

Auftragsverarbeitungs-Vertrag (AVV) — B2B-Variante

Kunden-Platzhalter ({KUNDE_*} in §1) werden bei jeder Signatur individuell gesetzt. Hinweis: Urheber + Zwischen-Lizenzgeberin aus Lizenz-Konstrukt (siehe `decisions/lakeware-lizenz-konstrukt.md`) tauchen in der B2B-AVV **nicht** auf — AVV-Partei ist ausschließlich der operative Auftragsverarbeiter (siehe §1).

1. Vertragsparteien

Verantwortlicher (Kunde, B2B): - Firma: {KUNDE_FIRMA} - Anschrift: {KUNDE_ADRESSE} - USt-IdNr.: {KUNDE_USTID} - Vertreten durch: {KUNDE_VERTRETER}

Auftragsverarbeiter: - Voss Mobil GmbH - Anschrift: Hirschanger 1, 82319 Starnberg - Vertreten durch: Geschäftsführer Christopher Voss - Kontakt: `dsb@lakeware.ai`

2. Gegenstand und Dauer

2.1 Gegenstand: Verarbeitung personenbezogener Daten (pbD) im Rahmen der Nutzung der Lakeware-Plattform (`lakeware.ai`), insbesondere Document Center, Legal Center, Health Center, Tender Center sowie zugehörige Add-Ons.

2.2 Dauer: Laufzeit des zugrundeliegenden Hauptvertrages (SaaS-AGB B2B, `cf/decisions/2026-04-22-agb-b2b.md`), verlängert sich automatisch mit diesem.

3. Art und Zweck der Verarbeitung

3.1 Art: Speichern, Abrufen, Analysieren (KI-Verarbeitung), Strukturieren, Übermitteln von pbD.

3.2 Zweck: Bereitstellung der vertraglich geschuldeten SaaS-Leistung durch den Auftragsverarbeiter gegenüber dem Verantwortlichen.

4. Art der pbD und Kategorien betroffener Personen

4.1 Kategorien pbD: - Stammdaten (Name, Anschrift, Kontakt) - Dokumenteninhalte (vom Kunden hochgeladen, können pbD Dritter enthalten) - Nutzungsdaten (Login, Aktivität, Suchhistorie) - Kommunikationsdaten (Support-Tickets, Chats) -

Bei Health Center: Gesundheitsdaten (Art. 9 DSGVO) — nur bei expliziter Einwilligung des Betroffenen - Bei Legal-Pro: Mandanten-bezogene Daten (u. U. Berufsgeheimnis)

4.2 Betroffene Personen: Mitarbeiter des Verantwortlichen, dessen Kunden/Mandanten/Patienten, deren Angehörige, Dritte aus Dokumenten.

5. Pflichten des Auftragsverarbeiters (Art. 28 DSGVO)

5.1 Verarbeitung ausschließlich auf dokumentierte Weisung des Verantwortlichen (die Nutzung der Plattform gilt als dokumentierte Weisung).

5.2 Vertraulichkeit aller Mitarbeiter (schriftlich verpflichtet).

5.3 Technisch-organisatorische Maßnahmen (TOMs) gemäß Anlage 1.

5.4 Unterauftragsverarbeiter nur mit Genehmigung — Liste in Anlage 2, Widerspruchsrecht des Verantwortlichen bei Neu-Engagement.

5.5 Unterstützung des Verantwortlichen bei Betroffenen-Rechten (Art. 12–22 DSGVO), DSFA (Art. 35) und Datenschutz-Verletzungen (Art. 33 — Meldung an Verantwortlichen binnen 24 h).

