SLA – Service Level Agreement für kloudease

v1.5 | gültig ab August 2026

Dokumentenhistorie

Version	Datum	Autor	Beschreibung
1.5	20.08.2026	Lukas Fröhner	Leistungserbringer in der Einleitung klargestellt (AOE Solutions GmbH); „öffentliche“ durch „gesetzliche Feiertage“ ersetzt (Support-Zeiten, Ziff. 1.1); Klarstellung in Ziff. 7.6, dass sich die Mehraufwände auf die Verweigerung oder Verzögerung von Updates beziehen; Dokumentenhistorie eingeführt.

Das SLA gilt für alle von der AOE Solutions GmbH („AOE“) bereitgestellten kloudease Plattform-Services, gewählte Add-Ons und Managed Services („kloudease-Dienste“) und definiert die Verfügbarkeits- und Service-Garantien für die kloudease-Dienste.

Die in diesem Service Level Agreement (SLA) definierten Service Level Objectives (SLO) gelten für die jeweiligen Tarif der kloudease-Dienste.
Der für den Kunden maßgebliche Tarif ergibt sich aus dem jeweils gültigen Statement of Work (SOW).

Sofern im Statement of Work (SOW) abweichende Regelungen getroffen wurden, gehen diese den im SLA definierten SLO vor.

1. Verfügbarkeit der kloudease-Dienste

1.1. Die Verfügbarkeit (auch „Availability“ genannt) der kloudease-Dienste richtet sich nach der nachfolgenden Tabelle für die jeweiligen Tarife:

	Starter	Business	Enterprise
Verfügbarkeit	99,5% p.A	99,75% p.A	99,9% p.A
Support-Zeiten	Montags bis Freitags von 9 bis 17 Uhr	Montags bis Freitags von 8 bis 18 Uhr (CET/CEST). Ausgenommen hiervon sind	

	(CET/CEST). Ausgenommen hiervon sind gesetzliche Feiertage in Deutschland und Hessen.	gesetzliche Feiertage in Deutschland und Hessen.

1.2. Die garantierte Verfügbarkeit bezeichnet den vertraglich zugesicherten prozentualen Anteil der Zeit innerhalb eines Messzeitraums von 12 Kalendermonaten („p.A“) ab Bereitstellung der Nutzungsmöglichkeit des jeweiligen Dienstes, in der der vereinbarte Dienst für den Kunden funktionsfähig und nutzbar ist. Die Verfügbarkeit wird anhand der tatsächlich gemessenen Betriebs- und Ausfallzeiten bestimmt.

1.3. Die garantierte Verfügbarkeit gilt als eingehalten, wenn die im Messzeitraum erreichte Verfügbarkeit mindestens dem vereinbarten Mindestwert entspricht.

1.4. Geplante und im Voraus kommunizierte Wartungsfenster bleiben bei der Berechnung der Verfügbarkeit unberücksichtigt.

1.5. Bei der Berechnung der Verfügbarkeit werden ausschließlich Incidents der Prioritätsstufen P1 und P2 berücksichtigt. Die Klassifizierung von Incidents erfolgt gemäß den in diesem SLA definierten Prioritätsstufen.

2. Wartungen

2.1. Geplante Wartungsarbeiten werden in definierten Wartungsfenstern durchgeführt, um die Auswirkungen auf die kloudease-Dienste zu minimieren. Die Wartungsfenster und der Zeitpunkt der Vorankündigung richten sich nach dem SOW.

2.2. Notfall-Wartungen können durch AOE jederzeit durchgeführt werden, wenn kritische Sicherheitslücken geschlossen werden müssen oder die garantierte Verfügbarkeit gefährdet wird.

	Starter	Business	Enterprise
Wartungsankündigung	nach Einplanung in ein Wartungsfenster		
Wartungsfenster	Jederzeit	montags und donnerstags, während der Support-Zeiten, zwischen 15 und 18 Uhr	priorisiert, montags und donnerstags, während der Support-Zeiten, zwischen 15 und 18 Uhr

2.3. Sofern geplante Wartungsmaßnahmen innerhalb eines Wartungsfensters nicht vollständig umgesetzt werden können, erfolgt die Durchführung im nächstfolgenden Wartungsfenster.

2.4. Kunden des Enterprise-Tiers werden bei der Priorisierung von Wartungsmaßnahmen bevorzugt berücksichtigt.

3. Incident Management

3.1. Service Level Objectives definieren die Mean Time To Acknowledge (MTTA) und Mean Time To Repair or Resolve (MTTR) für verschiedene Prioritäten. MTTA ist die Zeit bis zur Bestätigung/Reaktion, und MTTR die Zeit bis zur Wiederherstellung.

3.2. Prioritätsdefinitionen:

P1 (Kritisch): Vollständiger Ausfall der Plattform, keine Services erreichbar

P2 (Hoch): Teilausfall, kritische Funktionen betroffen

P3 (Mittel): Eingeschränkte Funktionalität, Workarounds verfügbar

P4 (Niedrig): Geringfügige Beeinträchtigungen, keine kritischen Auswirkungen

3.3. MTTA (*Mean Time To Acknowledge*) und MTTR (*Mean Time To Recover*) für die jeweiligen Prioritätsdefinitionen ergeben sich aus der nachfolgenden Tabelle für den jeweiligen Tarif:

		Starter	Business	Enterprise
P1	**MTTA**	im Rahmen der garantierten Verfügbarkeit	1h	30min
	MTTR	im Rahmen der garantierten Verfügbarkeit	4h	2h
P2	**MTTA**	im Rahmen der garantierten Verfügbarkeit	2h	1h
	MTTR	im Rahmen der garantierten Verfügbarkeit	16h	4h
P3	**MTTA**	best-effort während der Support-Zeiten	2 Tage während der Support-Zeiten	1 Tag während der Support-Zeiten
	MTTR	best-effort während der Support-Zeiten		3d während der Support-Zeiten
P4	**MTTA**	best-effort während der Service-Zeiten		1 Tag während der Support-Zeiten
	MTTR	best-effort während der Support-Zeiten		

3.4. Soweit eine Behebung „im Rahmen der garantierten Verfügbarkeit“ vorgesehen ist, besteht keine Zusage hinsichtlich einer bestimmten Behebungsdauer für den jeweiligen Incident. AOE gewährleistet insoweit ausschließlich die Einhaltung der vereinbarten Verfügbarkeit gemäß den Service Level Objectives (SLO).

3.5. Incidents, die durch Handlungen oder Unterlassungen des Kunden oder durch von diesem bereitgestellte Konfigurationen, Integrationen oder Workloads verursacht werden, sind nicht von den Service Level Objectives (SLO) umfasst. AOE ist berechtigt, hierdurch entstehende Aufwände gemäß den jeweils geltenden Konditionen für Service-Dienste in Rechnung zu stellen.

4. Sicherheitslücken (Vulnerabilities)

4.1. Sicherheitslücken (CVEs) werden nach ihrem CVSS-Score klassifiziert und entsprechend der Incident-Priorität behandelt:
Critical (CVSS 9.0-10.0): Wird als P2 (Hoch) Incident behandelt
High (CVSS 7.0-8.9): Wird als P3 (Mittel) Incident behandelt

4.2. CVSS < 7.0 werden nach best-effort behandelt

4.3. Die Behebung von Sicherheitslücken (z. B. CVEs) erfolgt, sofern ein vom jeweiligen Hersteller bereitgestellter Fix verfügbar ist oder eine Mitigation mit vertretbarem Aufwand umgesetzt werden kann.

4.4. Sofern weder ein Fix verfügbar ist noch eine Mitigation mit vertretbarem Aufwand möglich ist, ist AOE berechtigt, die betroffene Komponente vorübergehend zu deaktivieren, soweit dies zur Vermeidung einer Kompromittierung erforderlich ist.

4.5. Die Zeiträume zur Beseitigung der Sicherheitslücken ergeben sich aus den Incident-Prioritäten.

5. Business Continuity (BC) / Disaster Recovery (DR)

5.1. Die BC/DR-Ziele definieren die Recovery-Zeiten und Datenaufbewahrung:

- RTO (Recovery Time Objective): Maximale Zeit bis zur Wiederherstellung
- RPO (Recovery Point Objective): Maximaler Datenverlust bei Wiederherstellung

5.2. Die jeweiligen RTO bzw. RPO ergeben sich aus den folgenden SLOs für die jeweiligen Tarife:

	Starter	Business	Enterprise
RTO	best-effort	4h	2h
RPO	24h	4h	2h

6. Retention

6.1. Die Retention-Periode definiert, wie lange Daten gespeichert werden, wobei zwischen Logs, Metriken und Backups differenziert wird.

6.2. Backups werden im Rahmen einer zur Retention-Periode verhältnismäßigen GFS (Grandfather-Father-Son) Aufbewahrungsrichtline archiviert.
GFS ist ein Mehrstufiges Backup-Konzept mit zeitlich gestaffelten Generationen zur Sicherstellung der Wiederherstellbarkeit (z. B. tägliche, wöchentliche und monatliche Sicherungen).

6.3. Die jeweilige Retention-Periode ergibt sich aus der folgenden Tabelle für die jeweiligen Tarife:

	Starter	Business	Enterprise
Logs	30 Tage	90 Tage	180 Tage
Metriken	30 Tage	60 Tage	90 Tage
Backups	30 Tage (GFS)	90 Tage (GFS)	180 Tage (GFS)

7. Updates und Patches

7.1. Updates und Patches der kloudease-Dienste erfolgen im Rahmen der Wartungsplanung durch AOE.

7.2. Updates werden gemäß Semantic Versioning in Security Patches / Bugfixes (Patch-Version), Minor Updates, Major Updates sowie Notfall-Patches klassifiziert.
Die Klassifizierung erfolgt wie folgt:

a. Patch Updates: Änderungen zur Behebung von Sicherheitslücken oder funktionalen Fehlern ohne Erweiterung der bestehenden Funktionalität.
b. Minor Updates: Funktionale Erweiterungen oder Verbesserungen ohne grundlegende Systemänderungen oder inkompatible Schnittstellenänderungen.
c. Major Updates: Änderungen mit grundlegenden funktionalen Erweiterungen oder technischen Anpassungen, die potenziell inkompatible Änderungen beinhalten können.
d. Notfall-Patches: Updates, die zur Abwehr akuter Sicherheitsrisiken oder zur Sicherstellung der Einhaltung vertraglich vereinbarter Service Levels erforderlich sind.

7.3. Updates werden im Rahmen definierter Wartungsfenster durchgeführt; Notfall-Patches können, sofern erforderlich, auch außerhalb definierter Wartungsfenster erfolgen.

7.4. Soweit Updates nicht als Notfall-Patches klassifiziert sind, informiert AOE den Kunden vor deren Durchführung in angemessener Weise.

7.5. Verweigert oder verzögert der Kunde Updates, die für die Sicherheit, Stabilität oder Supportfähigkeit der kloudease-Dienste erforderlich sind, entfällt die SLA-Verpflichtung für alle kloudease-Dienste.

7.6. AOE ist berechtigt, durch Verweigerung oder Verzögerung von Updates entstehende Mehraufwände nach den in den Nutzungsbedingungen vereinbarten Konditionen für Service-Dienste in Rechnung zu stellen.

7.7. Die Einspielung von Updates erfolgt ausschließlich für solche Versionen, die durch die kloudease-Plattform freigegeben und technisch unterstützt werden.

7.8. Die konkreten Zielwerte für das Einspielen von Updates ergeben sich aus der folgenden Tabelle:

	Starter	Business	Enterprise
Patch	best-effort	10 Tage während der Support-Zeiten	5 Tage während der Support-Zeiten
Minor	best-effort		10 Tage während der Support-Zeiten
Major	best-effort		

8. Nutzung eigener Infrastruktur („Bring Your Own Infrastructure“, „BYOI“)

8.1. Sofern der Kunde sich dazu entscheidet, seine eigene Infrastruktur zu nutzen (On-Premise, Private Cloud oder andere Cloud-Provider) gelten vorrangig die nachfolgenden Regelungen zur jeweiligen Verantwortlichkeit.

8.2. AOE ist verantwortlich für:

a. Kubernetes-Plattform Management,
b. Plattform-Updates und Wartung,
c. Monitoring und Observability,
d. Security-Patches für die Plattform,
e. Support und Incident Management.

8.3. Der Kunde ist verantwortlich für:

a. Bereitstellung der Infrastruktur,
b. Infrastruktur-Wartung und Updates,
c. Netzwerk-Konfiguration,
d. Infrastruktur-Sicherheit,
e. Compliance und Governance der Infrastruktur.
f. permanenten Zugang zum Cloud-Provider für AOE mit den für den Betrieb notwendigen Berechtigungen herstellen