

Auftragsbearbeitungsvertrag (DPA)

Vorlage — Stand: 29. April 2026 · Version v1-2026-04

Dieser Auftragsbearbeitungsvertrag (nachfolgend «**DPA**») regelt die Bearbeitung personenbezogener Daten durch die TecMinds GmbH («**Auftragsbearbeiter**») im Auftrag der Kund:in («**Verantwortliche**») im Rahmen der Wield-Plattform. Er ergänzt den Hauptvertrag und gilt mit dessen Unterzeichnung als angenommen. Vorlage als editierbares [DOCX](#) oder [PDF](#) erhältlich.

1. Parteien und Rollen

Verantwortliche: die im Hauptvertrag genannte Kund:in (im Sinn von DSGVO Art. 4 Nr. 7 / nDSG Art. 5 lit. j).

Auftragsbearbeiter: TecMinds GmbH, Neustadtstrasse 8a, 6003 Luzern, Schweiz, UID CHE-334.650.060 (im Sinn von DSGVO Art. 4 Nr. 8 / nDSG Art. 5 lit. k).

2. Gegenstand und Zweck der Bearbeitung

Der Auftragsbearbeiter stellt der Verantwortlichen die SaaS-Plattform Wield zur Verfügung. Die Bearbeitung umfasst:

- Extraktion strukturierter Profile aus hochgeladenen Bewerbungsdokumenten (CV, Zeugnisse);
- Generierung von Kandidat:innen-Dossiers, Bewertungen und Briefings;
- Matching von Kandidat:innen gegen Stellenbeschreibungen und Anforderungsprofile;
- Kommunikations- und Workflow-Funktionen (Interviews, Notizen, Share-Links).

3. Art der Daten und betroffene Personen

Art der Daten: Stammdaten (Name, Kontaktangaben), Lebensläufe, Beschäftigungs- und Ausbildungshistorie, Sprachen, Qualifikationen, optional Foto, Bewertungen, Notizen, Zeugnisse. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO / Art. 5 lit. c nDSG) sind ausgeschlossen, sofern die Verantwortliche keine schriftliche Sondervereinbarung trifft.

Betroffene Personen: Bewerber:innen und Mitarbeitende, deren Daten die Verantwortliche im Rekrutierungsprozess bearbeitet.

4. Pflichten des Auftragsbearbeiters

1. Bearbeitung der Daten ausschliesslich auf dokumentierte Weisung der Verantwortlichen, insbesondere im Rahmen des Hauptvertrags und der Funktionsangebote von Wield.
2. Verpflichtung aller mit der Datenbearbeitung betrauten Personen auf Vertraulichkeit und Schulung in Datenschutz.
3. Umsetzung geeigneter technischer und organisatorischer Massnahmen (TOM) gemäss Anhang B.
4. Unterstützung der Verantwortlichen bei der Beantwortung von Anfragen betroffener Personen (Auskunft, Berichtigung, Löschung, Einschränkung, Datenportabilität, Widerspruch).
5. Unterstützung bei Datenschutz-Folgenabschätzungen (Art. 35 DSGVO) und vorheriger Konsultation der Aufsichtsbehörde (Art. 36 DSGVO).
6. Unverzügliche Meldung von Datenschutzverletzungen an die Verantwortliche, spätestens innerhalb von **72 Stunden** nach Kenntnisnahme, mit allen für eine Behördenmeldung

erforderlichen Informationen.

5. Unterauftragsverarbeiter

Der Auftragsbearbeiter ist berechtigt, weitere Auftragsbearbeiter beizuziehen. Die Verantwortliche stimmt dem Einsatz der in [Anhang A](#) aufgeführten Unterauftragsbearbeiter zu. Wechsel oder Erweiterungen werden mit einer Vorlauffrist von 30 Tagen mitgeteilt; die Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund widersprechen.

6. Datenort und Drittlandtransfers

Primärer Speicherort sämtlicher Kund:innen- und Kandidat:innen-Daten ist die Schweiz (Hosting bei Infomaniak, Genf; Datenbank PostgreSQL bei Infomaniak). LLM-Inferenz und Embeddings erfolgen innerhalb der EU/EWR (Google Vertex AI, Frankfurt und Zürich). Übermittlungen in Drittländer erfolgen ausschliesslich auf Basis der EU-Standardvertragsklauseln (SCC) bzw. eines Angemessenheitsbeschlusses, ergänzt durch geeignete technische Massnahmen (Verschlüsselung im Transit und bei Bedarf at-rest).

7. Aufbewahrung und Löschung

Kandidat:innen-Daten werden 180 Tage nach der letzten Aktivität automatisch gelöscht. Die Verantwortliche kann jederzeit eine vorzeitige Löschung anweisen. Bei Vertragsende werden alle für die Verantwortliche bearbeiteten Daten innerhalb von 30 Tagen gelöscht oder, auf Wunsch, in einem strukturierten, gängigen Format zurückgegeben.

8. Audit- und Kontrollrechte

Die Verantwortliche kann einmal jährlich sowie anlassbezogen (insbesondere nach einer Datenschutzverletzung) die Einhaltung dieses DPA prüfen, bevorzugt durch Vorlage aktueller Sicherheitszertifikate, Pen-Test-Berichten und einer Selbstauskunft des Auftragsbearbeiters. Vor-Ort-Audits sind nach 14-tägiger Voranmeldung möglich; Kosten trägt die anfragende Partei.

9. Haftung und Schlussbestimmungen

Es gilt das im Hauptvertrag vereinbarte Haftungsregime. Bei Widersprüchen zwischen diesem DPA und dem Hauptvertrag geht dieser DPA in Datenschutzfragen vor. Anwendbares Recht: Schweizer Recht; Gerichtsstand Luzern, soweit nicht zwingendes Recht entgegensteht.

Anhang A — Liste der Unterauftragsbearbeiter

Anbieter	Zweck	Standort
Infomaniak (CH)	Hosting, PostgreSQL	Genf, Schweiz
Coolify (CH)	Container-Orchestrierung	Schweiz
Google Vertex AI	LLM (Generierung, Extraktion)	europa-west3 Frankfurt, DE
Google Vertex AI	Text-Embeddings	europa-west6 Zürich, CH
Google Vertex AI	Template-Generierung (ohne PII)	global

Anbieter	Zweck	Standort
Stripe	Abrechnung, Zahlungen	USA (SCC)
Resend	Transaktionale E-Mails	USA (SCC)
Microsoft Azure (optional)	OCR (nur falls aktiviert)	EU

Anhang B — Technische und organisatorische Massnahmen

- Verschlüsselung im Transit (TLS 1.2+) und at-rest (AES-256, Datenbank).
- Tenant-Isolation auf Anwendungs- und (in Vorbereitung) Datenbankebene.
- Mehrstufige Authentifizierung für administrative Zugriffe.
- Tägliche Datenbank-Backups, 30 Tage Aufbewahrung, off-site verschlüsselt.
- Audit-Logs für sicherheitsrelevante Aktionen, mind. 12 Monate.
- Privilege-Minimierung; Trennung von Produktions- und Entwicklungsumgebung.
- Abuse-Schutz: Rate-Limits, Lockout, Web Application Firewall.
- Sicherheitsupdates innert 30 Tagen nach Veröffentlichung; kritische Lücken sofort.
- Schulungen Datenschutz/Sicherheit für alle Mitarbeitenden mit Datenzugriff.

Diese DPA-Vorlage wird vor Vertragsabschluss durch eine Schweizer Rechtsberatung geprüft. Bei Fragen erreichen Sie uns unter privacy@tecminds.ch.