BESCHREIBUNG SAAS HOPEX

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

DER KUNDE WIRD DARAUF HINGEWIESEN, DASS DIE VERWEIGERUNG DER MIGRATION AUF EINE UNTERSTÜTZTE VERSION NICHT NUR DAZU FÜHRT, DASS ER KEINE WARTUNGSLEISTUNGEN EINSCHLIESSLICH DER LIEFERUNG VON PATCHES IN ANSPRUCH NEHMEN KANN, SONDERN AUCH ZU SICHERHEITSPROBLEMEN FÜHRT. 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.
SLA-Anwendungszeitraum	Ist im entsprechenden Bestellformular definiert
Zeitraum der Nichtverfügbarkeit oder Ausfall des Services	Bezeichnet die Zeit innerhalb des SLA-Anwendungszeitraums, in der der Service für die Nutzer nicht verfügbar ist.
Release oder neue Version	Bedeutet eine neue Version der Software, die neue Funktionen und/oder neue Lösungen einführt
Fix	Solche Korrekturen werden in einem Service Pack gebündelt oder manchmal durch ein kumulatives Update bereitgestellt.
Service Pack (SP)	Bedeutet Aktualisierungen, um HOPEX zuverlässiger zu machen. SP bietet einen konsistenten Satz von Korrekturen sowie Sicherheits- und Leistungsverbesserungen, die für ein Release gelten.
Kumulative Aktualisierung	Bezeichnet eine Reihe von Fixes, die von MEGA außerhalb des Kontextes eines Releases oder eines Service Packs erstellt und bereitgestellt werden. Kumulative Updates reagieren in der Regel auf kritische Fehler und können nur auf dem letzten Service Pack 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 des 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 Vorfall, 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 Services mitgeteilt werden.

3. BENUTZERANMELDEINFORMATIONEN

MEGA stellt dem Kundenadministrator, der für die Einrichtung der Zugangsdaten für andere Benutzer verantwortlich ist, die Benutzerdaten zur Verfügung.

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 dazu auffordern, ein Passwort zu ändern oder eine Benutzerkennung ohne vorherige Zustimmung zu löschen.

4. SERVICEVERFÜGBARKEIT

MEGA wird sich in angemessener Weise bemühen, die Services 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. Internetstörungen und andere Ereignisse höherer Gewalt;
- Im Falle eines Sicherheitsproblems, wie z. B. einer anormalen, betrügerischen oder missbräuchlichen Nutzung der Services, eines Einbruchs, eines betrügerischen Zugriffs auf die Services durch Dritte oder einer illegalen Datenextraktion aller oder eines Teils der Daten usw., ist der Kunde verpflichtet, die dem Services-Team 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 Werktag	3 Geschäftsstunden
Maximaler monatlicher ungeplanter Ausfall	1 Werktag	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 Zugangsverbots im Bereich des Fallportals 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 laufenden 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. Die geltende Zeitzone ist die mitteleuropäische Zeit.

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 des Kunden und der Sicherheitseinrichtungen;
- Bei einem Störfall, der auf ein Softwareprodukt zurückzuführen ist, das auf dem Computersystem des Kunden installiert ist.
- Bei Nichtverfügbarkeit des Ansprechpartners beim Kunden während eines Ausfalls.
- Bei Weigerung des Kunden, unverzüglich Informationen (oder Zugangsberechtigungen) zur Verfügung zu stellen, die es MEGA ermöglichen könnten, einen Störfall oder einen Fehler zu beheben.

