Anlage AVV: Vereinbarung über die Auftragsverarbeitung

Zwischen der Jonas Meyer & Dayan Hindermann GbR, Nordring 1, 34519 Diemelsee, Auftragnehmer, im Folgenden „KBD“ genannt, und dem in der SOW benannten Unternehmen, Auftraggeber, im Folgenden „Kunde“ genannt.

1. Gegenstand und Dauer der Verarbeitung

(1) KBD verarbeitet personenbezogene Daten im Auftrag des Kunden zur Realisierung von Prozessoptimierungen, Automatisierungslösungen, Daten-Middleware, KI-gestützten Workflows, sowie Webdesign.

(2) Die Dauer dieser Vereinbarung richtet sich nach der Laufzeit der zugrunde liegenden Leistungsvereinbarung (SOW).

2. Art und Zweck der Verarbeitung

Zweck der Verarbeitung ist die Steigerung der betrieblichen Effizienz durch Automatisierung und Digitalisierung von Geschäftsprozessen. Dies umfasst das Erheben, Speichern, Filtern, Verknüpfen und Übertragen von Daten zwischen Drittsystemen via API-Schnittstellen sowie die Analyse durch Large Language Models (LLMs). Eine Nutzung der im Auftrag verarbeiteten Daten zum Training von KI-Modellen Dritter ist ausgeschlossen.
Eine Nutzung zum Training eigener KI-Modelle erfolgt ausschließlich anonymisiert oder auf dokumentierte Weisung des Kunden im Rahmen einer gesonderten Vereinbarung.

3. Kategorien betroffener Personen und Datenarten

- **Betroffene Personen:** Mitarbeiter des Kunden, Endkunden, Interessenten, Lieferanten und externe Dienstleister.
- **Datenarten:** Stammdaten (Namen, Titel), Kontaktdaten (E-Mail, Telefon), Vertrags- und Abrechnungsdaten, Kommunikationsinhalte (E-Mails, Chat-Protokolle), technische Metadaten und KI-generierte Analysedaten.

4. Technisch-Organisatorische Maßnahmen (TOMs)

KBD gewährleistet die Sicherheit der Verarbeitung gemäß Art. 32 DSGVO durch folgende Maßnahmen (Auszug):

- **Vertraulichkeit:** Umfassendes Secret-Management und Passwort-Sicherheit über **1Password**; strikte Erzwingung von Multi-Faktor-Authentifizierung (MFA) für alle administrativen Zugänge.
- **Integrität & Trennungsgebot:** Bereitstellung **dedizierter n8n-Instanzen** auf zertifizierten Servern zur physischen oder strikten logischen Datentrennung zwischen Kundenprojekten.
- **Verschlüsselung:** Einsatz von TLS 1.2+ für alle Datentransfers; Encryption-at-Rest für Datenbanken (Supabase/Postgres).
- **Verfügbarkeit:** Hosting auf Hochverfügbarkeits-Infrastrukturen mit automatisierten Backup-Szenarien.

5. Unterauftragsverhältnisse (Sub-Processor)

(1) Der Kunde erteilt KBD die allgemeine Genehmigung, weitere Unterauftragnehmer heranzuziehen oder bestehende zu ersetzen. (2) Die aktuell eingesetzten Unterauftragnehmer sind in **Anhang 1** dieser Vereinbarung aufgeführt. (3) KBD informiert den Kunden über jede beabsichtigte Änderung bezüglich der Hinzuziehung oder Ersetzung von Unterauftragnehmern (via Website-Update). Der Kunde hat das Recht, gegen solche Änderungen binnen 14 Tagen Widerspruch einzulegen. (4) Der Kunde nimmt zur Kenntnis, dass KBD eine tagesaktuelle und verbindliche Liste aller eingesetzten Unterauftragnehmer unter folgender URL bereitstellt: **kassel-bau-digital.de/unterauftragnehmer**

Soweit Unterauftragnehmer in Drittländern (insbesondere den USA) eingesetzt werden, erfolgt dies ausschließlich auf Grundlage geeigneter Garantien gemäß Art. 44 ff. DSGVO, insbesondere durch den Abschluss von EU-Standardvertragsklauseln sowie zusätzlicher technischer und organisatorischer Maßnahmen.

