

Stand 15. Juli 2020

DEFINITIONEN

Einige Begriffe (die im Original mit einem Großbuchstaben beginnen) werden in den vorliegenden besonderen Vertragsbedingungen sowie in dem Vertrag, auf den sich diese besonderen Bedingungen beziehen, und im OVHcloud-Glossar auf der OVHcloud-Website definiert. Die nachstehenden Definitionen ergänzen die Definitionen im Vertrag.

„Kundennetzwerk“: Ressourcen außerhalb der OVHcloud-Infrastruktur, die vom Kunden zur Kommunikation mit den von OVHcloud bereitgestellten Ressourcen verwendet werden. Dies können eigene Ressourcen des Kunden sein oder Ressourcen, die von Drittparteien im Auftrag des Kunden bereitgestellt und/oder gehostet werden.

„Hosted Private Cloud PREMIER“: Das gesamte auf der OVHcloud-Infrastruktur gehostete Virtuelle Datacenter. Die Hosted Private Cloud PREMIER wird vom Kunden über dessen Verwaltungsinterface und das Virtualisierungsinterface verwaltet. Host-Server und Speicherressourcen, die dem Kunden im Rahmen des Hosted Private Cloud Premier Dienstes bereitgestellt werden, sind für den Kunden reserviert.

„Host-Server“: In der Hosted Private Cloud Premier des Kunden deployter dedizierter Server. Dieser Server liefert über seinen Prozessor (CPU) und Arbeitsspeicher (RAM) zusätzliche Kapazitäten in der Hosted Private Cloud Premier, die über das VMware® User Interface verwaltet werden können.

„Infrastruktur“: Von OVHcloud errichtete Struktur für das Hosting der Hosted Private Cloud Premier des Kunden, darunter insbesondere das Netzwerk, die Bandbreite, physische Ressourcen und die Virtualisierung.

„Verwaltungsinterface“: Der „Kundencenter“-Bereich, der für den Kunden nach dem Login mit einer Kundenkennung und zugehörigem Passwort zugänglich ist.

„OVHcloud Connect“: Konnektivität zum internen dedizierten Netzwerk von OVHcloud („Backbone“), die einem Kunden an einem oder mehreren OVHcloud Points of Presence (Präsenzpunkten) bereitgestellt wird. OVHcloud Connect erlaubt dem Kunden, sein eigenes Kundennetzwerk (d. h. seine eigene Infrastruktur und eigene Rechenressourcen und/oder die von ihm verwendete Infrastruktur und Ressourcen von Drittparteien) mit seinem OVHcloud Connect zu verbinden.

„Paket“: Beinhaltet das Minimum an physischen Ressourcen, die für den Betrieb eines „Virtuellen Datacenters“ einer Hosted Private Cloud Premier erforderlich sind:

- Ein „Premier Private Cloud“-Paket besteht mindestens aus:
 - Zwei identischen Host-Servern (die CPU und RAM für die Virtualisierung bereitstellen), die für Computing-Aufgaben bestimmt sind. Der Kunde muss sicherstellen, dass er zu jeder Zeit über zwei identische Host-Server verfügt (d. h. Server mit den gleichen technischen Eigenschaften). Für den Fall, dass das Virtuelle Datacenter verschiedene Paare von Host-Servern enthält, wird das Paar mit den geringeren CPU- und RAM-Kapazitäten als „Paket“ für das Virtuelle Datacenter angesehen. Im Interesse der Klarheit: Sollte das Datacenter 2 Host-Server Premier mit „48 RAM“ und 2 Host-Server Premier mit „96 RAM“ beinhalten, so wird das betreffende „Paket“ aus den beiden Host-Servern Premier „48 RAM“ zusammengesetzt.

- *Zwei Datastore-Ressourcen. Für den Fall, dass das Virtuelle Datacenter verschiedene Paare von Datacenter-Ressourcen enthält, wird das Paar mit der geringeren Kapazität als „Paket“ für das Virtuelle Datacenter angesehen. Im Interesse der Klarheit: Sollte das Datacenter 2 Datastore-Ressourcen mit je 2 TB and 2 Datastore-Ressourcen mit je 3 TB beinhalten, so wird das betreffende „Paket“ aus den beiden Datastore-Ressourcen mit 2 TB zusammengesetzt.*
 - *Dem VMware vSphere Interface (das von VMware gelieferte Verwaltungsinterface bekannt als „vSphere Web Client“), das zur Verwaltung der dem Kunden bereitgestellten Ressourcen verwendet wird. Dieses Interface bietet logischen Zugriff auf die Plattform, die in der Regel aus 1 vCenter, 1 Virtuellen Datacenter und 1 Cluster, plus mindestens 2 Datastores und den softwaredefinierten Netzwerkressourcen besteht.*
- *Ein „Premier Private Cloud“-vSAN-Paket besteht mindestens aus:*
 - *Drei identischen Host-Servern (die CPU, RAM und lokalen Storage für die Virtualisierung bereitstellen), die für Computing-Aufgaben bestimmt sind. Der Kunde muss sicherstellen, dass er zu jeder Zeit über drei identische Host-Server verfügt (d. h. Server mit den gleichen technischen Eigenschaften). Für den Fall, dass das Virtuelle Datacenter verschiedene Gruppen von Host-Servern enthält, so werden die 3 Hosts mit den geringeren CPU-, RAM- und vSAN-Speicherkapazitäten als „Paket“ für das Virtuelle Datacenter angesehen. Im Interesse der Klarheit: Sollte das Datacenter 3 Host-Server vSAN Premier mit „192 RAM“ und 3 Host-Server vSAN Premier mit „384 RAM“ beinhalten, so wird das betreffende „Paket“ aus den 3 Host-Servern vSAN Premier „192 RAM“ zusammengesetzt.*
 - *Zwei Datastore-Ressourcen. Für den Fall, dass das Virtuelle Datacenter verschiedene Paare von Datastore-Ressourcen enthält, wird das Paar mit der geringeren Kapazität als „Paket“ für das Virtuelle Datacenter angesehen. Im Interesse der Klarheit: Sollte das Datacenter 2 Datastore-Ressourcen mit je 2 TB and 2 Datastore-Ressourcen mit je 3 TB beinhalten, so wird das betreffende „Paket“ aus den beiden Datastore-Ressourcen mit 2 TB zusammengesetzt.*
 - *Dem VMware vSphere Interface (das von VMware gelieferte Verwaltungsinterface bekannt als „vSphere Web Client“), das zur Verwaltung der dem Kunden bereitgestellten Ressourcen verwendet wird. Dieses Interface bietet logischen Zugriff auf die Plattform, die in der Regel aus 1 vCenter, 1 Virtuellen Datacenter und 1 Cluster, plus mindestens 2 Datastores, plus der Möglichkeit, den vSAN-Datastore zu konfigurieren, und den softwaredefinierten Netzwerkressourcen besteht.*

„Point of Presence“: *Physische Standorte im OVHcloud-Netzwerk von mit dem Internet verbundenen CDN-Servern, wie im kommerziellen Angebot dargestellt (CDN-Infrastruktur, Geocache Accelerator, CDN WebStorage).*

„Reihe“: *Definiert als die Hosted-Private-Cloud-Generation, die zur Infrastruktur des Kunden hinzugefügt wird.*

„Dienst“: *Basiseinheit zur Berechnung von Service Level Agreement und Dienstgutschriften, die vom Kunden eingefordert werden können. Die Einheit wird unter demselben vCenter und auf Ebene des Virtuellen Datacenters eingerichtet und ist abhängig von der hinzugefügten Reihe. Es kann sich auch um eine Mischung verschiedener Reihen handeln, soweit diese sich im selben Virtuellen Datacenter und somit im selben vCenter befinden.*

„Speicherressource“: *Dedizierte Speicherressource (in der Regel eine Art NAS-Ressource, die als Datastore präsentiert wird), die in der Hosted Private Cloud Premier eines Kunden bereitgestellt und*

verwaltet wird. Diese Ressource nutzt Speicherplatz in der Hosted Private Cloud Premier, um zusätzliche Kapazitäten zu liefern, die über das VMware® User Interface verwaltet werden können.

„Virtualisierungsinterface“: Von OVHcloud bereitgestellte Drittpartei-Software, mit der der Kunde seine Hosted Private Cloud Premier und zugehörige Dienste verwalten und vor allem seine Virtuellen Maschinen einrichten und verwalten kann.

„Virtuelle Maschine“: Ein nicht-physischer Workload, der Ressourcen des Virtuellen Datacenters verwendet und auf dem Hosted Private Cloud Premier Netzwerk installiert wird. Jeder virtuelle Workload wird von anderen unabhängig innerhalb des Virtuellen Datacenters des Kunden verwaltet.

„Virtualisierung“: Technologie, die es möglich macht, verschiedene Betriebssysteme, virtuelle Workloads und Anwendungen auf demselben physischen Server zu betreiben.

„vRack“: Ein oder eine Gruppe von Virtual Area Networks („VLANs“), die im internen privaten Netzwerk von OVHcloud („Backbone“) eingerichtet wurden und aus Ressourcen (Servern, Speicherressourcen etc.) bestehen, die dem Kunden von OVHcloud zur Verfügung gestellt werden. Ressourcen, die sich physisch in unterschiedlichen, geografisch entfernten OVHcloud-Rechenzentren befinden, können mit dem vRack verbunden werden. Manche OVHcloud-Ressourcen sind nicht mit dem vRack kompatibel. Informationen zur Kompatibilität von OVHcloud-Ressourcen mit vRack sind auf der OVHcloud-Website verfügbar.

Artikel 1: VERTRAGSGEGENSTAND

Zweck der vorliegenden besonderen Vertragsbedingungen ist, die besonderen Bedingungen – einschließlich, aber nicht beschränkt auf die Nutzungs- und finanziellen Bedingungen – zu definieren, die für OVHcloud Hosted Private Cloud Premier Dienste (im Folgenden „der Dienst“ oder „die Dienste“) gelten. Sie ergänzen die aktuell gültigen allgemeinen Geschäftsbedingungen von OVHcloud. Im Falle eines Widerspruchs haben diese besonderen Vertragsbedingungen Vorrang vor den allgemeinen Geschäftsbedingungen von OVHcloud.

Artikel 2: BESCHREIBUNG DES DIENSTES

2.1 Übersicht

Im Rahmen des Dienstes stellt OVH (im Folgenden „OVHcloud“) dem Kunden eine Hosted Private Cloud Premier bestehend aus einem oder mehreren Virtuellen Datacentern innerhalb eines sicheren, privaten Netzwerks zur Verfügung.

