

zwischen Verantwortlicher / Auftraggeber

Unternehmen / Name:

Anschrift:

Vertreten durch:

E-Mail:

nachfolgend Verantwortlicher - und Sandra Wöllner, handelnd unter NOEMA AI Am Höhenweg 6, 08371 Glauchau E-Mail: kontakt@noema-ai.de Telefon: 03763 6495508 nachfolgend Auftragsverarbeiter -

1. Gegenstand und Anwendungsbereich

- (1) Diese Vereinbarung gilt, soweit NOEMA AI personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet und die Voraussetzungen einer Auftragsverarbeitung nach Art. 28 DSGVO vorliegen.
- (2) Gegenstand, Dauer, Art und Zweck der Verarbeitung, die Datenarten und Kategorien betroffener Personen ergeben sich aus Anlage 1 sowie aus dem jeweiligen Hauptvertrag, Angebot oder Auftrag. Bei Widersprüchen gehen die datenschutzrechtlichen Regelungen dieser AVV für die Auftragsverarbeitung vor.
- (3) Diese AVV begründet keinen eigenständigen Anspruch auf Leistungen, die nicht im Hauptvertrag beauftragt sind.

2. Weisungsgebundene Verarbeitung

- (1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, soweit keine gesetzliche Verpflichtung zu einer abweichenden Verarbeitung besteht.
- (2) Weisungen können sich insbesondere aus dem Hauptvertrag, dieser AVV, einem dokumentierten Fernwartungsauftrag oder einer sonstigen nachweisbaren Mitteilung ergeben.
- (3) Hält der Auftragsverarbeiter eine Weisung für datenschutzrechtswidrig, informiert er den Verantwortlichen unverzüglich. Die Durchführung der betreffenden Weisung kann bis zur Klärung ausgesetzt werden.
- (4) Eine Verarbeitung zu eigenen, mit dem Auftrag unvereinbaren Zwecken findet nicht statt.
- (5) Ist der Auftragsverarbeiter nach dem Recht der Union oder der Mitgliedstaaten zu einer von dokumentierten Weisungen abweichenden Verarbeitung verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3. Vertraulichkeit

- (1) Der Auftragsverarbeiter stellt sicher, dass Personen, die Zugang zu personenbezogenen Daten erhalten, zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
- (2) Der Zugriff wird auf diejenigen Informationen und Systeme begrenzt, die für den jeweiligen Auftrag erforderlich sind.
- (3) Zugangsdaten, Kennwörter, private Schlüssel, API-Schlüssel und vergleichbare Geheimnisse werden nur über geeignete sichere Wege verarbeitet und nicht unnötig dokumentiert.

4. Technische und organisatorische Maßnahmen

- (1) Der Auftragsverarbeiter trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie Art, Umfang, Umständen und Zwecken der Verarbeitung angemessene technische und organisatorische Maßnahmen nach Art. 32 DSGVO.

(2) Die zum Zeitpunkt des Vertragsschlusses vorgesehenen Maßnahmen sind in Anlage 2 beschrieben. Gleichwertige oder bessere Maßnahmen dürfen weiterentwickelt werden, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Verantwortliche bleibt für die Beurteilung verantwortlich, ob die Maßnahmen für das konkrete Risiko seiner Verarbeitung ausreichend sind.

5. Unterstützung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen der beauftragten

Verarbeitung und unter Berücksichtigung der Art der Verarbeitung angemessen bei:

der Erfüllung von Betroffenenrechten, der Sicherheit der Verarbeitung, der Bewertung und Meldung von Verletzungen des Schutzes personenbezogener Daten, Datenschutz-Folgenabschätzungen und gegebenenfalls vorherigen Konsultationen, der Bereitstellung der zur Erfüllung der Pflichten nach Art. 28 DSGVO erforderlichen Informationen.

Soweit Unterstützungsleistungen nicht bereits vom Hauptvertrag umfasst sind und einen zusätzlichen Aufwand verursachen, kann dieser nach vorheriger Abstimmung gesondert vergütet werden, soweit gesetzlich zulässig.

6. Datenschutzverletzungen

(1) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Daten des Verantwortlichen betrifft.

