AVV – Auftragsverarbeitungsvertrag

für kloudease

v1.2 | gültig ab Juni 2026

AOE Solutions GmbH
Kirchgasse 6 · 65185 Wiesbaden
aoe.com · kloudease.com

Dokumentenhistorie

Version	Datum	Autor	Beschreibung
1.0	31.10.2025	Kevin Schu	Erstveröffentlichung
1.1	31.10.2025	Kevin Schu	Kleinere Korrekturen
1.2	5.6.2026	Daniel Wittich	Erweiterung Löschklausel (Ziff. 8.3); Anpassung Auditkosten (Ziff. 15); Korrektur Nummerierungsverweise (Ziff. 16.3, 16.2, 18.2); TOM-Anlage als separate Anlage A beigefügt; Ziff. 9 verweist auf Anlage A

AOE verarbeitet personenbezogene Daten im Auftrag des Kunden i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung ("DSGVO"). Dieser Auftragsverarbeitungsvertrag ("AVV") konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien in Bezug auf die Auftragsdatenverarbeitung durch AOE.

1. Definitionen

1.1. Personenbezogene Daten sind alle vom Kunden zur Verfügung gestellten Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person ("betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind (Art. 4 Nr. 1 DSGVO).

1.2. Verarbeitung bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Art. 4 Nr. 2 DSGVO).

1.3. Weisungen sind alle Anweisungen, die der Kunde dem AOE erteilt und mit denen AOE zur Verarbeitung personenbezogener Daten aufgefordert wird. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Kunden danach durch einzelne Weisungen geändert, ergänzt oder ersetzt werden ("Einzelweisungen").

2. Gegenstand des Vertrages, Verantwortlichkeit

AOE verarbeitet die personenbezogenen Daten im Auftrag des Kunden. Der Kunde ist für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Weitergabe der personenbezogenen Daten an AOE sowie die Rechtmäßigkeit der Verarbeitung dieser allein verantwortlich ("Verantwortlicher" im Sinne Art. 4 Nr. 7 DSGVO).

3. Dauer

Die Dauer dieses AVV entspricht der Laufzeit der Vertragsbeziehung. Das Recht zur außerordentlichen Kündigung bleibt hiervon unberührt.

4. Art der Verarbeitung

Im Rahmen der Bereitstellung und des Betriebs der kloudease-Plattform verarbeitet AOE personenbezogene Daten des Kunden ausschließlich im Auftrag des Kunden im Zusammenhang mit:

- dem Hosting und Betrieb von Applikationen und Workloads des Kunden,
- der Speicherung und Verarbeitung von Anwendungsdaten,
- der Bereitstellung von Plattformdiensten (z. B. Kubernetes-Cluster, Datenbanken, Messaging-Systeme),
- der Durchführung von Monitoring-, Logging- und Observability-Maßnahmen,
- der Sicherstellung der Verfügbarkeit, Stabilität und Sicherheit der Plattform (z. B. Backup, Restore, Incident Management),

– der Durchführung von Wartungs-, Support- und Sicherheitsmaßnahmen.

Die Verarbeitung erfolgt automatisiert im Rahmen des Betriebs der Plattform und der darauf betriebenen Dienste.

5. Zweck der Verarbeitung

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich zum Zweck der:

– Bereitstellung und des Betriebs der kloudease-Dienste,
– Speicherung und Verarbeitung von durch den Kunden bereitgestellten oder generierten Daten,
– Sicherstellung der Funktionalität, Sicherheit und Stabilität der Plattform,
– Fehleranalyse und Störungsbeseitigung,
– Durchführung von Backup- und Wiederherstellungsmaßnahmen,
– Erfüllung gesetzlicher Aufbewahrungspflichten, soweit diese den Kunden betreffen.

Eine Verarbeitung zu eigenen Zwecken von AOE erfolgt nicht.

6. Art der Daten

Die Verarbeitung kann insbesondere folgende Kategorien personenbezogener Daten umfassen:

– Identifikationsdaten (z. B. Name, Benutzername),
– Kontaktdaten (z. B. E-Mail-Adresse),
– Authentifizierungs- und Zugriffsdaten (z. B. Login-Daten, IP-Adressen),
– Nutzungs- und Logdaten,
– Inhaltsdaten, die durch den Kunden in den betriebenen Anwendungen verarbeitet werden,
– sonstige personenbezogene Daten, die im Rahmen der Nutzung der kloudease-Dienste verarbeitet werden.

7. Kreis der Betroffenen

Die Verarbeitung kann insbesondere folgende Kategorien betroffener Personen betreffen:

– Mitarbeiter des Kunden,
– Endnutzer der durch den Kunden betriebenen Anwendungen,
– Geschäftspartner und Kunden des Kunden,
– sonstige natürliche Personen, deren Daten im Rahmen der Nutzung der kloudease-Dienste verarbeitet werden.

