CLOUD-VERTRÄGE

WAS ANBIETER UND KUNDEN BESPRECHEN SOLLTEN

Katalog von empfohlenen Vertragsbestandteilen in Allgemeinen Geschäftsbedingungen (AGB) und Servicelevel-Vereinbarungen (SLA) für Cloud-Service-Anbieter.

Austrian Standards

EuroCloud AUSTRIA

wirtschafts agentur wien

IT-Cluster Wien

WKO WIRTSCHAFTSKAMMER WIEN Unternehmensberatung · IT

ADV

Katalog erstellt von:

EuroCloud.Austria (Editor)

Wirtschaftskammer Wien – Fachgruppe Unternehmensberatung und Informationstechnologie

Austrian Standards Institute, Arbeitsgruppe 001.38

„Cloud Qualitätskriterien“ IT-Cluster der Wirtschaftsagentur Wien

Weiters empfohlen von:

ADV Arbeitsgemeinschaft für Datenverarbeitung

Version 1.0 vom 01.11.2012

ZIELE DIESES KATALOGES

Für einen Nutzer von Cloud-Services sind diese Services ähnlich zu betrachten wie ein klassisches Outsourcing von IT-Leistungen. Daher sollten Cloud-Services Vereinbarungen enthalten, die auch bei einem klassischen IT-Outsourcing-Vertrag durchaus üblich sind.

Dies ist ein Katalog von empfohlenen Vertragselementen, die in Allgemeinen Geschäftsbedingungen (AGB) oder Servicelevel-Vereinbarungen (SLA) von Cloud-Service-Unternehmen berücksichtigt sein sollten. Es sind jedoch keine Musterklauseln formuliert, denn diese müssen immer den jeweiligen Kontext des Cloud-Services berücksichtigen. Beispielsweise sind Cloud-Services für den privaten Foto-Upload mit Sicherheit anders in den Vertragsvereinbarungen zu behandeln als eine Cloud-Rechnungslegungssoftware für Unternehmen.

Diese Zusammenstellung erhebt keinen Anspruch auf Vollständigkeit.

1 RAHMENBEDINGUNGEN DES CLOUD-SERVICES

In diesem inhaltlichen Bereich sollten sämtliche wesentlichen Informationen und erforderlichen Regelungen angeführt werden, die bei Vertragsabschluss und bei der Vertragsbeendigung eines Cloud-Services wichtig sind. Insbesondere sind dies Informationen über die an der Leistungserbringung beteiligten Unternehmen.

1.1 Regelung betreffend alle an der Leistungserbringung beteiligten Unternehmen

Folgende Punkte sollten im Vertrag berücksichtigt, bestätigt bzw. in ausreichender Detaillierung angeführt werden:

1.1.1 Relevante Informationen zum Unternehmen, mit dem der Vertrag abgeschlossen werden soll, entsprechend den öffentlichen Registern wie z.B. Firmenbuch, Gewerberegister oder Vereinsregister.

1.1.2 Darstellung, woher der Anbieter des Services kommt und welche nationalen Rechte betroffen sein können (Headoffice und Niederlassungen).

1.1.3 Informationen zu bestehenden Zertifizierungen des Vertragspartners. Detaillierte Beschreibung der bestehenden, gültigen Zertifizierungen des Rechenzentrums.

1.1.4 Informationen zu Unternehmen, die an der Leistungserbringung beteiligt sind. Auch Subunternehmen, Rechenzentren oder Cloud-Services anderer Unternehmen, die in den eigenen gesamten Service integriert sind. Insbesondere Darstellung, welche Unterauftragnehmer in Österreich oder in Ländern mit vergleichbaren Datenschutzgesetzen eingesetzt werden. Beispielsweise: welcher Rechtsordnung (wenn auch nur teilweise) die Subunternehmer unterworfen sind, welche Datenschutzrechte die Subunternehmer beachten müssen, welche wesentlichen Insolvenzrechte gelten (Zugriff auf Daten, Aussonderungsrechte, Zwangsbestimmungen, Insolvenzverwalter usw.).

1.1.5 Darstellung, dass Subauftragnehmer vom Auftragnehmer an dieselben Verpflichtungen gebunden werden, die der Auftragnehmer mit dem Auftraggeber eingeht.

