

Vertrag über Auftragsverarbeitung (AVV)

Ausgefüllte Version – Kibo AI GmbH als Auftragsverarbeiter

Vertragsparteien

zwischen

– nachfolgend „Verantwortlicher“ genannt –

und

Kibo AI GmbH

Laufertorgraben 2

90489 Nürnberg

– nachfolgend „Auftragsverarbeiter“ genannt –

und gemeinsam als „Vertragsparteien“ bezeichnet – wird Folgendes vereinbart.

Anhang 1 – Auflistung der beauftragten Dienstleistungen und Kontaktdaten

Gegenstand der Verarbeitung

Bereitstellung, Betrieb und Maintenance (Wartung, Updates, technischer Support) der webbasierten SaaS-Plattform **Claritava** zur Umsetzung der EU Entgelttransparenzrichtlinie (2023/970) und des Entgelttransparenzgesetzes. Der Auftraggeber nutzt die Plattform zur Durchführung von Entgeltgleichheitsanalysen, Jobbewertungen nach der Hay-Methode und zur Erfüllung seiner gesetzlichen und internen Berichtspflichten.

Art und Zweck der Verarbeitung

Art der Verarbeitung:

- Erheben durch Übermittlung/Upload von Datensätzen (insb. Gehalts- und Beschäftigtendaten) durch den Auftraggeber in die Plattform des Auftragnehmers
- Speichern, Organisieren, Strukturieren und Zusammenführen der Datensätze in der Plattform
- Auswerten und Analysieren der Daten anhand der Vorgaben der Entgelttransparenzrichtlinie sowie ggf. weiterer, vom Auftraggeber vorgegebener

Kriterien (Vergleich von Entgeltgruppen, Abteilungen, Geschlechtern, Hierarchieebenen)

- Erstellung von Auswertungen, Berichten, Dashboards und Kennzahlen (Statistiken, Aggregationen, Vergleichsanalysen)
- Anonymisierung gemäß § 5 dieses Vertrages
- Einsichtnahme durch Mitarbeiter des Auftragnehmers ausschließlich, soweit dies zur Erbringung der vertraglich geschuldeten Leistungen (Support, Fehleranalyse, Wartung) erforderlich ist

Zweck der Verarbeitung:

- Prüfung und Sicherstellung der Einhaltung der EU Entgelttransparenzrichtlinie 2023/970
- Durchführung interner Entgeltgleichheits- und Entgeltstruktur-Analysen beim Auftraggeber
- Erstellung von Nachweisen und Dokumentationen gegenüber Aufsichtsbehörden oder internen Gremien (Betriebsrat)
- Nutzung der Plattformfunktionen zur nachhaltigen Steuerung und Kontrolle von Vergütungsstrukturen

Art der personenbezogenen Daten

Soweit vom Auftraggeber in die Plattform übermittelt:

- **Stammdaten:** Vorname, Nachname, Personalnummer oder interne Kennungen, ggf. Geburtsjahr, Geschlecht
- **Beschäftigtendaten:** Stellenbezeichnung, Funktion, Abteilung, Organisationseinheit, Eintrittsdatum, Beschäftigungsumfang (Vollzeit/Teilzeit), Hierarchieebene (L1–L8, EX-1), Standort
- **Vergütungsdaten:** Grundgehalt, variable Vergütungsbestandteile (Boni, Provisionen), Zulagen, Sachleistungen, Aktien/Equity, Benefits, historische Vergütungsdaten
- **Vertrags- und Organisationsdaten:** Art des Beschäftigungsverhältnisses, Vollzeit-/Teilzeitstatus, ggf. Informationen zu Abwesenheiten

Besondere Kategorien personenbezogener Daten i. S. d. Art. 9 DSGVO sind vom Auftraggeber grundsätzlich nicht zu übermitteln.

Kategorien betroffener Personen

- Aktive Beschäftigte des Auftraggebers
- Ggf. ehemalige Beschäftigte (rückwirkende Analysen)
- Ggf. Praktikanten, Werkstudenten, Auszubildende, Leiharbeitnehmer

Dauer der Verarbeitung

Für die Dauer des zwischen den Parteien bestehenden Hauptvertrags (SaaS-Nutzungsvertrag Claritava). Nach Vertragsende: Löschung oder Rückgabe gemäß § 10 dieses Vertrages innerhalb von 30 Tagen.

Datenschutzbeauftragte/r

Verantwortlicher (Kundenseite):

Der Verantwortliche hat keinen Datenschutzbeauftragten bestellt.

Auftragsverarbeiter (Kibo AI GmbH):

Der Auftragsverarbeiter hat keinen Datenschutzbeauftragten bestellt.

(Kontakt für Datenschutzfragen: datenschutz@kibo-ai.com – Platzhalter, bitte einrichten)

Anhang 2 – Liste der beauftragten Unterauftragnehmer

Unterauftragnehmer	Anschrift	Verarbeitungsstandort	Beschreibung der Verarbeitung
Google Cloud EMEA Limited	70 Sir John Rogerson's Quay, Dublin 2, Irland	Google Cloud Region europe-west3, Frankfurt am Main, Deutschland	Cloud-Hosting (Cloud Run), Datenbankbetrieb (Cloud SQL PostgreSQL), Speicherung aller Kundendaten, automatische verschlüsselte Backups
Anthropic, LLC	548 Market St, PMB 90375, San Francisco, CA 94104, USA	USA (Verarbeitung auf Anthropic-Servern)	KI-gestützte Generierung von Stellenbeschreibungen und Compliance-Empfehlungen. Hinweis: Es werden ausschließlich nicht-personenbezogene Daten übermittelt (Jobtitel, Level, Abteilungsbezeichnung). Keine Mitarbeiter- oder Vergütungsdaten. Rechtsgrundlage: Art. 46 DSGVO (Standarddatenschutzklauseln / DPA mit Anthropic)
HR4You AG (geplant, nach Aktivierung der Integration)	Stadttor 1, 40219 Düsseldorf, Deutschland	Deutschland	HR-Datensync: Übermittlung von Mitarbeiterstamm- und Vergütungsdaten für automatischen Datenabgleich.

