# Auftragsdatenverarbeitung (AVV)

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) wird geschlossen zwischen

dem Kunden
(nachfolgend „Auftraggeber“)

und

Capacities Labs GmbH
St. Martinsweg 3, 66606 St. Wendel
Handelsregister: HRB 108844, Amtsgericht Saarbrücken
E-Mail: team@capacities.io
(nachfolgend „Auftragsverarbeiter“).

Gegenstand dieses Vertrages sind die Rechte und Pflichten der Parteien, die sich aus der Verarbeitung von personenbezogenen Daten im Auftrag gemäß Art. 28 DSGVO ergeben. Dieser Vertrag wird durch die Annahme der Nutzungsbedingungen des Auftragsverarbeiters durch den Auftraggeber wirksam. Eines Zugangs der Annahmeerklärung bedarf es hierbei nicht.

**§ 1 Allgemeines**

1.1. Der Auftragsverarbeiter verarbeitet im Rahmen der Durchführung des zwischen den Parteien geschlossenen Vertrages personenbezogene und sonstige Daten (im Folgenden: „Auftraggeberdaten"), für deren Verarbeitung der Auftraggeber bzw. ggf. weitere berechtigte Gesellschaften verantwortliche Stelle i.S.d. DSGVO ist.

1.2. Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien gemäß Art. 28 DSGVO und ggf. EU KI-Verordnung sowie des Servicevertrages.

1.3. Der Vertrag gilt für alle von Capacities bereitgestellten SaaS-Dienste, inklusive KI-Funktionen, Apps, Schnittstellen und Kommunikationsdienste.

**§ 2 Gegenstand und Zweck der Verarbeitung**

2.1. Die Verarbeitung umfasst insbesondere:

- Hosting und Bereitstellung von Plattformen und Apps zur persönlichen und beruflichen Verwaltung digitaler Informationen;
- Erhebung, Speicherung und Übermittlung von Nutzerdaten (Notizen, Medien, Dokumente etc.);
- Ausführung von KI-basierten Funktionen (z.B. Chat-Assistent, automatische Analysen, Eigenschafts-Zuweisung);
- Synchronisierung und Verarbeitung von Inhalten zwischen Endgeräten und Cloud;
- Verwaltung, Support und Analyse von Nutzungsverhalten zur Verbesserung, Steuerung und Erfolgskontrolle von digitalen Produkten;
- Einbindung externer KI-Dienstleister; Integration weiterer Drittanbieter nach Serviceumfang.

2.2. Zweck ist die Bereitstellung und Verbesserung der vertraglich vereinbarten SaaS-Dienste, einschließlich KI-Feature sowie datenschutzkonforme Performance- und Nutzeranalysen.

2.3. Kategorien personenbezogener Daten:

- Stammdaten (Name, Vorname, E-Mail),
- Inhaltsdaten (Notizen, Texte, Dokumente, Medien, Profilinformationen),
- Kommunikations- und Nutzungsdaten (IP-Adresse, Gerätedaten, App- und Webseiten-Nutzung),

- Metadaten, Kalender-/Task-Daten,
- besonders schützenswerte Daten gemäß Art. 9 DSGVO nur auf ausdrückliche Weisung/Auswahl,
- Support-/Feedback-Daten (Helpdesk),
- Abrechnungsdaten bei Bestellung.

2.4. Die Verarbeitung erfolgt ausschließlich in der EU/EWR, es sei denn, die Beauftragung externer KI-/Cloud-Dienstleister macht einen Drittlandtransfer erforderlich, der den Anforderungen nach Art. 44 ff. DSGVO genügt.

2.5. Im Rahmen der Leistungserbringung kann der Auftragsverarbeiter (z.B. für Support, Reporting, Betrieb der KI-Funktionen) fristweise Daten exportieren und auf eigenen IT-Systemen oder bei Unterauftragsverarbeitern (z.B. Amazon Web Services, Cloudflare, Digital Ocean, Google Ireland, Paddle) zwischenspeichern und analysieren. Diese Verarbeitung dient ausschließlich der Vertragserfüllung.

**§ 3 Rechte und Pflichten des Auftraggebers**

3.1. Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

3.2. Er wahrt die Rechte der Betroffenen und erfüllt Meldepflichten nach Art. 33, 34 DSGVO.

3.3. Der Auftraggeber kann jederzeit schriftlich (auch per E-Mail) Weisungen bezüglich Art, Umfang und Verfahren der Datenverarbeitung erteilen; die Rechtmäßigkeit der Weisungen trägt er selbst.

