Data-Processing Agreement (Controller ➔ Processor)

This Data-Processing Agreement ("DPA") forms part of and supplements the Master Subscription Agreement or other main service contract (the "Principal Agreement") between the undersigned:

Party	**Role under GDPR**	**Details**
[CONTROLLER_LEGAL_NAME]	Data Controller	Registered office: [CONTROLLER_ADDRESS]
Company/Registry nº: [CONTROLLER_REGISTRY_NUMBER]		
Maciej Mazurek, conducting business as “Usługi IT Maciej Mazurek” (trading name “ShortlistKit”)	Data Processor	Registered office: ul. Targowa 5/3, 21-450 Stoczek Łukowski, Poland
Business ID: NIP 5223234720 / REGON 522940561		

*(Controller and Processor each a **“Party”**, together the **“Parties”**.)*

Effective date: [25/04/2025] (or the date both Parties sign, whichever is later)

---

1 Object, Subject-Matter & Term

1.1 This DPA governs Processor’s processing of Personal Data on behalf of Controller in connection with the résumé-parsing and short-listing software branded **“ShortlistKit”** (the “Services”).
1.2 It shall remain in force for as long as Processor Processes Personal Data on behalf of Controller under the Principal Agreement.

2 Nature & Purpose of Processing

Processor shall carry out **automated extraction, structuring, scoring and export of Candidate CV data** solely for the purpose of enabling Controller to screen and shortlist applicants for recruitment-related roles described by Controller.

3 Types of Personal Data & Categories of Data Subjects

See **Annex I** (Details of Processing). Examples include: identification data, contact details, employment & education history, skills, screening scores.

4 Documented Instructions

4.1 Processor shall Process Personal Data **only** on documented instructions from Controller as set out in the Principal Agreement, this DPA, or in any further written instructions Controller issues.
4.2 Controller’s initial instructions are: *“Process Candidate Data uploaded to the Services for CV parsing, scoring and export; retain for up to 30 days after workspace closure **or subscription termination**; delete on request according to Clause 12.”*

5 Confidentiality & Personnel

Processor shall ensure that all persons authorised to Process Personal Data are bound by confidentiality obligations at least as protective as this DPA.

6 Security of Processing

Processor shall implement the technical and organisational measures (**"TOMs"**) set out in **Annex II** and maintain a level of security appropriate to the risk per GDPR Art 32.

7 Sub-Processors

7.1 Controller **authorises** the sub-processors listed in **Annex III**.
7.2 Processor shall notify Controller at least **14 days** before replacing or adding a sub-processor; Controller may object on reasonable, GDPR-related grounds.
7.3 Processor shall impose on all sub-processors data-protection obligations no less protective than those in this DPA.

8 International Transfers

8.1 Primary hosting is located in the **EEA (AWS Region: Stockholm)**.
8.2 Where Processor or an authorised sub-processor is located outside the EEA and not covered by an adequacy decision, the Parties **incorporate by reference** the EU Commission Standard Contractual Clauses 2021/914 (**Module Two – Controller ➔ Processor**), completed as follows:

- Exporter: Controller; Importer: Processor (or relevant sub-processor).
- Clause 9 – Option 2 (general written authorisation, 14-day notice).
- Clause 11(a) – Independent dispute-resolution not selected.
- Annexes IA, IB and II are fulfilled by Annex I and Annex II of this DPA.
- Clause 17 – Governing law: **Polish law.**
- Clause 18(b) – Courts of **Warsaw, Poland**.

8.3 If the Controller is established outside the EEA, the Parties incorporate **Module 4 (Processor → Controller) (Exporter: Processor; Importer: Controller)**.
8.4 For either module, the SCC Annexes are satisfied by Annex I and Annex II of this DPA. Clause 9 option 2 (14-day notice) applies.

9 Assistance to Controller

Processor shall assist Controller, so far as possible, with:

- Responding to data-subject requests (Art 12 – 23);
- Data-protection impact assessments and prior consultations (Art 35 – 36);
- Compliance with Articles 32 – 36 taking into account the nature of processing and information available to Processor.

10 Personal-Data Breach

Processor shall notify Controller **without undue delay and in any event within 24 hours** after becoming aware of a Personal-Data Breach, providing at least the information required by Art 33 (3) GDPR.

11 Audits & Documentation

11.1 Processor shall make available, on request, all information necessary to demonstrate compliance with this DPA (e.g. latest ISO 27001 certificate, SOC 2 Type II report, penetration-test summary).
11.2 Controller may audit Processor's compliance **once per 12-month period** with 30-day prior written notice; remote documentary reviews are preferred. On-site audits are limited to business hours and subject to confidentiality and cost-reimbursement.

