Leistungsbeschreibung & zusätzliche Bedingungen
VERSIEGELTE CLOUD

Stand: 20.10.2017

Impressum

Herausgeber

Telekom Deutschland GmbH

Landgrabenweg 151

53227 Bonn

WEEE-Reg.-Nr. DE60800328

nachfolgend – Telekom – genannt

www.telekom.de/pflichtangaben

Inhaltsverzeichnis

Impressum **2**

1 Einleitung **4**

2 Leistungen der Telekom **4**

2.1 Bereitstellung der Leistung 4
2.2 Betrieb, Service, Service Qualität 4
2.2.1 Betrieb 4
2.2.2 Service 4
2.2.3 Service Qualität 5
2.3 Funktionen 5
2.3.1 Versiegelte Cloud allgemein 5
2.3.2 Zugriff auf die Projekträume 5
2.3.3 Security 6
2.3.4 Privacy Boxen 6
2.3.5 Produktivitätswerkzeug 6
2.4 Optionale Leistungen 6
2.4.1 Revisionssichere Datenräume. 6
2.4.2 Zusätzliche Nutzer und Speicher 7
2.4.3 Zweifaktor-Authentisierung 7
2.5 Änderungen zu Gunsten des Kunden 7
2.6 Betrieb, Service, Service Qualität 7
2.6.1 Betrieb 7
2.6.2 Service 7
2.6.3 Service Qualität 8

3 Mitwirkungsleistungen des Kunden **8**

4 Kommerzielle Rahmenbedingungen, Vertragsbeendigung **9**

5 Datenabholung am Vertragsende **9**

6 Glossar **9**

1 Einleitung

Die Telekom stellt dem Kunden mit der Versiegelten Cloud virtuelle Projekträume (Privacy Boxes und Datenräume) und versiegelte Kommunikationsmöglichkeiten als SaaS-Lösung zur Verfügung.

Die Lösung dient dazu, dass sich verschiedene, für den jeweiligen Projektraum zugelassene Nutzer treffen können und dort Dokumente und Nachrichten austauschen und zusammenarbeiten können. Die SealedCloud Technologie bietet ein automatisiertes Schlüsselmanagement und verhindert so einen nicht autorisierten Datenzugriff. Der Sicherheitsstandard des Systems ist sehr hoch und die Nutzung gleichzeitig sehr komfortabel.

2 Leistungen der Telekom

2.1 Bereitstellung der Leistung

Der Kunde kann unter verschiedenen Leistungspaketen wählen. Die jeweiligen Leistungspakete enthalten eine unterschiedliche Anzahl von Volllizenzen, Gastlizenzen und Speicherblöcken. Die Qualität der Lizenz entscheidet darüber, welcher Funktionsumfang dem jeweiligen Nutzer zugewiesen ist. Einzelheiten hierzu ergeben sich aus dem Glossar.

Nach Beauftragung erhält der Kunde einen Aktivierungslink per E-Mail. Die Leistung ist ab dem Zeitpunkt bereitgestellt, zu dem die E-Mail mit dem Aktivierungslink eingeht (Bereitstellungstermin).

Anschließend führt der Kunde mit Hilfe des bereitgestellten Links eine Selbstregistrierung durch. Dabei vergibt der, vom Kunden bestimmte Administrator des Kunden ein nur ihm bekanntes Passwort und einen nur ihm bekannten Nutzernamen (Administratorkennung). Passwort und Nutzername werden bei der Telekom nicht gespeichert und die Telekom erhält diese aus Sicherheitsgründen nicht und kann diese auch nicht rekonstruieren. D.h. seitens der Telekom besteht keine Möglichkeit, den Nutzernamen oder das Passwort des Administrators zurückzusetzen. Der Administrator des Kunden sollte deshalb das Passwort, die Administratorkennung und den PUK (Passwort Unlocking Key) sehr gut an einem geheimen und sicheren Ort aufbewahren, denn bei Verlust kann der Kunde nicht mehr auf den Account zugreifen.