3.4. Weisungspflichtige Personen werden in Textform benannt und Änderungen dem Auftragsverarbeiter unverzüglich angezeigt.

3.5. Der Auftraggeber informiert den Auftragsverarbeiter unverzüglich bei Fehlern, Unregelmäßigkeiten oder Missbrauch in Bezug auf die Verarbeitung personenbezogener Daten.

**§ 4 Allgemeine Pflichten des Auftragsverarbeiters**

4.1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der Verträge und nach Weisung des Auftraggebers. Gesetzlich verpflichtende anderweitige Verarbeitung wird vorab angezeigt, soweit zulässig.

4.2. Datenverarbeitung findet grundsätzlich in Mitgliedsstaaten der EU/EWR statt. Ausnahmen bei Unterauftragsverarbeitung werden in Anlage 1 dokumentiert und bedürfen Einhaltung der besonderen Voraussetzungen nach Art. 44 ff. DSGVO.

4.3. Der Auftragsverarbeiter kann die Durchführung von Weisungen aussetzen, wenn sie gegen geltende Gesetze verstoßen oder eine eigene Haftung nach Art. 82 DSGVO begründen könnten.

4.4. Beschäftigte sind zur Vertraulichkeit und Verschwiegenheit verpflichtet (schriftlich und/oder aus sonstigem Rechtsgrund).

**§ 5 Datenlöschung und Datensparsamkeit**

5.1. Nach Vertragsende werden sämtliche Auftraggeberdaten vollständig und unwiderruflich nach dokumentiertem Verfahren gelöscht. Löschungen erfolgen manuell durch autorisierte Personen und werden protokolliert.

5.2. Daten in Backups werden nach Löschung maximal 30 Tage vorgehalten und dann endgültig gelöscht.

5.3. Es werden nur die zur Vertragserfüllung erforderlichen Daten verarbeitet. Darüber hinausgehende Daten bleiben ausschließlich beim Auftraggeber.

**§ 6 Meldepflichten**

6.1. Der Auftragsverarbeiter informiert den Auftraggeber über Verstöße gegen Datenschutzvorschriften oder vertragliche Regelungen unverzüglich, spätestens innerhalb von 72 Stunden nach Bekanntwerden.

6.2. Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, wenn eine Aufsichtsbehörde tätig wird und die Auftragsdatenverarbeitung betrifft.

6.3. Unterstützung bei der Umsetzung der Meldepflichten nach Art. 33/34 DSGVO und bei unbefugtem Zugriff erfolgt unverzüglich.

**§ 7 Kontrollbefugnisse**

7.1. Der Auftraggeber kann mindestens einmal jährlich die Einhaltung von Datenschutzvorgaben und Weisungen überprüfen; bei konkretem Verdacht auf Verstöße auch öfter.

7.2. Der Auftragsverarbeiter erteilt alle erforderlichen Auskünfte. Kosten für Audits sowie für Personalaufwand bei Betreuung von Auditierenden trägt der Auftraggeber.

7.3. Ein Nachweis der Einhaltung kann durch Zertifikate, Auditberichte unabhängiger Stellen oder -- bei Zweifeln -- durch Vor-Ort-Kontrolle erfolgen.

**§ 8 Unterauftragsverhältnisse**

8.1. Der Auftragsverarbeiter setzt die in Anlage 1 genannten Unterauftragsverarbeiter ein.

8.2. Ein Wechsel oder eine Erweiterung des Kreises kann innerhalb von zwei Wochen vom Auftraggeber widerrufen werden.

8.3. Der Auftragsverarbeiter haftet nicht für Verstöße Dritter, sofern er Auswahl und Kontrolle nach Maßgabe dieses Vertrages wahrgenommen hat.

**§ 9 Unterstützung bei Betroffenenrechten**

9.1. Der Auftragsverarbeiter unterrichtet den Auftraggeber unverzüglich über Anfragen von Betroffenen bezüglich ihrer Rechte (Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Übertragbarkeit).

9.2. Der Auftragsverarbeiter unterstützt wie angewiesen bei der Beantwortung und Umsetzung der Betroffenenrechte und kann bei erheblichen Mehraufwänden eine Vergütung fordern.

9.3. Bei Datenschutz-Folgenabschätzung (Art. 35 DSGVO) und bei Konsultation der Aufsichtsbehörde (Art. 36 DSGVO) unterstützt der Auftragsverarbeiter nach Maßgabe der Weisung.

**§ 10 Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO**

Der Auftragsverarbeiter trifft die in Anlage 2 beschriebenen Maßnahmen. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit beeinträchtigen können, werden vorab abgestimmt; weniger gravierende Änderungen werden informiert und dokumentiert.

**Anlagen**

**Anlage 1 -- Unterauftragsverarbeiter**

Der Auftragsverarbeiter setzt folgende Unternehmen als Unterauftragsverarbeiter im Rahmen der Vertragserfüllung ein (weitere/aktuelle Liste auf Anfrage):

- Amazon Web Services, Inc. (Hosting, Serverinfrastruktur, Datenspeicherung; EU-Regionen)
- Cloudflare, Inc. (Content Delivery Network, DDoS-Schutz, Web-Performance-Optimierung)
- DigitalOcean, LLC (Zusätzliche Hosting-Services, Infrastrukturdienste)

- Google Ireland Ltd. (Bereitstellung von Google Workspace, Drive/Docs/Cloud; Datenspeicherung, Kollaboration)
- Paddle Ltd. (Abwicklung von Zahlungen; Vertragsrecht UK/EU)
- u.U. weitere KI-Provider und Auftragsverarbeiter nach aktuellem Stand auf Anfrage dokumentiert.

**Anlage 2 -- Technische und organisatorische Maßnahmen (TOM von Capacities 2025)**

1. Vertraulichkeit
   - Zutrittskontrolle Rechenzentrum, gesicherte Endgeräte, Mobilgeräte in verschlossenen Räumen.
   - Zugangskontrolle: persönliche Konten, 2FA, Passwortmanager, regelmäßige Passwortänderung, sichere Cloud-Infrastruktur (ISO-Zertifikate AWS/Google/Cloudflare).
   - User-Daten nur für strikt autorisierte Personen zugänglich; Dokumente und Dateistrukturen mandantenbezogen.
2. Integrität
   - Serverseitige Validierung der Nutzereingaben; mandantengetrennte Speicherung.
   - Datentransfer nur verschlüsselt (HTTPS/TLS); Zugriff auf Datenbanken via Whitelist/Authentifizierung.
   - Endnutzerdaten (z.B. Formulardaten) werden bei Speicherung symmetrisch verschlüsselt.
3. Verfügbarkeit und Belastbarkeit
   - Firewall, aktuelle Sicherheitsupdates, Backup-Konzept (tägliche und stündliche Backups), Testwiederherstellungen vierteljährlich.
   - Beschränkung gleichzeitiger Verbindungen (Rate-Limiting, Überlastungsschutz).
   - Monitoring mit Alarmsystem, Sicherheitsprotokolle und Fehlerberichte monatlich geprüft.
4. Datensparsamkeit und Löschung
   - Minimalprinzip bei Verarbeitung; Löschung von Backups nach Frist, Löschdokumentation.
   - Personenbezogene Daten aus Formularen werden nur für maximal 30 Tage vorgehalten, dann automatisiert gelöscht.
5. Audit und regelmäßige Überprüfung
   - Kontrolle von Zugriffsrechten, Aktualität der Softwarekomponenten, Überwachung sicherheitsrelevanter Systeme.
   - Bei geänderter Verarbeitung oder aktualisierter rechtlicher Lage erneute Bewertung und Anpassung der TOM.
6. Besondere KI-Maßnahmen
   - Verarbeitung von Kontextdaten durch externe KI-Dienstleister wie in der Datenschutzerklärung und den Nutzungsbedingungen vereinbart, Übermittlung ausschließlich auf Grundlage SCC/geeignete Garantien; keine personenbezogenen Daten ins Training/KI-Modelle, Datenspeicherung bei Anbietern nur temporär.
   - Widerspruchs-/Widerrufsrecht für Nutzer („Opt-Out"); Protokollierung aller KI-Datenverarbeitung; Labeling und Transparenzpflicht gemäß EU AI Act.

**§ 11 Sonstiges**

11.1. Anpassungen des Vertrags sind nur nach gemeinsamer Abstimmung und schriftlich wirksam.

11.2. Gerichtsstand und geltendes Recht: Für sämtliche Ansprüche gilt deutsches Recht; Gerichtsstand ist Saarbrücken, soweit zulässig.