8. Berichtigung, Löschung, Sperrung und Herausgabe von Daten

8.1. Der Kunde kann jederzeit während und nach Beendigung des Vertrages im Rahmen einer rechtmäßigen Einzelweisung die Berichtigung, Löschung, Sperrung und Herausgabe von personenbezogenen Daten verlangen.

8.2. Der Kunde legt die Maßnahmen zur Herausgabe der überlassenen Datenträger und/oder Löschung der gespeicherten personenbezogenen Daten nach Beendigung des Vertrages vertraglich oder durch Einzelweisung fest.

8.3. Nach Beendigung des Vertrages hat AOE sämtliche in seinem Besitz befindlichen Daten sowie erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren und dem Auftraggeber auf Anfrage nachzuweisen. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

9. Technisch-organisatorische Maßnahmen

9.1. AOE trifft technische und organisatorische Maßnahmen zur angemessenen Sicherung der personenbezogenen Daten vor Missbrauch und Verlust, die den Anforderungen der Art. 24, 32 DSGVO entsprechen. Die konkreten technischen und organisatorischen Maßnahmen sind in ***Anlage A*** zu diesem AVV detailliert beschrieben. Anlage A ist Bestandteil dieses Vertrages.

9.2. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es AOE gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, sind zu dokumentieren und dem Kunden auf Anfrage mitzuteilen.

10. Weisungen

10.1. Der Kunde hat das Recht, jederzeit Einzelweisungen über Art, Umfang und Verfahren der Verarbeitung personenbezogener Daten gegenüber AOE zu erteilen. Einzelweisungen müssen schriftlich erfolgen.

10.2. AOE darf personenbezogene Daten nur im Rahmen der vertraglichen Regelungen und Einzelweisungen verarbeiten, es sei denn, dass AOE nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung der personenbezogenen Daten verpflichtet ist.

10.3. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Einzelweisungen des Kunden bei AOE entstehen, bleiben unberührt.

10.4. AOE muss den Kunden von Ausnahmen von der Weisungspflicht aufgrund für ihn geltendem Recht unterrichten, es sei denn gerade dieses Recht verbietet solche Mitteilung wegen eines wichtigen öffentlichen Interesses.

11. Sonstige Rechte und Pflichten von AOE

11.1. AOE hat einen Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 37, 38, 39 DSGVO ausübt. Dessen Kontaktdaten werden dem Kunden zum Zweck der direkten Kontaktaufnahme auf Anfrage mitgeteilt.

11.2. AOE stellt sicher, dass die mit der Verarbeitung der personenbezogenen Daten befassten Mitarbeiter auf das Datengeheimnis verpflichtet werden (Art. 29 DSGVO) und in die Schutzbestimmungen der DSGVO eingewiesen worden sind. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

11.3. AOE unterrichtet den Kunden bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten. Dies gilt auch für etwaige Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach Art. 51–59 DSGVO oder Ermittlungen nach Art. 83, 84 DSGVO.

11.4. Es ist bekannt, dass AOE nach Art. 33 DSGVO Informationspflichten im Falle der unrechtmäßigen Übermittlung oder Kenntniserlangung von bestimmten personenbezogenen Daten treffen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Kunden mitzuteilen. Die Meldung von AOE an den Kunden muss insbesondere folgende Informationen beinhalten:

- Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der betroffenen personenbezogenen Datensätze;
- Eine Beschreibung der von AOE ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

AOE hat angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

11.5. AOE ist verpflichtet, dem Kunden jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen von einer Verletzung des Schutzes personenbezogener Daten betroffen sind. Die datenschutzkonforme Vernichtung von Material übernimmt AOE auf Grund einer Einzelbeauftragung durch den Kunden auf dessen Kosten. In besonderen, vom Kunden schriftlich zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

11.6. Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten von AOE) wird vom Kunden gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, sichert AOE zu, dass die Maßnahmen nach Art. 32 DSGVO auch für Tele- und Heimarbeit sichergestellt werden.

11.7. Soweit AOE nach diesem AVV Leistungen erbringt, die nicht vertraglich vergütet werden, kann AOE eine angemessene Vergütung verlangen.

12. Rechte und Pflichten des Kunden

12.1. Der Kunde ist für die Beurteilung der Zulässigkeit der Verarbeitung personenbezogener Daten sowie für die Wahrung der Rechte der Betroffenen allein verantwortlich.

12.2. Der Kunde hat AOE unverzüglich und vollständig schriftlich zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

12.3. Dem Kunden obliegen die aus Art. 33 DSGVO resultierenden Informationspflichten.

12.4. AOE unterstützt den Kunden bei der Durchführung von Datenschutzfolgenabschätzungen (Art. 35 DSGVO) und bei Konsultationen der Aufsichtsbehörde (Art. 36 DSGVO).