6. SCHWERE DES VORFALLS UND REAKTIONSZEIT

SEVERITY	SITUATION	REAKTIONSZEIT & ERWARTUNG
Kein Zugang	Sicherheitsfragen Plattform außer Betrieb/kein Zugang für alle Nutzer	1 Arbeitsstunde
Kritisch	Erhebliche Beeinträchtigung einer oder mehrerer Funktionalitäten Kritische Auswirkungen auf den Betrieb	Der Kunde wird innerhalb von 4 Arbeitsstunden kontaktiert. • Tägliche kontinuierliche Arbeit während der Arbeitszeit. • Schnelle Eskalation an den technischen Support und an die Produktmanager. • Zeitnahe Zuteilung geeigneter Ressourcen. • Aufstellung eines Aktionsplans. • Je nach Komplexität des Fehlers kann ein Workaround (frühzeitige Lösung) bereitgestellt werden, um die Betriebsunterbrechung zu minimieren.
Mäßig	Beeinträchtigung der Funktionsfähigkeit. Die Arbeit kann zufriedenstellend fortgesetzt werden, ist aber beeinträchtigt. Mäßige Auswirkungen auf den Betrieb	Der Kunde wird innerhalb von 1 Arbeitstag kontaktiert. • Zuteilung von Ressourcen zur Aufrechterhaltung einer konstanten Leistung während der Arbeitszeit. • Ein Aktionsplan kann vorgelegt werden.
Unerheblich	Geringfügige Beeinträchtigung einer oder mehrerer Funktionalitäten. Keine Auswirkungen auf den Betrieb.	Der Kunde wird innerhalb von 2 Arbeitstagen kontaktiert. Höchster Aufwand während der Arbeitszeit.

Die Reaktionszeit wird ab dem Tag berechnet, nachdem der Kunde MEGA über den Case Portal-Bereich der Community (https://community.mega.com) über den Fehler informiert hat.

Der technische Support von MEGA kann den Schweregrad herabsetzen, wenn der Kunde nicht in der Lage ist, die notwendigen Ressourcen oder Antworten bereitzustellen, damit MEGA ihre 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 auf der Website des Kunden tätig werden. Der Kunde verschafft MEGA Zugang zu seinen Ressourcen 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	Die neue Version von HOPEX wird während der folgenden Zeiträume gepflegt: 27 Monate lang mit Full Support, dann 9 Monate lang mit Limited Support, und regelmäßig durch Service Packs erweitert. Die spezifische Dauer für jede Version ist in den Support-Richtlinien der MEGA-Community aufgeführt.
Full Support (Volle Unterstützung)	Zeitraum, in dem der Kunde Wartungs- und Supportleistungen erhält, einschließlich der Verbesserung bestehender Funktionen, neuer Funktionen und Produkte sowie Fixes.
Limited Support (Begrenzte Unterstützung)	Zeitraum, der auf den Zeitraum des Full Supports folgt und in dem der Kunde nur kritische Vorfälle durch Hotfixes beheben kann.

8. BACKUP- UND DISASTER-WIEDERHERSTELLUNGSPLAN (erweiterte DRP (Disaster Recovery Plan)-Option)

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 ihre 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, gelten als Archive 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 Arbeitsstunden Archiv: 6 Geschäftsstunden		

8.2. Disaster Recovery Plan (Erweiterte DRP-Option).
Der Kunde kann einen erweiterten DRP erhalten, wenn ein Fehler die Datenbank oder ein Problem die Server betrifft, 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 der Kunde zur Durchführung seines Wiederherstellungsplans (RPO) verwendet,
- Wiederherstellung der Daten des Kunden vom letzten Backup innerhalb des unten definierten Zeitrahmens. Diese Wiederherstellungszeit (RTO) wird von MEGA für die Wiederherstellung des 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 den SaaS-Service durch. Solche Tests werden mit den Full Support Releases (letztes Service Pack) durchgeführt, die am Tag des Penetrationstests auf dem Markt sind. Für jede andere Anforderung des Kunden können zusätzliche Gebühren anfallen. 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-Ansprechpartner bezeichneten Personen sind befugt, Anfrageservices durchzuführen.