Im Rahmen dieses Dienstes bereitgestellte Ressourcen sind allein dem Kunden vorbehalten.

Der Hosted Private Cloud Premier Dienst ist für professionelle Benutzer vorgesehen und ermöglicht es dem Kunden, sein eigenes gesichertes, privates Netzwerk zu verwenden.

Für den Dienst können Einschränkungen gelten (z. B. in Bezug auf die Anzahl Virtueller Maschinen, die in einer Hosted Private Cloud Premier verwendet werden können, Traffic, Bandbreite etc.). Diese Einschränkungen werden in den auf der OVHcloud-Website verfügbaren



Dokumentationen/Spezifikationen aufgeführt. Der Kunde erklärt sich bereit, diese Einschränkungen einzuhalten.

Im Rahmen des Dienstes ist der Kunde allein für die Verwaltung seiner IP-Adressressourcen verantwortlich. Es obliegt allein dem Kunden, seine IP-Ressourcen ordnungsgemäß zu verwalten und so den störungsfreien Betrieb seines Dienstes sicherzustellen. Der Kunde stellt außerdem sicher, dass stets ausreichend IP-Adressen vorhanden sind, um jedem seiner virtuellen Workloads, gegebenenfalls per Hypervisor, eine IP-Adresse zuzuweisen. Folglich ist der Kunde alleinverantwortlich für die Verwendung der IP-Adressressourcen, die im Rahmen des Dienstes zugewiesen oder gemietet werden.

Jede Hosted Private Cloud Premier verfügt über ein eigenes, gesichertes privates Netzwerk. Die von der Hosted Private Cloud Premier ausgehende Bandbreite ist auf eine maximale Datengeschwindigkeit begrenzt.

Der Kunde kann die History der Bandbreitennutzung seiner Hosted Private Cloud Premier sowie die durchschnittliche Geschwindigkeit über das Verwaltungsinterface einsehen.

OVH stellt dem Kunden eine Reihe an Paket-Konfigurationen zur Verfügung. Beschreibungen für diese Konfigurationen werden auf der OVHcloud-Website aufgeführt.

Die Produktreihe der Host-Server sowie die Auswahl des Pakets bestimmen die Funktionen, die über das Virtuelle Datacenter verfügbar sind, sowie das Leistungsniveau.

2.2 Funktionen

VIRTUALISIERUNGSINTERFACE

Der Dienst basiert auf intrinsisch enthaltenen Funktionen integrierter Drittpartei-Produkte aus dem Softwarepaket des OVHcloud-Partners VMware®, die Server- („vSphere® Hypervisors“), Netzwerk- („NSX®“) und Speicher- („vSAN®“) Visualisierung gemäß der aktuell geltenden Vertragsbedingungen von VMware® ermöglicht. Alle Drittpartei-Produkte aus dem VMware® Softwarepaket (die ein Visualisierungsinterface bilden) werden auf Ressourcen gehostet, die von OVHcloud verwaltet werden und sich außerhalb der Hosted Private Cloud Premier des Kunden befinden.

Jedes Visualisierungsinterface verfügt über eigene Funktionen. Der Kunde ist dafür verantwortlich, eine fundierte Wahl des Visualisierungsinterface zu treffen, und er ist sich darüber bewusst, dass die Wahl des vSphere® Hypervisors nicht im Nachhinein geändert werden kann. Der Kunde erkennt außerdem an, dass die vollständige Kompatibilität der Funktionen sowie die Interoperabilität zwischen Virtualisierungsinterfaces nicht garantiert werden können.

VIRTUAL MACHINE Encryption (VM Encryption)

VM Encryption nutzt eine in vSphere 6.5 und höher enthaltene Funktion zur Verschlüsselung von VM-Daten im laufenden Betrieb mithilfe eines Verschlüsselungsschlüssels, der von einer Komponente außerhalb der Hosted Private Cloud Premier geliefert wird (Box Encryption), um im Datastore der Hosted Private Cloud Premier gespeicherte Daten zu verschlüsseln.

Der Kunde ist für die Verwaltung seines Verschlüsselungsschlüssels zuständig; OVHcloud übernimmt in dieser Hinsicht keinerlei Verantwortung.

FEDERATION

Diese Funktion ermöglicht es Nutzern, ihren eigenen LDAP- (Lightweight Directory Access Protocol) Server mit ihrer Hosted Private Cloud Premier zu verbinden, um die Authentifizierung und



Identifizierung auf den vorhandenen Accounts zu verwalten. Der Kunde ist allein dafür verantwortlich, dass sein LDAP-Server über eine angemessene Konnektivität verfügt.

2FA (ZWEI-FAKTOR-AUTHENTIFIZIERUNG)

Die 2FA-Funktion bietet eine doppelte Authentifizierungsmethode für den Login in die Verwaltungsinterfaces. Zusätzlich zu einem Benutzernamen und Passwort benötigt der Kunde einen temporären Zugriffstoken für den Login. Der Kunde ist für die Generierung der Zugriffstoken verantwortlich.

vRACK

vRack ermöglicht es dem Kunden, einige oder alle von OVHcloud bereitgestellten Ressourcen (Host-Server und Speicherressourcen), darunter Ressourcen aus verschiedenen Umgebungen und/oder geografisch entfernten OVHcloud-Rechenzentren, untereinander zu verbinden. Es wird verwendet, damit Virtuelle Workloads auf dedizierten VLANs betrieben werden und diese VLANs auf andere Virtuelle Maschinen in anderen Hosted Private Clouds Premier in anderen OVHcloud-Rechenzentren oder mit anderen OVHcloud-Diensten propagiert werden können.

Das vRack des Kunden ist von anderen OVHcloud-Backbone-Komponenten logisch getrennt.

Der Kunde übernimmt die alleinige Verantwortung für die Verwaltung seines vRack und die darauf deployten Ressourcen. Der Kunde bestimmt die Zusammenstellung (verbundene Ressourcen) und logische Konfiguration (logische Netzwerk- und Subnetzwerk-Architektur) des vRack. Der Kunde verwaltet sein vRack direkt über das Verwaltungsinterface. Der Kunde kann seine eigene Infrastruktur und externen Ressourcen beispielsweise über OVHcloud Connect mit dem vRack verbinden.

2.3 Zusätzliche Dienste

Der Kunde kann im Rahmen des Hosted Private Cloud Premier Dienstes die folgenden zusätzlichen Dienste, für die die jeweiligen besonderen Vertragsbedingungen gelten, abonnieren:

- Veeam Managed Backup
- Notfallwiederherstellungsplan (Disaster Recovery Plan)
- OVHcloud Connect

Artikel 3: NUTZUNGSBEDINGUNGEN DES DIENSTES

3.1 Anspruchsberechtigung

Das Abonnement des Hosted Private Cloud Premier Dienstes ist nur für Kaufleute, Unternehmer und Profis (nicht für Privatpersonen/Verbraucher) verfügbar, die nicht dem anwendbaren Verbraucherrecht unterliegen. Abweichend von den Bestimmungen in den allgemeinen Geschäftsbedingungen gelten die Kündigungsregelungen nicht für diesen Dienst.

3.2 Abonnement

Zusätzlich zum gewählten Paket kann der Kunde auch weitere Ressourcen und Dienste, wie einen zusätzlichen Host-Server, eine Speicherressource oder im nachstehenden Anhang oder auf der OVHcloud-Website aufgeführte Optionen, zum Paket hinzufügen.

Der Kunde kann außerdem für jedes Virtuelle Datacenter zusätzliche Ressourcen abonnieren (weitere Host-Server- oder Speicherressourcen), um einen vorübergehenden oder dauerhaften Bedarf zu decken. Der Kunde hat die Wahl, ob ihm der laufende Monat oder nur die Stunden, in denen diese Ressourcen verwendet werden, berechnet werden.

3.3. Anwendbare Bedingungen

Hosted Private Cloud Premier Dienste unterliegen den geltenden Servicebedingungen, darunter die vorliegenden besonderen Vertragsbedingungen, die allgemeinen Geschäftsbedingungen von OVHcloud sowie jegliche aktuell geltenden Produktbedingungen von Drittparteien. Hosted Private Cloud Premier Dienste müssen gemäß der aktuellsten Version der zuvor genannten Servicebedingungen verwendet werden.

3.4. Pflichten und Haftung des Kunden

Der Kunde ist für die Nutzung seiner Dienste alleinverantwortlich. Hierzu gehört die Verwaltung der Token, die verwendet werden, um Authentifizierungsdaten und den Zugriff zum Dienst zu verwalten, die Verwendung der von OVHcloud zur Verfügung gestellten APIs, Software und Tools sowie die Verwaltung der Abonnements und Daten, die er in Zusammenhang mit den Diensten verwendet. Der Kunde muss über die erforderlichen technischen Kenntnisse und Kompetenzen verfügen und sich vor der Verwendung der Dienste mit deren Eigenschaften vertraut machen.

OVHcloud ist lediglich für die Instandhaltung der Infrastruktur sowie für Energieversorgung und Netzwerkanschluss der Hosted Private Cloud Premier des Kunden verantwortlich.

Der Kunde bestätigt, dass er über alle notwendigen technischen Kenntnisse verfügt, um die fachgerechte Verwaltung eines Virtualisierungsdienstes wie der OVHcloud Hosted Private Cloud Premier zu gewährleisten.

Der Kunde ist alleiniger Verwalter seiner Virtuellen Datacenter, Host-Server und Speicherressourcen. Der Kunde verpflichtet sich, den Dienst und insbesondere die zugewiesenen Netzwerkressourcen verantwortungsvoll einzusetzen, und ist dafür zuständig, sicherzustellen, dass er über ausreichend Ressourcen verfügt, um das ordnungsgemäße Funktionieren seiner Virtuellen Maschinen zu gewährleisten.

3.5 Instandhaltung

Um die Dienste bereitzustellen, führt OVHcloud Wartungsarbeiten durch. Der Kunde wird vor jeder geplanten Wartung durch mindestens eine der nachfolgend genannten Methoden darüber informiert: per E-Mail an die Adresse, die der Kunde über seinen NIC-Admin/Tech angegeben hat, durch Veröffentlichung auf der OVHcloud-Status-Website (Travaux) oder, indem der Kunde direkt per Telefon oder über andere Mittel kontaktiert wird. Diese Kommunikation wird die Art der auszuführenden Wartungsarbeiten eindeutig angeben.