Zusätzliche Schutzmaßnahmen umfassen insbesondere:

- Verschlüsselung personenbezogener Daten vor Übermittlung
- Soweit technisch durch KBD beeinflussbar, erfolgt die Schlüsselverwaltung innerhalb der EU.
- Pseudonymisierung der Daten
- Beschränkung auf technisch notwendige Metadaten

6. Pflichten von KBD

(1) Verarbeitung erfolgt ausschließlich auf dokumentierte Weisung des Kunden.

(2) Verpflichtung aller Mitarbeiter auf das Datengeheimnis.

(3) Unterstützung des Kunden bei der Erfüllung von Betroffenenrechten und bei Datenschutz-Folgenabschätzungen.

(4) Unverzügliche Meldung von Verletzungen des Schutzes personenbezogener Daten an den Kunden. Spätestens jedoch innerhalb von 48 Stunden

7. Kontrollrechte

Der Kunde ist berechtigt, die Einhaltung dieser Vereinbarung durch angemessene Überprüfungen (z. B. Self-Assessments oder Audits durch qualifizierte Dritte) zu kontrollieren. Audits erfolgen nach angemessener Vorankündigung und während der üblichen Geschäftszeiten und dürfen den Geschäftsbetrieb nicht unverhältnismäßig beeinträchtigen.

8. Löschung und Rückgabe

Nach Beendigung der Leistungserbringung löscht KBD alle im Auftrag verarbeiteten Daten innerhalb von 30 Tagen, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

9. Haftung

Es gelten die Haftungsregelungen der Hauptvereinbarung (MSA), sofern die DSGVO keine zwingende gesamtschuldnerische Haftung vorsieht.

Anhang 1: Liste der Unterauftragnehmer

Hinweis: Die nachfolgende Liste entspricht dem Stand bei Vertragsschluss. Da wir unsere Infrastruktur zur Maximierung der Prozesseffizienz stetig optimieren, finden Sie die jeweils verbindliche, tagesaktuelle Fassung unserer Sub-Prozessoren online unter:
> kassel-bau-digital.de/unterauftragnehmer

Unterauftragnehmer	Sitz	Funktion	Ort der Verarbeitung	Rechtsgrundlage
Hetzner Online GmbH	DE	Hosting der n8n-Kundeninstanzen	DE (Nürnberg/Falkenstein)	AVV (DE)

Google Cloud EMEA Ltd.	IE	KI-Infrastruktur (Vertex AI)	DE (Region Frankfurt)	AVV + EU-SCC
Microsoft Ireland Ltd.	IE	Cloud-Collaboration (M365)	EU (Irland / DE)	
Supabase Inc.	USA	Datenbank & Auth-Middleware	EU (Frankfurt)	AVV + EU-SCC
Notion Labs Inc.	USA	CRM & Projektmanagement	USA	AVV + SCC / TIA
Slack Technologies	USA	Error-Handling, Monitoring & Interne Kommunikation	USA	AVV + SCC / TIA
Cohere Inc.	USA	KI-Optimierung (Rerank)	USA / EU	AVV + SCC / TIA
Documentero	PL	PDF-Automatisierung	EU / USA	AVV + EU-SCC
Softr Platforms Inc.	USA	Frontend für Kunden-Apps & Kundendashboard	USA	AVV + SCC / TIA
Calendly LLC	USA	Termin-Automatisierung	USA	AVV + SCC / TIA
Figma Inc.	USA	Prozessmodellierung	USA	AVV + SCC / TIA
Strato AG / Hostinger	DE / EU	Webhosting & Interne Systeme	DE / EU	AVV (DE/EU)