13. Anfragen Betroffener

13.1. Ist der Kunde auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Verarbeitung dessen personenbezogener Daten zu geben, wird AOE den Kunden, soweit erforderlich, dabei unterstützen, diese Informationen bereitzustellen, vorausgesetzt der Kunde hat AOE hierzu schriftlich aufgefordert.

13.2. AOE wird den Kunden darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber AOE geltend machen.

14. Zusammenarbeit mit der Aufsichtsbehörde

Der Kunde und AOE und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

15. Kontrollpflichten des Kunden

Der Kunde überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen von AOE und dokumentiert das Ergebnis. Hierfür kann er etwa:

- Selbstauskünfte und Nachweise von AOE einholen (z. B. Zertifikate, Auditberichte, Testate),
- auf eigene Kosten ein Audit durchführen oder durch Dritte durchführen lasse.

Audits sind vorab schriftlich anzukündigen und auf das erforderliche Maß zu beschränken. Pro Kalenderjahr ist ein reguläres Audit ohne gesonderten Nachweis eines Anlasses zulässig. Ergeben sich konkrete Anhaltspunkte für eine Verletzung datenschutzrechtlicher Pflichten durch AOE, sind Audits unabhängig von dieser Begrenzung zulässig.

16. Subunternehmer

16.1. Die Beauftragung von Subunternehmen ist im Rahmen dieses AVV und der in Ziff. 4, 5, 6 konkretisierten Tätigkeiten möglich, sofern AOE sicherstellt, dass der Subunternehmer die Pflichten aus diesem AVV gegenüber AOE übernimmt. Es gelten insbesondere die in diesem AVV festgelegten Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit.

16.2. Dem Kunden sind Kontroll- und Überprüfungsrechte entsprechend Ziff. 15 einzuräumen. Durch schriftliche Aufforderung ist der Kunde berechtigt, von AOE Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

16.3. Die von AOE beauftragten Subunternehmer können hier eingesehen werden: https://kloudease.com/de/auftragsverarbeitungsvertrag/

Die zum Zeitpunkt des Vertragsschlusses dort aufgeführten Subunternehmer gelten als vom Kunden genehmigt. AOE ist berechtigt, weitere Subunternehmer zu beauftragen, sofern sie die Anforderungen gemäß Ziff. 16.1 erfüllen und AOE den Kunden hiervon in Kenntnis setzt und dieser nicht binnen sieben Tagen schriftlich widerspricht.

17. Vertraulichkeitsverpflichtung

AOE ist bei der Verarbeitung von personenbezogenen Daten zur Wahrung der Vertraulichkeit verpflichtet. AOE verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Kunden obliegen. Der Kunde ist verpflichtet, AOE etwaige besondere Geheimnisschutzregeln schriftlich mitzuteilen.

18. Allgemeine Regelungen, Informationspflichten, Schriftformklausel, Rechtswahl

18.1. Sollten personenbezogene Daten bei AOE durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat AOE den Kunden unverzüglich darüber zu informieren. AOE wird alle in diesem Zusammenhang

Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den personenbezogenen Daten ausschließlich beim Kunden als "Verantwortlichem" im Sinne der DSGVO liegen.

18.2. Die Verarbeitung der personenbezogenen Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Kunden und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44, 45, 46 DSGVO erfüllt sind. Soweit die Verarbeitung durch einen in Ziff. 16.3 genannten Subunternehmer erfolgt, erteilt der Kunde hiermit seine Zustimmung.

Änderungen und Ergänzungen dieses AVV und aller seiner Bestandteile – einschließlich etwaiger Zusicherungen von AOE – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieses AVV handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

Anlage A zum AVV kloudease

Technisch-organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO

Plattform: kloudease | Infrastruktur: STACKIT (Deutschland) | Stand: Juni 2026

1. Zutrittskontrolle

kloudease wird als vollständig cloudbasierte Plattform ohne eigene physische Rechenzentrumsinfrastruktur betrieben. Die zugrundeliegende Infrastruktur wird durch STACKIT (Schwarz IT GmbH & Co. KG) bereitgestellt, einem deutschen Cloud-Anbieter mit Rechenzentren ausschließlich in Deutschland.