Die anfängliche Abdeckung und die verfügbaren Serviceanfragen hängen von dem **SaaS-Plattformpaket ab,** wofür der Kunde abonniert ist:

- Starter
- Standard
- Erweitert

Bei der Initialisierung des Services erhält jeder Kunde einen Basiswert und kann zusätzliche Serviceanfragen mit den folgenden Einschränkungen anfordern:

SaaS-Plattform-Paket		Starter	Standard	Erweitert
Produktion		Ja	Ja	Ja
Vorproduktion		Ja * nur für die Releaseverwaltung	Ja	Ja
Entwicklung		Nicht verfügbar	Ja	Ja
HOPEX 360 Portal		(Option)	1	1
Basislinie				
HOPEX-Instanz		1 Instanz und 1 Repository als Standard (mit maximal 2 Repositories)		
Zugang zum Service		IP-Whitelisting OR Web Application Firewall (WAF, je nach SaaS-Paket, oder als Option erhältlich)		
Authentifizierung		SSO (SAML 2.0, OpenID Connect) und HOPEX-Authentifizierung		
Datenspeicherung		20 GB		
Serviceanfrage inklusive		**Frequenz/Menge MAX**		
Servicekategorie	**Art der Serviceanfrage**	**Starter**	**Standard**	**Erweitert**
Anpassungsmanagement	Ausrichtung nach oben (In die Produktion verschieben)	1 pro Jahr	4 pro Jahr	12 pro Jahr
	Abgleich (Down-alignment)	1 pro Jahr	4 pro Jahr	12 pro Jahr
Benutzerverwaltung	Benutzerverbindungs-protokoll exportieren	1 pro Monat	1 pro Monat	1 pro Monat
	Neuzuweisung eines Benutzers/Profils zu einer Token-Lizenz (benannt)	5 Versetzungen pro Jahr	10 Versetzungen pro Jahr	20 Versetzungen pro Jahr
Zugangsverwaltung	Änderung des Domänennamen des Services	Ersteinrichtung + 1 Änderung pro Jahr	Ersteinrichtung +1 Veränderung pro Jahr	Ersteinrichtung +1 Veränderung pro Jahr
Integrationsmanagement	Planung von Aufgaben	2 Anträge pro Jahr	4 Anträge pro Jahr	6 Anträge pro Jahr
	Anzahl der verfügbaren API/WebService-Verbindungen	Bis zu 1	Bis zu 3	bis zu 6
HOPEX-Laden	Einsatz eines Moduls	10 Anfragen pro Jahr	10 Anfragen pro Jahr	10 Anfragen pro Jahr

Für jede Änderung der Häufigkeit und/oder der Höchstmenge der Serviceanfragen werden zusätzliche Gebühren erhoben.
Für zusätzliche Services, die von der obigen Beschreibung abweichen (im untenstehenden Katalog aufgeführt), werden zusätzliche Gebühren erhoben.

Nicht gelistete Serviceanfragen müssen MEGA zur Genehmigung vorgelegt werden und können aus Sicherheitsgründen abgelehnt werden. Für solche Serviceanfragen wird ein spezielles Angebot erstellt.

In der Produktion/Vorproduktion wird keine Software von Drittanbietern eingesetzt.
Für alle Software von Drittanbietern, die für die Entwicklung angefordert wird (einschließlich Word, Excel usw.), fallen zusätzliche Gebühren an.
Bitte beachten Sie, dass keine integrierte Entwicklungsumgebung (IDE) erlaubt ist (auch nicht in der Entwicklungsphase).

10.1. SLA für Serviceanfragen

Für Standard- und zusätzliche Serviceanfragen gilt das folgende Service Level Agreement.