Der Kunde bzw. der Administrator des Kunden kann weitere Nutzer selbst anlegen, die dann ihrerseits eine Selbstregistrierung durchführen. Einzelheiten zu den jeweiligen Rollen und Berechtigungen siehe hinten unter „Glossar“.

2.2 Betrieb, Service, Service Qualität

2.2.1 Betrieb

Die Telekom stellt dem Kunden die Versiegelte Cloud als SAAS bereit. Die Lösung wird in einem deutschen Rechenzentrum betrieben.

2.2.2 Service

Die Kunden können ihre Supportanfragen bezüglich Störungen oder Funktionen der Versiegelten Cloud an das Supportteam der Telekom richten (Service Desk). Dieses steht von Montag bis Freitag (ohne bundeseinheitliche Feiertage) von 08:00 bis 20:00 zur Verfügung. Der Support kann

bei Fragen zur Bedienung unterstützen, allerdings ist der administrative Zugriff auf die Kundendaten ausgeschlossen, weil Supportmitarbeiter aus Sicherheitsgründen nicht auf die Daten in der Versiegelten Cloud zugreifen können.

2.2.3 Service Qualität

Für die Versiegelte Cloud gelten die folgenden Leistungsparameter:

Ziel	Werte / Zeitfenster
Verfügbarkeit	Es wird keine Mindestverfügbarkeit angeboten. Telekom wird die Einschränkungen der Verfügbarkeit so gering wie möglich halten.
Betriebszeit	Montag – Sonntag, 24 x 7 Stunden, ausgenommen sind Wartungsfenster
Störungsannahme per E-Mail	Montag – Sonntag, 24 x 7 Stunden
Störungsannahme über den Service Desk	Montag bis Freitag (ohne bundeseinheitliche Feiertage) 08:00 Uhr bis 20:00 Uhr

2.3 Funktionen

2.3.1 Versiegelte Cloud allgemein

Die Versiegelte Cloud ist ein Webdienst, der die digitale Kommunikation und Zusammenarbeit zwischen dem Kunden und seinen Partnern absichert und vereinfacht.
Der Kunde bzw. die hierfür berechtigten Nutzer können

- virtuelle Projekträume anlegen,
- in den virtuellen Projekträumen Dokumente austauschen,
- gemeinsam an Dokumenten arbeiten,
- Nachrichten austauschen und
- chatten.

Bestandteil des Service ist ein mehrstufiges Berechtigungsmanagement, mit Hilfe dessen festgelegt werden kann, welcher Nutzer zu welchen konkreten Handlungen berechtigt sein soll. Einzelheiten ergeben sich aus dem Benutzerhandbuch, das dem Kunden im Hilfebereich der Versiegelten Cloud zur Verfügung gestellt wird.

2.3.2 Zugriff auf die Projekträume

Der Zugriff auf die Projekträume erfolgt verschlüsselt sowie mittels Internet per App oder Browser. Bei mobiler Nutzung können die Nutzer des Kunden Smartphones mit den Betriebssystemen Android oder iOS einsetzen. Die Nutzer des Kunden installieren die App eigenständig je nach Betriebssystem aus dem Google® Play-Store und dem Apple® App-Store. Andere Möglichkeiten der Bereitstellung können individuell mit dem Kunden als optionale Leistung vereinbart werden.

2.3.3 Security

Zur Anwendung kommt die in Europa, USA und China patentierte „Sealed Cloud Technologie“, die unter Berücksichtigung der technischen und betrieblichen Gegebenheiten dafür sorgt, dass vom Kunden eingebrachten Daten für Unberechtigte unzugänglich bleiben (sog. „technische Versiegelung“ des Rechenzentrums).
Die Technologie ist so konstruiert, dass der Betreiber des Rechenzentrums keinen Zugriff auf die Daten des jeweiligen Kunden hat. Die Technologie schützt die Daten auch während der Verarbeitung. Die Telekom erhält keinen Zugriff auf die Schlüssel. Der Zugriff von Telekom Mitarbeitern auf die Anwendungs-Server ist erst wieder möglich, wenn die Daten dort nicht mehr vorhanden sind. Die Daten werden bereits beim Transfer vom Kunden in das Rechenzentrum, in dem die Daten gehostet werden, verschlüsselt

Der Kunde bzw. seine Nutzer sind alleine dafür verantwortlich, dass die, dem Administrator bzw. den Nutzern zugeordneten Nutzungs- und Zugangsberechtigungen bzw. die zugeordneten Passwörter und Schlüssel vor dem Zugriff Dritter geschützt sind und nicht an unberechtigte Nutzer weitergegeben werden. Die Verantwortung für das Zugreifen, Verändern oder Herunterladen von Daten, die im Projektraum des Kunden gespeichert sind, sowie die Vergabe der Berechtigungen hierfür obliegt den Nutzern des Kunden, d.h. zunächst dem Administrator des Kunden sowie dann hieraus abgeleitet denjenigen, an die der Administrator Berechtigungen vergibt.

2.3.4 Privacy Boxen

Der Kunde kann eigene Speicherbereiche für Dateien aller Art und Nachrichten erzeugen, so genannte „Privacy Boxes“. Zu diesen Speicherbereichen haben nur der Nutzer und von ihm eingeladene andere Nutzer auf Basis der jeweils zugewiesenen Berechtigung Zugriff.

2.3.5 Produktivitätswerkzeug

Das Produktivitätswerkzeug bietet eine automatische Synchronisation zwischen den, in der Versiegelten Cloud angelegten Privacy Boxen und dem Dateisystem auf der lokalen Festplatte des jeweiligen Nutzers. Die Funktion wird in den Windows Datei-Explorer des Nutzers integriert. Mit dem Produktivitätswerkzeug lassen sich Dokumente mit einem Klick sperren, um eine Änderung des Dokuments durch andere Nutzer zu verhindern. Die Nutzer können auch bestimmte Privacy Boxen von der Synchronisation ausschließen.

2.4 Optionale Leistungen

Die nachfolgenden optionalen Leistungen werden bei gesonderter Beauftragung gegen zusätzliche Vergütung erbracht.

2.4.1 Revisionssichere Datenräume.

Revisionssichere Datenräume sind Privacy Boxes mit besonderen Funktionen. Sie enthalten ein Journal, mit dem die Aktionen (Up- & Downloads, Ansehen des Dokuments, Löschungen usw.) der Nutzer dokumentiert werden und Maßnahmen zum Verbreitungsschutz (Wasserzeichen etc.) ergriffen werden können.
Die folgenden Funktionen zur Erhöhung des Verbreitungsschutzes gelten für die Datenräume:

- Bei einem Download eines Nutzers wird ein Wasserzeichen auf dem Dokument angebracht, aus dem der Nutzername sowie Datum und Uhrzeit des Downloads zu ersehen sind (gilt nur für Dokumente im Format PDF).

- Für ein Dokument kann festgelegt werden, dass es nur am Bildschirm betrachtet werden kann (gilt nur für Dokumente im Format PDF).
- Es wird ein Alarm generiert, wenn ein Nutzer mehr als eine einstellbare Anzahl an Dokumenten in einem einstellbaren Zeitraum herunterlädt, d.h. es wird ein untypisches Nutzerverhalten dokumentiert und im Journal angezeigt.

Die vorgenannten Funktionen dienen der Erschwerung der Verbreitung der Dokumente, können eine Verbreitung jedoch nicht vollständig verhindern.
Aus Betriebsgründen erfolgen Eintragungen im Journal über Zugriffe mit einer Verzögerung von einigen Minuten. Die Angaben im Journal sind grundsätzlich komplett, allerdings kann unter sehr besonderen technischen Bedingungen die Aufzeichnung einer Aktion verloren gehen.
Jede Privacy Box lässt sich in einen Datenraum umwandeln.

2.4.2 Zusätzliche Nutzer und Speicher

Es können zu jedem Leistungspaket weitere Volllizenzen, Gastlizenzen und zusätzlicher Speicher hinzu gebucht werden.

2.4.3 Zweifaktor-Authentisierung

Um die Login Sicherheit zu erhöhen kann eine Zweifaktor-Authentisierung aktiviert werden. Für den Login ist dann neben dem kundenindividuell vergebenen Passwort zusätzlich eine PIN erforderlich, die dem Nutzer per kostenpflichtiger SMS zugesandt wird.

2.5 Änderungen zu Gunsten des Kunden

Die Telekom behält sich einseitige Leistungsänderungen und Entgeltreduzierungen zu Gunsten des Kunden vor. Der Kunde erklärt sich mit diesen Anpassungen bereits mit Vertragsunterzeichnung einverstanden. In Abweichung zu dem vereinbarten Schriftformerfordernis wird die Telekom den Kunden per E-Mail informieren. Die bestehenden Unterlagen werden damit durch die neu übersandten Unterlagen ersetzt.

2.6 Betrieb, Service, Service Qualität

2.6.1 Betrieb

Die Telekom stellt dem Kunden die Versiegelte Cloud als SAAS bereit. Die Lösung wird in einem deutschen Rechenzentrum betrieben.

2.6.2 Service

Die Kunden können Ihre Supportanfragen bezüglich Störungen oder Funktionen der Versiegelten Cloud an das Supportteam der Telekom richten (Service Desk). Dieses steht von Montag bis Freitag (ohne bundeseinheitliche Feiertage) von 08:00 bis 20:00 zur Verfügung. Der Support kann bei Fragen zur Bedienung unterstützen, allerdings ist der administrative Zugriff auf die Kundendaten ausgeschlossen, weil Supportmitarbeiter aus Sicherheitsgründen nicht auf die Daten in der Versiegelten Cloud zugreifen können.

2.6.3 Service Qualität

Für die Versiegelte Cloud gelten die folgenden Leistungsparameter:

Ziel	Werte / Zeitfenster
Verfügbarkeit	Es wird keine Mindestverfügbarkeit angeboten. Telekom wird die Einschränkungen der Verfügbarkeit so gering wie möglich halten.
Betriebszeit	Montag – Sonntag, 24 x 7 Stunden, ausgenommen sind Wartungs-fenster
Störungsannahme per E-Mail	Montag – Sonntag, 24 x 7 Stunden
Störungsannahme über den Service Desk	Montag bis Freitag (ohne bundeseinheitliche Feiertage) 08:00 Uhr bis 20:00 Uhr

3 Mitwirkungsleistungen des Kunden

Der Kunde verpflichtet sich alle erforderliche Mitwirkungsleistungen, die zur ordnungsgemäßen Leistungserbringung erforderlich sind, unentgeltlich, rechtzeitig und in erforderlichem Umfang, insbesondere jedoch Folgende zu erbringen:

a. Der Kunde versichert, dass er keine Inhalte auf dem vertragsgegenständlichen Speicherplatz speichern und in das Internet einstellen wird, deren Bereitstellung, Veröffentlichung oder Nutzung gegen geltendes Recht oder Rechte Dritter verstößt, dies gilt insbesondere für ehrverletzenden, volksverhetzenden oder rechtsradikalen Inhalte. Der Kunde wird dafür sorgen, dass er die, für die Speicherung und Bearbeitung seiner Daten im Projektraum erforderlichen Rechte besitzt.

b. Der Kunde wird Handlungen unterlassen, die eine Gefährdung oder Störung für Leistungen Dritter, oder die Infrastruktur der Telekom bewirken können (z.B. auf Grund einer DDoS Attacke). In einem solchen Fall ist die Telekom ohne vorherige Benachrichtigung des Kunden berechtigt, die betroffene Leistung bis zur Behebung der Gefährdung oder Störung zu deaktivieren. Dies gilt auch, wenn der Kunde Inhalte nutzt, auf dem vertragsgegenständlichen Speicherplatz speichert oder sonst zugänglich macht, die Malicious Codes oder sonstige Schadsoftware enthalten. Unberührt bleiben in diesen Fällen weitergehende Ansprüche der Telekom. Die Telekom wird den Kunden soweit möglich über entsprechende Vorfälle und Maßnahmen informieren.

c. Der Kunde prüft eigenverantwortlich die Einhaltung aller für ihn im Zusammenhang mit der Nutzung der Leistung relevanten und anwendbaren rechtlichen Vorschriften, Gesetze, Verordnungen und branchenspezifischen Bestimmungen und stellt deren Einhaltung sicher. Dazu zählen insbesondere auch die Einhaltung von Geheimhaltungs-verpflichtungen, die z.B. aus einer beruflichen Tätigkeit herrühren. Der Kunde versichert, dass geheimnisrelevante Daten oder personenbezogene Daten nur bei Vorliegen einer wirksamen Einwilligung gespeichert werden.

d. Die Nutzer des Kunden sind verpflichtet, Daten ausschließlich unter Nutzung und Anerkennung der gemäß des Internetprotokolls http/https, verabschiedeten Standards zu übermitteln. Er darf ausschließlich die standardmäßig anerkannten oder durch die Telekom vorgegebenen Schnittstellen nutzen. Abweichungen bedürfen der schriftlichen Genehmigung.

e. Der Kunde erklärt sich mit dem Schriftwechsel per E-Mail einverstanden und wird stets eine aktuelle E-Mail-Adresse hinterlegen. Dem Kunden ist bekannt und willigt darin ein, dass für die Leistungserbringung wesentliche Informationen, wie Zugangsdaten,

Informationen zu Änderungen der Leistungen und der rechtlichen Bedingungen ausschließlich per Mail versendet werden.

f. Der Kunde ist verpflichtet seine Daten in anwendungsadäquaten Intervallen in geeigneter Form auf anderen, eigenen Systemen zu sichern, damit diese mit vertretbarem Aufwand wiederhergestellt werden können. Eine Datensicherung durch Telekom findet nicht statt. Aus diesem Grund sollte der Kunde im eigenen Interesse seine Daten auch spätestens bis Vertragsende in geeigneter Form in andere Systeme überführt haben.

4 Kommerzielle Rahmenbedingungen, Vertragsbeendigung

Der Kunde bucht ein Basispaket, das eine bestimmte Anzahl von Voll- und Gastlizenzen sowie Speicherblöcke enthält. Dazu können dann gegen gesondertes Entgelt zusätzliche Voll- bzw. Gastlizenzen sowie o.g. Optionen gebucht werden.

Der Kunde kann gegen Zahlung eines zusätzlichen Entgelts zu seinem Paket zusätzliches Speichervolumen dazu buchen (Optionale Leistung). Das gebuchte Speichervolumen (bzw. auch das zusätzliche optional gebuchte Speichervolumen) steht für die vom Kunden genutzten Privacy Boxes oder Datenräume insgesamt zur Verfügung.

Der Vertrag wird für eine feste Laufzeit von einem Monat abgeschlossen, maßgebend für den Beginn der Monatsfrist ist das Datum der Registrierung. Die feste Laufzeit verlängert sich automatisch immer um einen Monat, wenn der Vertrag nicht von einer Partei spätestens einen Monat vor Ablauf der jeweils maßgebenden Laufzeit gekündigt wird (durch den Kunden über das Cloud-Portal per Button im Bereich Vertragsverwaltung bzw. durch die Telekom durch Übersendung einer eMail an die angegebene eMail-Adresse des Kunden). Der Kunde kann jeweils zum Ende der festen Laufzeit zwischen den angebotenen Paketen wechseln.

Es gelten die Allgemeinen Geschäftsbedingungen der Telekom Deutschland GmbH für IT-Leistungen, abrufbar unter https://cloud.telekom.de/agb sowie das auf der Website https://cloud.telekom.de/magenta-security/versiegelte-cloud abrufbare Preisblatt.

5 Datenabholung am Vertragsende

Der Kunde muss selbst dafür sorgen, dass am Vertragsende seine Daten per Datenfernübertragung aus dem Projektraum in einen anderen, für ihn verfügbaren Speicher übernommen werden. Der Kunde sollte deshalb in seinem eigenen Interesse den Kündigungstermin so wählen, dass er noch während der Laufzeit des Vertrags für die Datenabholung Zeit hat. Mit Beendigung des Vertrages werden alle innerhalb der Versiegelten Cloud angelegten Daten gelöscht.

6 Glossar

SaaS	Software as a Service

DDoS	Distributed-Denial-of-Service
Privacy Box	• Vertraulicher Projekt-Arbeitsraum mit Dateiablage, Notizen und Chat • Privacy Boxen verhalten sich wie Netzlaufwerke. Der Zugriff erfolgt ohne Software-Installation mit allen modernen Browsern oder per WebDAV, Windows-Client und Mobile-App (iOS, Android) • Nur vom Box-Ersteller eingeladene Nutzer haben Zugang.
Datenraum	• Ein Datenraum hat die gleichen Eigenschaften wir die Privacy Box, hat aber zusätzliche Funktionen, nämlich Journal und Verbreitungsschutz.
Projektraum	• Übergeordneter Begriff mit dem der/die vom Kunden genutzten Datenraum/-räume und Privacy Box/-es zugleich (gemeinsam) bezeichnet werden.

Volllizenz	• Eine Lizenz, die einem Mitarbeiter des Kunden zugeordnet wird.
	• Berechtigungsumfang:
	  ○ Privacy-Boxen erstellen (derzeit bis zu 2.000 Boxen je Paket)
	  ○ Dokumente hoch- und herunterladen
	  ○ Nachrichten schreiben, chatten
	  ○ Vergabe von Gastlizenzen

Volllizenz mit Administrator-Rolle	• Der erste Nutzer übernimmt immer zwingend für die Gesamtlaufzeit die Administratorrolle.
	• Jede Volllizenz kann eine Administrator-Rolle erhalten. Es ist zu empfehlen, dass neben dem registrierenden (d.h. dem ersten) Administrator mindestens zwei weitere Administratoren benannt werden.
	• Der Administrator übernimmt weitere administrative Aufgaben.
	• Berechtigungsumfang:
	  ○ Buchung von Voll- und Gastlizenzen
	  ○ Buchung Datenraumlizenzen
	  ○ Buchung von zusätzlichem Speicher
	  ○ Vergabe von weiteren Administrator-Rollen
	  ○ Vergabe Voll- und Gastlizenzen (d.h. Zuordnung von gebuchten Voll- und Gastlizenzen an Mitarbeiter oder Externe)

Gastlizenz	• Gastlizenzen sind für externe Nutzer vorgesehen.
	• Gastlizenzen können dauerhaft oder temporär vergeben werden. Temporäre Lizenzen verfallen nach 30 Tagen Inaktivität und gehen in den Pool der Gastlizenzen zurück.
	• Die Nutzer von Gastlizenzen können zu Mitgliedern in Privacy-Boxen gemacht werden bzw. als Mitglieder eingeladen werden.
	• Berechtigungsumfang:
	  ○ Dokumente hoch- und herunterladen,
	  ○ Nachrichten schreiben, chatten.
	• Nutzer von Gastlizenzen können keine Privacy-Boxen erstellen und keine weiteren Gäste einladen.
	•

Einmaliger Lesezugriff (kostenfrei)	• Ein einmaliger Lesezugriff kann nur von dem Inhaber des jeweiligen Projektraums vergeben werden. • Die Berechtigung wird über einen Link vergeben, der mit einem Passcode schützbar ist. • Dokumente lassen sich damit ohne Gastlizenz, d.h. kostenfrei, herunterladen • Durch die Übersendung des Links und des Passcodes wird der jeweilige Projektraum zugänglich gemacht. Bei Vergabe des Lesezugriffs liegt es deshalb nicht in der Verantwortung der Telekom, wenn der Empfänger der Zugangsdaten diese an Nichtberechtigte weitergibt.
Nutzer	Grundsätzlich sind alle Nutzer damit gemeint, d.h. • Nutzer mit Administratorrolle, • Nutzer mit Volllizenz • Nutzer mit Gastlizenz • Nutzer mit einmaligem Lesezugriff