Unterauftragnehmer	Anschrift	Verarbeitungsstandort	Beschreibung der Verarbeitung
			Zertifiziert nach ISO/IEC 27001 + 27701. (3-Wochen-Vorankündigung gemäß § 7 erfolgt gesondert)

Hinweis Anthropic / Drittland: Kibo AI GmbH aktiviert bei Anthropic die Option „Zero Data Retention“ (ZDR), so dass keine übermittelten Daten für Trainingszwecke verwendet werden. Der Abschluss von Standarddatenschutzklauseln (SCCs) mit Anthropic ist dokumentiert.

Anhang 3 – Technische und organisatorische Maßnahmen (TOM)

A. Zutrittskontrolle – Serverräume

A1.0: Ja – personenbezogene Daten werden auf Servern gespeichert.

A1.1 Serverstandort: Google Cloud Platform, Region europe-west3, Rechenzentrumsstandort Frankfurt am Main, Deutschland.

A1.2 Mehrere Standorte: Ja – automatische Backups ebenfalls in Region europe-west3 (georedundant innerhalb Frankfurt).

A1.4 Einheitliche Maßnahmen: Ja – alle Standorte unter Google Cloud Infrastruktur mit einheitlichen Sicherheitsmaßnahmen.

Physische Zutrittskontrolle: Liegt vollständig bei Google Cloud (ISO 27001 zertifiziert, SOC 2 Type II). Google-Rechenzentren sind mit biometrischer Zugangskontrolle, 24/7-Videoüberwachung, Multifaktor-Authentifizierung und Sicherheitspersonal gesichert.

B. Zugangskontrolle (IT-Systeme)

Maßnahme	Umsetzung
Authentifizierung	JWT-Token (RS256), OAuth 2.0 (Google Login), Session-Timeout 24h
Passwort-Policy	Passwörter werden mit bcrypt (Cost Factor 12) gehasht gespeichert (<i>Implementierung bis Go-Live</i>)
Multifaktor-Authentifizierung	Via Google OAuth (wenn Kunde Google-Login nutzt); natives MFA geplant

Maßnahme	Umsetzung
Admin-Zugang	Nur 2 Personen (Entwicklungsteam) haben direkte Datenbankzugriff
Fernzugriff	Ausschließlich über verschlüsselte Verbindung (GCP IAP / VPN)

C. Zugriffskontrolle (Berechtigungen)

Rolle	Datenzugriff	Umfang
ADMIN (Kundenseite)	Alle Daten des eigenen Mandanten	Lesen + Schreiben + Konfiguration
HR	Alle Mitarbeiterdaten des Mandanten	Lesen + Schreiben
MANAGER	Eigene Abteilung	Lesen + eingeschränkt Schreiben (Merit-Proposals)
USER	Eigene Personaldaten	Nur Lesen
Kibo AI Support	Nur mit dokumentierter Kundenerlaubnis, protokolliert	Technischer Support

Mandantentrennung: Strikte TenantId-Filterung auf Datenbankebene bei jeder Abfrage. Technisch kein tenant-übergreifender Datenzugriff möglich.

D. Weitergabekontrolle / Übertragungssicherheit

Maßnahme	Umsetzung
Verschlüsselung in Transit	HTTPS / TLS 1.2+ (erzungen via Cloud Run, HSTS)
Verschlüsselung at Rest	AES-256 (Google Cloud SQL Managed Encryption)
API-Dateiexport	CSV-Export ausschließlich über authentifizierte API-Endpunkte
Drittland-Transfers	Nur Anthropic API (USA) – ausschließlich nicht-personenbezogene Daten; SCCs vorhanden

E. Verfügbarkeitskontrolle

Maßnahme	Umsetzung
Uptime SLA	Google Cloud Run: 99,9 %
Autoscaling	Cloud Run automatische Skalierung
Datenbankbackups	Automatische tägliche Backups (Cloud SQL, 7 Tage Aufbewahrung)
Wiederherstellungszeit	RTO < 4h, RPO < 24h
Monitoring	GCP Cloud Monitoring + Alerting

F. Trennungskontrolle

- Strikte logische Mandantentrennung auf Datenbankebene (TenantId auf jeder Tabelle)
 - Produktions-, Test- und Entwicklungsumgebungen sind getrennt
 - Anonymisierte Benchmark-Daten werden in separater Tabelle gespeichert (kein Join mit Personaldaten)
-

G. Auftragsverarbeitungskontrolle

- Alle Mitarbeiter mit Datenzugang sind zur Vertraulichkeit verpflichtet
- Unterauftragsverarbeiter sind in Anhang 2 dokumentiert
- Datenschutzverletzungen werden unverzüglich (spätestens innerhalb von 24h intern) gemeldet; Weiterleitung an Verantwortlichen innerhalb von 48h