Service-kategorie	Serviceanfrage	Beschreibung des Services	Lieferzeit des Services
Anpassungs-management	Angleichung (Up-alignment) (Zu Prod verschieben)	Bereitstellen einer Anpassung - aus der Entwicklungsplattform zur Vorproduktionsplattform, - aus der Vorproduktionsplattform auf die Produktionsplattform (vorbehaltlich der Validierung durch den Kunden in der Vorproduktion vor der Produktionsbereitstellung))	1 Arbeitstag Erste Vorproduktion (obligatorisch) + 1 Arbeitstag Produktion
	Abwärtsgerichtete	Wiederherstellung von HOPEX-Daten und/oder Anpassungen aus der Produktion in - Vorproduktion, - Entwicklung.	2 Arbeitstage
Hosting	WebSite / Portal (Hopex 360)	Hosting für mehrere Portale (außer SSO)	5 Arbeitstage
Benutzer-verwaltung	Benutzerverbindungs-protokoll exportieren	Bereitstellung einer HOPEX-Protokolldatei mit allen Benutzerverbindungen, einschließlich Benutzerlizenzen, Benutzernamen, Profilen und Plattformverfügbarkeit.	1 Arbeitstag
	Neuzuweisung eines Benutzers/Profils zu einem Lizenz-Token	Weist bei benannten Lizenzen einem Lizenz-Token einen Benutzer neu zu. Ein Benutzer kann ein Hauptbenutzer, ein Mitwirkender oder ein Betrachter sein. Dieser Service gilt nicht für Floating-Lizenzen.	
Repository-Verwaltung	Zusätzliches Repository	Ein zusätzliches Repository in der Produktion einrichten	1 Arbeitstag
	Repository umbenennen	Ändern Sie den Namen eines vorhandenen Repositorys.	1 Arbeitstag
Zugangs-verwaltung	Ändern Sie den Domänennamen des Services	Ändern Sie die HOPEX-URL von einem Domänennamen "aaa.hopexcloud.com" in "bbb.hopexcloud.com".	2 Arbeitstage
	Whitelisting für eingehende IP aktivieren	Aktivieren Sie autorisierte IP-Bereiche und tragen Sie sie in die Whitelist der Firewall ein. Pro Satz von 5 IP-Bereichen.	1 Arbeitstag
Integrations-management	Planen von Aufgaben	Planen Sie wiederkehrende Aufgaben für das Hoch- oder Herunterladen (falls zutreffend) in und aus der Umgebung des Kunden unter Verwendung eines Secure File Transfer Protocol (SFTP). Bei den geplanten Aufgaben handelt es sich hauptsächlich um Import/Export und die Erstellung statischer Websites. (Entwurf, Produktion und Validierung verbleiben in der Verantwortung des Kunden).	2 Arbeitstage Erste Vorproduktion (obligatorisch) + 1 Arbeitstag Produktion
	API-Schlüssel	Generierung eines API-Schlüssels für die Integration auf Basis von GraphQL (HOPEX WebService) (Design, Produktion und Validierung einer solchen Integration verbleiben in der Verantwortung des Kunden).	1 Arbeitstag
Kontinuitäts-management	Produktionssicherung exportieren	Überträgt eine von MEGA erstellte Produktionssicherungsdatei auf einen SFTP-Server.	1 Arbeitstag
	Einsatz von Advanced DRP	Dieser Service ist erforderlich, wenn Sie nach der Erstinstallation Ihrer HOPEX Cloud die Option Advanced Disaster Recovery Plan abonnieren.	5 Arbeitstage
HOPEX-Laden	Bereitstellung eines im Store verfügbaren Moduls	Liste der verfügbaren Module (evolvierend): https://store.mega.com/modules. (vorbehaltlich der Kundenvalidierung in Preprod vor der Produktionsbereitstellung)	1 Arbeitstag Erste Vorproduktion (obligatorisch) + 1 Arbeitstag Produktion

Darüber hinaus ist MEGA nur dann zu Serviceleistungen verpflichtet, wenn:
- Die Serviceanfrage über das MEGA Community Case Portal geöffnet wird (per E-Mail gesendete Serviceanfragen werden nicht bearbeitet);
- Der MEGA-Ansprechpartner bestätigt, MEGA alle Informationen zur Verfügung gestellt zu haben, die für die Durchführung einer Serviceanfrage erforderlich sind. Die Zeit, die für das Sammeln von Informationen benötigt wird, wird abgezogen.

Für Anfragen, die nicht im Katalog für Serviceanfragen aufgeführt sind:
- Geschätzte Antwortzeit innerhalb von 2 Werktagen
- Untersuchung und Behandlung je nach Antrag

11. ANSPRECHPARTNER UND GOVERNANCE

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

- Verwaltung der Nutzer 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 sie alle notwendigen Informationen zu den Umständen, unter denen der Vorfall aufgetreten ist, sammeln und bereitstellen;
  - jedes Sicherheitsproblem unverzüglich auf dem geeignetsten Weg melden;
- Für eine größere operative Effizienz nehmen an den von der MEGA organisierten Management- und Schlichtungssitzungen teilnehmen.