3.5.1 Arten der Wartungsarbeiten

Es gibt drei (3) Arten von Wartungsarbeiten, die von OVHcloud vorgenommen werden können.

- a) Notfalländerungen bei kritischen Zwischenfällen. Diese Art der Wartung ist gekennzeichnet durch besonders dringliche und kritische Updates, Patches und/oder Änderungen der Infrastruktur, Hardware, Firmware, Software oder jeglicher anderen Komponente. Bei der Unterlassung dieser Arbeit sind unter anderem, aber nicht ausschließlich, folgende Auswirkungen möglich:

- a. Verlust der Konformität für Sicherheitszertifikate
- b. Gefährdung der Sicherheit und Stabilität des Systems
- c. Bloßlegung kritischer Schwachstellen
- d. Serviceverlust für eine breitere Kundenbasis

Sobald sich OVHcloud des Problems bewusst ist und die Auswirkungen klar erkannt hat, wird der Kunde darüber in Kenntnis gesetzt, dass wir an der Behebung des Problems arbeiten. Innerhalb von 24 Stunden werden wir den Kunden darüber informieren, welcher Prozess verfolgt wird, wann und wie dieser auf die Umgebung angewendet wird, welche Maßnahmen durchgeführt werden und wie hoch die Auswirkungen für den Kunden sind, angefangen bei geringfügigen Auswirkungen auf eine bestimmte Komponente bis hin zu schwerwiegenden Auswirkungen, die zum Ausfall einer oder aller Komponenten führen.

Da es nicht möglich ist, vorauszusagen, wie viele Schwachstellen zu einem bestimmten Zeitpunkt in einem Kalendermonat entdeckt werden, ist die Anzahl der auszuführenden Notfalländerungsarbeiten nicht begrenzt. Aufgrund der Kritikalität der auszuführenden Arbeiten können diese zu jeder Zeit während des Kalendermonats vorgenommen werden. In solchen Fällen, in denen wir von der Bereitstellung eines Patches oder Korrekturupdates durch den Herausgeber abhängig sind, muss OVHcloud diesen Zeitraum für die vollständige Korrektur um die vom Herausgeber benötigte Vorlaufzeit verlängern.

- b) Standard. Diese Wartungsarbeiten sind nicht kritisch oder dringend. Sie sind von mittlerer Kritikalität und können den Kunden allein oder das ganze Unternehmen betreffen, stellen jedoch weder ein Sicherheitsproblem noch einen Konformitätsverlust dar. Der Kunde wird mindestens zweiundsiebzig (72) Stunden im Voraus über diese Wartungsarbeiten informiert. Die Arbeiten können eine Ausfallzeit verursachen oder auch nicht. Dem Kunden wird in jedem Fall empfohlen, voranzuplanen, um eine mögliche Ausfallzeit zu vermeiden. Diese geplanten Wartungsarbeiten werden außerhalb der regulären Arbeitszeiten (normalerweise 9:00 Uhr - 17:00 Uhr) durchgeführt. Diese Arbeiten müssen vom Change Management Board genehmigt werden und sind auf zwei (2) Wartungsarbeiten pro Kalendermonat begrenzt.
- c) Normal. Diese Wartungsarbeiten haben geringe oder gar keine materiellen Auswirkungen, die zu einem Serviceverlust des Kunden führen würden. Sie können einen niedrigen bis hohen Kritikalitätsgrad aufweisen. Der Kunde wird mindestens zweiundsiebzig (72) Stunden im Voraus über die Arbeiten informiert. Diese Wartungsarbeiten haben den ordnungsgemäßen Change-Advisory-Board-Prozess durchlaufen, um genehmigt zu werden. Die Anzahl der möglichen Wartungsarbeiten ist unbegrenzt.

Als Teil des Lebenszyklusmanagements aktualisiert OVHcloud die Infrastruktur mit geplanten Wartungsarbeiten. Bei diesem Prozess werden auch die Host-Server aktualisiert. Wenn die Private-Cloud-Umgebung entsprechend dimensioniert ist (mit ausreichend freien Rechen- und Speicherressourcen), um der Automatisierung den sicheren Neustart der Host-Server zu erlauben, startet OVHcloud die Host-Server neu, damit diese ohne jegliche Ausfallzeit auf den neuesten Stand gebracht werden. Ist die Umgebung nicht entsprechend dimensioniert, um der Automatisierung einen

sicheren Neustart zu erlauben, so obliegt es dem Kunden, die Host-Server innerhalb eines (1) Monats nach Installation der neuen Version neu zu starten. Wird der Neustart nicht durchgeführt, startet die Automatisierung nach Ablauf der 30 Tage die Host-Server automatisch neu. Bei diesem Neustart ist es nicht möglich, die Host-Server in den Wartungsmodus zu versetzen, und es wird zu Ausfallzeiten kommen.

OVHcloud liefert Updates für vCenter, NSX-Optionen und vROps. Die durchgeführten Updates sind diejenigen, die von VMware veröffentlicht werden, und werden in Übereinstimmung mit den aktuell geltenden Bedingungen der Drittpartei durchgeführt. vCenter-Updates können automatische Updates des ESXi-Hypervisors nach sich ziehen.

Was ESXi-Installationen auf dedizierten Ressourcen (Host-Server) des Kunden betrifft, wird OVHcloud den Kunden wie zuvor beschrieben über Updates in Kenntnis setzen. Der Kunde ist selbst voll verantwortlich für geringfügige Updates (Patches) für ESXi und hat diese umgehend durchzuführen. Daher empfiehlt OVHcloud dem Kunden, regelmäßig nach verfügbaren Updates des VMware-Herausgebers zu suchen. Zu diesem Zweck kann der Kunde den VUM (Virtual Update Manager) von VMware verwenden. OVHcloud übernimmt keinerlei Verantwortung für Dienststörungen, die aus vom Kunden auf dem Hypervisor installierten Updates resultieren. Ebenso übernimmt der Kunde die volle Verantwortung für die Nichtdurchführung von Updates oder Upgrades für den Hypervisor.

Wenn ein Kunde ein von OVHcloud geliefertes Upgrade verweigert, so wird er keine Verbesserungen oder neue Funktionen für das Virtualisierungsinterface erhalten. OVHcloud behält sich das Recht vor, ältere Hypervisor-Versionen nicht instand zu halten oder für diese keine Verbesserungen vorzunehmen. Der Kunde muss unter Umständen zu einer neueren Version des Virtualisierungsinterface wechseln, um einen effektiven Dienstbetrieb zu gewährleisten. Ältere Hypervisor-Versionen werden als zwei Hauptversionen hinter der zuletzt von OVHcloud gelieferten Version verstanden.

Darüber hinaus behält sich OVHcloud das Recht vor, im Falle eines Sicherheitsrisikos (für den Kunden, OVHcloud und/oder Dritte), das auf die Unterlassung eines Updates auf Seiten des Kunden zurückzuführen ist, den Dienst des Kunden einzuschränken oder auszusetzen. In diesen Fällen wird OVHcloud den Kunden umgehend darüber in Kenntnis setzen.

Der Kunde ist alleinverantwortlich für die Instandhaltung und Aktualisierung von Systemen und Anwendungen, die er auf Virtuellen Maschinen installiert, die außerhalb des Wirkungsbereichs von OVHcloud liegen.

Der Kunde erkennt an, dass Hosted Private Cloud Premier Dienste ausschließlich nach Ermessen von OVHcloud, seinen Partnern und Drittpartei-Herausgebern entwickelt werden, die als Teil des Dienstes verwendete Lösungen nach ihrem eigenen Zeitplan bereitstellen. Der Kunde muss unter Umständen zu einer neueren Version der Hosted Private Cloud Premier Dienste wechseln, um einen effektiven Dienstbetrieb zu gewährleisten.

3.6 Grenzen und Einschränkungen

Der Kunde erkennt an, dass aus Sicherheitsgründen manche Funktionen und Protokolle (wie IRC- oder Peer-to-Peer-Filesharing) im Rahmen des Dienstes eingeschränkt werden können. Von der Verwendung von Proxys und Anonymisierungsdiensten im Rahmen des Dienstes wird nachdrücklich abgeraten. Anwendbare Einschränkungen werden in der auf der OVHcloud-Website verfügbaren Dokumentation aufgeführt.

Der Kunde ist dafür verantwortlich, den Dienst in Übereinstimmung mit den Benutzerlizenzen integrierter Lösungen zu verwenden. OVHcloud behält sich das Recht vor, die Einhaltung dieser Nutzungsbedingungen durch den Kunden zu überprüfen und den Dienst gemäß den im Vertrag

festgelegten Bedingungen auszusetzen, wenn der Kunde die Nutzungsbedingungen des Dienstes, geltende Gesetze und Vorschriften und/oder die Rechte von Drittparteien nicht respektiert.

Wie in der Paket-Definition beschrieben, ist für manche Funktionen gegebenenfalls eine Mindestanzahl an Host-Servern erforderlich.

3.7 Betriebskontinuität

Der Kunde wird daran erinnert, dass, sofern nicht anders vereinbart, der Hosted Private Cloud Premier Dienst weder einen Business Continuity Plan („BCP“) noch einen Disaster Recovery Plan („DRP“) enthält. Daher ist der Kunde dafür verantwortlich, einen eigenen BCP und/oder DRP einzurichten. Er kann Hosted Private Cloud Premier Dienste in unterschiedlichen Rechenzentren bestellen, um so über Ressourcen in unterschiedlichen Risikoumgebungen zu verfügen. Der Kunde muss die erforderlichen technischen und organisatorischen Maßnahmen ergreifen, um die Kontinuität seiner Geschäftstätigkeit im Falle einer größeren Störung, die die Verfügbarkeit, Integrität oder Vertraulichkeit des Dienstes beeinträchtigen könnte, gewährleisten zu können. Der Kunde kann die DRP-Option verwenden, deren besondere Bedingungen diesem Dokument angehängt sind.

3.8 Backups

OVHcloud übernimmt keinerlei Verpflichtung, was das Backup von auf der Hosted Private Cloud Premier gehosteten Kundendaten betrifft. Daher liegt es in der Verantwortung des Kunden, alle notwendigen Maßnahmen zu ergreifen, um seine Daten im Falle von Verlust, Beschädigung geteilter Daten, aus welchem Grund auch immer, zu sichern. Dies gilt auch für Daten, die nicht ausdrücklich in diesen Bedingungen genannt werden. Der Kunde kann die Backup-Option verwenden, deren besondere Bedingungen diesem Dokument angehängt sind.