(2) Die Mitteilung enthält, soweit zu diesem Zeitpunkt verfügbar, die zur Bewertung des Vorfalls erforderlichen Informationen, insbesondere Art des Vorfalls, betroffene Daten und Systeme, bereits ergriffene Maßnahmen sowie eine Kontaktmöglichkeit für Rückfragen.

(3) Die Entscheidung über Meldungen an Aufsichtsbehörden oder betroffene Personen obliegt dem Verantwortlichen, soweit nicht gesetzlich etwas anderes gilt.

7. Weitere Auftragsverarbeiter

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine schriftliche Genehmigung, weitere Auftragsverarbeiter einzusetzen, soweit diese in Anlage 3 aufgeführt oder später nach diesem Abschnitt ordnungsgemäß angekündigt werden.

(2) Beabsichtigte Änderungen durch Hinzuziehung oder Ersetzung eines weiteren Auftragsverarbeiters werden dem Verantwortlichen grundsätzlich mindestens 14 Kalendertage vor dem geplanten Einsatz in Textform mitgeteilt. Der Verantwortliche kann innerhalb dieser Frist aus sachlich begründeten Datenschutzgründen widersprechen.

(3) Bei dringenden Sicherheits- oder Betriebsmaßnahmen kann eine kürzere Frist erforderlich sein. Der Verantwortliche wird dann unverzüglich informiert.

(4) Der Auftragsverarbeiter verpflichtet weitere Auftragsverarbeiter vertraglich im Wesentlichen zu denselben Datenschutzpflichten, die für ihn aus dieser AVV gelten, soweit diese für die jeweilige Verarbeitung einschlägig sind.

(5) Der Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen für die Erfüllung der datenschutzrechtlichen Pflichten des weiteren Auftragsverarbeiters nach Maßgabe des geltenden Rechts verantwortlich.

8. Externe generative KI-Dienste

(1) Externe generative KI-Dienste werden nicht automatisch als weitere Auftragsverarbeiter genehmigt.

(2) Projektbezogene personenbezogene oder pseudonymisierte Daten dürfen an einen externen

generativen KI-Dienst nur übermittelt werden, wenn:

der konkrete Anbieter und Dienst dokumentiert wurden, Zweck und Datenkategorien festgelegt wurden, der Einsatz mit den Weisungen des Verantwortlichen vereinbar ist, der Anbieter datenschutzrechtlich als weiterer Auftragsverarbeiter zulässig eingebunden wurde, soweit dies erforderlich ist, die Anforderungen an eine etwaige Drittlandübermittlung erfüllt sind, und der Verantwortliche den Einsatz ausdrücklich schriftlich freigegeben hat.

(3) Eine Verarbeitung ausschließlich tatsächlich anonymisierter technischer Informationen, bei denen kein Personenbezug hergestellt werden kann, fällt nicht unter die Verarbeitung personenbezogener Daten nach dieser AVV. Pseudonymisierte Daten gelten für diese Vereinbarung weiterhin als personenbezogene Daten.

(4) Die konkrete KI-Freigabe kann im Fernwartungsauftrag oder in einer gesonderten Zusatzvereinbarung dokumentiert werden.

9. Drittlandübermittlungen

(1) Eine Übermittlung personenbezogener Daten außerhalb des Europäischen Wirtschaftsraums erfolgt nur auf dokumentierte Weisung des Verantwortlichen und unter Einhaltung der Vorgaben des Kapitels V DSGVO.

(2) Soweit ein Angemessenheitsbeschluss, Standardvertragsklauseln oder ein anderer zulässiger Übermittlungsmechanismus erforderlich ist, wird dieser vor Beginn der betreffenden Übermittlung dokumentiert.

10. Kontroll- und Nachweisrechte

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen die Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO erforderlich sind.

(2) Der Verantwortliche kann angemessene Kontrollen durchführen oder durch einen zur Vertraulichkeit verpflichteten Prüfer durchführen lassen. Kontrollen sollen mit angemessener Vorankündigung erfolgen und den Geschäftsbetrieb nicht unverhältnismäßig beeinträchtigen.

(3) Vor-Ort-Prüfungen sind nur erforderlich, wenn ein angemessener Nachweis auf anderem Weg nicht genügt oder ein konkreter Anlass besteht.

(4) Zusätzlicher Aufwand für außergewöhnliche Prüfungen kann nach vorheriger Abstimmung berechnet werden, soweit die Prüfung nicht durch einen vom Auftragsverarbeiter zu vertretenden Datenschutzverstoß veranlasst wurde.

