Data Processing Agreement

This Data Processing Agreement ("DPA") forms part of the Terms of Service between Zink Labs LLC ("Processor," "we," "us") and you and governs the processing of personal data in connection with the Job Agent service ("Service"). In this DPA, "you" refers to the individual user of the Service.

Last Updated: April 15, 2026 | Version 1.2

1. Definitions

- **"Personal Data"** means any information relating to an identified or identifiable natural person, as defined by applicable data protection laws (including GDPR and CCPA).
- **"Processing"** means any operation performed on Personal Data, including collection, recording, storage, retrieval, use, transmission, and deletion.
- **"Data Subject"** means the identified or identifiable person to whom the Personal Data relates.
- **"Sub-processor"** means any third party engaged by the Processor to process Personal Data on your behalf.

2. Scope and Purpose

2.1 Scope

This DPA applies to all Personal Data that the Processor processes on your behalf in connection with providing the Service.

2.2 Purpose

The Processor processes Personal Data solely to provide the Service as described in the Terms of Service, including:

- Storing and managing user profiles and job preferences
- Matching users with job listings using automated scoring algorithms
- Submitting job applications on behalf of users via browser automation
- Generating application answers and cover letters using artificial intelligence (currently Anthropic Claude)
- Reading application-related emails via IMAP (verification codes, confirmations, interview invitations, rejections)
- Processing subscription payments

3. Categories of Personal Data

The Processor processes the following categories of Personal Data:

Category	Examples
Identity Data	Full name, email address, phone number

Location Data	City, state, country, work authorization status
Resume Data	Work history, education, skills, uploaded resume files
Job Preferences	Desired titles, salary range, remote preferences, company blacklist
Demographic / EEO Data	Gender, race/ethnicity, veteran status, disability status
Email Access Data	Gmail app password (AES-256-GCM encrypted), application-related email content
Application Data	Application history, submission status, job match scores, AI-generated answers, form screenshots
Payment Data	Stripe customer ID, subscription plan, billing status (no full card numbers)

4. Categories of Data Subjects

- Users of the Service (job seekers)

5. Processor Obligations

The Processor agrees to:

- **(a)** Process Personal Data only on your instructions through the Service and as described in the Terms of Service
- **(b)** Ensure that persons authorized to process Personal Data are bound by confidentiality obligations
- **(c)** Implement appropriate technical and organizational security measures, including:
    - Encryption of data in transit (TLS/SSL) and at rest
    - AES-256-GCM encryption for stored Gmail credentials
    - Row-level security (RLS) on all database tables ensuring multi-tenant data isolation
    - Secure authentication via Supabase Auth
    - Access controls limiting data access to authorized personnel
- **(d)** Not engage Sub-processors without prior disclosure (see Section 6)
- **(e)** Assist you in responding to Data Subject rights requests
- **(f)** Delete or return all Personal Data upon termination, subject to the data retention terms in the Terms of Service
- **(g)** Make available information necessary to demonstrate compliance with this DPA

6. Sub-processors

6.1 Approved Sub-processors

We use the following Sub-processors, which you authorize by using the Service:

Sub-processor	Purpose	Location	Data Processed
Supabase, Inc.	Database, authentication, file storage	United States (AWS us-east-1)	All user data, resumes, application records
Stripe, Inc.	Payment processing	United States	Email, subscription data, payment method
Google LLC	Email access (IMAP) for application status emails	United States	Gmail credentials, application confirmations, interview invitations, rejection notices, verification codes
Anthropic, PBC	AI-powered text generation for job application answers and cover letters	United States	Name, resume text, work history, education, skills, location, and other profile data sent via API for real-

			time generation. Not used for model training. Retained by Anthropic for up to 7 days per standard API policy for safety monitoring, then automatically deleted.
Voyage AI, Inc.	Vector embeddings for job-to-profile matching	United States	Short skill and keyword summaries derived from your profile and from job descriptions. No raw resume text or personal contact data is sent. Not used for model training.
OpenRouter, Inc.	Low-cost LLM API gateway for job description extraction	United States	Raw job description text only (no personal data). Used to extract required skills and structured requirements from public job postings.
Amazon Web Services, Inc.	Cloud compute infrastructure for application pipeline	United States (us-east-1)	All data processed during job matching, application submission, and email scanning passes through AWS ECS/EC2 compute.
Vercel, Inc.	Web application hosting and privacy-friendly analytics	United States (global edge)	IP address, browser metadata, page views. Cookieless analytics — no cross-site tracking.
Resend, Inc.	Transactional and marketing email delivery	United States	Email address, recipient first name, HTML email body content (welcome, lifecycle, support replies). Acts as our outbound SMTP provider; does not retain message bodies beyond delivery logs.
TikTok Inc. (ByteDance, Ltd.)	Ad conversion measurement on TikTok campaigns	United States (data may transit Singapore / EU per TikTok's published data flows)	Page visits, conversion events, hashed identifiers. Pixel does not fire inside the Capacitor mobile WebView.
Google LLC (Google Tag Manager)	Tag/script loader for analytics and advertising pixels	United States	Loader for the analytics and conversion pixels listed elsewhere in this Schedule. GTM itself transmits only the configuration needed to load those scripts.
Firecrawl, Inc.	Public web page extraction for reduced-pricing LinkedIn profile validation and source page enrichment	United States	Public URLs you provide (e.g., LinkedIn profile URL submitted during reduced-pricing application); extracted page text and metadata. No account credentials, resume content, or