Artikel 4: ABWEHR (SCHUTZ VOR DoS (Denial of Service) UND DDoS (Dynamic Denial of Service) ANGRIFFEN)

OVHcloud setzt Schutzmaßnahmen gegen DoS- und DDoS-Cyberangriffe (Denial-of-Service-Angriffe) ein, sofern diese in großem Umfang durchgeführt werden. Diese Funktion hat zum Ziel, den Dienst des Kunden über die gesamte Dauer des Angriffs funktionsfähig zu erhalten.

Die Funktion beinhaltet, Traffic von außerhalb des OVHcloud-Netzwerks zum Dienst des Kunden hin zu überprüfen. Als rechtswidrig eingestuftes Traffic wird zurückgewiesen, bevor er die Infrastruktur des Kunden erreicht, was es rechtmäßigen Benutzern ermöglicht, trotz des Cyberangriffs auf die vom Kunden bereitgestellten Anwendungen zuzugreifen.

Diese Schutzmaßnahmen greifen nicht bei anderen Cyberangriffen wie SQL-Injection, Brute Force oder der Ausnutzung von Sicherheitslücken.

Aufgrund der hohen Komplexität des Schutzdienstes unterliegt OVHcloud lediglich einer Sorgfaltspflicht. Daher ist möglich, dass ein Angriff nicht von den vorhandenen Systemen erkannt wird oder dass diese Systeme die Dienstkontinuität nicht aufrechterhalten können.

Abhängig von der Art und Komplexität des Angriffes verwendet OVHcloud verschiedene Traffic-Schutzniveaus, um seine Infrastruktur und den Dienst des Kunden zu schützen.

Die Abwehr ist nicht aktiv, solange kein Angriff von den Tools von OVHcloud erkannt wird. Daher ist der Dienst dem Angriff bis zur Aktivierung der Abwehr direkt ausgesetzt, was zu dessen Nichtverfügbarkeit führen kann.



Wenn der Angriff einmal erkannt und die Abwehr automatisch aktiviert wurde, so kann diese nicht deaktiviert werden, bevor der Angriff beendet ist.

Während die Abwehr aktiv ist, kann OVHcloud die Verfügbarkeit der Anwendungen des Kunden nicht garantieren, bemüht sich jedoch, die Auswirkungen des Angriffs auf den Dienst und die OVHcloud-Infrastruktur zu minimieren.

Sollte es dem Cyberangriff trotz aktiver Abwehrmaßnahmen gelingen, die Integrität von OVHcloud- und Kunden-Infrastrukturen zu beeinträchtigen, so wird OVHcloud seine Schutzmaßnahmen verstärken, was eine Verringerung der Dienstqualität oder die Nichtverfügbarkeit des Dienstes nach sich ziehen kann.

Schließlich ist es möglich, dass ein Teil des durch den Cyberangriff generierten Traffics nicht von den OVHcloud-Systemen erkannt wird und den Dienst des Kunden negativ beeinflusst. Die Wirksamkeit der Abwehrmaßnahmen hängt außerdem von der Konfiguration des Dienstes ab. Daher ist es Aufgabe des Kunden, sicherzustellen, dass er über die notwendigen Kompetenzen für eine fachgerechte Verwaltung verfügt.

Es wird ausdrücklich darauf hingewiesen, dass diese Abwehrmaßnahmen den Kunden nicht davon befreien, für die Sicherheit seines Dienstes zu sorgen, Sicherheitstools (Firewall etc.) zu installieren, seine Systeme regelmäßig zu aktualisieren, seine Daten zu sichern oder die Sicherheit seiner Computerprogramme (Skripte, Codes etc.) zu überwachen.

Artikel 5: MASSNAHMEN GEGEN DEN VERSAND VON SPAM AUS DEM OVHcloud-NETZWERK

OVHcloud verwendet ein System technischer Maßnahmen, um gegen den Versand betrügerischer E-Mails sowie gegen den Versand von SPAM-Mails aus seinen Infrastrukturen vorzugehen.

Zu diesem Zweck überprüft OVHcloud den ausgehenden Traffic, der über den vom Kunden verwendeten Dienst an Port 25 (SMTP-Server) versendet wird. Dieser Vorgang beinhaltet Traffic-Monitoring durch automatische Systeme.

E-Mails werden weder gefiltert noch abgefangen, sondern mit einer Verzögerung von wenigen Sekunden überprüft. Diese Operationen werden parallel und nicht frontal zwischen dem Server und dem webbasierten Netzwerk durchgeführt.

Ebenso wird kein Eingriff an den versendeten E-Mails vorgenommen: OVHcloud nimmt keine Markierung (Tag) der E-Mails vor und ändert in keiner Weise die vom Kunden versendeten Nachrichten. Abgesehen von statistischen Daten werden bei diesen Operationen keinerlei Daten gespeichert.

Dieser Vorgang wird regelmäßig und vollautomatisch durchgeführt. Für das Monitoring des Traffics an Port 25 (SMTP-Port) erfolgt keinerlei menschliche Intervention.

Werden mehrere E-Mails, die vom Server des Kunden aus versendet wurden, als SPAM- oder Phishing-Mails identifiziert, so informiert OVHcloud den Kunden darüber per E-Mail und sperrt den SMTP-Port für die betreffende IP.

OVHcloud speichert keine Kopien der vom SMTP-Port des Dienstes aus gesendeten E-Mails, selbst wenn diese als SPAM identifiziert wurden.

Der Kunde kann über sein Verwaltungsinterface die Entsperrung des SMTP-Ports anfordern.

Jede weitere E-Mail, die als SPAM identifiziert wird, führt zur erneuten Sperrung des SMTP-Ports für einen längeren Zeitraum.

Ab der dritten Sperrung behält sich OVHcloud vor, jede weitere Anfrage zur Entsperrung des SMTP-Ports abzulehnen.

Artikel 6: SERVICE LEVEL AGREEMENT

Um das nachstehend definierte Service Level Agreement in Anspruch zu nehmen, muss der Kunde:

- i. über mindestens zwei identische Host-Server mit den gleichen technischen Eigenschaften verfügen (d. h. für CPU & RAM müssen identische Komponenten verwendet werden); für die vSAN-Produktreihe sind mindestens drei identische Host-Server erforderlich,
- ii. die High-Availability-Option („HA“, und zugehörige Komponenten) auf seinem Virtualisierungsinterface aktivieren.

Wartungsarbeiten (wie definiert in Artikel 3.5.1) mit expliziten Auswirkungen sind vom Service Level Agreement („SLA“) ausgenommen.

Das SLA wird auf einer Dienstebene basierend auf dem Virtuellen Datacenter und der hinzugefügten Reihe angewendet. Wenn der Kunde über ein (1) Virtuelles Datacenter verfügt, dessen Host-Server alle von derselben Reihe stammen, so gilt ein individuelles SLA für dieses Virtuelle Datacenter. Wenn der Kunde über verschiedene Reihen innerhalb desselben vCenters und über ein Virtuelles Datacenter mit verschiedenen Reihen verfügt, so wird das SLA auf Basis der betroffenen Reihe berechnet. Falls eine geteilte Komponente, die von einer oder mehreren Reihen verwendet wird, vorhanden ist, so wird dies als individuelle Störungen behandelt, sodass der Kunde mehrere Dienstgutschriften beanspruchen kann, falls und wenn eine geteilte Komponente (d. h. SSL Gateway, vCenter oder eine andere geteilte Komponente) beeinträchtigt und von Nichtverfügbarkeit betroffen ist.

Wenn der Kunde beschließt, von einer bestimmten Reihe auf eine andere zu migrieren – unabhängig davon, ob es sich dabei um eine neue, höhere oder niedrigere Reihe handelt – so bestimmt die Ziel-Reihe, welche besonderen Vertragsbedingungen und SLA von diesem Zeitpunkt an gelten.

Die monatliche Verfügbarkeitsrate dieses SLA ist für den gesamten Dienst auf 99,9 % festgesetzt. Wenn sie auf unter 99,9 % fällt, stehen dem Kunden 10 % des monatlichen Dienstes zu. Wenn sie auf unter 99 % fällt, stehen dem Kunden 30 % des monatlichen Dienstes zu.

Die Verpflichtung bei der Lieferung eines Ersatz-Hosts beträgt 43 Minuten.

Dienstgutschriften sind durch Öffnen eines Anfragen-Tickets zu beantragen. Der Kunde hat diese Dienstgutschriften nicht später als 30 Tage nach Auftreten der Störung zu beantragen.

„**Monatliche Verfügbarkeitsrate**“ bezeichnet die Gesamtminutenzahl des betreffenden Monats abzüglich der Anzahl der Minuten, in denen der Dienst im betreffenden Monat nicht verfügbar war, geteilt durch die Gesamtminutenzahl des betreffenden Monats. Für die Berechnung von Dienstgutschriften werden Zeiten von Nichtverfügbarkeit ab Beginn der Störung, bis das Problem behoben und von OVHcloud über die Problemlösung kommuniziert wurde, berechnet.

„**Nichtverfügbarkeit**“ bezieht sich hier auf:

- Für Host-Server (einschließlich vSAN): Zugriff auf (einen oder mehrere) dem Kunden bereitgestellte Host-Server aufgrund einer Störung oder Ausfallzeit der Host-Server nicht möglich. Ausfallzeiten und Störungen, die den Zugriff auf Host-Server nicht verhindern, werden auch dann nicht als Nichtverfügbarkeit angesehen, wenn eine Verringerung des Leistungsniveaus der Infrastruktur beobachtet wird. Wird ein Host-Server durch den Kunden oder aufgrund einer geplanten und angekündigten Wartungsarbeit neu gestartet, so wird das Monitoring der Verfügbarkeit des Host-Servers dreißig (30) Minuten nach dem Neustart fortgesetzt.
- Für Speicherressourcen (ausschließlich vSAN): Zugriff auf Speicherressourcen (inklusive zusätzlicher NFS Datastores) aufgrund einer Störung oder Ausfallzeit der Speicherressourcen nicht möglich. Ausfallzeiten und Störungen, die den Zugriff auf Host-Server nicht verhindern, werden nicht als Nichtverfügbarkeit angesehen.
- Für Netzwerk und Konnektivität: Zugriff auf Host-Server und/oder Speicherressourcen aufgrund einer Störung oder Ausfallzeit des Netzwerk- oder Konnektivitätsequipments nicht möglich. Ausfallzeiten und Störungen des Netzwerk- oder Konnektivitätsequipments, die den Zugriff auf Host-Server oder Speicherressourcen nicht verhindern, werden auch dann nicht als Nichtverfügbarkeit angesehen, wenn eine spürbare Verringerung des Leistungsniveaus der Infrastruktur beobachtet wird.
- Für Virtualisierungsinterfaces: Verwendung von einigen oder allen Virtualisierungsinterface-Funktionen aufgrund eines Problems im Zusammenhang mit der Anwendung nicht möglich (ausschließlich Fehler und Bugs in VMware-Produkten sowie Konfigurationsprobleme und -störungen aufgrund unzureichender Wartung oder Aktualisierung der Anwendung, was weiterhin in den Verantwortungsbereich des Kunden fällt).