1.2 Regelung betreffend Änderungen von Vertragsbedingungen von Cloud-Services

Folgende Punkte sollten im Vertrag berücksichtigt, bestätigt bzw. in ausreichender Detaillierung angeführt werden:

1.2.1 Klärung, in welcher Form der Vertrag zur Verfügung gestellt wird (z.B. elektronisch signiertes PDF oder Papierform) sowie der Vorgehensweise, die im Falle von Vertragsänderungen angewendet wird.

1.2.2 Bestätigung, dass keine einseitigen Änderungen an den Vertragsinhalten vorgenommen werden.

1.2.3 Auflistung jener Subunternehmer, bei deren Wechsel die ausdrückliche Zustimmung des Kunden eingeholt werden muss.

1.3 Regelung betreffend die Vertragsbeendigung von Cloud-Services

Regelungen betreffend das Vertragsende sollten im Vertrag ausreichend detailliert berücksichtigt, bestätigt bzw. deutlich dargestellt werden:

1.3.1 Darstellung der Laufzeit des Vertrages und der Regelung von eindeutigen Kündigungsgründen und deren Fristen für beide Seiten. Sonderkündigungsrecht des Auftraggebers, wenn der Anbieter wichtige Subunternehmer wechselt

(falls Beibehaltung des bisherigen Subunternehmers nicht möglich ist).

1.3.2 Darstellung der Regelungen, die die Mitwirkung des Auftragnehmers bei der Datenbereitstellung nach einer Vertragskündigung festlegen.

1.3.3 Regelungen zum Schutz der Daten des Auftraggebers und der Verfügbarkeit der Anwendung bei Insolvenz des Auftragnehmers, z.B. durch vorbeugende Maßnahmen.

1.3.4 Ausreichend detaillierte Beschreibung der Prozesse bei Vertragsbeendigung wie z.B. Datenrückgabe, Datenlöschung, Zugangsbeendigung, finale Abrechnung, technische Formate der Datenübermittlung, Fristen, Übergabe der elektronischen Schlüssel usw.

2 LEISTUNGSERBRINGUNG VON CLOUD-SERVICES

In diesem inhaltlichen Bereich sollten sämtliche wesentlichen Informationen und erforderlichen Regelungen angeführt werden, die für die Leistungserbringung eines Cloud-Services wichtig sind. Insbesondere sind dies alle Informationen zur verwendeten Infrastruktur, zur Leistung und deren Implementierung und zum Betrieb.

2.1 Regelung betreffend die eingesetzte Infrastruktur

Folgende Punkte sollten bestätigt bzw. in ausreichender Detaillierung angeführt werden:

2.1.1 Explizite Nennung aller Rechenzentren (samt Ortsanagabe), die für die Anwendung zum Einsatz kommen. Die rechtlichen Konsequenzen des Einsatzes von Rechenzentren außerhalb des EU-Rechtsrahmens sollten transparent gemacht werden.

2.1.2 Darstellung, wie das Rechenzentrum mit möglichen Risiken (Naturkatastrophen, technischen Gebrechen, Kriminalität und menschlichen Fehlleistungen) umgeht und welche Maßnahmen und Prozesse zur Minimierung möglicher Folgen angewendet werden.

2.1.3 Detaillierte Darstellung der Verfügbarkeit der Infrastruktur im Rechenzentrum, der Anbindung an einen oder mehrere Internet-Carrier, der Handbücher zu Betriebsführung & Notfällen, der Zertifizierungen und der Verfügbarkeit von redundanter Stromversorgung und Kühlung.

2.2 Regelung betreffend den Inhalt der Leistung

Der Bedeutung der Leistungsbeschreibung als wesentliches Element des Vertrages sollte durch eine detaillierte Beschreibung ausreichend Raum gegeben werden. Folgende Punkte sollten im Vertrag berücksichtigt, bestätigt bzw. in ausreichender Detaillierung angeführt werden:

2.2.1 Ausreichend detaillierte Beschreibung der Cloud-Leistung selbst und der Art des Cloud-Services, z.B. Infrastructur as a Services (IaaS) usw.

