dynamisch angepasst werden, um das erforderliche Schutzniveau aufrecht zu erhalten.

Zur Einhaltung dieses Schutzes sind sowohl der Nutzer als auch der Anbieter jeweils für sich gesetzlich verpflichtet.

Von den beim Anbieter getroffenen technisch-organisatorischen Maßnahmen im Sinne des DSG – also den Maßnahmen zur Sicherheit der Daten – muss sich der Nutzer vor Beginn der Verarbeitung der Daten beim Anbieter überzeugen (§ 10 Abs. 1 DSG). Im Interesse beider Parteien kann dies nach dem Vertragsschluss – also der finalen Auswahl – erfolgen, solange sich der Nutzer vor Beginn der tatsächlichen Datenverarbeitung die Überzeugung verschafft hat. In der praktischen Konsequenz bedeutet das, dass die erforderlichen Maßnahmen selbstverständlich bei Vertragsschluss geklärt worden sein müssen.

Technisch-organisatorische Maßnahmen zum Schutz der personenbezogenen Daten müssen vertraglich und konkret geregelt sein.

Eine Überzeugungsbildung muss nicht zwingend vor Ort beim Anbieter erfolgen. Diese kann auch durch Vorlage entsprechender Testate, Zertifikate oder Erklärungen des Anbieters erfolgen. Je schutzbedürftiger die Daten aus der Sicht der Betroffenen – also derjenigen, auf die sich diese Daten beziehen – sind, umso gründlicher muss die Überzeugungsbildung erfolgen.

Diese Überzeugungsbildung muss nach der initialen Überprüfung regelmäßig wiederholt werden. Das sollte so auch im Vertrag vorgesehen werden. Eine konkrete Vorgabe zum Turnus ist dem Gesetz nicht zu entnehmen. Der Turnus ist daher nach der Schutzbedürftigkeit der Daten aus der Sicht der Betroffenen zu bewerten. In jedem Fall muss eine erneute Überprüfung dann erfolgen, wenn Zweifel an der Einhaltung der Sicherheitsmaßnahmen durch den Dienstleister auftreten.

Über die Prüfung hinaus ist aus gesetzlicher Sicht die Dokumentation dieser Überzeugungsbildung entscheidend. Das Ergebnis der jeweiligen Prüfung hat der Nutzer zu dokumentieren. Es muss also festgehalten sein, dass und mit welchem Ergebnis die Überzeugungsbildung stattgefunden hat.

5.7 Einschaltung von Subunternehmern und deren Kontrolle

Das DSG fordert, dass im Dienstleistervertrag vorzusehen ist, dass weitere Dienstleister nur mit Bewilligung des Auftraggebers heranzuziehen sind und deshalb der Auftraggeber von der beabsichtigten Heranziehung eines weiteren Dienstleisters („Subdienstleister“) so rechtzeitig zu verständigen ist, dass er dies allenfalls untersagen kann.

Von einem Subdienstleister sollte ausgegangen werden, wenn der Zugriff des Subunternehmers auf die für den Nutzer verarbeiteten Daten nicht ausgeschlossen werden kann. Eine Übermittlung an den Subdienstleister ist nicht erforderlich. Zugriff etwa in Form des Remote-Einpflegens von Daten oder der Fernwartung ist ausreichend. Ferner kommt es nicht darauf an, ob der Subdienstleister die Daten verarbeiten soll, sondern ob er tatsächlich darauf zugreifen kann.

Das Gesetz fordert damit nach seinem Wortlaut nur eine Regelung über das „Ob“ der Zulässigkeit von Subdienstleistern.

Als praxistaugliche Regelung, die sowohl den Interessen des Auftragnehmers als auch des Auftraggebers dient, kann sich eine Gestaltung erweisen, die zwischen Kategorien von Subunternehmern differenziert. Damit können bestimmte Kategorien unter einen Zustimmungsvorbehalt des Auftraggebers gestellt werden, während in anderen Kategorien die Einschaltung von Subunternehmern ohne gesonderte Einwilligung zulässig ist, sofern bestimmte definierte Anforderungen eingehalten sind. In jedem Fall sollte der Auftraggeber über die Subunternehmer und deren Tätigkeit informiert werden.