Dienstgutschriften aufgrund von Nichteinhaltung des Service Level Agreements stellen einen festen Pauschalbetrag für jeglichen Schaden oder Verlust dar, der aus dieser Nichteinhaltung resultiert. Daher wird der Kunde darüber hinaus keine weiteren Forderungen stellen und/oder rechtlichen Schritte einleiten.

Sollte ein einziges Ereignis zur Nichteinhaltung mehrerer Verpflichtungen des SLA für denselben Dienst führen, können die Dienstgutschriften nicht kumuliert werden. In diesen Fällen wird die für den Kunden vorteilhafteste Dienstgutschrift angewendet.

Der kumulative monatliche Gesamtbetrag (für alle Störungen und SLAs zusammen) der von OVHcloud zu bezahlenden Dienstgutschriften ist auf 30 % der monatlichen Kosten des betroffenen Dienstes begrenzt.

Dienstgutschriften werden ausgestellt, falls und wenn der Kunde alle ausstehenden Rechnungen beglichen hat, und werden von der Rechnung für den Monat nach Erhalt der Forderung des Kunden bei OVHcloud abgezogen, vorausgesetzt, alle früheren und ausstehenden Rechnungen wurden bereits vom Kunden beglichen.

Wenn eine Aktion des Kunden erforderlich ist, um eine Diagnose anzustellen oder eine Störung zu beheben, und der Kunde nicht erreichbar ist oder nicht mit OVHcloud kooperiert, wird die entsprechende Zeitspanne nicht als Zeitraum von Nichtverfügbarkeit, Eingriff oder Wiederherstellung gezählt.

Eine Dienstgutschrift wird nicht fällig, wenn die Nichteinhaltung des SLA zurückzuführen ist auf (i) Ereignisse und Faktoren, die außerhalb der Kontrolle von OVHcloud liegen, einschließlich, aber nicht beschränkt auf Fälle höherer Gewalt, ein Verschulden Dritter, Pandemie, Fehler oder fehlerhafte Bedienung der Hardware oder Software unter der Kontrolle des Kunden, (ii) Verletzung der Pflichten aus diesem Vertrag durch den Kunden (z. B. unterlassene Mitwirkung bei der Behebung einer Störung oder der Bestätigung eines Tokens auf Anfrage von OVHcloud), (iii) unsachgemäße oder zweckwidrige Verwendung des Dienstes durch den Kunden (z. B. eine fehlerhafte Netzwerkkonfiguration, Überlastung der Speicherressourcen, zweckwidrige Verwendung der Systeme, Software oder anderer vom Kunden im Rahmen des Dienstes verwendeter Elemente), (iv) geplante Wartungsarbeiten, (v) eine Aussetzung von Diensten gemäß Artikel 3 der allgemeinen Geschäftsbedingungen von OVHcloud oder (vi) einen Hackerangriff oder Softwarepiraterie. In diesen Fällen und vorbehaltlich Punkt (iv) behält sich OVHcloud das Recht vor, dem Kunden gegebenenfalls Maßnahmen zur Wiederherstellung der Verfügbarkeit zu berechnen. Solche Maßnahmen werden auf einer Rechnung ausgewiesen, die dem Kunden zur Genehmigung eingereicht wird.

Ursachen der Nichtverfügbarkeit, insbesondere in den oben beschriebenen Ausschlussfällen, können mit allen Mitteln auf der Grundlage von aus dem Informationssystem von OVHcloud stammenden Beweisen (wie z. B. Verbindungsdaten) festgestellt werden, die aufgrund ausdrücklicher Vereinbarung zulässig sind.

Artikel 7: LAUFZEIT, ABRECHNUNG, VERLÄNGERUNG UND BEENDIGUNG DES DIENSTES

7.1 Laufzeit

Der Kunde willigt ein, den Dienst für die gesamte bei Bestellung gewählte Dauer des Abonnements zu verwenden.

- Während des Verpflichtungszeitraums ist der Kunde für die unter die Verpflichtung fallende Ressource:
 - dazu berechtigt, seine Hosted Private Cloud Premier auf eine höhere Hosted Private Cloud Premier Referenz (höher bedeutet hier mit mehr RAM- und CPU-Ressourcen je Host-Server) zu upgraden. In diesem Fall erneuert der Kunde die Dauer seines Abonnements um dieselbe Laufzeit wie die ursprünglich gewählte. Der Kunde ist für die Verwaltung der Fälligkeitsdaten all seiner Hosted Private Cloud Premier Produkte zuständig. Die Upgrade-Flexibilität ist auf eine Änderung pro Verpflichtungszeitraum begrenzt.
 - nicht dazu berechtigt, seine Hosted Private Cloud Premier zu downgraden. Sollte der Kunde den Dienst downgraden, für den die vertragliche Verpflichtung gilt, so werden die Preise des Dienstes auf die öffentlich auf der OVHcloud-Website aufgeführten Preise zurückgesetzt.
- Nach Ablauf dieser Erstlaufzeit wird das Benutzerabonnement automatisch für aufeinanderfolgende Zeiträume gleicher Dauer zum ermäßigten Preis auf Grundlage des gewählten Verpflichtungsniveaus und unter denselben Bedingungen wie im ursprünglichen Vertrag verlängert. Wenn der Kunde die automatische Verlängerung über das

Verwaltungsinterface deaktiviert hat, so wird der Preis unverbindlich auf den öffentlichen Preis angepasst.

Die anwendbaren Preise und Zahlungsarten sind auf der OVHcloud-Website einsehbar.

Bei der Bestellung wählt der Kunde die anfängliche Laufzeit seines Dienst-Abonnements („Erstlaufzeit“). Die Erstlaufzeit beginnt an dem Tag, an dem der Dienst aktiviert wird. Nach Ablauf der Erstlaufzeit wird der Dienst automatisch für aufeinanderfolgende Zeiträume gleicher Dauer („Verlängerungsintervall(e)“) verlängert, es sei denn, der Dienst wird mit einer geänderten Laufzeit verlängert oder in Übereinstimmung mit den oben genannten Bedingungen bzw. den aktuell geltenden allgemeinen Geschäftsbedingungen gekündigt.

Die Verpflichtung gilt nicht für die folgenden Dienste: (i) Backup-Dienst (ii) Disaster-Recovery-Plan-Dienst.

Darüber hinaus kann der Vertrag gemäß den allgemeinen Geschäftsbedingungen von OVHcloud beendet werden.

Der Kunde kann eine Konfigurationsänderung des abgerechneten Dienstes vornehmen. In diesem Fall wird dem Kunden die Umstellung auf eine höhere Konfiguration entsprechend dem für die neue Konfiguration zum Zeitpunkt der Anfrage geltenden Preis, der auf der OVHcloud-Website einsehbar ist, in Rechnung gestellt.

Der Lieferzeitpunkt wird von OVHcloud auf Basis der in seinem Informationssystem verfügbaren Daten festgestellt, die authentisch und für den Kunden vollständig bindend sind.

7.2 Abrechnung

Bei der Bestellung sowie bei jeder Verlängerung des Dienstes wird eine Rechnung erstellt und automatisch über das vom Kunden hinterlegte Zahlungsmittel beglichen. Der Kunde willigt ein, zu jeder Zeit ein gültiges Zahlungsmittel aus den verfügbaren Zahlungsmethoden zu hinterlegen.

Der Kunde verpflichtet sich, auf seinem Bankkonto sowie dem verwendeten Zahlungsmittel stets über ausreichende Mittel zu verfügen, damit seine Rechnungen innerhalb der vereinbarten Fristen beglichen werden können.

Wenn es OVHcloud nicht möglich ist, die Kosten vom zugehörigen Zahlungsmittel abzubuchen, so wird der Kunde per E-Mail dazu aufgefordert, den ausstehenden Betrag seiner Rechnung schnellstmöglich zu begleichen. Wird der Betrag nicht gezahlt, so wird OVHcloud den Dienst von Rechts wegen sperren.

7.3 Verlängerung

Der Kunde kann die Dauer künftiger Verlängerungsintervalle seiner Dienste über sein Verwaltungsinterface ändern, solange dies mindestens 24 Stunden vor Ablauf der Erstlaufzeit bzw. des laufenden Verlängerungsintervalls erfolgt.

Wenn die Erstlaufzeit nicht am ersten Tag des Kalendermonats beginnt (Vertragsbeginn im laufenden Monat), wird der Verlängerungszyklus des Dienstes bei der ersten Verlängerung an den Kalenderzyklus angepasst, sodass die nachfolgenden Verlängerungsintervalle am ersten Tag eines Kalendermonats

beginnen. (Zum Beispiel: Ein erstmals am 24. Mai 2017 für eine Laufzeit von einem (1) Jahr bestellter Dienst wird bei der automatischen Verlängerung zum Ablauf der Erstlaufzeit am 24. Mai 2018 bis zum 31. Mai 2019 verlängert.)

Wenn der Kunde nicht wünscht, dass ein Dienst nach Ablauf der Erstlaufzeit bzw. des laufenden Verlängerungsintervalls („Verlängerungsdatum“) automatisch verlängert wird, muss er die automatische Zahlungsfunktion in seinem Verwaltungsinterface deaktivieren.

Damit die Deaktivierung wirksam wird und die Kündigung des Dienstes nach Ablauf der Erstlaufzeit bzw. des laufenden Verlängerungsintervalls nach sich zieht, muss die automatische Zahlungsfunktion unter folgenden Bedingungen deaktiviert werden:

- a. Was Dienste mit monatlichem Verlängerungszyklus betrifft, spätestens am 19. Tag des Kalendermonats vor 23 Uhr (Pariser Ortszeit).
- b. Was Dienste mit nicht-monatlichem Verlängerungszyklus betrifft (vierteljährlich, halbjährlich, jährlich etc.), spätestens am 19. Tag des Kalendermonats vor dem Verlängerungsdatum vor 23 Uhr Pariser Ortszeit. (Zum Beispiel: Um einen Dienst, der im Juni 2018 für ein (1) Jahr abonniert wurde, nach Ablauf seiner Erstlaufzeit zu kündigen, muss die automatische Zahlung vor dem 19. Mai 2019, 23 Uhr Pariser Ortszeit, deaktiviert werden).