12. REVERSIBILITÄT

Die Daten des Kunden werden für einen Zeitraum von 3 Monaten ab dem Datum der Kündigung 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 Reversibilitätsservices, wie unten definiert.

Verlängerungen der Aufbewahrungsfrist und/oder Reversibilitätsservices müssen MEGA spätestens 2 Monate nach dem Datum der Kündigung oder des Auslaufens der Services zugehen.

Die Verlängerung der Retentions- und/oder Reversibilitätsservices wird gemäß der Preisliste von MEGA in Rechnung gestellt, die an dem Tag gilt, an dem MEGA dem Kunden ihr Angebot schickt.

Der Zweck der Reversibilitätsservices ist die Wiederherstellung der Daten des Kunden in der HOPEX-Datenbank.

MEGA bietet zwei Arten von Reversibilitätsservices an: einfache und komplexe Services.

- Grundlegende Reversibilität: MEGA stellt dem Kunden Sicherungskopien der Produktionsdaten zur Wiederherstellung in der gleichen Version des MS-SQL-Server DBMS für eine Verwendung mit der gleichen HOPEX-Lösung in der gleichen Version zur Verfügung.

  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 besteht darin, eine solche zu bieten.
  - Ein UTF-8-kodierter XML-Export des Datenbank-Dumps;
  - Eine Dokumentation über die Verarbeitung des XML-Formats;
  - Anerkannter 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 bestellen möchte, muss er MEGA seinen detaillierten Bedarf schriftlich mitteilen. MEGA führt eine Machbarkeitsstudie durch und/oder unterbreitet ein Angebot.

13. 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 angegeben ist, wird er für jeden Geschäftstag von 9 bis 18 Uhr berechnet. Die geltende Zeitzone ist die mitteleuropäische Zeitzone.

Der Zeitpunkt des Ereignisses oder der Mitteilung, das bzw. die den Beginn der Frist auslöst, wird nicht berücksichtigt.

Wenn ein Zeitraum in Arbeitstagen angegeben ist, werden nur die Wochentage von Montag bis Freitag berücksichtigt, mit Ausnahme der Feiertage, die für die MEGA-Filiale, die Auftragnehmer des Kunden ist, gelten.

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.

14. EXTENDED SERVICES OPTIONEN

MEGA bietet im Rahmen des SaaS-Abonnements eine Reihe von optionalen Services an, darunter Premium-Support, Adoptionsservices und Verwaltungsservices, wie unten beschrieben. Diese Services werden als "Extended Services" bezeichnet und zielen darauf ab, den Kunden einen erstklassigen Support und Erfahrungen nach der Implementierung zu bieten.

14.1. Premium-Wartung

Objekt	Beschreibung
Premium Support	
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	
Korrektur 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	Eine funktionale Validierung der Konfiguration nach dem Upgrade auf die neueste HOPEX-Version durchführen
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.

14.2. 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
Follow-up von 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

14.3. Managed Services

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.
Regeln für den Datenzugriff definieren	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 im Kontext einer benutzerdefinierten Plattform.
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.
Coaching und Unterstützung	
Leitfaden	Bereitstellung von bewährten 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 von bewährten Verfahren und Standardanleitungen für die Verwendung von HOPEX
Integration und Schulung der Nutzer	Integration und Schulung neuer Benutzer auf der Grundlage der vorhandenen Dokumentation und Schulungsunterlagen.
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.
Laufende Entwicklung	
Konfiguration	Weiterentwicklung der bestehenden Konfiguration.