- Physische Zutrittssicherung der Rechenzentrumsstandorte obliegt STACKIT gemäß deren Sicherheitskonzept (ISO 27001-zertifiziert)
- AOE-Mitarbeiter haben keinen physischen Zugang zu den Serverräumen
- Nachweise der physischen Sicherheitsmaßnahmen von STACKIT können auf Anfrage bereitgestellt werden

2. Zugangskontrolle

- Zentrales Identity & Access Management über Keycloak als zentralen Identity Provider
- Multi-Faktor-Authentifizierung (MFA): Alle Zugänge zu Produktionssystemen erfordern MFA; Zugang ohne zweiten Faktor ist technisch ausgeschlossen
- Keine generischen Accounts: Jeder Mitarbeiter erhält ausschließlich persönlich zugewiesene Zugangsdaten
- Remote-Zugriff auf Produktionsinfrastruktur ausschließlich über verschlüsselte Verbindungen
- Automatische Session-Timeouts bei Inaktivität

3. Zugriffskontrolle

- Least-Privilege-Prinzip: Zugriffsrechte werden ausschließlich nach dem Prinzip der minimalen Rechtevergabe erteilt
- Rollenbasiertes Berechtigungskonzept (RBAC): Kubernetes-native RBAC-Mechanismen steuern den Zugriff auf Cluster-Ressourcen
- Dedizierte Datenbanken je Kunde: Jeder Auftraggeber erhält eine eigene, dedizierte Datenbankinstanz; ein Datenzugriff zwischen Mandanten ist technisch ausgeschlossen
- Namespace-Isolation: Kundensysteme werden in separaten Kubernetes-Namespaces betrieben
- Regelmäßige Berechtigungsüberprüfung: mindestens quartalsweise; sofortige Deaktivierung bei Mitarbeiterausscheiden
- Physische Datenträger werden protokolliert durch zertifizierte Dienstleister vernichtet

4. Weitergabekontrolle

- Verschlüsselung in Transit: Alle Datenübertragungen über TLS 1.2 oder höher; unverschlüsselte Verbindungen technisch unterbunden
- Verschlüsselung at Rest: Kundendaten werden verschlüsselt auf den STACKIT-Speichersystemen abgelegt
- Kein Datentransfer in Drittländer: Verarbeitung ausschließlich auf STACKIT-Infrastruktur in Deutschland

5. Eingabekontrolle

- Zentrales Logging: Alle Zugriffe, Änderungen und administrativen Aktionen werden in Loki (zentrales Log-Aggregationssystem) erfasst

- Audit-Trail: Administrative Aktionen auf Plattformebene werden mit Benutzeridentität, Zeitstempel und Art der Aktion protokolliert
- Monitoring und Visualisierung über Grafana
- Logs werden basierend auf dem gewählten kloudease Paket aufbewahrt, siehe hierzu SLA

6. Trennungskontrolle

- Mandantentrennung: Daten verschiedener Auftraggeber auf physisch und logisch getrennten Systemen (eigene Cloud Provider Accounts)
- Trennung Produktions-/Testumgebungen: In Testumgebungen werden keine echten personenbezogenen Daten verarbeitet, es sei denn der Kunde richtet dies eigenständig ein

7. Verfügbarkeitskontrolle

- Regelmäßige Backups werden als Teil des Platform Betriebs erstellt. Für Backup-Frequenz, Aufbewahrungsdauer, und Widerherstellungszeiten siehe SLA
- Redundante Infrastruktur: Kritische Plattformkomponenten sind hochverfügbar ausgelegt
- Proaktives Monitoring über Grafana; Schwellenwertüberschreitungen lösen automatische Alarmierungen aus
- DDoS-Schutz durch STACKIT auf Netzwerkebene

8. Auftragskontrolle

- Weisungsgebundene Verarbeitung: Verarbeitung personenbezogener Daten außerhalb des AVV und etwaiger Einzelweisungen findet nicht statt
- Unterauftragsverarbeiter werden ausschließlich nach Abschluss eines AVV gemäß Art. 28 DSGVO beauftragt
- Alle mit der Verarbeitung betrauten Mitarbeiter sind auf das Datengeheimnis verpflichtet und in den Anforderungen der DSGVO geschult

9. Wiederherstellung nach einem Zwischenfall

- Automatisiertes Konfigurationsmanagement: Konfiguration aller Systemkomponenten als Infrastructure-as-Code (IaC) versioniert; ermöglicht automatisierte Wiederherstellung
- Incident-Response-Prozess: unverzügliche Information des Auftraggebers bei Sicherheitsvorfällen oder Datenschutzverletzungen
- Widerherstellungszeiten und Reaktionszeiten basieren auf dem gewählten kloudease Paket und sind den Service Level Agreements zu entnehmen

10. Regelmäßige Überprüfung der Wirksamkeit

- Interne Audits: Sicherheitsmaßnahmen und Berechtigungskonzept mindestens quartalsweise überprüft
- Externer Datenschutzbeauftragter: jährliche Überprüfung des Datenschutzmanagementsystems
- Aktuelle Zertifizierungsnachweise werden auf Anfrage bereitgestellt
- Alle im Cluster verwendeten Container Images werden mit *Trivy* auf bekannte Schwachstellen gescannt und anschließend mit *cosign* signiert

AOE Solutions GmbH	**Auftraggeber (Kunde)**
Ort, Datum	Ort, Datum
Unterschrift, Stempel	Unterschrift, Stempel