Wenn die automatische Zahlung gemäß den vorstehenden Bestimmungen deaktiviert wurde, wird der betreffende Dienst zum Ablauf der Erstlaufzeit bzw. des laufenden Verlängerungsintervalls („Ablaufdatum“) automatisch beendet und gelöscht, und zwar einschließlich aller vom Kunden im Rahmen dieses Dienstes gespeicherten Inhalte und Daten. Es obliegt allein dem Kunden, alle notwendigen Maßnahmen zu ergreifen, um die Erhaltung seiner Inhalte und Daten rechtzeitig vor der Beendigung des Dienstes sicherzustellen.

Allerdings hat der Kunde weiterhin die Möglichkeit, den betreffenden Dienst 24 Stunden vor dessen Ablaufdatum zu verlängern, indem er entweder die automatische Zahlungsfunktion erneut aktiviert oder die Zahlung für das nächste Verlängerungsintervall im Voraus leistet.

Die Laufzeit sowie die Bedingungen für Verlängerung und Kündigung mancher mit dem Dienst verbundener Optionen oder Funktionen können sich von den für den Dienst geltenden Bestimmungen unterscheiden. Es liegt in der Verantwortung des Kunden, hierauf zu achten.

7.4 Beendigung des Dienstes

Im Falle von Nichtverlängerung oder Kündigung des Hosted Private Cloud Premier Dienstes, aus welchem Grund auch immer, werden alle enthaltenen Virtuellen Workloads, Daten und Informationen automatisch und unwiderruflich gelöscht (einschließlich Backups und Duplizierungen).

Der Kunde ist dafür verantwortlich, vor Ablauf des Hosted Private Cloud Dienstes bzw. vor Kündigung oder Entfernen eines Hosted Private Cloud Dienstes alle für eine kontinuierliche Speicherung erforderlichen Backups und Datentransfers vorzunehmen.

OVHcloud löscht und zerstört Festplatten nach Beendigung eines Dienstes entsprechend festgelegter, dokumentierter Verfahren:

- Das Löschen von Daten auf Festplatten oder Arrays geschieht durch das Überschreiben von Daten (Vernichtung durch Überschreiben, ein Durchgang).

- Das Löschen von Daten auf SSD-Festplatten oder -Arrays geschieht durch das logische Lösungsverfahren (Blocklöschen, ein Durchgang) oder durch Entfernen des Verschlüsselungsschlüssels (PSID-Revert).
- Wenn ein Speichergerät aus seinem Rack entfernt wird, werden die Daten in allen Fällen vor Entfernen aus dem Rack gelöscht. Tritt während des Löschvorgangs ein Fehler auf, wird das Gerät zerstört.
- Speichergeräte werden mithilfe dedizierter Maschinen in einem sicheren Bereich in jedem Rechenzentrum zerstört.

Artikel 8: SCHLUSSBESTIMMUNGEN

8.1 Rechnungsstellung

OVHcloud bietet möglicherweise, wie auf der OVHcloud-Website beschrieben, verschiedene Arten der Preisgestaltung für dasselbe Produkt an. Es obliegt dem Kunden, die Preisangebote zu verwalten und sicherzustellen, dass das gewählte Angebot seinen Anforderungen entspricht. Im Interesse der Klarheit: Das stündliche Preisangebot kann teurer ausfallen als das monatliche Abonnement. Kunden werden entsprechend dem abonnierten Angebot und nach Verbrauch abgerechnet.

OVHcloud kann den Kunden vor Ende des laufenden Monats zur Zahlung der Beträge seiner Infrastruktur, seines Verbrauchs und/oder seiner für den laufenden Monat abonnierten Optionen auffordern, sobald der Gesamtbetrag den von OVHcloud für den Kunden genehmigten ausstehenden Betrag übersteigt. Darüber hinaus behält sich OVHcloud das Recht vor, den Kunden zur Zahlung einer Sicherheitsleistung aufzufordern, die den Verbrauch des Kunden deckt.

Im Interesse der Klarheit: Wenn der Kunde eine Private Cloud Premier am 15. Tag eines gegebenen Monats abonniert, so wird ihm eine 30-tägige Vorauszahlung in Rechnung gestellt und abgebucht. Zu Beginn des nächsten Kalendermonats, nach dem Abonnement der Dienste, und falls der Kunde dasselbe Produkt und genau dieselben Optionen behält, stellt OVHcloud eine Rechnung für den Rest des laufenden Monats aus. Diese Rechnung wird dann zur vollständigen Bezahlung an den Kunden versendet. Nach dieser Regularisierung werden alle Rechnungen für dasselbe Produkt, mit denselben Optionen, zu Beginn der nachfolgenden Kalendermonate in Rechnung gestellt, solange der Kunde den Dienst abonniert. Sollte der Kunde zu irgendeinem Zeitpunkt zusätzliche Ressourcen (Host-Server, Speicherressourcen) während eines Kalendermonats hinzufügen, wird der gleiche Prozess erneut angewendet, um alle Rechnungen zu Beginn eines Kalendermonats zu synchronisieren und diese Ordnung beizubehalten.

8.2 Zusätzliche Ressourcen

Der Kunde kann, auf Anfrage, die Speicherressource erhöhen und/oder Host-Server zu seinem Virtuellen Datacenter hinzufügen. Diese zusätzlichen Infrastrukturen werden dem Kunden gemäß den zum Zeitpunkt des Abonnements anwendbaren und auf der OVHcloud-Website verfügbaren Preisen in Rechnung gestellt und werden direkt per Lastschrift bezahlt.

8.3 Pay as you go

Zusätzliche Infrastruktur (Host-Server, Speicherressourcen etc.) sowie zusätzliche Optionen können auch stündlich abgerechnet werden. In diesem Fall wird OVHcloud am Ende des laufenden Monats den Gesamtbetrag für die vom Kunden für den laufenden Monat abonnierten, stündlich abgerechneten Dienste in Rechnung stellen. Jede angefangene Stunde wird berechnet. Die Rechnung wird am Ende des Monats ausgestellt und direkt per Lastschrift bezahlt.

8.4 Abrechnungszeitraum und Zahlungsverzug

Alle Dienste werden monatlich für einen Monat im Voraus in Rechnung gestellt und direkt per Lastschrift bezahlt. Jeder Zahlungsverzug bei Fälligkeit, einschließlich teilweiser Zahlungen, führt zu einer Dienstunterbrechung. Falls eine Zahlungserinnerung per E-Mail vier (4) Tage nach Benachrichtigung ungelöst bleibt. Folgen für einen Zahlungsverzug sind:

- 1) Der Kunde kann keine Dienste hinzufügen.
- 2) Sieben (7) Tage nach Dienstunterbrechung ist OVHcloud dazu berechtigt, (i) den Dienst endgültig abzuschalten und (ii) sämtliche auf der Infrastruktur gespeicherten Daten zu löschen.

ARTIKEL 9: LEBENSZYKLUSRICHTLINIEN

OVHcloud wird innerhalb von sechs (6) Monaten nach dem Start einer neuen Generation jeder Hosted Private Cloud für die neue und vorherige Generationen die genauen Daten für die folgenden Begriffe bekanntgeben:

- **End of Sales.** Dies bezeichnet den Zeitpunkt, ab dem die vorherige Generation eingestellt wird. Nach dem End of Sales für eine bestimmte Hosted Private Cloud Generation können Kunden weiterhin vergrößern und einzelne zusätzliche Host-Server hinzufügen. Es werden jedoch keine Pakete von dieser vorherigen oder jeglicher anderen Generation davor mehr erhältlich sein. Es werden Pakete für die neue Hosted Private Cloud Generation auf den Markt gebracht.
- **End of Support.** Dies bezeichnet den Zeitpunkt, ab dem die vorherige Hosted Private Cloud Generation von OVHcloud keinen Support mehr erhält, einschließlich, aber nicht beschränkt auf, keine automatischen Ersatzteile, nur auf einer kommerziell vernünftigen Aufwandsbasis aufgrund begrenzter Lagerbestände. Die Lieferung solcher Hosts wird nicht innerhalb eines bestimmten Zeitrahmens garantiert und das SLA wird ebenfalls auf 99 % begrenzt.
- **End of Life.** Dies bezeichnet den Zeitpunkt, ab dem die Auslaufgeneration eingestellt wird, keine weiteren Verkäufe einzelner Hosts mehr möglich sind, kein SLA und keine Support-Dienste mehr für die Hosted Private Cloud Generation, die dieses Stadium erreicht hat, bereitgestellt werden. Kunden können vorübergehend bis zur endgültigen Beendigung der Reihe weiter auf dieser Hardware-Generation verbleiben, mit einer maximalen Karenzzeit von 3 Monaten nach diesem Datum. OVHcloud behält sich das Recht vor, keine Karenzzeit zu gewähren. Es wird ausdrücklich empfohlen, auf die neueste verfügbare Generation zu wechseln.

Weitere Begriffe im Zusammenhang mit dem Lebenszyklus der Hosted Private Cloud sind die folgenden:

- **Beta.** Dies bezeichnet eine Phase, in die ein Produkt eintreten kann oder auch nicht, um es Kunden zu ermöglichen, das Produkt zu testen, bevor es allgemein verfügbar ist. Während dieser Phase gibt es weder ein SLA noch offiziellen Support. Ein Produkt in der Beta-Phase sollte niemals in Produktion verwendet werden.
- **General Availability.** Dies ist das Datum, an dem das Produkt für den gesamten Markt verfügbar wird. Es ist das Datum, an dem das Produkt gestartet wird. An diesem Punkt geht die vorherige Generation des Produkts automatisch für Pakete in die End-of-Sales-Phase über.
- **End of Marketing.** Dies wird nach alleinigem Ermessen von OVHcloud verwendet. Während des Lebens eines Produkts werden Marketingmaßnahmen durchgeführt. OVHcloud kann zu jeder Zeit ohne Benachrichtigung der Kunden beschließen, in diese Phase einzutreten.
- **Support for Middleware.** OVHcloud bietet innerhalb deren letzten beiden (2) Hauptversionen Support für Drittpartei-Software. OVHcloud empfiehlt seinen Kunden, auf die neueste bei OVHcloud verfügbare Version zu upgraden. Support für Drittpartei-Software wird so lange angeboten, wie der Herausgeber solcher Software das Produkt allgemein verfügbar hält, öffentlichen Support dafür beibehält und unter denselben Bedingungen anbietet. OVHcloud behält sich das Recht vor, das Angebot von Drittpartei-Software zu jedem beliebigen Zeitpunkt einzustellen. OVHcloud wird Kunden mindestens 3 Monate im Voraus über eine solche Änderung in Kenntnis setzen.