11. Rückgabe und Löschung

(1) Nach Abschluss der Auftragsverarbeitung löscht oder gibt der Auftragsverarbeiter personenbezogene Daten nach Wahl des Verantwortlichen zurück, soweit keine gesetzliche Aufbewahrungspflicht oder ein anderer zulässiger Rechtsgrund einer Löschung entgegensteht.

(2) Gesetzlich aufzubewahrende Daten werden für andere Zwecke gesperrt beziehungsweise nur im rechtlich zulässigen Umfang verarbeitet.

(3) Technisch unvermeidbare Sicherungskopien werden im Rahmen regulärer Löscho- und Überschreibzyklen entfernt und bis dahin nicht für andere Zwecke verwendet.

12. Verantwortlichkeit des Auftraggebers

(1) Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung, die Wahrung der Rechte betroffener Personen und die Zulässigkeit seiner Weisungen verantwortlich.

(2) Der Verantwortliche informiert den Auftragsverarbeiter über besondere Schutzanforderungen, insbesondere wenn besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO, strafrechtliche Daten oder besonders schutzbedürftige Personengruppen betroffen sind.

13. Laufzeit und Beendigung

Diese AVV beginnt mit Unterzeichnung und gilt für die Dauer jeder von ihr erfassten Auftragsverarbeitung. Sie endet, wenn keine personenbezogenen Daten des Verantwortlichen mehr im Auftrag verarbeitet werden und die Rückgabe- beziehungsweise Löschpflichten erfüllt sind.

14. Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser AVV sollen mindestens in Textform dokumentiert werden, soweit nicht strengere gesetzliche Anforderungen gelten.

(2) Soweit einzelne Bestimmungen unwirksam sind oder werden, bleibt die Wirksamkeit der übrigen Regelungen unberührt. An die Stelle der unwirksamen Regelung tritt die gesetzliche Regelung.

(3) Im Übrigen gelten die gesetzlichen Vorschriften, insbesondere die DSGVO.

Unterschriften

Verantwortlicher / Auftraggeber

Ort / Datum:

Name / Funktion:

Unterschrift:

Auftragsverarbeiter - NOEMA AI

Ort / Datum:

Sandra Wöllner

Unterschrift:

Anlage 1 - Beschreibung der Verarbeitung

Hauptvertrag / Auftrag / Referenz:

Gegenstand der Verarbeitung:

Dauer:

- ☐ einmaliger Auftrag
☐ für die Dauer des Hauptvertrags
☐ sonstige Dauer: _____

Art und Zweck der Verarbeitung:

- ☐ IT-Support / Fehleranalyse
☐ Fernwartung
☐ Server- oder Systemadministration
☐ Migration / Konfiguration
☐ Web- oder Anwendungsbetrieb
☐ Backup / Wiederherstellung

☐ Sonstiges: _____

Verarbeitungsvorgänge:

- ☐ Einsehen
☐ Erfassen
☐ Ordnen / Strukturieren
☐ Ändern
☐ Übermitteln im Auftrag
☐ Speichern
☐ Löschen
☐ Sonstiges: _____

Kategorien personenbezogener Daten:

- ☐ Stammdaten
☐ Kontaktdaten
☐ Benutzer- und Accountdaten
☐ Kommunikationsdaten
☐ Vertrags- und Abrechnungsdaten
☐ Nutzungs- und Protokolldaten
☐ technische Identifikatoren / IP-Adressen
☐ Inhaltsdaten / Dokumente
☐ besondere Kategorien nach Art. 9 DSGVO - nur nach gesonderter Festlegung
☐ Sonstige: _____

Kategorien betroffener Personen:

- ☐ Beschäftigte
☐ Kunden / Interessenten
☐ Lieferanten / Dienstleister
☐ Nutzer von IT-Systemen oder Websites
☐ Ansprechpartner
☐ Sonstige: _____

Besondere Weisungen / Einschränkungen:**Anlage 2 - Technische und organisatorische Maßnahmen**

Die konkreten Maßnahmen werden risikoadäquat auf den jeweiligen Auftrag angewendet.