15. MEGAS SICHERHEITSVERPFLICHTUNG

15.1. Globale Sicherheit

Thema	Beschreibung
TLS	Auf den HOPEX-Cloud-Plattformen erforderlich, 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 der MEGA im Voraus mitgeteilt werden, um Zugang zu den Services zu erhalten.
Dedizierte Plattform	Die HOPEX-Instanzen jedes Kunden werden auf einem eigenen Server in einem eigenen VLAN installiert, das vollständig von den anderen getrennt ist.
Völlig voneinander getrennte virtuelle Plattformen werden eingesetzt	Die HOPEX-Cloud-Plattformen werden in der Regel im Standardmodus mit einem virtuellen Server pro Kunde für die Produktionsumgebung bereitgestellt. Wenn Sie das "SaaS-Plattform-Paket" der Standard- oder Premiumstufe abonnieren, werden drei isolierte Instanzen bereitgestellt, z. B: • ENTWICKLUNG: Dedizierter Server, der es dem Kunden ermöglicht, die HOPEX-Lösungen anzupassen und Updates zu testen; • PRE-PRODUCTION: Dedizierte HOPEX-Instanz, die bei Bedarf mit der Produktionsinstanz synchronisiert wird, so dass der Kunde Updates vor ihrer Implementierung in der Produktion validieren und testen kann (z. B. Konfiguration, kumulatives Update, Service Pack); • PRODUKTION: Die in der Produktion bereitgestellten Inhalte wurden zuvor in der Vorproduktionsinstanz getestet und genehmigt.
Verschlüsselung der Daten	Standard-Speicherverschlüsselung von Microsoft Azure SSE mit AES-256-Bit-Verschlüsselung

15.2. Organisation und Management der Informationssicherheit .

Thema	Beschreibung
Organisation der Informationssicherheit und Information Risk Mgt	MEGA hat eine Informationssicherheitspolitik eingeführt, die alle Mitarbeiter einschließt. Die Hauptaufgaben des MEGA-Personals sind: • 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 der Einhaltung von Vorschriften befassen.
Risikomanagement im Unternehmen	MEGA hat ein Programm zum Management von Unternehmensrisiken entwickelt und implementiert, um Risiken proaktiv für alle MEGA-Aktivitäten zu analysieren und zu mindern.
Unabhängige Versicherungsstandards Bewertung	Das HOPEX Cloud Enterprise-Angebot unterliegt einem jährlichen SOC2-Audit durch eine unabhängige dritte Partei.

15.3. Richtlinien für die Informationssicherheit .

Thema	Beschreibung
Sicherheitspolitik 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 mitgeteilt.
SOC 2 Typ 2 Zertifizierung	MEGA bestätigt, dass die Services zum Zeitpunkt der Unterzeichnung dieser Vereinbarung 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 identifiziert die Vermögenswerte der Organisation (Inventar, Eigentum, zulässige Nutzung und Rückgabe) und definiert die entsprechenden Schutzverantwortlichkeiten
Klassifizierung von Informationen	MEGA hat eine Reihe geeigneter Verfahren zur Kennzeichnung von Informationen gemäß dem Informationsklassifizierungsschema eingeführt.
Umgang mit Medien	MEGA hat eine Verbesserung der Sicherheitsrichtlinien für alle MCS-IT-Teams vorgenommen. Auf den Plattformen sind keine austauschbaren Speichermedien erlaubt.

15.5. Sicherheit der Humanressourcen .

Thema	Beschreibung
Vor der Einstellung	MEGA führt bei allen Bewerbern um eine Stelle die erforderlichen Prüfungen und Abgleiche gemäß den geltenden Gesetzen, Vorschriften und ethischen Grundsätzen durch, die den Bedürfnissen des Unternehmens, der Klassifizierung der Informationen, auf die zugegriffen wird, und den wahrgenommenen Risiken entsprechen.
Während der Beschäftigung	MEGA-Mitarbeiter und externe Benutzer nehmen an einem Programm zur Förderung des Sicherheitsbewusstseins teil. Sie erhalten Anweisungen, Schulungen und regelmäßige Aktualisierungen zu den Sicherheitsrichtlinien und -verfahren, die für ihre jeweilige Funktion erforderlich sind.
Beendigung und Wechsel des Beschäftigungsverhältnisses	MEGA verfügt über ein HR-Verfahren, um jede Beendigung oder jeden Wechsel des Beschäftigungsverhältnisses zu verwalten.