ANHANG 1

VERTEILUNG DER AUFGABEN UND VERANTWORTUNG ZWISCHEN DEM KUNDEN UND OVHcloud

	OVHcloud	KUNDE
Instandhaltung		
Hardware der Private-Cloud-Infrastruktur	X	
Virtualisierungsinterface	X	X
Vom Kunden installierte Software		X
Von OVHcloud bereitgestellte Software	X	
Backup		
Virtuelle Maschine und Kundeninhalte		X
Von OVHcloud bereitgestellte Konfigurationen	X	
Wartung von VEEAM Backup	X	
Verwendung von VEEAM Backup (einschließlich der Gewährleistung von angemessener Backup-Leistung und -Integrität)		X
Dienstbetrieb		
Verwaltung		X
Verfügbarkeit der Infrastruktur	X	
Reversibilität		
Datenrückgewinnung		X
Datenlöschung bei Beendigung	X	
Sicherheit		
Hosted Private Cloud Infrastruktur	X	
In der Hosted Private Cloud gehostete virtuelle Architektur		X
Sichern von VM-Inhalten		X
PCI-DSS-SPEZIFISCH		
In PCI DSS aufzunehmen		

ANHANG 2 VEEAM MANAGED BACKUP

Das vorliegende Dokument beschreibt die anwendbaren besonderen Vertragsbedingungen für den Veeam Managed Backup Dienst, der von OVHcloud als Teil des Hosted Private Cloud Dienstes angeboten wird, (nachfolgend als „Backup-Option“ oder „Veeam Managed Backup“ bezeichnet) und legt diese fest. Es ergänzt die besonderen Vertragsbedingungen der Hosted Private Cloud Premier und stellt einen integralen Bestandteil dieser Bedingungen dar. Im Falle von Abweichungen hat dieser Anhang Vorrang.

Beschreibung: Die Backup-Option erlaubt dem Kunden Backups der Virtuellen Maschinen auf seiner Hosted Private Cloud Premier sowie der auf diesen gespeicherten Daten (nachfolgend das „Backup“) durchzuführen. Diese Backup-Funktion ist in die Verwaltungs- und Virtualisierungsinterfaces integriert. Bei der Backup-Option handelt es sich um einen optionalen Dienst, der nicht standardmäßig in den Kosten des Hosted Private Cloud Premier Dienstes enthalten ist. Diese Option muss Gegenstand einer spezifischen Bestellung oder Aktivierung sein und führt zu einer zusätzlichen Abrechnung.

Software: Die Software, die dem Kunden die Nutzung der Backup-Option ermöglicht, wurde von Drittanbietern entwickelt („Drittpartei-Produkte“). OVHcloud ist nicht an der Erstellung und Entwicklung dieser Drittpartei-Produkte, die dem Kunden als Teil der Option zur Verfügung gestellt werden, beteiligt. Aus diesem Grund ist OVHcloud nicht verantwortlich für Drittpartei-Produkte, die als Teil des Dienstes bereitgestellt werden, was technische Fehler, Sicherheitsschwachstellen, Inkompatibilitäten und Instabilität beinhalten kann, und übernimmt keinerlei Garantie für Drittpartei-Produkte, die als Teil des Dienstes zur Verfügung gestellt werden. Der Kunde ist nur dazu berechtigt, die von OVHcloud im Rahmen des Dienstes bereitgestellten Drittpartei-Produkte gemäß den aktuell geltenden anwendbaren Nutzungsbedingungen der Drittpartei zu verwenden. Dies schließt insbesondere jede Möglichkeit der Dekompilierung, des Zugriffs auf Quellen, der Neuinstallation auf anderen Infrastrukturen und der Vergabe von Unterlizenzen für die zur Verfügung gestellten Drittpartei-Produkt-Programme oder -Systeme aus. OVHcloud und der Drittanbieter behalten sich das Recht vor, die Drittpartei-Produkte jederzeit zu ändern.

Mechanismen der Backup-Option: Backups werden unter Verwendung des „Veeam Managed Backup“-Drittpartei-Produkts durchgeführt. Über das OVHcloud Kundencenter. Der Kunde aktiviert die Veeam Managed Backup Option über sein Verwaltungsinterface und kann aus drei Angebotsniveaus wählen: „Standard, Advanced oder Premium“. Sobald eines dieser Angebote ausgewählt und auf der Hosted Private Cloud des Kunden aktiviert wurde, ist dieses das einzige Angebot, das für das Backup all seiner Virtuellen Maschinen verfügbar ist. Die Anzahl der inkrementellen Backups, vollständigen Backups und verfügbaren zusätzlichen Funktionen ist abhängig vom über das Verwaltungsinterface gewählten Dienstniveau. Backups werden nicht standardmäßig repliziert, und sind nur für höhere Angebote verfügbar. Bei jedem Update wird automatisch über eine Kontrollanwendung eine Konsistenzprüfung zwischen der gesicherten Virtuellen Maschine und ihrem Backup durchgeführt. Diese Überprüfung betrifft ausschließlich die Konsistenz der Backup-Datei gegenüber der Quelldatei und überprüft nicht die Integrität des Backups oder der in ihm enthaltenen Daten. Falls hierbei eine Inkonsistenz oder ein Fehler festgestellt wird, wird vom System automatisch ein neues Backup durchgeführt. Falls hierbei eine Inkonsistenz oder ein Fehler festgestellt wird, wird dies im täglichen, dem Kunden übermittelten Backup-Bericht erwähnt. Diese Konsistenzprüfung ist eine Verpflichtung der Mittel (wirtschaftlich vertretbare Anstrengungen) und OVHcloud übernimmt keinerlei Verantwortung oder Haftung im Falle eines Scheiterns dieser Prüfung oder einer Schädigung der gesicherten oder duplizierten Daten. Die Backup-Optionen wurden für das Backup Virtueller Maschinen konzipiert, die zwei (2) Terabyte nicht überschreiten.

Speicherplatz: Die der Backup-Option zugewiesenen Speicherressourcen werden geteilt. Die dem Kunden zugewiesenen Speicherressourcen werden logisch von den anderen OVHcloud-Kunden zugewiesenen Ressourcen isoliert und sind physisch von der Infrastruktur, auf der der Kunde seine Hosted Private Cloud Premier eingerichtet hat, getrennt. Der für die Backup-Option verwendete Speicherplatz befindet sich in demselben Rechenzentrum wie der Hosted Private Cloud Premier Dienst, für den das Backup durchgeführt wird. Es liegt in der Verantwortung des Kunden, sicherzustellen, dass der Standort des Rechenzentrums seinen Bedürfnissen und Anforderungen entspricht.

Nutzungsbedingungen: Der Kunde ist alleinverantwortlich für die Verwendung der Backup-Option und insbesondere (a) für die Auswahl der zu sichernden Virtuellen Maschinen auf seiner Hosted Private Cloud, (b) für die Überprüfung der ordnungsgemäßen Durchführung der Backups, (c) für die Überprüfung der Backup-Integrität mit den vom Kunden als angemessen erachteten Tools, und, (d) im Falle eines Fehlers, für die Durchführung einer neuen Backup-Operation falls nötig durch Kontaktieren des OVHcloud-Kundendienstes. OVHcloud verwaltet weder Backup- noch Wiederherstellungsoperationen, die als Teil des Dienstes durchgeführt werden. OVHcloud kann im Falle von Ausfall, Fehlfunktion oder Fehler in den Backup-Operationen nicht verantwortlich gemacht werden. Der Kunde erklärt sich bereit, die Entdeckung einer Fehlfunktion, eines Fehlers oder einer Schwachstelle in der Backup-Operation umgehend zu melden. Der Kunde trägt die alleinige Verantwortung für den Inhalt seiner Backups. Der Kunde stellt sicher, dass er über die erforderlichen Rechte verfügt und die geltenden Vorschriften einhält. OVHcloud hat keinerlei Kenntnis über den Inhalt und die Aktivitäten, für die der Kunde die Backup- und Wiederherstellungslösung verwendet. Die Backup-Option kann gemäß den für den Hosted Private Cloud Premier Dienst geltenden allgemeinen Geschäftsbedingungen und besonderen Vertragsbedingungen ausgesetzt und unterbrochen werden. OVHcloud unterliegt einer Sorgfaltspflicht.

Rechnungsstellung: Die Rechnungsstellung an den Kunden richtet sich nach (i) der Anzahl der gesicherten Virtuellen Maschinen, (ii) der Größe der gesicherten Virtuellen Maschinen und (iii) dem gewählten Backup-Dienst.

Beendigung der Dienste: Im Falle von Löschen, Neuinstallation oder Konfigurationsänderung einer Virtuellen Maschine oder eines Backups sowie im Falle von Beendigung oder Nichtverlängerung eines Hosted Private Cloud Dienstes oder einer Backup-Option werden alle Backups (einschließlich der darin enthaltenen Daten und Informationen) automatisch und unwiderruflich gelöscht. Es liegt in der Verantwortung des Kunden, vor Beginn einer solchen Operation sowie vor dem Ablaufdatum seiner Backup-Option oder Hosted Private Cloud Dienste seine Virtuellen Maschinen (einschließlich aller darauf enthaltenen Daten und Informationen) zu sichern oder auf andere Geräte zu übertragen, um sich so vor jeglichem Verlust und jeglicher Veränderung zu schützen.

Service Level Agreement. SLA wird definiert als die Verfügbarkeit des Veeam Managed Backup Dienstes, der Kunden von OVHcloud bereitgestellt wird, um diesen die tägliche Durchführung von Backup-Operationen zu ermöglichen und ihnen diese Operationen zur Verfügung zu stellen. Hierzu werden wir eine Kombination von Metriken wie unter anderem (aber nicht ausschließlich) die folgenden sammeln:

- Verfügbarkeit des Veeam-Dienstes
- Verfügbarkeit der Infrastruktur, auf der Veeam-Dienste installiert sind
- Netzwerkverfügbarkeit
- Speicherverfügbarkeit

Darüber hinaus werden wir, falls vorhanden, auf Fehler bei API-Aufrufen für mehr als 120 ms achten. Das SLA betrifft weder den Backup-Inhalt noch die Zeit, die für die Durchführung des Backups nötig ist.