2.2.2 Informationen zu Herkunft und Hersteller der Leistung und zu bestehenden Zertifizierungen.

2.2.3 Klare Aussagen zu Regelungen, für welche Länder der Betrieb der Anwendung zugesichert wird, der angebotenen Sprachversionen und Lokalisierungen, der eingesetzten Standards, welche Browser und welche Schnittstellen unterstützt werden.

2.2.4 Deutliche Beschreibung der angebotenen Möglichkeiten der Verwaltung der eigenen Rechte, der Authentifizierungsmöglichkeiten und der Benutzerverwaltung.

2.3 Regelung betreffend die Implementierung der Leistung

Folgende Punkte sollten im Vertrag berücksichtigt, bestätigt bzw. in ausreichender Detaillierung angeführt werden:

2.3.1 Ausreichend detaillierte Beschreibung der Trial-Versionen (Kosten, Dauer, Funktionen) und Darstellung der Umstiegsszenarien auf Vollversionen.

2.3.2 Sämtliche Optionen bei der Implementierung und bei den Customizing-Möglichkeiten und damit verbundene Kosten.

2.3.3 Schulungskonzepte, Betriebshandbücher und Anwenderhandbücher.

2.3.4 Abnahmeprozesse und deren Konsequenzen (z.B. Leistungsbeginn, Gewährleistung, Zahlungsverpflichtungen).

2.4 Regelung betreffend den Betrieb der Leistung

Folgende Punkte sollten im Vertrag berücksichtigt, bestätigt bzw. in ausreichender Detaillierung angeführt werden:

2.4.1 Ausreichend detaillierte Darstellung des Release Managements (Zeitpunkt, Vorlauf, Wechselpflicht, kundenspezifische Konfigurationen).

2.4.2 Ausreichend detaillierte Darstellung des Fehler- bzw. Mängelmanagements (Meldepflicht, Kommunikationsstrategie wie z.B. Ticketsystem, Telefonservices [Hotline], Eskalationsprozesse, Patch-Termine usw.).

2.4.3 Ausreichend detaillierte Darstellung, welche Verfügbarkeitswerte zugesichert werden und wie die laufenden Performancemessungen erfolgen sowie wie der Auftraggeber vom Stand der Serviceerfüllung informiert wird (wie erfolgen Monitoring und Reporting?).

2.4.4 Ausreichend detaillierte Darstellung, welche Servicelevels (SLA) angeboten werden und wie die Einhaltung der Servicelevels kontrolliert, dokumentiert und kommuniziert wird.

2.4.5 Ausreichend detaillierte Darstellung, wie die Störungsbehebung organisiert ist.

2.4.6 Ausreichend detaillierte Darstellung, wie die Kapazitätsplanung für die erforderliche Infrastruktur des Services erfolgt.

2.4.7 Ausreichend detaillierte Darstellung aller Möglichkeiten des Datenexports sowie der dafür erforderlichen Schnittstellen und Programme.

2.4.8 Regelungen für elektronische Dokumente (Rechnungen und sonstige geschäftsrelevante Belege), die zu Verpflichtungen seitens des Auftraggebers gegenüber der Finanzbehörde führen.

2.5 Regelung betreffend die Erreichbarkeit des Cloud-Services

Folgende Punkte sollten im Vertrag berücksichtigt, bestätigt bzw. in ausreichender Detaillierung angeführt werden:

2.5.1 Detaillierte Regelungen für die Kommunikationskanäle für den Support zum Endkunden und Regelung der verfügbaren Sprachen für den Support.

2.5.2 Regelungen für 1st und 2nd Level Support und für die jeweilige Verfügbarkeit und die garantierten Antwortzeiten.

2.5.3 Darstellung des Kundensupports und des Einsatzes eines unterstützenden Systems wie z.B. eines Ticketsystems.

3 VERRECHNUNG VON CLOUD-SERVICES

In diesem inhaltlichen Bereich sollten sämtliche wesentlichen Informationen und erforderlichen Regelungen angeführt werden, die für die Leistungsverrechnung eines Cloud-Services wichtig sind.

3.1. Detaillierte Darstellung des Inhalts und der Form der Leistungsmessung und Leistungsverrechnung sowie aller möglichen Abweichungen von diesen Regelungen, insbesondere von separat zu verrechnenden Sonderleistungen, Mengenrabatten und dem Preis von Sonderleistungen.