15.6. Physische und ökologische Sicherheit .

Thema	Beschreibung
Sichere Bereiche	MEGA definierte Sicherheitsperimeter und physische Richtlinien zum Schutz von Bereichen, die entweder sensible oder kritische Informationen und Informationsverarbeitungseinrichtungen enthalten.
Ausrüstung	MEGA hat physische Maßnahmen ergriffen, um ihre Anlagen vor unbefugtem Zugriff und Stromausfällen zu schützen. Alle Speichermedien werden vor der Wiederverwendung oder Außerbetriebnahme gescannt, um sicherzustellen, dass sensible Daten und lizenzierte Software sicher entfernt oder überschrieben wurden. MEGA hat eine Informationssicherheitspolitik für Arbeitsplätze eingeführt: Schutz von Papierdokumenten und Wechseldatenträgern, Bildschirmsperre. Das HOPEX Cloud Enterprise-Angebot basiert auf der Microsoft Azure-Infrastruktur und erfüllt eine Vielzahl internationaler branchenspezifischer Compliance-Standards wie ISO 27001, HIPAA, FedRAMP, SOC 1 und SOC 2 sowie länderspezifische Standards wie Australien IRAP, UK G-Cloud und Singapur MTCS (https://azure.microsoft.com/en-us/support/trust-center/).

15.7. Zugangskontrolle.

Thema	Beschreibung
Zugangskontrolle	Die globale Zugangspolitik von MEGA basiert auf dem Prinzip des geringsten Privilegs. Regelmäßige Überprüfungen werden vom CISO (Chief Information Security Officer) durchgeführt.
Benutzer Zugangsverwaltung	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 Funktionsadministrator 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. Operative Sicherheit - Systemsicherheit .

Thema	Beschreibung
Operative Verfahren und Zuständigkeiten	MCS dokumentiert alle Betriebsabläufe nach ITIL Best Practices, 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.
Sicherung	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 zu dem in alle Kundenplattformen eingebetteten Überwachungstool HOPEX Server Supervisor, mit dem der HOPEX-Administrator jede auf dem System durchgeführte Aktion verfolgen kann (z. B. erfolgreiche/fehlgeschlagene Benutzerauthentifizierung, Änderung von Benutzerprofilen/Rechten usw.), alle Plattformprotokolle über eine MCS-Drittlösung 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 verwalten und das Risiko einer möglichen Ausnutzung und Gefährdung zu verringern.
Überlegungen 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 Kunden-HOPEX-Instanzen sind dediziert. Jede Kunden-HOPEX-Instanz ist auf einem dedizierten Server installiert, der innerhalb eines separaten VLANs von den anderen isoliert ist. Jeder Server 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 Kundenseite(n) 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 Datensicherheitsbelehrung 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. Anschaffung, Entwicklung und Wartung von Systemen .

Thema	Beschreibung
Sicherheitsanforderungen an Informationssysteme	MEGA liefert alle 18 bis 24 Monate Hauptversionen und alle 3 Monate ein Service Pack mit allen Sicherheitspatches.
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 bei der Entwicklung ihrer Lösung nicht auf Outsourcing. 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 Geschäftskontinuitätsmanagements .

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.
Entlassungen	MEGA implementiert alle dispositiven Services, um eine hohe Verfügbarkeit zu gewährleisten
Geschäftskontinuitätsplan	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. Management von Vorfällen im Bereich der Informationssicherheit .

Thema	Beschreibung
Management von Informationssicherheitsvorfällen und Verbesserungen	MEGA hat einen Prozess für das Incident Management 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 ZUSATZSICHERHEIT

Thema	Beschreibung
Verschlüsselte Speicherung	Die HOPEX-Instanzen des Kunden werden auf verschlüsselten Speichersystemen bereitgestellt.
CyberArk Bastion	Die Sitzungen der Administratoren auf den Plattformen des Kunden werden durch bastion aufgezeichnet.