SLA	Verfügbarkeit	GTI*	GTR**
Standard	99,9 %	12 h	72 h
Advanced	99,9 %	8 h	48 h
Premium	99,9 %	4 h	24 h

* : Backup-Operationen ausgeschlossen

** : Start ab Backup-Bericht für Backup-Operationen

GTI (Goal Time for Intervention). Maximale Zeit, die OVHcloud benötigt, um bei einer Störung einzugreifen. Beginnt, wenn ein Task vom Kunden gestartet wird und in einem Fehler resultiert, und endet, wenn OVHcloud den Kunden mit einer Support-Ticket-ID kontaktiert, oder wenn Mitarbeiter des OVHcloud-Kundendienstes zum ersten Mal auf ein vom Kunden geöffnetes Störungsticket antworten.

GTR (Goal Time for Recovery). Maximale Zeit, die OVHcloud benötigt, um die entweder automatisch vom System oder vom Kunden durch Erstellung eines Störungstickets gemeldete Störung zu beheben. Beginnt, wenn ein Task vom Kunden gestartet wird und in einem Fehler resultiert, und endet, wenn die Störung mit dem Status „done“ (abgeschlossen) oder „cancel“ (abgebrochen, mit Zustimmung des Kunden) behoben ist.

Bedingungen

Dies sind die Bedingungen für die Anwendung des SLA:

- Der Kunde hat eine Veeam Backup Server VM, die in der Hosted Private Cloud Infrastruktur bei OVHcloud gehostet wird und in funktionsfähigem Zustand ist.
- Diese VM ist zu jeder Zeit durch High Availability geschützt.
- Die VM befolgt Veeam Backup Best Practices.
- VMs mit einer Größe von mehr als 2 TB unterliegen nicht dem vorliegenden SLA.
- Sollte der Kunde versuchen, das Backup einer die erlaubte Größe übersteigenden VM durchzuführen, oder wird die Backup-Operation durch den Kunden abgebrochen, so gilt das SLA nicht.
- OVHcloud behält sich das Recht vor, den Kunden aufzufordern, eine zuvor fehlgeschlagene Backup-Operation erneut zu starten. Ist der Kunde nicht dazu in der Lage und/oder nicht verfügbar, um dieser Aufforderung nachzukommen, so gilt das SLA nicht.

ANHANG 3 „Disaster Recovery Plan“-Option

Der vorliegende Anhang beschreibt die anwendbaren besonderen Vertragsbedingungen für die „Disaster Recovery Plan“-Option, die als Teil der Private Cloud Dienste von OVHcloud angeboten wird, (nachfolgend als „DRP“ bezeichnet) und legt diese fest. Diese Option stellt eine der möglichen Komponenten eines „Disaster Recovery Plans“ dar, bei dem es sich um ein vom Kunden erstelltes, getestetes und betriebenes globales Geschäftsprojekt handelt. Der vorliegende Anhang ergänzt die besonderen Vertragsbedingungen der Hosted Private Cloud Premier und stellt einen integralen Bestandteil dieser Bedingungen dar. Im Falle von Abweichungen hat dieser Anhang Vorrang.

Beschreibung: Die „Disaster Recovery Plan“-Option erlaubt es dem Kunden, seine Virtuellen Maschinen, ob diese nun lokal beim Kunden oder in einer Hosted Private Cloud Premier gehostet werden, sowie die auf diesen gespeicherten Daten auf eine andere Hosted Private Cloud Infrastruktur zu übertragen. Diese Übertragungsfunktion ist über ein dediziertes Interface verfügbar. Bei dieser Option handelt es sich um einen optionalen Dienst, der nicht standardmäßig in den Kosten des Hosted Private Cloud Premier Dienstes enthalten ist. Diese Option muss Gegenstand einer spezifischen Bestellung oder Aktivierung sein und führt zu einer zusätzlichen Abrechnung.

Software: Die Software, die dem Kunden die Nutzung dieser Option ermöglicht, wurde von Drittanbietern entwickelt („Drittpartei-Produkte“). OVHcloud ist nicht an der Erstellung und Entwicklung dieser Drittpartei-Produkte, die dem Kunden als Teil der Option zur Verfügung gestellt werden, beteiligt. Aus diesem Grund ist OVHcloud nicht verantwortlich für Drittpartei-Produkte, die als Teil des Dienstes bereitgestellt werden, was technische Fehler, Sicherheitsschwachstellen, Inkompatibilitäten und Instabilität beinhalten kann, und übernimmt keinerlei Garantie für Drittpartei-Produkte, die als Teil des Dienstes zur Verfügung gestellt werden. Der Kunde ist nur dazu berechtigt, die von OVHcloud im Rahmen des Dienstes bereitgestellten Drittpartei-Produkte gemäß den aktuell geltenden anwendbaren Nutzungsbedingungen der Drittpartei zu verwenden. Dies schließt insbesondere jede Möglichkeit der Dekompilierung, des Zugriffs auf Quellen, der Neuinstallation auf anderen Infrastrukturen und der Vergabe von Unterlizenzen für die zur Verfügung gestellten Drittpartei-Produkt-Programme oder -Systeme aus. OVHcloud und der Drittanbieter behalten sich das Recht vor, die Drittpartei-Produkte jederzeit zu ändern. Als Teil dieser Option stellt OVHcloud dem Kunden die für die Nutzung des Dienstes erforderlichen Lizenzen für die Verwendung des „Zerto“-Drittpartei-Produkts zur Verfügung.

Mechanismen der Option: Synchronisierung und/oder Kopieren der VMs wird mithilfe des „Zerto“-Drittpartei-Produkts durchgeführt. Der Kunde wählt über das dedizierte Interface des Drittpartei-Produkts die Virtuellen Maschinen auf seinem Hosted Private Cloud Premier Dienst aus, die auf seiner Hosted Private Cloud Premier Backup-Infrastruktur synchronisiert werden sollen. Die Backup Hosted Private Cloud Premier muss sich in einem anderen Rechenzentrum als dem primären Hosted Private Cloud Premier Rechenzentrum befinden. Für jede ausgewählte Virtuelle Maschine wird eine kontinuierliche Synchronisierung mit hoher Bandbreite durchgeführt. Die Datenreplikation ist sowohl asynchron als auch kontinuierlich, mit einer RPO (Recovery Point Objective), die über das dedizierte Interface des Drittpartei-Produkts verfügbar und einsehbar ist. Kundendaten werden über das OVHcloud-Glasfasernetzwerk zwischen OVHcloud-Rechenzentren, in denen die Hosted Private Cloud Premier Lösung vorhanden ist, synchronisiert. Daten werden über einen VPN zwischen entfernten Standorten übertragen, damit alle Datentransfers gesichert sind. In einem Notfall kann der Kunde sofort auf den Hosted Private Cloud Premier Backup-Standort (den DRP-Standort) wechseln, indem er im Interface des Drittpartei-Produkts auf „FailOver“ klickt, um seine Backup-Infrastruktur zu starten.

Die Verwaltung des „FailOvers“ sowie der Wechsel auf den Backup-Standort liegen in der Verantwortung des Kunden.

Die im VMware-vSphere-Verwaltungsinterface verfügbare „VMware DRS“-Option muss aktiviert sein, um diese Option zu verwenden.

Nutzungsbedingungen: Der Kunde trägt die alleinige Verantwortung für die Verwendung der „Disaster Recovery as-a-Service“-Option und insbesondere (a) für die Auswahl der zu synchronisierenden Virtuellen Maschinen in seiner Hosted Private Cloud Premier, (b) für die Konfiguration seiner VPGs („Virtual Protection Groups“, ein Konzept des Drittpartei-Produkts) sowie für die Überprüfung des ordnungsgemäßen Funktionierens dieser VPGs, (c) für die Überprüfung der ordnungsgemäßen Durchführung der Synchronisierung, (d) für die Überprüfung der Integrität der Synchronisierung mit den vom Kunden als angemessen erachteten Tools, und, im Falle eines Fehlers, für die Durchführung einer neuen Synchronisierungsoperation falls nötig durch Kontaktieren des OVHcloud-Kundendienstes. OVHcloud ist im Rahmen der Dienste nicht für die Verwaltung von Synchronisierungs- oder Failover-Operationen zwischen den beiden Infrastrukturen des Kunden zuständig. OVHcloud kann im Falle von Ausfall, Fehlfunktion oder Fehler beim Durchführen von Synchronisierungs- oder Failover-Operationen nicht verantwortlich gemacht werden. Der Kunde erklärt sich bereit, die Entdeckung einer Fehlfunktion, eines Fehlers oder einer Schwachstelle beim Durchführen der Synchronisierungsoperation umgehend zu melden. Der Kunde stellt sicher, dass er über die erforderlichen Rechte verfügt und die geltenden Vorschriften einhält. OVHcloud hat keinerlei Kenntnis über den Inhalt und die Aktivitäten, für die der Kunde die Disaster-Recovery-Plan-Lösung verwendet. Diese Option kann gemäß den für den Hosted Private Cloud Premier Dienst geltenden allgemeinen Geschäftsbedingungen und besonderen Vertragsbedingungen ausgesetzt und unterbrochen werden. OVHcloud unterliegt einer Sorgfaltspflicht.

Rechnungsstellung: Die Rechnungsstellung an den Kunden richtet sich nach der Anzahl der durch die „Disaster Recovery Plan“-Option geschützten Virtuellen Maschinen.

Beendigung der Dienste: Im Falle von Löschen, Neuinstallation oder Konfigurationsänderung einer Virtuellen Maschine sowie im Falle von Beendigung oder Nichtverlängerung eines Hosted Private Cloud Dienstes oder dieser Option werden alle Synchronisierungen (einschließlich der darin enthaltenen Daten und Informationen) automatisch und unwiderruflich gelöscht. Es liegt in der Verantwortung des Kunden, vor Beginn einer solchen Operation sowie vor dem Ablaufdatum seiner „Disaster Recovery Plan“-Option oder der Hosted Private Cloud Dienste seine Virtuellen Maschinen (einschließlich aller darin enthaltenen Daten und Informationen) zu sichern oder auf andere Geräte zu übertragen, um so jeglichen Datenverlust oder jegliche Datenänderung zu verhindern.