3.2. Klärung der Vorgangsweise betreffend mögliche zukünftige Preisanpassungen.

3.3. Detaillierte Beschreibung der Möglichkeiten im Falle von Leistungsstörungen wie Entgeltminderung, Pönalen und Schadenersatz.

3.4. Detaillierte Beschreibung der Regelungen bei Streitigkeiten über Leistungserbringung oder Zahlungsverzug. Ausschluss von Regelungen betreffend die Zurückbehaltung oder Löschung von Daten des Auftraggebers ohne dessen ausdrückliche Zustimmung.

Sicherheit

4 SICHERHEIT VON CLOUD-SERVICES

In diesem inhaltlichen Bereich sollten sämtliche wesentlichen Informationen und erforderlichen Regelungen angeführt werden, die für die Sicherheit der Daten des Auftraggebers eines Cloud-Services wichtig sind.

4.1 Regelung betreffend den Datenschutz

Folgende Punkte sollten im Vertrag zur nachweislichen Einhaltung des Datenschutzes in ausreichender Detaillierung angeführt werden:

4.1.1 Beschreibung des Dienstes im Zusammenhang mit datenschutzrelevanten Aspekten, Beschreibung des Umfangs und von Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen sowie die Definition der Dauer der Verarbeitung und der Löschung der Daten.

4.1.2 Darstellung der Regelungen für personenbezogene Datenbestände (Registereintrag oder gleichwertige Regelungen). Insbesondere die Nennung einer Ansprechstelle, die gegenüber dem Auftraggeber für alle Belange des Datenschutzes beim Auftragnehmer und seinen Unterauftragnehmern als Ansprechpartner zur Verfügung steht. Diese Belange betreffen insbesondere die Unterstützung bei der Ausübung von Betroffenenrechten (Auskunft, Berichtigung, Löschung von Daten von Betroffenen).

4.1.3 Darstellung, wie Mitarbeiter des Auftragnehmers und aller Subunternehmer, die auf Daten Zugriff haben könnten, auf das Datengeheimnis und andere anzuwendende Vertraulichkeitsregelungen verpflichtet werden.

4.1.4 Regelung der Verantwortlichkeiten zwischen dem Auftraggeber, der die grundsätzliche datenschutzrechtliche Verantwortlichkeit trägt, und dem Auftragnehmer, der für die Umsetzung von datenschutzrelevanten Weisungen des Auftraggebers verantwortlich ist und die technischen Schutzmaßnahmen etc. zu etablieren hat.

4.1.5 Definitionen von Sachverhalten, 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 anzeigt werden müssen.

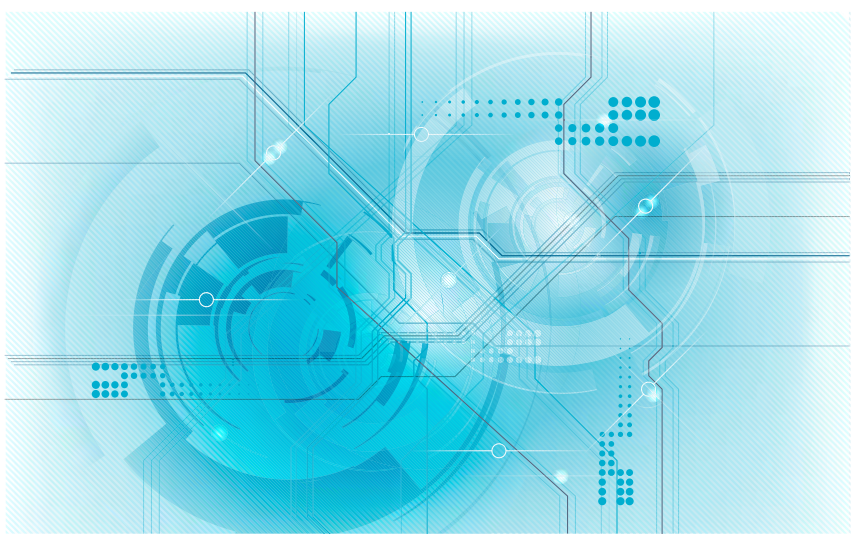
4.1.6 Regelung über rechtlich zulässige und verpflichtende Information des Auftragnehmers an den Auftraggeber, wenn Zugriffe durch Strafverfolgungsbehörden und andere staatliche Stellen erfolgt sind.