Die Informationspflicht kann vereinfacht werden, indem der Anbieter online eine zugangsgeschützte Liste von Subunternehmern führt, die der Kunde einsehen kann und über deren Änderungen der Kunde per E-Mail informiert wird. Die Liste enthält Name und Anschrift des Subunternehmers und eine Kurzbeschreibung der erbrachten Dienstleistung. Auf Verlangen des Kunden legt der Anbieter die datenschutzrelevanten Vertragsbedingungen des Subdienstleistervertrags offen.

Die mögliche Beauftragung von Subdienstleistern muss vertraglich geregelt sein.

Die Beauftragung von Subdienstleistern ist nur zulässig, sofern durch Subunternehmer dasselbe Schutzniveau in Bezug auf die personenbezogenen Daten sichergestellt ist, wie sie der Vertrag zwischen Nutzer und Anbieter für den Anbieter vorgibt. Die Verträge des Anbieters mit Subdienstleistern müssen also das gleiche Schutzniveau sicherstellen wie der Vertrag mit dem Kunden, insbesondere hinsichtlich technischer und organisatorischer Sicherheitsmaßnahmen. Der Anbieter sollte dies auch aus Eigeninteresse sicherstellen, um nicht in eine Schere zwischen seinen „hohen“ Pflichten gegenüber dem Nutzer und nur niedrigen Pflichten seines Subunternehmers zu geraten.

Der Nutzer muss sich beim Zulassen von Subdienstleistern bewusst sein, dass er im Außenverhältnis für diese genauso haftet wie für den Anbieter als seinen Hauptauftragnehmer.

Der Nutzer muss durch vertragliche Vorgaben sicherstellen, dass er gegenüber den Subunternehmern dieselben, eigenen Kontrollrechte hat wie gegenüber dem Anbieter.

5.8 Laufzeit und Rückgabe von Daten

Die „Rückgabe“ der personenbezogenen Daten bei Vertragsbeendigung muss aufgrund der gesetzlichen Vorgabe in § 11 Abs. 1 Z 5 DSG ebenfalls geregelt werden. Diese Bestimmung verlangt, dass nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten sind.

Der Vertrag muss Angaben zu Laufzeit und Rückgabe der Daten beinhalten.

Die drei Grundszenarien sind die Rückübertragung der Daten plus Löschung in den Systemen des Anbieters oder die weitere Aufbewahrung der Daten oder die bloße Löschung der Daten in den Systemen des Anbieters. Ein Grundszenario muss ohne zusätzliches Entgelt in dem Vertrag vorgesehen sein. Auch wenn der Dienstleistervertrag beendet ist, sollte die datenschutzrechtliche Dienstleistung so ausgestaltet sein, dass die Pflichten aus dem Dienstleistervertrag bis zur eindeutigen Bestätigung der Löschung durch den Anbieter fortgelten.

Der Nutzer sollte sich bereits bei Vertragsschluss entscheiden, welche Anforderungen an die Rückgabe – Übertragungsweg (z.B. per SFTP) und in welchem Dateiformat oder ob Erläuterungen zur Dateistruktur erforderlich werden – zu stellen sind, damit er zu einem anderen Anbieter wechseln oder die Aufgabe wieder selbst wahrnehmen kann.

Für den Anbieter ist neben dem vorgenannten kostenrelevanten Aspekt auch entscheidend, wann er die Daten löschen kann, falls der Nutzer die Vergütung nicht (mehr) zahlt oder insolvent wird.

6 Produkt- und branchenspezifische Besonderheiten

Besondere Anforderungen können sich in bestimmten Fallkonstellationen ergeben, wie etwa bei Kunden

- aus dem Finanzdienstleistungssektor (§ 25 WAG)
- aus dem Telekommunikationsbereich (TKG)
- als Träger von Berufsgeheimnissen (z.B. § 121 StGB, Ärzte, Anwälte)
- mit Anwendungen steuerrelevanter Daten (BAO)

6.1 Finanzdienstleistungen

Der Finanzsektor weist Besonderheiten auf, die an dieser Stelle kurz angerissen, aber nicht abschließend besprochen werden können: § 25 Wertpapieraufsichtsgesetz (WAG) regelt die Auslagerung von wesentlichen betrieblichen Aufgaben an Dienstleister. „Kern" dieser Regelung ist die Verpflichtung, dass beim Rückgriff auf Dritte (Dienstleister) zur Wahrnehmung betrieblicher Aufgaben, die für die kontinuierliche und zufrieden stellende Erbringung von Dienstleistungen für Kunden und die Ausübung von Anlagetätigkeiten wesentlich sind, angemessene Vorkehrungen (die in einer Anlage zum WAG festgehalten sind) getroffen werden, um unnötige zusätzliche Geschäftsrisiken zu vermeiden.