5.6 Löschung/Rückgabe aller pbD nach Vertragsende (Wahl des Verantwortlichen). Export-Frist 90 Tage nach Kündigung.

5.7 Nachweis der Einhaltung durch Vorlage TOMs + optional Audit-Right (1×/Jahr, 10 AT Vorankündigung, eigene Kosten).

6. Technisch-organisatorische Maßnahmen (TOMs) — Anlage 1 (Zusammenfassung)

Kategorie	Maßnahme
Zutritt	Server bei services/developer-Host (Deutschland, self-hosted), kein physischer Zugriff durch Dritte
Zugang	OIDC-Auth via Azure-IdP, MFA pflicht, Role-Based-Access-Control
Zugriff	PostgreSQL Row-Level-Security (29 Assertions, 25 Tabellen)
Weitergabe	TLS 1.3, HTTPS-only, Cloudflare-Tunnel
Eingabe	Audit-Log aller schreibenden Operationen, Unveränderbarkeit via Append-Only
Verfügbarkeit	Daily-Backup, Offsite-Replikation, age-verschlüsselt

Kategorie	Maßnahme
Trennbarkeit	Multi-Tenant via RLS, Mandantenfähigkeit über Tenant-ID
Integrität	Gitleaks/Credential-Drift-Block, Code-Review via CI, signierte Commits

Vollständige TOMs separat auf Anfrage.

7. Unterauftragsverarbeiter — Anlage 2

Sub-AV	Zweck	Sitz	DPA
Stripe Payments Europe, Ltd.	Payment-Processing	IE	https://stripe.com/legal/dpa
Mollie B.V.	Payment-Processing (Kanzlei/B2B-Enterprise)	NL	https://www.mollie.com/gb/dpa
Microsoft Ireland Operations Ltd.	MS 365 / Azure-IdP (OIDC)	IE	MS Data Protection Addendum https://
Cloudflare, Inc.	DNS, WAF, Tunnel, Access	US (EU-Data-Boundary aktiv)	www.cloudflare.com/cloudflare-customer-dpa/
Anthropic Ireland Ltd.	KI-LLM für Legal/Document-Analyse	IE	https://www.anthropic.com/legal/data-processing-addendum
OpenAI Ireland Ltd.	KI-LLM (sekundär)	IE	https://openai.com/policies/data-processing-addendum
Google Ireland Ltd.	KI-LLM Gemini (sekundär)	IE	Google DPA

Widerspruchs-Recht: Der Verantwortliche kann der Hinzunahme eines neuen Sub-AV binnen 30 Tagen widersprechen. Bei Widerspruch gegen zwingend erforderlichen Sub-AV: Sonderkündigungsrecht des Verantwortlichen.

8. Pflichten des Verantwortlichen

8.1 Rechtmäßigkeit der Datenerhebung (Rechtsgrundlagen, Einwilligungen).

8.2 Information der Betroffenen (Art. 13/14 DSGVO).

8.3 Prüfung der TOMs des Auftragsverarbeiters vor Vertragsbeginn (siehe §6).

9. Haftung

9.1 Gemäß Art. 82 DSGVO + Regelungen des Hauptvertrages.

9.2 Haftungs-Obergrenze Auftragsverarbeiter: 12-Monats-Netto-Umsatz aus Hauptvertrag, außer bei Vorsatz/grober Fahrlässigkeit.

10. Schlussbestimmungen

10.1 Schriftform. Vorrang dieses AVV vor Hauptvertrag bei Widerspruch in Datenschutz-Punkten.

10.2 Gerichtsstand: Sitz des Auftragsverarbeiters, wenn Verantwortlicher Kaufmann/ juristische Person.

10.3 Salvatorische Klausel.

Ort, Datum: _____

Verantwortlicher: _____

Auftragsverarbeiter (Voss Mobil GmbH): _____

Metadaten für CFO-interne Use

- **Signatur-Flow:** DocuSign via finance@lakeware.ai Admin-Account (ab Do 30.04 scharf)
- **Archivierung:** /legal-archive/avv/{kunden-id}/{datum}.pdf — GoBD-konform via Lexware-Upload
- **Rezert-Takt:** bei Sub-AV-Änderungen → Neuversand an alle aktiven B2B-Kunden innerhalb 30 Tage