12 Return & Deletion of Data

Upon termination of the Services, or earlier at Controller's request for specific data, Processor shall:

- Provide Controller with an export of all Candidate Data in CSV/JSON format; and
- **Delete or irreversibly anonymise** remaining Personal Data from live systems within 30 days, and from backups within 60 days, unless EU or Member-State law requires longer storage.

13 Liability & Indemnity

Each Party's aggregate liability arising out of or related to this DPA shall be subject to the limitations and exclusions of liability in the Principal Agreement, except such limits shall **not** apply to unlawful Processing, breach of confidentiality, or fines imposed by a supervisory authority attributable to the breaching Party.

14 Governing Law & Jurisdiction

14.1 This DPA shall be governed by the **laws of Poland**.
14.2 Any dispute arising from or related to this DPA shall be submitted to the competent courts of **Warsaw, Poland**, unless the SCCs in Clause 8.2 specify otherwise.

Signatures

For the Controller	**For the Processor (ShortlistKit)**
Name: _____	Name: Maciej Mazurek
Title: _____	Title: Owner & Sole Proprietor
Date: _____	Date: 23-05-2025
Signature: _____	Signature: Maciej Mazurek

Annex I – Details of Processing

Item	**Description**
A. Subject-matter	Parsing and short-listing of job-applicant CVs and associated metadata
B. Duration	For the term of the Principal Agreement and deletion period specified in Clause 12

Item	Description
C. Nature & purpose	Automated extraction of résumé fields; relevance scoring against job templates; export to Controller's HR tools
D. Personal-data categories	Name, e-mail, phone, address, employment history, education, skills, certifications, languages, screening scores and justification, free-text cover-letter content, and any other data contained in résumés or provided by the Controller
E. Special categories	Not intentionally processed; any sensitive data processed is incidental to the résumés provided by the Controller. Controller is responsible for ensuring lawful basis for any special-category data
F. Data-subject categories	Job applicants, internship candidates, or other individuals whose résumés are provided by the Controller
G. Frequency	Continuous, on-demand uploads or e-mails forwarded by Controller
H. Retention	Active database – up to 30 days after account closure or subscription termination; backups – deletion within 60 days after account closure or subscription termination

---

Annex II – Technical & Organisational Measures (Art 32 GDPR)

1. **Encryption** – TLS 1.2 **or higher** in transit; AES-256 server-side encryption at rest in AWS (EBS, S3, RDS). Redis (Upstash) – max 24 h TTL; backups disabled.
2. **Access control** – Role-based access controls; principle of least privilege; Multi-Factor Authentication (MFA) enforced for personnel with access to production systems; quarterly access reviews.
3. **Logging & monitoring** – Centralised log aggregation for security and operational purposes; anomaly alerts; audit logs retained for at least 90 days.
4. **Physical security** – AWS ISO 27001-certified data centres (Stockholm region).
5. **Business continuity & DR** – Daily encrypted backups; cross-Availability Zone replication; annual recovery drills. Backups retained according to a rolling 30-day schedule for operational recovery.
6. **Vulnerability management** – Regular vulnerability scanning (e.g. weekly); critical patches applied within 72 hours; penetration-test findings remediated within 30 days for high-risk issues.
7. **Pen-testing** – Independent penetration test at least once every 12 months; executive summary available under NDA.
8. **Employee vetting & training** – Background checks for personnel with production access, where legally permissible; annual GDPR & security awareness training.
9. **Data deletion** – Secure overwrite or cryptographic erasure; purge from backups via lifecycle policy within the timeframe specified in Clause 12 and Annex I.

Annex III – Authorised Sub-Processors

#	Name	Service	Location	Transfer mechanism
1	Amazon Web Services EMEA SARL	Infrastructure (compute, storage, network) and inbound e-mail ingestion (Amazon SES)	Stockholm, SE	EEA (no transfer)
2	Microsoft Ireland Operations Ltd (Azure OpenAI Service)	LLM API for résumé parsing & scoring	Sweden (EU North)	EEA (no transfer)
3	MailerSend (MailerLite Ltd)	Transactional e-mail delivery	EU (Germany & Finland)	EEA (no transfer)
4	Google LLC (Google Workspace / GCP)	Optional Google Sheet export (when initiated by Controller)	USA	SCC 2021/914 (C-to-P)
5	Upstash, Inc. (managed Redis)	In-memory queue & cache	Frankfurt, Germany (eu-central-1)	EEA (no transfer)

Processor shall maintain an up-to-date list of sub-processors and inform Controller of any intended changes in accordance with Clause 7.2 of this DPA.