A. Zugriff und Berechtigungen

individuelle Zugänge, soweit technisch möglich rollen- und aufgabenbezogene Berechtigungen sichere Authentisierung; bevorzugt Mehrfaktor-Authentisierung, wenn verfügbar SSH-Schlüssel statt Passwortzugang, soweit geeignet kein unnötiger permanenter Fernzugriff zeitliche oder organisatorische Begrenzung von Wartungszugängen

B. Vertraulichkeit und Geheimnisse

Vertraulichkeitsverpflichtung für zugriffsberechtigte Personen keine Speicherung von Kennwörtern in Auftragsformularen sichere Übermittlung von Zugangsdaten über getrennte oder geeignete Kanäle keine Eingabe von Passwörtern, privaten Schlüsseln, API-Schlüsseln oder Wiederherstellungscodes in externe generative KI-Dienste

C. Übertragung und Transport

verschlüsselte Übertragung, insbesondere TLS/HTTPS, SSH oder verschlüsselte Fernwartungsverbindungen Beschränkung von Freigaben auf die für den Auftrag erforderlichen Systeme Prüfung von Zieladressen und Empfängern bei Datenübertragungen

D. System- und Betriebssicherheit

zeitnahe Sicherheitsupdates der eingesetzten Administrationssysteme Firewall- und Zugriffsbeschränkungen, soweit im jeweiligen System verfügbar Schutz vor Schadsoftware nach dem jeweiligen technischen Umfeld Protokollierung sicherheitsrelevanter Vorgänge, soweit erforderlich und verhältnismäßig angemessene Datensicherungs- und Wiederherstellungsverfahren, wenn beauftragt

E. Datenminimierung und Löschung

Zugriff nur auf auftragsrelevante Daten Verwendung anonymisierter Daten, wenn der Zweck dies erlaubt Pseudonymisierung, soweit zweckmäßig; pseudonymisierte Daten bleiben geschützt Löschung oder Rückgabe nach Auftragsende nach Maßgabe dieser AVV

F. Vorfallmanagement

interne Bewertung sicherheitsrelevanter Vorfälle unverzügliche Information des Verantwortlichen bei bekannten Datenschutzverletzungen Mitwirkung bei Ursachenanalyse und erforderlichen Abhilfemaßnahmen

Anlage 3 - Weitere Auftragsverarbeiter

Grundsatz: Nur tatsächlich für die konkrete Auftragsverarbeitung eingesetzte Anbieter werden dokumentiert. Externe generative KI-Dienste sind nicht pauschal freigegeben.

Eintrag 1

Anbieter / Anschrift:

WIIT AG (webtropia), Joachim-Erwin-Platz 3, 40212 Düsseldorf, Deutschland

Dienst / Zweck:

VPS / Mailserver-Infrastruktur und Hosting technischer Systeme, soweit im konkreten Auftrag eingesetzt.

Verarbeitungsort / Drittlandbezug:**Schutzmechanismus, falls erforderlich:**

☐ vom Verantwortlichen genehmigt

Eintrag 2

Anbieter / Anschrift:

AnyDesk Software GmbH, Türlenstraße 2, 70191 Stuttgart, Deutschland

Dienst / Zweck:

Fernwartung / Remote-Support und technische Verbindungsabwicklung, soweit im konkreten Auftrag eingesetzt.

Verarbeitungsort / Drittlandbezug:**Schutzmechanismus, falls erforderlich:**

☐ vom Verantwortlichen genehmigt

Eintrag 3

Anbieter / Anschrift:

TeamViewer Germany GmbH, Bahnhofsplatz 2, 73033 Göppingen, Deutschland

Dienst / Zweck:

Fernwartung / Remote-Support und technische Verbindungsabwicklung, soweit im konkreten Auftrag eingesetzt.

Verarbeitungsort / Drittlandbezug:**Schutzmechanismus, falls erforderlich:**

☐ vom Verantwortlichen genehmigt

Externe generative KI-Dienste

☐ Für diesen Auftrag nicht zugelassen.

☐ Nur nach gesonderter schriftlicher KI-Freigabe gemäß Abschnitt 8 und dem Fernwartungsauftrag.

Datum der zuletzt abgestimmten Liste:

Stand: 01.10.2026. Die tatsächliche Rollenverteilung richtet sich nach der konkreten Verarbeitung und nicht allein nach der Bezeichnung des Vertrags.