Daher muss jeweils im Einzelfall geprüft werden, ob die in die Cloud transferierten Aufgaben und Prozesse „wesentlich" nach § 25 WAG sind und ob sie vom Begriff der „Auslagerung" erfasst sind. Dann müssen – ebenfalls gemäß § 25 WAG – für die Auslagerung angemessene Vorkehrungen zum Datenschutz und zur Vermeidung übermäßiger zusätzlicher Risiken getroffen werden (beispielsweise die sorgfältige Auswahl des Cloud-Anbieters, die Überwachung der Dienstleistung, die Festlegung von Methoden zur Bewertung der Leistung sowie die Vereinbarung einer Notfallplanung).

6.2 Telekommunikationsgesetz

Generell gelten auch für die im TKG geregelten Sachverhalte die Bestimmungen des DSG. Allerdings sind in der Telekommunikationsbranche die Spezialregelungen des Telekommunikationsgesetzes (TKG) zu beachten. §§ 92 ff TKG liegt das Prinzip zugrunde, dass eine Übermittlung personenbezogener Daten – Stamm- und Verkehrsdaten – an Dritte nur erfolgen darf, soweit das für die Erbringung jener Kommunikationsdienste, für die diese Daten ermittelt und verarbeitet worden sind, durch den Betreiber erforderlich ist. Soweit diese Grenzen im konkreten Fall nicht eingehalten werden können, verbleibt als Alternative die Gestaltung als Dienstleistervertrag (§ 11 DSG). Dies ist jedoch nach §§ 12 f DSG nur innerhalb der EU genehmigungsfrei. Eine Überschreitung dieser Grenzen ist im Rahmen von Cloud-Services problematisch.

6.3 Steuerrechtliche Buchführungspflicht

Gemäß § 132 Abs. 2 Bundesabgabenordnung (BAO) kann die Aufbewahrung der aufbewahrungspflichtigen Unterlagen auf Datenträger geschehen. Erfolgt die Aufbewahrung von aufbewahrungspflichtigen Unterlagen auf Datenträgern, muss die vollständige, geordnete, inhaltsgleiche und urschriftsgetreue Wiedergabe bis zum Ablauf der gesetzlichen Aufbewahrungspflicht (7 Jahre) jederzeit gewährleistet sein.

§ 131 Abs. 1 BAO bestimmt unter anderem, dass Bücher und Aufzeichnungen auf Verlangen der Abgabenbehörde innerhalb angemessen festzusetzender Frist in das Inland zu bringen sind.

Die Erlaubnis, Aufzeichnungen im Ausland zu führen und dort aufzubewahren, sowie die Pflicht, diese Unterlagen auf Verlangen innerhalb angemessener Frist ins Inland zu bringen, gilt hinsichtlich jener Vorgänge, die einem im Inland gelegenen Betrieb, einer im Ausland gelegenen Betriebsstätte oder einem im Ausland gelegenen Grundbesitz zuzuordnen sind.

Die übrigen Grundaufzeichnungen dürfen zwar im Ausland geführt werden, sind aber innerhalb angemessener Frist in das Inland zu bringen und dort aufzubewahren.

In diesem Zusammenhang ist § 18 Abs. 8 UStG zu beachten, wonach Bücher oder Aufzeichnungen im Inland zu führen und mit dazugehörigen Unterlagen im Inland aufzubewahren sind, sofern die Besteuerung von einem buchmäßigen Nachweis abhängt.

6.4 Unternehmensrechtliche Buchführungspflicht

Jeder Unternehmer muss nach dem Unternehmensgesetzbuch (UGB) Belege für Buchungen in den von ihm nach § 190 Abs. 1 UGB zu führenden Büchern sieben Jahre lang bereit halten. Grundsätzlich ist das unter den Voraussetzungen des § 190 Abs. 5 UGB auch in elektronischer Form auf Datenträgern und auch in Clouds möglich. Das Unternehmensrecht stellt keine Pflicht auf, Bücher im Inland zu führen.