4.1.7 Regelung von Kontrollrechten des Auftraggebers und/oder eines vom Auftraggeber beauftragten Dritten vor Ort beim Auftragnehmer oder seinen Unterauftragnehmern. Regelungen für (kumulativ oder alternativ zu Kontrollen durch den Auftraggeber) regelmäßige Kontrollen/Audits und Zertifizierungen, die den Datenschutz beim Auftragnehmer und die Einhaltung der Verpflichtungen gegenüber dem Auftraggeber kontrollieren und zertifizieren. Regelung zur Mitwirkung des Auftragnehmers bei diesen Aktivitäten und den damit verbundenen Kosten.

4.2 Regelung betreffend die IT-Sicherheit

Folgende Punkte sollten im Vertrag berücksichtigt, bestätigt bzw. in ausreichender Detaillierung angeführt werden:

4.2.1 Beschreibung der eingesetzten IT-Sicherheitslösungen wie der Einsatz von Firewallsystemen, Virenscannern zum Schutz vor Viren, Trojanern, Malware, Schutz vor DoS usw.



4.2.2 Beschreibung von Security-Checks bzw. Penetration-Tests, die beim Auftragnehmer durchgeführt werden.

4.2.3 Beschreibung der Verschlüsselungsmethoden und des Key-Managements für den Datenverkehr zwischen Auftraggeber und Auftragnehmer, der Verschlüsselung auf den Speichermedien und einer End-to-End-Verschlüsselung, die einen Dateneinblick durch Personal des Anbieters vollständig ausschließt.

4.2.4 Detaillierte Beschreibung der sicheren Authentifizierung zur Nutzung des Services, der Auditierbarkeit von Login-Vorgängen (vom Kunden einsehbar) und der Möglichkeit, ein Kundensystem zur Authentifizierung zu integrieren.

4.3 Regelung betreffend die Datensicherung und Datenlöschung

Folgende Punkte sollten im Vertrag berücksichtigt, bestätigt bzw. in ausreichender Detaillierung angeführt werden:

4.3.1 Ausreichend detaillierte Regelung betreffend die Spiegelung von Anwendungsdaten und die Failover-Verfahren, um Daten permanent verfügbar zu halten.

4.3.2 Ausreichend detaillierte Regelung von Datensicherung und -archivierung (z.B. wann, wie oft, wie lange, Dauer der Rücksicherung, Lagerung der Speichermedien), Regelung der Verwahrung der Sicherungsmedien (z.B. räumliche Trennung, Regelung der Verschlüsselung der Sicherungen und Regelungen des Zugriffs des Kunden auf Datensicherungen), Regelungen zur Löschung der Daten und zur Rückgabe von Datenträgern nach Beendigung des Vertrags, Regelung zur nachweislichen Löschung von Daten des Auftraggebers.

EuroCloud

EuroCloud.Austria - gemeinnütziger Verein für Förderung von Cloud Computing
Museumstraße 5/14
1070 Wien
info@eurocloud.at
www.eurocloud.at

ADV

ADV Arbeitsgemeinschaft für Datenverarbeitung
Trattnerhof 2
1010 Wien
office@adv.at
www.adv.at

UBIT

Wiedner Hauptstraße 63
1045 Wien
ubit@wko.at
www.ubit.at

IT Cluster

IT-Cluster der Wirtschaftsagentur Wien
Ebendorferstraße 2
A-1010 Wien
info@wirtschaftsagentur.at
www.clusterwien.at

Austrian Standards Institute

Austrian Standards Institute / Österreichisches Normungsinstitut (ON)
Heinestraße 38
1020 Wien
office@as-institute.at
www.as-institute.at

Austrian Standards

EuroCloud AUSTRIA

wirtschaftsagentur wien

IT-Cluster Wien

WKO WIRTSCHAFTSKAMMER WIEN Unternehmensberatung · IT

ADV