			application answers are transmitted.

6.2 Changes to Sub-processors

We will notify you of any intended changes to Sub-processors by updating this DPA. You may object to a new Sub-processor by contacting us within 30 days of notification. If we cannot reasonably accommodate your objection, you may terminate the Service.

7. Data Transfers

Personal Data is processed and stored in the United States. Where Personal Data is transferred from the EU/EEA to the United States, such transfers are conducted in compliance with applicable data protection laws, including through:

- Standard Contractual Clauses (SCCs) approved by the European Commission, where applicable with our Sub-processors
- The EU-U.S. Data Privacy Framework, where our Sub-processors are certified participants

By using the Service, you acknowledge that Personal Data will be transferred to and processed in the United States.

8. Security Measures

The Processor maintains the following security measures:

- **Access Control:** Role-based access controls; row-level security ensuring users can only access their own data
- **Encryption:** TLS 1.2+ for data in transit; AES-256 encryption at rest (via Supabase infrastructure); AES-256-GCM encryption for stored Gmail credentials
- **Authentication:** Secure password hashing; session-based authentication via Supabase Auth
- **Infrastructure:** Cloud-hosted on Supabase (AWS infrastructure) and AWS ECS Fargate for compute; no direct database connections exposed
- **Monitoring:** Audit logging of application submissions and system events; immutable admin audit log

9. Data Breach Notification

9.1 Notification

In the event of a security breach that affects Personal Data, we will notify you without undue delay and in any event within 72 hours of becoming aware of the breach.

9.2 Breach Notice Content

The notification will include:

- **(a)** A description of the nature of the breach, including the categories and approximate number of Data Subjects affected
- **(b)** The name and contact details of the Processor's point of contact
- **(c)** A description of the likely consequences of the breach
- **(d)** A description of the measures taken or proposed to address the breach

9.3 Cooperation

We will cooperate with you in investigating and mitigating the breach and in meeting any legal notification obligations.

9.4 Florida Information Protection Act (FIPA) Compliance

In addition to the general breach notification obligations above, the Processor will comply with the Florida Information Protection Act of 2014 (FL § 501.171) for breaches affecting Florida residents:

- **(a)** Notification to affected individuals will be provided no later than thirty (30) days after determination of the breach or reason to believe a breach occurred.
- **(b)** If the breach affects 500 or more individuals, the Processor will notify the Florida Department of Legal Affairs within 30 days of the breach determination.
- **(c)** If the breach affects 1,000 or more individuals at the same time, the Processor will also notify all consumer reporting agencies.

Non-compliance with FIPA notification timelines may result in civil penalties of up to $500,000 ($1,000 per day for the first 30 days, $50,000 per subsequent 30-day period, capped at $500,000). The Processor acknowledges this obligation and commits to meeting these deadlines.

10. Data Subject Rights

We will assist you in exercising your data rights, including:

- **Access:** Providing copies of Personal Data
- **Rectification:** Correcting inaccurate data
- **Deletion:** Deleting Personal Data (subject to legal retention requirements)
- **Portability:** Exporting data in a machine-readable format
- **Restriction:** Restricting processing upon request
- **Objection:** Ceasing processing where the Data Subject objects

Data Subjects may exercise these rights through the Service's account settings or by contacting legal@jobagent.sh.

11. Term and Termination

This DPA remains in effect for the duration of the Terms of Service. Upon termination:

- **(a)** You may request export of your Personal Data within 30 days
- **(b)** The Processor will delete all Personal Data within 30 days after the data export period, unless retention is required by law
- **(c)** Deletion will be performed using secure, industry-standard methods

12. Governing Law

This DPA is governed by the same governing law as the Terms of Service (the laws of the State of Florida).

13. Contact

For questions about this DPA or to exercise data rights:

Zink Labs LLC

Email: legal@jobagent.sh