6.5 Berufsgeheimnisträger

Für die durch §§ 121 f Strafgesetzbuch (StGB) betroffenen Bereiche besonderer Verschwiegenheitspflicht (beispielsweise des Gesundheitswesens oder der Kranken-, Unfall- und Lebensversicherungen) ist die Zulässigkeit (und damit auch die Strafbarkeit) von Auslagerungen auf Dritte, z.B. Cloud-Anbieter, nicht unumstritten. Da dies – allenfalls – eine heikle Abgrenzungsfrage sein kann, muss die Zulässigkeit anhand der jeweiligen Umstände des Einzelfalles geprüft werden.



7 Checkliste Vertragselemente

In Anlehnung an das EuroCloud SaaS-Gütesiegel werden die wichtigsten Fragen hinsichtlich der vertraglichen Ausgestaltung aufgeführt. 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 ab Anfang 2011 offiziell vergeben. Eine Reihe von Anbietern bereiten sich gerade auf die Zertifizierung vor.

Folgende Punkte sollten bei der Vertragsgestaltung entsprechend umgesetzt werden und werden im Rahmen der EuroCloud SaaS-Gütesiegel-Zertifizierung geprüft:

7.1 Vertragsabschluss und Vertragsgestaltung

» Wie wird der Vertrag geschlossen?
- online
- schriftlich

» Kann der Kunde auf einen schriftlichen Vertrag bestehen?

7.2 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?

7.3 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?

7.4 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?

7.5 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?

7.6 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?

7.7 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?

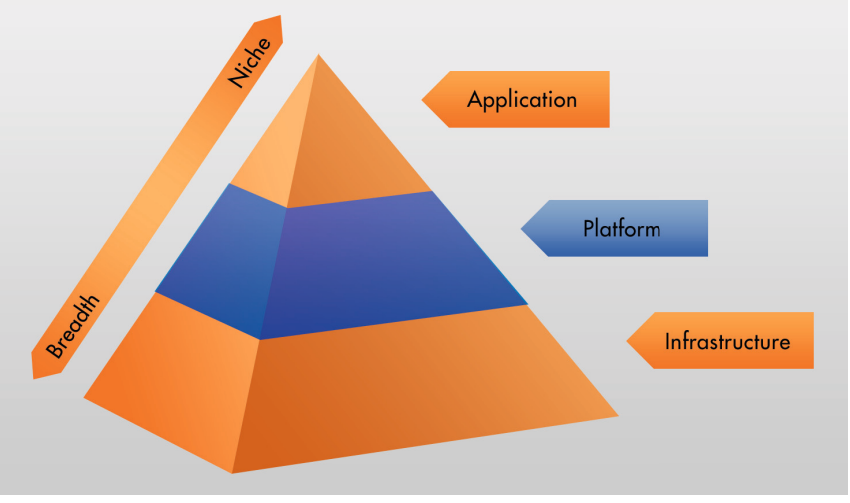
» Datenlöschung bei Vertragsende
  - Existieren Regelungen zur Löschung der Daten und zur Rückgabe von Datenträgern nach Beendigung des Vertrags?
  - Wird gewährleistet, dass die Daten auf Wunsch des Auftraggebers tatsächlich gelöscht werden?

8 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.

9 Rechtlicher Hinweis

9.1 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.

9.2 Inhalt des Leitfadens

Der Herausgeber / die Autoren übernehmen keine Gewähr für die Vollständigkeit, Richtigkeit oder Aktualität der bereit gestellten 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.

9.3 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.

9.4 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 beinhaltet. Gleiches gilt für Veröffentlichungen oder sonstige Arbeiten.

9.5 Vergütung

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

10 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 Dr. Markus Andréewitch
andréewitch & simon, Wien
office@andsim.at

Rechtsanwalt Mag. Gerald Steiner
andréewitch & simon, Wien
office@andsim.at

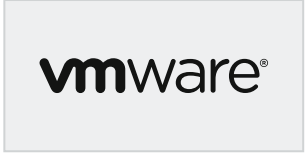
Der deutsche Leitfaden sowie nähere Angaben zu dessen Verfassern können unter www.eurocloud.de abgerufen werden.

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













EuroCloud AUSTRIA

EuroCloud Austria e.V.

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 Leitfaden wurde freundlicherweise durch Sponsoren der EuroCloud Austria finanziert:











