BESCHREIBUNG VON „SAAS HOPEX"

DIE HIER BESCHRIEBENEN SERVICES GELTEN NUR FÜR DIE STANDARDVERSION VON HOPEX. WENN DER KUNDE WÜNSCHT, DASS SIE EBENFALLS AUF SPEZIFISCHE ENTWICKLUNGEN UND ANPASSUNGEN ANWENDBAR SIND, MUSS DER KUNDE AUF DIE PREMIUM MAINTENANCE OPTION ABONNIERT SEIN.

DER KUNDE WIRD DARAUF HINGEWIESEN, DASS DIE VERWEIGERUNG DER MIGRATION AUF EINE UNTERSTÜTZTE VERSION ZU SICHERHEITSPROBLEMEN FÜHREN KANN. ZUDEM WERDEN DEM KUNDEN KEINE WARTUNGSLEISTUNGEN EINSCHLIESSLICH KORREKTURPAKETE MEHR GEWÄHRT. MEGA HAFTET NICHT FÜR FOLGEN, DIE HÄTTEN VERMIEDEN WERDEN KÖNNEN, WENN DER KUNDE AUF EINE UNTERSTÜTZTE VERSION MIGRIERT ODER DIE INSTALLATION EINES KORREKTURPAKETS ODER HOTFIXES AKZEPTIERT HÄTTE.

1. DEFINITIONEN

TERMIN	DEFINITION
Spezifische Entwicklung/Anpassung	Jede spezifische Entwicklung oder Parametrisierung des HOPEX-Produkts, die die Funktionalitäten entsprechend den spezifischen funktionalen Anforderungen des Kunden modifiziert. Änderungen können sich auf die Datenstruktur, Bildschirme, Arbeitsabläufe, Datenzugriffsregeln, Schnittstellen, die eine Entwicklung erfordern, spezifische Exporte wie eine Intranet-Website oder komplexe Berichte, die eine Programmierung erfordern, beziehen. Die Benutzerverwaltung und die von den Endbenutzern vorgenommenen Konfigurationen (z. B. Anzeigepräferenzen, Abfragen, Standardberichtsfunktionen) werden nicht als Anpassungen behandelt, sondern lediglich als Grundkonfiguration des Standardprodukts.
Fehler	Verhalten des Services, das nicht mit den Unterlagen übereinstimmt. Jeder Fehler sollte reproduzierbar sein, eindeutig identifizierbare Symptome aufweisen und funktionelle Auswirkungen auf den Standardservice haben.
Abhilfe	Alternative Betriebsart zur Überwindung eines Fehlers.
Störfall	Verhaltensweisen, die nicht zum Standardbetrieb des Services gehören und die den Service in der Produktion unterbrechen oder die Qualität des Services verringern.
Fall	Beispiel, das vom technischen Support von MEGA verwendet wird, um einen vom Kunden gemeldeten Störfall zu verfolgen.
Zeitraum der Nichtverfügbarkeit oder Ausfall des Services	Die Zeitspanne innerhalb des Geltungszeitraums der Service Level Agreements, in der der Service für die Nutzer nicht verfügbar ist.
Release oder neue Version	Neue Version der Software, einschließlich neuer Funktionen.
Fix	Änderung des Servicess, entwickelt von MEGA, um einen Fehler zu beheben. Korrekturen werden in der Regel in einem Korrektur-Patch gebündelt oder manchmal durch einen Hotfix bereitgestellt.
Korrekturpakete (CP) oder Minor Version	Bedeutet Aktualisierungen, um HOPEX noch zuverlässiger zu machen. CP bietet einen konsistenten Satz von Korrekturen sowie Sicherheits- und Leistungsverbesserungen, die für ein Long-Term-Support-Release gelten.
Hotfix	Fix, der von der MEGA außerhalb des Kontextes eines Releases oder eines CP gesetzt und bereitgestellt wird. Hotfixes reagieren in der Regel auf kritische Fehler und können nur auf dem letzten CP eines Releases installiert werden.

2. ZUGANG ZUM SERVICE

Der Zugriff auf den Service ist auf vordefinierte, vom Kunden bereitgestellte IP-Adressen beschränkt. Bei den IP-Adressen muss es sich um öffentliche (routingfähige), statische und gelistete IPs handeln.
Roaming-Benutzer stellen zunächst eine Verbindung zum Relay-Standort eines Kunden her, der ihnen eine IP-Adresse gibt, zu der MEGA den Zugang erlaubt, und verbinden sich dann mit dem Service.
Der Kunde meldet MEGA unverzüglich jeden Störfall, der den Zugang zum Service betrifft. Der Kunde darf den Service, einschließlich der Server von MEGA oder des Hosting-Providers von MEGA, nicht stören oder unterbrechen und muss sich an die Empfehlungen, Verfahren und Regeln halten, die von MEGA von Zeit zu Zeit für die angemessene Nutzung des Service mitgeteilt werden.

3. BENUTZERANMELDEINFORMATIONEN

MEGA stellt die Benutzeranmeldeinformationen für den Client-Administrator bereit, der für die Einrichtung der Benutzeranmeldeinformationen zuständig ist.

Der Kunde muss alle notwendigen Maßnahmen ergreifen, um die Vertraulichkeit der Benutzerdaten zu gewährleisten. MEGA haftet nicht für Schäden, die aus der Nutzung des Services durch einen unbefugten Dritten entstehen. Im Falle des Verlusts oder der Weitergabe der Anmeldedaten eines Benutzers an einen unbefugten Dritten muss der Kunde MEGA unverzüglich schriftlich benachrichtigen. Aus Sicherheitsgründen kann MEGA den Kunden jederzeit auffordern, ein Passwort zu ändern oder eine Benutzerkennung ohne vorherige Zustimmung zu löschen.

4. SERVICEVERFÜGBARKEIT

MEGA wird sich in angemessener Weise bemühen, die Serviceleistungen wie darin beschrieben zur Verfügung zu stellen, außer:

- Während der Wartungszeiten. Geplante Wartungsarbeiten müssen mit angemessener Frist angekündigt werden, während ungeplante Wartungsarbeiten mit einer Frist von einem Werktag angekündigt werden müssen (außer im Falle von Sicherheitsvorfällen);
- Als Folge von Umständen, die außerhalb der Kontrolle von MEGA liegen, wie z.B. Internetunterbrechungen und jedes andere Ereignis höherer Gewalt;
- Im Falle eines Sicherheitsproblems, wie z. B. einer anormalen, betrügerischen oder missbräuchlichen Nutzung der Services, eines Eindringens, eines betrügerischen Zugriffs auf die Services durch Dritte oder einer illegalen Datenextraktion aller oder eines Teils der Daten usw., ist der Kunde verpflichtet, die den Services entstandenen Kosten zu tragen.

MEGA wird sich nach besten Kräften bemühen, die Folgen zu minimieren und den Service wiederherzustellen, nachdem die oben genannten Ursachen weggefallen sind.

SERVICEVERFÜGBARKEIT	ENTWICKLUNG	PRODUKTION
Maximale Dauer eines ungeplanten Ausfalls	1 Arbeitstag	3 Geschäftsstunden
Maximaler monatlicher ungeplanter Ausfall	1 Arbeitstag	4 Geschäftsstunden

Alle Nichtverfügbarkeitsperioden werden bei der Berechnung der oben genannten Ausfallzeiten berücksichtigt, außer:

- Geplante Nichtverfügbarkeitszeiträume, wie z. B. vom Kunden im Voraus genehmigte Zeiträume im Rahmen von Änderungsmanagementmaßnahmen
- Außerplanmäßige Nichtverfügbarkeitszeiten, die sich aus dem in diesem Abschnitt dargelegten Haftungsausschluss ergeben.

Die Unterbrechung wird ab dem Zeitpunkt berechnet, an dem der Kunde MEGA kontaktiert: Erklärung eines *Nichtzugangs* über den Support-Bereich unserer Community (https://community.mega.com).

Bei Nichteinhaltung der Verfügbarkeitsverpflichtungen kann der Kunde eine Servicegutschrift beantragen. Eine Servicegutschrift entspricht der Anzahl zusätzlicher Servicetage (zusätzlich zum aktuellen Abonnementzeitraum), die dem Kunden für den Ausfall gewährt werden. Jede Servicegutschrift muss schriftlich beantragt werden. Ein solcher Antrag muss innerhalb von 3 Monaten nach dem Datum des erzeugenden Ereignisses gestellt werden. Die Servicegutschrift ist das einzige und ausschließliche Rechtsmittel des Kunden im Falle der Nichtverfügbarkeit des Services.

Der Service ist von Montag bis Freitag von 9.00 bis 18.00 Uhr verfügbar, außer an Feiertagen.

5. BESCHRÄNKUNG DER HAFTUNG VON MEGA

Die Haftung von MEGA ist in den folgenden Fällen beschränkt oder ausgeschlossen:

- Bei Nichteinhaltung der in den Unterlagen und im Benutzerhandbuch enthaltenen Anweisungen zur Nutzung des Services durch den Kunden;
- Bei Leistungseinbußen aufgrund der Netzwerkkonfiguration und der Sicherheitsvorrichtungen des Kunden;
- Bei einem Störfall, der auf ein Softwareprodukt zurückzuführen ist, das auf dem Computersystem des Kunden installiert ist.
- Bei Nichtverfügbarkeit des Ansprechpartners eines Kunden während eines Ausfalls.
- Bei Weigerung des Kunden, unverzüglich Informationen (oder die Berechtigung zum Zugriff darauf) bereitzustellen, die es MEGA ermöglichen, einen Vorfall oder einen Fehler zu beheben.

6. SCHWERE DES STÖRFALLS UND REAKTIONSZEIT

Schweregrad	Sachverhalt	Reaktionszeit und Erwartung
Kein Zugriff	Sicherheitsprobleme Plattform außer Betrieb / kein Zugang	1 Geschäftsstunde
Kritisch	Erhebliche Verschlechterung einer Funktionalität. Kritische geschäftlichen Auswirkungen.	Der Kunde wurde innerhalb von 4 Geschäftsstunden kontaktiert. - Kontinuierliche Anstrengungen jeden Tag, während der Geschäftszeiten. - Schnelle Eskalation durch Technischen Support und Produktgruppen. - Zeitnahe Allokation geeigneter Ressourcen. - Erstellung eines Aktionsplans. - Je nach Komplexität des Fehlers kann eine frühzeitige Lösung oder Abhilfe bereitgestellt werden, um Betriebsstörungen zu minimieren.
Mäßig	Mäßige Verschlechterung einer Funktionalität, die Arbeit kann vernünftigerweise mit gewissen Beeinträchtigungen fortgesetzt werden. Mäßige geschäftlichen Auswirkungen.	Der Kunde wird innerhalb von 1 Werktag kontaktiert. Allokation von Ressourcen zur Aufrechterhaltung der Bemühungen während der Geschäftszeiten. Ein Aktionsplan könnte erstellt werden.
Unerheblich	Geringfügige Beeinträchtigung einer Funktionalität. Keine geschäftlichen Auswirkungen.	- Der Kunde wird innerhalb von 2 Werktagen kontaktiert. Höchster Aufwand während der Geschäftszeiten.

Die Reaktionszeit wird ab dem Tag berechnet, nachdem der Kunde MEGA über das Support Center, das über die Online-Community zugänglich ist, über den Fehler informiert hat.
Der technische Support von MEGA kann den Schweregrad herabsetzen, wenn der Kunde nicht in der Lage ist, die erforderlichen Ressourcen oder Antworten bereitzustellen, damit MEGA seine Bemühungen zur Behebung des Vorfalls fortsetzen kann.
Die Standard-Supportleistungen umfassen keine Unterstützung vor Ort. In besonderen Fällen und nach Zustimmung des Kunden zu den Bedingungen für den Einsatz von MEGA kann MEGA nach eigenem Ermessen am Standort des Kunden tätig werden. Der Kunde verschafft MEGA Zugang zu den Ressourcen des Kunden und zu ausreichend qualifiziertem Personal, um alle erforderlichen Informationen zu erteilen. Der Kunde stellt die für den Support erforderlichen Daten zur Verfügung und stellt sicher, dass er über alle geistigen Eigentumsrechte an den MEGA zur Verfügung gestellten Gegenständen Dritter verfügt.

7. LEBENSZYKLUSPOLITIK

DEFINITION	BESCHREIBUNG
Release (Long Term Support)	Die neue Version von Hopex wird während der folgenden Zeiträume aufrechterhalten: 27 Monate lang mit Full Support, dann 9 Monate lang mit Limited Support, und regelmäßig von CP verbessert.
Full Support	Zeitraum, in dem der Kunde Wartungs- und Supportleistungen erhält, einschließlich der Verbesserung bestehender Funktionen, der Hinzufügung neuer Funktionen und Produkte sowie CP.
Limited Support	Zeitraum nach dem Full Support-Zeitraum, in dem nur kritische Störfälle durch Hotfixes behoben werden können.

8. BACKUP- UND WIEDERHERSTELLUNGSPLAN (DRP: Disaster Recovery Plan)

8.1. Backup.
Im Rahmen der (nicht optionalen) Hosting-Services verpflichtet sich MEGA, die in diesem Abschnitt angegebene Anzahl von Datensicherungen durchzuführen.
Im Falle einer Katastrophe, die die Hosting-Server betrifft, verpflichtet sich MEGA, die Services innerhalb des in diesem Dokument festgelegten Zeitrahmens wiederherzustellen.
Standardmäßig wird die Wiederherstellung ab der letzten Sicherung durchgeführt. Alle anderen Backups, die gemäß den Bestimmungen dieses Dokuments aufbewahrt werden, werden als Archive betrachtet und können wiederhergestellt werden.

BACKUP	TÄGLICH	WÖCHENTLICH	MONATLICH
Aufbewahrungsfrist für Backup ab einem periodischen Backup	7 Tage	4 Wochen	6 Monate
Zeit für die Wiederherstellung	Letzter Backup: 4 Geschäftsstunden Archiv: 6 Arbeitsstunden		

8.2. Disaster-Recovery-Plan

Der Kunde erhält einen Disaster-Recovery-Plan für den Fall, dass ein Fehler in der Datenbank auftritt oder ein Problem mit den Servern auftritt, auf denen die Plattform, die Lösungen und/oder die Daten des Kunden gehostet werden.
MEGA verpflichtet sich zu:

- Durchführung von Sicherungskopien der Daten des Kunden in einer vordefinierten Häufigkeit. Letzteres bezieht sich auf das letzte Backup, das zur Durchführung seines Wiederherstellungsplans (RPO) verwendet wird,
- Wiederherstellung der Kundendaten vom letzten Backup innerhalb des unten definierten Zeitrahmens. Diese Wiederherstellungszeit (RTO) wird von MEGA für die Wiederherstellung der Services benötigt.

Der Kunde kann nach eigenem Ermessen die Option "Advanced DRP" abonnieren, um von häufigeren Backups und/oder kürzeren Wiederherstellungszeiten zu profitieren.

	Recovery Time Objective (RTO)	Recovery Plan Objective (RPO)
Standardangebot	1 Woche	25 Stunden
Mit erweiterter DRP-Option	24 Stunden	25 Stunden

9. PENETRATIONSTESTS

MEGA führt jährlich Penetrationstests durch Dritte für ihren SaaS-Service durch. Diese Tests werden für die Full Support Releases (letzte CP) durchgeführt, die am Tag des Penetrationstests auf dem Markt verfügbar sind. Jede andere Anforderung des Kunden kann mit zusätzlichen Gebühren verbunden sein. Auf Anfrage stellt MEGA dem Kunden ein Gutachten und einen zusammenfassenden Bericht über die Ergebnisse dieser Penetrationstests zur Verfügung.

10. SERVICEANFRAGEN

Eine Serviceanfrage ist eine formalisierte Anfrage für einen Eingriff in die SaaS-Plattform(en) des Kunden.
Nur die vom Kunden als "MEGA-Kontakte" bezeichneten Personen sind befugt, Anfrageservices zu erbringen.

10.1. In der Norm enthaltene Serviceleistungen.

Servicele-Kategorie	Unterkategorie der Service	Beschreibung des Servicess	Frequenz/Menge max.	Reaktionszeit
Release-Management	Upgrades	Bereitstellen eines HOPEX-Updates auf einer der SaaS-Plattformen (DEV; PRE-PROD; PROD); HotFix, Korrektur-Pack, Release.	4 pro Jahr	HotFix, korrigierender Patch 2 Arbeitstage (PPROD zuerst) Version Muss im Voraus geplant werden
Nutzermanagement	Benutzeranmeldung	Bereitstellen einer Protokolldatei (TXT-Format), in der alle Benutzerverbindungen einschließlich Benutzerlizenzen, Benutzernamen, Profile und Plattformverfügbarkeit aufgeführt sind.	1 pro Monat	1 Arbeitstag
	Neuzuweisung eines Benutzers/Profils zu einer Token-Lizenz	Bei benannten Lizenzen wird einem Benutzer ein Lizenz-Token neu zugeordnet. Ein Nutzer kann sein: Hauptnutzer, Mitwirkender oder Leser. Dieser Service gilt nicht für Floating-Lizenzen.	10 Umwidmungen (alle Nutzer) pro Jahr	
Zugangsmanagement	Service Domain-Name ändern	HOPEX Cloud URL von "aaa.hopexcloud.com" auf "bbb.hopexcloud.com" ändern.	2 Änderungen pro Jahr	2 Arbeitstage
	Zusätzliche eingehende IPs auf der Whitelist deklarieren	Hinzufügen von bis zu 5 zusätzliche IP-Adressbereiche zur Liste der IP-Adressen, die auf das HOPEX-Softwarepaket zugreifen dürfen.	3 Anträge pro Jahr	1 Arbeitstag
Integrations-management	Aufgabenplanung	Planung von wiederkehrenden Aufgaben mit vor- oder nachgelagerter Übertragung (falls zutreffend) in und aus der Umgebung des Kunden unter Verwendung des "Secure File Transfer Protocol" (SFTP). Die geplanten Aufgaben betreffen hauptsächlich Importe/Exporte und die statische Website-Generierung. Der Entwurf, die Realisierung und die Validierung (über eine Workbench) der zu planenden Elemente verbleiben in der Verantwortung des Kunden.	6 Anträge pro Jahr	2 Arbeitstage (PPROD zuerst)
	Einsatz von Webservices	Stellen Sie einen Webdienst in der Produktion bereit. Entwurf, Erstellung und Validierung eines Webdienstes liegen in der Verantwortung des Auftraggebers.		3 Arbeitstage (PROD zuerst)
HOPEX-Laden	Einsatz von Modulen	Liste der sich entwickelnden Module: https://store.mega.com/modules	10 Anfragen pro Jahr	2 Arbeitstage (PPROD zuerst)

Serviceanfragen unterliegen diesem Service Level Agreement.
Für jede Änderung der Häufigkeit und/oder der Höchstmenge der Serviceanfragen werden zusätzliche Gebühren erhoben.
Darüber hinaus kann MEGA nur dann zu Serviceleistungen verpflichtet werden, wenn:

- Die Serviceanfrage von der MEGA Community-Website aus geöffnet wird (per E-Mail gesendete Serviceanfragen werden nicht bearbeitet);
- Der " Beauftragte Ansprechpartner" MEGA alle für die Bearbeitung einer Serviceanfrage erforderlichen Informationen zur Verfügung gestellt hat. Die Zeit, die für die Bereitstellung solcher Informationen, Antworten, Tests usw. benötigt wird, wird nicht berücksichtigt.

Für Anfragen, die nicht im Katalog für Serviceanfragen aufgeführt sind:

- Geschätzte Antwortzeit innerhalb von 2 Werktagen
- Untersuchung und Behandlung je nach Antrag

10.2. Leistungsstufen des "SaaS-Plattform-Pakets".

Service-Levels	Art der Plattform	Anzahl der Produktionsanläufe
Starter	Vorproduktion und Produktion	1 pro Jahr
Standard	Entwicklung, Vorproduktion und Produktion	4 pro Jahr
Fortgeschrittene	Entwicklung, Vorproduktion und Produktion	12 pro Jahr

11. OPTIONEN

11.1. Premium-Wartung

Objekt	Beschreibung
Premium-Unterstützung	
Proaktives monatliches Follow-up	Monatliche Sitzungen zur Berichterstattung über die Falllösung mit einer einzigen Kontaktstelle
Überwachung von Gesundheitsindikatoren	Monatliche Überprüfung der Gesundheitsindikatoren, einschließlich der Anzahl der Fälle und SLAs.
Pflege von Anpassungen	
Berichtigung von Konfigurationen/Anpassungen einschließlich Unterlagen	Unterstützung und Korrektur der Änderungen, die ausschließlich von MEGA vorgenommen wurden. Dazu gehören auch die Änderungen, die für ein Upgrade des Services erforderlich sind.
Upgrade-Verwaltung	
Upgrade-Funktionsvalidierung	Führen Sie eine funktionale Validierung der Konfiguration nach dem Upgrade auf die neueste HOPEX-Version durch.
Verwaltung der Auswirkungen kleinerer Releases auf die Benutzer	Bewertung der Auswirkungen von Änderungen an Benutzer-Upgrades auf die Benutzerbasis. Daraus ergeben sich Aktivitäten wie die Kommunikation mit den Nutzern und die Ermittlung von Nutzern, die zusätzliche Schulungen benötigen.

11.2. Adoptionspaket

Objekt	Beschreibung
Bewertung und Überwachung des Reifegrads	
Workshops zur Reifegradbewertung	Jährliche funktionale Workshops zur Verbesserung der Akzeptanz, der Nutzung von HOPEX und der Demonstration des Nutzens auf der Grundlage der MEGA-Methode zur Bewertung des Reifegrads, einschließlich eines Vorverkaufsexperten und eines CSM
Folgemaßnahmen zu den Empfehlungen	Überwachung der HOPEX-Annahme anhand von Schlüsselindikatoren und Umsetzung der Expertenempfehlungen
e-Learning	
eLearning-Sitzungen	eLearning-Sitzungen zur Verbesserung der Akzeptanz innerhalb des Teams

11.3. Hopex-Verwaltung

Objekt	Beschreibung
Verwaltung des Zugangs	
Verwaltung des HOPEX-Authentifizierungsmodus	Verwalten des HOPEX-Authentifizierungsmodus der HOPEX-Benutzer.
Verwalten von Geschäftsrollen	Ordnen Sie Geschäftsrollen zu. Eine Geschäftsrolle definiert die Funktion einer Person oder einer Personengruppe im Unternehmen. Eine Geschäftsrolle wird auf einer Repository-Ebene definiert.
Verwalten von Personengruppen	Einrichten, Entfernen und Konfigurieren von Personengruppen in einer Gruppe, die dieselbe Verbindung nutzt. Eine Personengruppe ist eine Liste von Personen, die der gleichen Gruppe angehören.
Benutzerzugang/Gruppenverwaltung	Einrichten, Entfernen, Konfigurieren von Benutzern, Benutzergruppen, Benutzerprofilen, Zugriffs- und Berechtigungsstufen.
Definition von Regeln für den Datenzugriff	Einrichten, Entfernen und Konfigurieren von Benutzerberechtigungsstrukturen.
Ein Benutzerpasswort zurücksetzen	Benutzerpasswort setzen/zurücksetzen (dies umfasst nur das Zurücksetzen des Passworts für MEGA-Benutzer).
Content Management - Benutzerarbeit	
Verwalten doppelter Objekte	Identifizierung doppelter Objekte (in Zusammenarbeit mit den Eigentümern der Inhalte), Validierung der Duplikate und Durchführung von Maßnahmen zur Beseitigung von Duplikaten, z. B. Zusammenführung oder Löschung.
Verwalten isolierter Objekte	Identifizierung isolierter Objekte, um die Zuweisung von Eigentumsrechten zu ermöglichen, Identifizierung zur Löschung, Meldung von Objekten, die nicht in Diagrammen enthalten sind (wo erwartet wird, dass sie durch Diagramme beschrieben werden), Meldung von Objekten, die nicht in Assoziationen enthalten sind.
Zu löschende Objekte verwalten	Objekte löschen, wobei der modellierende Benutzer keine Berechtigung hat, Objekte zu löschen, die außerhalb seiner aktuellen Transaktionen erstellt wurden. Objekte können von Benutzern zum Löschen markiert werden.
Verwalten der Zusammenführung von Objekten	Zusammenführen von Objekten (d.h. Duplikaten) innerhalb eines Repositorys.
Verwalten des Datenzugriffs	Einrichtung und Pflege von Objektberechtigungsstufen, die die Änderung von Objekten durch einen bestimmten Benutzer/Benutzerprofil erlauben/verhindern.
Verwalten des Objektschutzes	Aktivieren oder deaktivieren Sie den Schutz bestimmter Objekte innerhalb eines Repositorys.
Content Management - Verwaltung	
Vergleich und Abgleich des Repository/der Teilmenge von Inhalten	Vergleichen und Verschieben von Objekten/Objektbereichen aus verschiedenen Repositories. Das Ziel-Repository kann mit dem Basis-Repository abgeglichen werden.
Logische Sicherung der Inhaltsgruppe	Erstellung einer logischen Baseline für eine bestimmte Inhaltsgruppe (z. B. Bibliothek, Projekt usw.), die die Erstellung unabhängiger Baselines für Segmente des Repository-Inhalts ermöglicht.
Verwalten von Bibliotheken	Einrichtung und Pflege von Bibliotheken und Sicherstellung einer klaren Inhaltsstruktur innerhalb des Repositorys. Bibliotheken können zur logischen Trennung von Repository-Inhalten verwendet werden.
Abfragen und Berichte erstellen	Schreiben Sie Abfragen, die registriert und für alle Benutzer in der Umgebung zur Wiederverwendung verfügbar sind. Konfigurieren Sie Berichte auf der Grundlage der Report Studio-Funktionen.
Verwaltung von Arbeitsabläufen	Verwalten Sie den Übergang von Workflows zur Unterstützung der Genehmigung, Autorisierung und Bewegung von Objekten. Überwachung von Workflow-Aktionen und Neuzuweisungen.
Datenimport	Verwalten Sie den regelmäßigen Datenimport unter Verwendung vorhandener XLS-Vorlagen.
Management von Zwischenfällen	
Verwaltung der internen Unterstützung	Verwalten der ersten Ebene des Supports für die funktionalen Anwendungsfälle des Kunden in einem benutzerdefinierten Plattformkontext.
Verwalten der Fallverfolgung	Erstellung, Priorisierung und Weiterverfolgung von Fällen mit dem technischen Support von MEGA. Stellen Sie ihnen alle notwendigen Elemente zur Verfügung, um das angesprochene Problem zu diagnostizieren.
Funktionelle Unterstützung	
Leitfaden	Bereitstellung bewährter Verfahren und Standardanleitungen für die Verwendung von HOPEX
Modell Transkription	Manuelle Übertragung bestehender Modelle (MS Word, PPT, Visio, ...) oder strukturierter Daten (XLS-Format) in HOPEX Nicht anwendbar bei Massenverladung.
Wartung von Diagrammen verwalten	Aktualisierung bestehender Diagramme auf der Grundlage eines formalisierten Änderungsantrags. Verwaltung der Auswirkungen von Änderungen an zentralen Datenkonzepten auf Zeichnungen.
Leitfaden	Bereitstellung bewährter Verfahren und Standardanleitungen für die Verwendung von HOPEX

Integration und Schulung der Nutzer	Integration und Schulung neuer Benutzer auf der Grundlage der vorhandenen Unterlagen und Schulungsmaterialien.
EA-Modellierung	Von der Befragung der KMU bis zur Validierung Ihres EA-Assets auf HOPEX-Diagrammen
Einarbeitung und Schulung der Benutzer	Einarbeitung und Schulung neuer Endbenutzer auf der Grundlage bestehender Kundenschulungen und -unterlagen.

12. KONTAKTE UND LEITUNG

Bei Abschluss des Vertrags ernennt der Kunde maximal 3 benannte Ansprechpartner, die für die Serviceleistungen geschult sind und denen MEGA Supportleistungen anbietet. Die benannten Ansprechpartner müssen mindestens die folgenden Funktionen ausführen können:

- Verwaltung der Benutzer und ihrer Zuweisung zu den verschiedenen Profilen der MEGA-Lösung(en), die den Service bilden;
- Im Falle eines Zwischenfalls:
    - Einen "Fall" auf dem MEGA-Portal melden, indem alle notwendigen Informationen zu den Umständen, unter denen der Vorfall aufgetreten ist, gesammelt und bereitgestellt werden;
    - Jedes Sicherheitsproblem sofort auf dem am besten geeigneten Weg melden;
- Für eine größere betriebliche Effizienz an den von der MEGA organisierten Management- und Schlichtungssitzungen teilnehmen.

13. REVERSIBILITÄT

Die Daten des Kunden werden für einen Zeitraum von 3 Monaten ab dem Datum der Beendigung oder des Auslaufens der Services aufbewahrt. Während dieses Zeitraums hat der Kunde keinen Zugang mehr zu den Services. Der einzige Zweck dieses Zeitraums besteht darin, dem Kunden die Möglichkeit zu geben, im Bedarfsfall eine Rückgängigmachungsfrist einzurichten. Nach Ablauf dieses 3-monatigen Zeitraums werden die Daten endgültig gelöscht.
Der Kunde kann dies beantragen:

- Nur die Aufbewahrung von Daten für einen Zeitraum, der über den genannten Zeitraum von 3 Monaten hinausgeht.
- Oder zur Ausführung von Umkehrbarkeitsdiensten, wie unten definiert.

Verlängerungen der Aufbewahrungsfrist und/oder Reversibilitätsdienste müssen spätestens 2 Monate nach dem Datum der Beendigung oder des Auslaufens der Services bei der MEGA eingehen.
Die Verlängerung der Retentions- und/oder Reversibilitätsdienste wird gemäß der Preisliste der MEGA in Rechnung gestellt, die an dem Tag gilt, an dem MEGA ihr Angebot an den Kunden sendet.
Der Zweck der Reversibilitätsdienste ist die Wiederherstellung der Daten des Kunden in der HOPEX-Datenbank.
MEGA bietet zwei Arten von Reversibilitätsdiensten an: einfache und komplexe Reversibilität.

- Grundlegende Reversibilität: MEGA stellt dem Kunden Backups der Produktionsdaten zur Wiederherstellung in der gleichen Version des MS-SQL-Server DBMS zur Verfügung, die mit der gleichen HOPEX-Lösung in der gleichen Version verwendet werden können.
  Die Daten werden entweder (i) dem Kunden auf einem MEGA-FTP-Server zum Herunterladen zur Verfügung gestellt oder (ii) auf den Server des Kunden oder seines Lieferanten gesendet (SFTP). Es liegt in der alleinigen Verantwortung des Kunden, das Recht auf Zugang zum Repository zu gewähren. MEGA empfiehlt eine entsprechende Schulung für die Verwaltung der Lösung.
- Komplexe Reversibilität: Diese Services sind anwendbar, wenn die grundlegende Reversibilität den Bedürfnissen des Kunden nicht entspricht. Sie können geeignet sein, wenn Daten in eine alternative Softwarelösung hochgeladen werden müssen.
  Der Zweck einer komplexen Reversibilität ist die Bereitstellung von:
    - Einem UTF-8-kodierter XML-Export des Datenbank-Dumps;
    - Unterlagen über die Verarbeitung des XML-Formats;
    - Einem anerkannten Transfer von sowohl funktionalen als auch technischen Fähigkeiten an das mit der Übernahme beauftragte Team, um das Datenmodell der Lösung sowie die Besonderheiten der implementierten Lösung und den bereitgestellten Export zu verstehen.

  Der Kunde ist dafür verantwortlich, dass die übernommenen Daten korrekt sind und vollständig in die neue Lösung integriert werden.
  Die komplexe Reversibilität unterliegt einem Festpreis.
- Sonstiges: Wenn der Kunde zusätzliche Services in Auftrag geben möchte, muss er MEGA seinen detaillierten Bedarf schriftlich mitteilen. MEGA führt eine Machbarkeitsstudie durch und/oder unterbreitet ein Angebot.

14. ZEITBERECHNUNG

Wenn ein Zeitraum in Stunden angegeben wird, wird er an 7 Tagen in der Woche und 24 Stunden am Tag berechnet.
Wenn ein Zeitraum in Geschäftsstunden ausgedrückt wird, wird er für jeden Werktag von 9 bis 18 Uhr Berliner Zeit berechnet.
Der Zeitpunkt des Ereignisses oder der Mitteilung, das bzw. die den Beginn der Frist auslöst, wird nicht berücksichtigt.
Wenn ein Zeitraum in Arbeitstagen ausgedrückt wird, werden nur die Wochentage von Montag bis Freitag berücksichtigt, mit Ausnahme der französischen Feiertage.
Der Tag des Ereignisses oder der Mitteilung, das bzw. die den Beginn der Frist auslöst, wird nicht berücksichtigt.
Wenn ein Zeitraum in Monaten angegeben ist, wird er unter Berücksichtigung des Datums berechnet.
Der Tag des Ereignisses oder der Mitteilung, das bzw. die den Fristbeginn auslöst, wird nicht mitgezählt.
Fehlt ein solches Datum, verlängert sich die Frist bis zum darauffolgenden ersten Arbeitstag bis Mitternacht.
Wenn eine Frist in Stunden angegeben ist, läuft sie am Ende der Stunde ab.
Wenn eine Frist in Tagen oder Monaten angegeben ist, läuft sie am Ende des letzten Tages um 12 Uhr ab.
Eine in Tagen angegebene Frist, die an einem Samstag, Sonntag oder Feiertag ablaufen würde, wird auf den folgenden ersten Werktag bis Mitternacht verlängert.
Bei Zustellungen per Einschreiben mit Rückschein gilt das Datum der erstmaligen Vorlage des Schreibens mit Rückschein, wobei der Poststempel als Beweis gilt.

15. MEGAS SICHERHEITSVERPFLICHTUNG

15.1. GLOBALE SICHERHEIT

Thema	Beschreibung
TLS	Erforderlich auf den HOPEX-Cloud-Plattformen, um die Sicherheit der Transaktionen zwischen dem Web-Frontend und dem Terminal des Kunden zu gewährleisten. Das Zertifikat, das auf der TLS 1.2 AES256-SHA256-Verschlüsselung basiert, wird vollständig vom MCS-Team (MEGA Cloud Services) zur Verfügung gestellt.
Öffentliches IP-Whitelisting	Die öffentlichen IP-Adressen der Kunden müssen MEGA im Voraus mitgeteilt werden, um Zugang zu den Services zu erhalten.
Nichtmandantenfähige (Single-Tenant) Plattform	Alle Kundenplattformen sind vollständig nichtmandantenfähig (Single-Tenant). Die Umgebungen jedes Kunden werden auf einem dedizierten Server in einem dedizierten VLAN installiert, vollständig voneinander getrennt.
Völlig voneinander getrennte virtuelle Plattformen werden eingesetzt	Die HOPEX-Cloud-Plattformen werden in der Regel im Standardmodus mit einem virtuellen Server pro Client für die Produktionsumgebung bereitgestellt. Wenn der Kunde das "SaaS-Plattform-Paket" der Standard- oder Premiumstufe bestellt, werden drei isolierte Instanzen bereitgestellt, z. B. : • ENTWICKLUNG: Dedizierter Server, der es dem Kunden ermöglicht, die HOPEX-Lösungen anzupassen und Updates zu testen; • VORPRODUCTION: Dedizierter Server, der bei Bedarf mit der Produktionsplattform synchronisiert wird, so dass der Kunde Aktualisierungen vor ihrer Implementierung in die Produktion validieren und testen kann (z. B. technische und funktionale Einstellungen, Korrektur-Pack (CP)); • PRODUKTION: Die Inhalte, die auf der Produktionsplattform bereitgestellt werden, wurden zuvor auf der Vorproduktionsplattform getestet und freigegeben.
Datenverschlüsselung	Standard-Speicherverschlüsselung von Microsoft Azure SSE mit AES-256-Bit-Verschlüsselung

15.2. Organisation und Management der Informationssicherheit.

Thema	Beschreibung
Informationssicherheitsorganisation und Information Risk Management	MEGA hat eine Informationssicherheitsrichtlinie implementiert, die mit allen Mitarbeitern, einschließlich der Geschäftsleitung, geteilt wird. Die Hauptrollen der MEGA-Mitarbeiter sind wie folgt: • Die Geschäftsleitung genehmigt, fördert und unterstützt Maßnahmen zur Verbesserung der Sicherheit von Informationssystemen; • Der Chief Information Security Officer (CISO) ist für die Sicherheit, Verfügbarkeit und Integrität des Informationssystems verantwortlich; • Der Chief Information Officer (CIO) ist für den Betrieb und die strategische Ausrichtung des Informationssystems verantwortlich; • Es werden Sicherheitsausschüsse gebildet, die sich mit allen Sicherheitsthemen, Risiken, Vorfällen und Compliance befassen.
Enterprise Risk Management	MEGA hat ein Enterprise Risk Management Programm entwickelt und implementiert, um Risiken proaktiv für alle MEGA-Aktivitäten zu analysieren und zu minimieren. Alle Risiken werden jährlich überprüft.
Unabhängige Bewertung des Prüfungsstandards	MEGA HOPEX Cloud Enterprise führt jährlich eine SOC2-Bewertung durch, die von einem externen Auditor durchgeführt wird.

15.3. Richtlinien für die Informationssicherheit.

Thema	Beschreibung
Sicherheitsrichtlinie für Informationssysteme	Dies ist die Politik zur Sicherheit des Informationssystems, die von der MEGA-Leitung umgesetzt und bestätigt und den betroffenen Parteien mitgeteilt wurde. Dieses Dokument wird jährlich überprüft.
Verfahren und Strategien	Grundsätze der Informationssicherheit (Datenklassifizierung, Kryptographie, Passwörter usw.), Normen, Verfahren und Leitlinien werden im Intranet veröffentlicht, jährlich überprüft und bekannt gegeben.
SOC 2 Typ 2 Zertifizierung	MEGA bescheinigt, dass die Services zum Zeitpunkt der Unterzeichnung dieser Vertrag die Kriterien für die SOC2 Typ 2 Zertifizierung erfüllen. Der Klarheit halber sei gesagt, dass MEGA nicht verpflichtet ist, diese Einhaltung während der gesamten Dauer des Abkommens zu gewährleisten.

15.4. Vermögensverwaltung.

Thema	Beschreibung
Verantwortung für Vermögenswerte	MEGA benennt organisatorische Vermögenswerte (Inventar, Eigentum, akzeptable Nutzung und Rückgabe) und definiert angemessene Schutzverantwortlichkeiten.
Klassifizierung von Informationen	MEGA hat eine Reihe geeigneter Verfahren zur Kennzeichnung von Informationen gemäß dem Klassifizierungsschema für Informationen eingeführt.
Umgang mit Medien	MEGA hat eine Sicherheitsabsicherung für MCS-Computer-Teams implementiert. USB-Ports sind deaktiviert. Auf Plattformen werden keine Wechselspeicher verwendet.

15.5. Sicherheit im Personalwesen.

Thema	Beschreibung
Vor Einstellung	MEGA hat alle Background-Checks für alle Kandidaten für eine Anstellung in Übereinstimmung mit den einschlägigen Gesetzen, Vorschriften und Ethikrichtlinien und angemessen zu den Geschäftsanforderungen, der Klassifizierung der zu erreichenden Informationen und den wahrgenommenen Risiken.
Während des Arbeitsverhältnisses	Mitarbeiter von MEGA und externe Nutzer erhalten ein entsprechendes Programm und Schulungen zum Thema Security Awareness sowie regelmäßige Aktualisierungen der Unternehmensrichtlinien und -verfahren, die für ihre Arbeitsaufgaben relevant sind.
Beendigung des Arbeitsverhältnisses und Jobwechsel	MEGA verfügt über ein HR-Verfahren, um jede Beendigung oder jeden Wechsel des Beschäftigungsverhältnisses zu verwalten.

15.6. Physische und ökologische Sicherheit.

Thema	Beschreibung
Sicherheitsbereiche	MEGA hat Sicherheitsperimeter und Richtlinien zur physischen Sicherheit definiert, um Bereiche zu schützen, die entweder sensible oder kritische Informationen und Informationsverarbeitungseinrichtungen enthalten.
Einrichtung	MEGA hat eine Richtlinie zur physischen Sicherheit erstellt, um Geräte vor unbefugtem Zugriff und Stromausfällen zu schützen. Alle Geräte, die Speichermedien enthalten, werden überprüft, um sicherzustellen, dass sensible Daten und lizenzierte Software vor der Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben wurden. Eine Clean-Desk-Richtlinie für Papiere und Wechselmedien und eine Clean-Screen-Policy für Informationsverarbeitungsanlagen sind eingeführt worden. Microsoft Azure erfüllt eine Vielzahl internationaler und branchenspezifischer Compliance-Standards wie ISO 27001, HIPAA, FedRAMP, SOC 1 und SOC 2 sowie beispielsweise länderspezifische Standards: Australien IRAP, Großbritannien G-Cloud und Singapur MTCS (https://azure.microsoft.com/en-us/support/trust-center/).

15.7. Zugriffskontrolle.

Thema	Beschreibung
Zugriffskontrolle	Die globale Zugangspolitik von MEGA basiert auf dem Prinzip des geringsten Privilegs. Regelmäßige Überprüfungen werden vom CISO (Chief Information Security Officer) durchgeführt.
Verwaltung des Nutzerzugriffs	Die Verwaltung der HOPEX-Cloud-Plattformen ist nur für das MCS-Team (MEGA Cloud Services) über einen Bastion-Server zugänglich, der alle auf den Plattformen des Kunden durchgeführten Aktionen aufzeichnet (Log und Video). Die öffentliche IP-Adresse des Kunden muss dem MCS-Team mitgeteilt werden, um den Service zu verbinden.
Verantwortlichkeiten der Nutzer	Jeder Kunde erhält einen HOPEX-Funktionsadministrator-Zugang, der es ihm ermöglicht, alle Benutzer innerhalb des HOPEX-Repository zu verwalten. Dieser Administrator ist auch der Kontakt zwischen dem Unternehmen des Kunden und MEGA.
Zugangskontrolle für Systeme und Anwendungen	Die Authentifizierung gegenüber dem HOPEX Cloud Service kann über ein SSO mit SAML 2.0, OpenID Connect (OIDC) Protokollen erfolgen.

15.8. Betriebssicherheit - Systemsicherheit.

Thema	Beschreibung
Betriebssicherheit	MCS dokumentierte alle Betriebsverfahren gemäß ITIL Best Practices (CAB), um die Plattformen des Kunden unter optimalen Bedingungen zu erhalten.
Schutz vor Malware	MEGA hat Kontrollen zur Erkennung, Vorbeugung und Wiederherstellung zum Schutz vor Malware implementiert. Diese technischen Maßnahmen werden mit einer entsprechenden Sensibilisierung der Administratoren kombiniert.
Backup	Auf den HOPEX-Cloud-Plattformen werden regelmäßig automatische, verschlüsselte Backups durchgeführt, die es ermöglichen, die Produktionsdaten des Kunden im Falle eines Vorfalls wiederherzustellen.
Protokollierung und Überwachung	Auf den HOPEX Cloud Enterprise-Plattformen werden zusätzlich zum Überwachungs-Tool HOPEX Server Supervisor, das in alle Client-Plattformen eingebettet ist und dem HOPEX-Administrator ermöglicht, jede auf dem System durchgeführte Aktion zu verfolgen (z. B. erfolgreiche/ fehlgeschlagene Benutzerauthentifizierung, Änderung von Benutzerprofilen/Rechten usw.), alle Plattformprotokolle durch eine MCS-Drittanbieterlösung zur Analyse aufgezeichnet. Das MCS-Team überwacht kontinuierlich die Verfügbarkeit der Plattformen jedes Kunden mit Hilfe eines speziellen Überwachungssystems, das die MCS-Administratoren im Falle einer Anomalie benachrichtigt.
Kontrolle der Betriebssoftware	MCS verwaltet das Informationssystem gemäß den ITIL-Empfehlungen (Änderungsmanagement, usw.).
Technisches Schwachstellenmanagement	MEGA R&D verwendet die Coverity-Lösung, um den HOPEX-Quellcode auf Schwachstellen zu überprüfen (tägliche Überprüfung). Bei jeder größeren Version wird ein Audit durch einen Dritten durchgeführt. MEGA hat einen Schwachstellenprozess entwickelt, um Bedrohungen und Schwachstellen von Systemen, Software und Anwendungen effektiv und zeitnah zu managen und so das Risiko einer möglichen Ausnutzung und Kompromittierung zu mindern.
Bemerkungen zur Prüfung von Informationssystemen	Planmäßige Wartung (Betriebssystem, Hardware usw.): System- und Software-Wartungen werden am Wochenende für ein paar Stunden durchgeführt. Außerplanmäßige Wartung: Patches, Anpassungen oder kritische Updates von HOPEX können außerhalb der Arbeitszeiten durchgeführt werden und werden gemeinsam mit dem Kunden geplant.

15.9. Kommunikationssicherheit - Netzwerksicherheit.

Thema	Beschreibung
Verwaltung der Netzsicherheit	Alle Client-Plattformen sind vollständig nichtmandantenfähig (Singletenant). Jede Client-Plattform ist auf einem dedizierten Server installiert, der innerhalb eines separaten VLANs von den anderen isoliert ist. Jede Plattform verfügt über eine eigene Firewall (MS Azure Network Security Group) zur Durchsetzung und Kontrolle des Netzwerkverkehrs.
Übertragung von Informationen	Web-Transaktionen müssen TLS-verschlüsselt sein, um die Transaktionen zwischen dem/den Webserver(n) und der/den Client-Site(s) zu sichern. Das TLS 1.2-Zertifikat, das auf der AES256-SHA256-Verschlüsselung basiert, wird vollständig vom MCS-Service (MEGA Cloud Services) verwaltet. Darüber hinaus müssen die öffentlichen IP-Adressen des Kunden an MEGA übermittelt werden, um dem Service beizutreten. Diese technische Maßnahme wird von einer Datensicherheitsschulung für die Administratoren und einer Vertraulichkeits- und Geheimhaltungsvereinbarung begleitet. Im Falle einer Datenübertragung müssen die Daten über eine Übertragung vom Typ SFTP übertragen werden.

15.10. Systembeschaffung, -entwicklung und -wartung

Thema	Beschreibung
Sicherheitsanforderungen an Informationssysteme	MEGA liefert Hauptversionen alle 18 bis 24 Monate und Nebenversionen alle 3 Monate, einschließlich aller Sicherheitspatches und Weiterentwicklungen.
Sicherheit in Entwicklungs- und Supportprozessen	Das Design von HOPEX wird vollständig von MEGA verwaltet. In der Forschungs- und Entwicklungsabteilung von MEGA gibt es einen SSM (Software Security Manager), der für die Entwicklung zuständig ist: • Festlegung der besten Kodierungspraktiken unter dem Gesichtspunkt der Sicherheit; • Überprüfung der Spezifikationen aller Entwicklungsprojekte unter Sicherheitsaspekten; • Persönliche Leitung der Entwicklung von sicherheitsrelevanten Modulen (Authentifizierung usw.); • Verwaltung von Kampagnen für Code-Scans und Folgemaßnahmen zur Schadensbegrenzung. MEGA setzt keine Outsourcing-Entwicklung ein, um seine Lösung zu entwickeln. Für den Fall, dass Kunden ihre HOPEX-Plattform anpassen müssen (z. B. Änderungen am Metamodell), ist eine optionale HOPEX Cloud Workbench erforderlich.
Testdaten	MEGA verwendet eine Testdatenbank mit Dummy-Daten.

15.11. Informationssicherheitsaspekt des Business Continuity Managements.

Thema	Beschreibung
Kontinuität der Informationssicherheit	Die Datenintegrität wird durch die Geo-Redundant Storage (GRS)-Technologie gewährleistet, die es ermöglicht, Sicherungsdaten in ein sekundäres Rechenzentrum zu replizieren, das die gleiche Sicherheitsstufe wie das primäre Rechenzentrum aufweist.
Redundanzen	MEGA hat alle Dispositiv-Serviceleistungen implementiert, um eine hohe Verfügbarkeit zu gewährleisten.
Business-Continuity-Plan	MEGA hat einen Geschäftskontinuitätsplan entworfen und umgesetzt. Der Plan enthält 9 Szenarien auf hoher Ebene, die die Geschäftskontinuität gefährden könnten, sowie vordefinierte Reaktionen für die optimale Behandlung von Problemen.

15.12. Informationssicherheit und Verwaltung von Störfällen

Thema	Beschreibung
Verwaltung von Informationssicherheitsvorfällen und Verbesserungen	MEGA hat einen Prozess zur Verwaltung von Störfällen implementiert, um den normalen Servicebetrieb so schnell wie möglich wiederherzustellen und die negativen Auswirkungen auf den Geschäftsbetrieb zu minimieren, um so die bestmögliche Servicequalität und Verfügbarkeit zu gewährleisten. Dieser Prozess umfasst ein Eskalationsverfahren.

15.13. SOC 2 ADD-ON-SICHERHEIT

Thema	Beschreibung
Verschlüsselung	Die Plattformen des Kunden befinden sich auf verschlüsselten Speichersystemen.
CyberArk Bastion	Die Sitzungen der Administratoren auf den Plattformen des Kunden werden durch Bastion aufgezeichnet.