Data Processing Agreement (DPA)

Template — Updated: 29 April 2026 · Version v1-2026-04

This Data Processing Agreement (the **"DPA"**) governs the processing of personal data by TecMinds GmbH (the **"Processor"**) on behalf of the customer (the **"Controller"**) within the Wield platform. It supplements the main contract and takes effect on its signing. Available as editable DOCX or PDF.

1. Parties and roles

Controller: the customer named in the main contract (within the meaning of GDPR Art. 4(7) / FADP Art. 5(j)).
Processor: TecMinds GmbH, Neustadtstrasse 8a, 6003 Lucerne, Switzerland, UID CHE-334.650.060 (within the meaning of GDPR Art. 4(8) / FADP Art. 5(k)).

2. Subject and purpose

The Processor provides the Wield SaaS platform to the Controller. Processing covers:

- Extraction of structured profiles from uploaded application documents (CVs, references);
- Generation of candidate dossiers, evaluations and briefings;
- Matching of candidates against job descriptions and requirement profiles;
- Communication and workflow features (interviews, notes, share-links).

3. Data categories and data subjects

Data categories: identity data (name, contact details), CVs, employment and education history, languages, qualifications, optionally photo, evaluations, notes, references. Special categories of personal data (GDPR Art. 9 / FADP Art. 5(c)) are excluded unless the Controller signs a separate written agreement.

Data subjects: applicants and employees whose data the Controller processes during recruitment.

4. Processor obligations

1. Process data only on documented Controller instructions, in particular within the scope of the main contract and Wield's product features.
2. Bind every person processing data to confidentiality and provide data-protection training.
3. Implement appropriate technical and organisational measures (TOMs) per Annex B.
4. Assist the Controller in responding to data-subject requests (access, rectification, erasure, restriction, portability, objection).
5. Assist with data-protection impact assessments (GDPR Art. 35) and prior consultation with the supervisory authority (GDPR Art. 36).
6. Notify the Controller of any data breach without undue delay, and at the latest within **72 hours** of becoming aware, providing all information required for a regulator filing.

5. Sub-processors

The Processor may engage further processors. The Controller consents to the sub-processors listed in Annex A. Changes or additions are notified with 30 days' lead time; the Controller may object on important data-protection grounds.

6. Data location and third-country transfers

Customer and candidate data are stored primarily in Switzerland (hosting with Infomaniak, Geneva; PostgreSQL database with Infomaniak). LLM inference and embeddings run within the EU/EEA (Google Vertex AI, Frankfurt and Zurich). Third-country transfers happen only on the basis of EU Standard Contractual Clauses (SCC) or an adequacy decision, with supplementary technical measures (encryption in transit and, where applicable, at rest).

7. Retention and deletion

Candidate data are automatically deleted 180 days after the last activity. The Controller may request earlier deletion at any time. On contract termination, all Controller-processed data are deleted within 30 days or, on request, returned in a structured, common format.

8. Audit rights

The Controller may verify compliance with this DPA once per year and on cause (in particular after a data breach), preferably by reviewing current security certifications, penetration-test reports and a Processor self-assessment. On-site audits are possible with 14 days' notice; the requesting party bears the cost.

9. Liability and final provisions

The liability regime agreed in the main contract applies. In conflicts between this DPA and the main contract, this DPA prevails on data-protection matters. Governing law: Swiss law; venue: Lucerne, except as overridden by mandatory law.

Annex A — sub-processor list

Provider	Purpose	Location
Infomaniak (CH)	Hosting, PostgreSQL	Geneva, Switzerland
Coolify (CH)	Container orchestration	Switzerland
Google Vertex AI	LLM (generation, extraction)	europe-west3 Frankfurt, DE
Google Vertex AI	Text embeddings	europe-west6 Zurich, CH
Google Vertex AI	Template generation (no PII)	global
Stripe	Billing, payments	USA (SCC)
Resend	Transactional email	USA (SCC)

Provider	Purpose	Location
Microsoft Azure (optional)	OCR (only if enabled)	EU

Annex B — technical and organisational measures

- Encryption in transit (TLS 1.2+) and at rest (AES-256, database).
- Tenant isolation at application and (in preparation) database layer.
- Multi-factor authentication for administrative access.
- Daily database backups, 30-day retention, off-site encrypted.
- Audit logs for security-relevant actions, retained ≥12 months.
- Least-privilege access; separation of production and development environments.
- Abuse mitigation: rate limits, account lockout, web-application firewall.
- Security updates within 30 days of release; critical vulnerabilities immediately.
- Privacy/security training for all staff with data access.

This DPA template is reviewed by Swiss legal counsel before contract signing. Questions? privacy@tecminds.ch.