Privacy Policy

Zink Labs LLC ("Company," "we," "us," or "our") operates Job Agent ("Service"). This Privacy Policy explains how we collect, use, disclose, and protect your personal information when you use the Service.

This Service is available to United States residents only. If you are located outside the United States, you are not authorized to use the Service.

By creating an account or using the Service, you acknowledge that you have read and understood this Privacy Policy. If you do not agree with our practices, please do not use the Service.

Last Updated: May 5, 2026 | Version 1.6

1. Information We Collect

1.1 Information You Provide

- **Account Information:** name, email address, password
- **Profile Information:** phone number, location (city, state), work authorization status
- **Resume Data:** uploaded resume files and parsed resume content
- **Job Preferences:** desired job titles, roles, salary expectations, remote/hybrid/on-site preferences, companies to avoid
- **Demographic and EEO Data:** gender, race/ethnicity, veteran status, disability status (provided voluntarily for job application forms)
- **Gmail Access:** IMAP credentials (app password) for reading application-related emails

1.2 Information Collected Automatically

- Usage Data: pages visited, features used, application submission history, job match scores
- Device Information: browser type, operating system, IP address
- Authentication Data: Supabase session tokens

1.3 Information from Third Parties

- Payment Information: Stripe provides us with transaction confirmations and subscription status (we do not store full credit card numbers)
- Job Board Data: publicly available job listing information scraped from employer career pages and applicant tracking systems. We do not collect personal information about other individuals from these pages — only job listing details (title, description, location, requirements, company name, application URL).

2. How We Use Your Information

We use your personal information to:

- (a) Provide the Service, including matching you with job listings and submitting applications on your behalf
- (b) Auto-fill job application forms with your profile data, resume, and demographic information
- (c) Scan your Gmail account via IMAP to identify application-related emails, including verification codes, application confirmations, interview invitations, interview scheduling links, and rejection notices. Email scanning is limited to messages matching known recruiter and applicant tracking system (ATS) sender patterns. We extract email subjects, sender addresses, dates, and relevant body content (such as company names, interview dates, and status updates) to update your application tracking dashboard.
- (d) Process payments and manage your subscription through Stripe
- (e) Send you application status updates, daily progress reports, and service notifications
- (f) Improve the Service, including job matching algorithms and application success rates
- (g) Respond to your support requests
- (h) Comply with legal obligations

2.1 Artificial Intelligence and Automated Processing

The Service uses artificial intelligence (AI) to enhance the job application process. Specifically:

- Application Answer Generation: We use AI language models (currently Anthropic Claude) to generate answers to free-text application questions based on your profile data, resume, and work history. These AI-generated answers are submitted as part of job applications on your behalf.
- Cover Letter Generation: If enabled, AI generates cover letters tailored to each job posting using your resume and work experience.
- Form Field Selection: AI assists in selecting appropriate options from dropdown menus and multi-select fields on application forms.
- Screenshot Analysis: Anthropic Claude's vision model analyzes screenshots of application forms to identify and fill empty required fields. These screenshots may contain personal information you have entered into the form. Screenshots are transmitted directly to Anthropic via API, are not retained by us, and are subject to the same 7-day safety-retention policy described above.

You can control AI features through your profile settings (e.g., enabling or disabling auto-generated cover letters). The data sent to AI providers is used solely for generating application content and is subject to the AI provider's data processing terms. Our AI providers do not use your data to train their public models. Anthropic retains API inputs and outputs for up to 7 days for safety monitoring before automatic deletion; Voyage AI and OpenRouter do not retain inputs after the request completes (see the DPA for full sub-processor retention details).

3. How We Share Your Information

We share your personal information only in the following circumstances:

3.1 Job Board Platforms

When we submit job applications on your behalf, your personal information (name, email, phone, resume, demographic data, and other application fields) is transmitted to the employer's applicant tracking system (ATS). This is the core function of the Service and is done at your direction.

3.2 Service Providers

We use the following third-party service providers:

Provider	Purpose	Data Shared
Supabase, Inc.	Database, authentication, file storage	Account data, profile data, application

		records, resume files
Stripe, Inc.	Payment processing	Email, subscription plan, payment method
Google LLC (Gmail via IMAP)	Email scanning for application status	Email credentials (app password), application confirmations, interview invitations, rejection notices, verification codes
Anthropic, PBC (Claude)	AI-powered text generation: resume tailoring, cover letters, bio generation, in-app AI assistant, application question answers	Name, resume text, work history, education, skills, location, application question prompts, and other profile data used to generate application answers and cover letters
Voyage AI, Inc.	Vector embeddings for job-to-profile matching	Short skill and keyword summaries derived from your profile and job descriptions. No raw resume text or personal contact data is sent.
OpenRouter, Inc.	Low-cost LLM API gateway for job description extraction	Raw job description text (not your personal data) for extracting required skills and structured requirements.
Amazon Web Services, Inc.	Cloud infrastructure for application pipeline	All data processed during job matching, application submission, and email scanning passes through AWS compute infrastructure
Vercel, Inc.	Web application hosting and aggregate analytics	IP address, browser metadata, page views
Google LLC (Google Analytics 4 + Google Ads)	First-party site analytics + ad conversion measurement	Page visits, device type, IP address (anonymized), conversion events (signup, checkout)
Meta Platforms, Inc. (Meta Pixel)	Ad conversion measurement on Facebook / Instagram campaigns	Page visits, conversion events, hashed email at checkout (PII never sent in clear text)
Reddit, Inc. (Reddit Pixel)	Ad conversion measurement on Reddit campaigns	Page visits, conversion events
X Corp. (X Pixel)	Ad conversion measurement on X / Twitter campaigns	Page visits, conversion events
Resend, Inc.	Transactional and marketing email delivery	Email address, recipient name, first name; HTML email body content (welcome, lifecycle/re-engagement, support replies). Resend acts as our outbound SMTP provider and does not retain message bodies beyond delivery logs.
TikTok Inc. (ByteDance, Ltd.)	Ad conversion measurement on TikTok campaigns	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	Loader for the analytics and conversion pixels listed elsewhere in this table; GTM itself transmits only the configuration needed to load those scripts.
Firecrawl, Inc.	Public web page extraction (used for reduced-pricing LinkedIn profile validation and source page enrichment)	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.

3.3 Legal Requirements

We may disclose your information if required by law, regulation, legal process, or government request.

3.4 Business Transfers

In the event of a merger, acquisition, or sale of assets, your information may be transferred to the acquiring entity. Any such successor entity will be required to honor this Privacy Policy or provide you with notice and a reasonable opportunity to delete your data before applying materially different privacy terms.

We do not sell your personal information for monetary or other valuable consideration.

To measure advertising effectiveness, we use first-party conversion pixels and analytics: Reddit Pixel, Google Ads, X (Twitter) Pixel, Meta Pixel, and Google Analytics 4. These tools share event-level data (page visits, account creations, checkout completions) with their respective platforms so we can attribute paid ads we run to actual sign-ups. They are not used for behavioral profiling across other websites. You may block these pixels using browser-level ad blockers or by enabling Global Privacy Control.

3.5 Automated Decision-Making

The Service uses automated processing to match you with job listings and to generate content for job applications. Specifically:

- Job Matching: An automated scoring algorithm evaluates job listings against your profile preferences (job titles, location, salary, keywords) to produce a match score (0.0–1.0). Only jobs above your match threshold are selected for application.
- AI Content Generation: Artificial intelligence generates answers to application questions and optional cover letters based on your profile data.

IMPORTANT: These automated processes do not make employment decisions about you and do not constitute automated decision-making within the meaning of GDPR Article 22. The matching algorithm only assists in submitting applications — it does not determine your suitability for employment. All hiring decisions are made solely and independently by employers. The Service has no role in, and is not responsible for, any employer's hiring decision.

You have the right to: (a) obtain information about the logic involved in the matching and scoring process; (b) request human review of any automated processing; and (c) contest outcomes by contacting us at security@jobagent.sh.

4. Data Retention

- Active Accounts: We retain your data for as long as your account is active.
- After Deletion: When you delete your account, we will delete your personal data within 30 days, except where retention is required by law (e.g., payment records for tax compliance, consent records for legal proof of agreement acceptance).
- Application Records: Application metadata (job title, company, submission status, AI-generated answers) is retained for the duration of your account. Application screenshots are retained on a 90-day rolling basis and automatically deleted thereafter.
- Gmail Credentials: Your encrypted Gmail app password is deleted immediately upon disconnection or account deletion. We do not retain email content after processing — only extracted metadata (company name, email date, status classification) is stored.

- AI Processing: Profile data and resume content sent to Anthropic via the Claude API for answer generation is not used for model training. Per Anthropic's standard API data retention policy, API inputs and outputs are retained by Anthropic for up to 7 days for safety monitoring, after which they are automatically deleted.
- Anonymized Data: We may retain anonymized, aggregated data that cannot identify you for analytical and service improvement purposes.
- Legal Consent Records: Records of your agreement acceptance (timestamps, IP address, document version) may be retained after account deletion as proof of consent, as permitted by law.

5. Data Security

We implement appropriate technical and organizational measures to protect your personal information, including:

- Encryption of data in transit (TLS/SSL) and at rest
- Role-based access controls and row-level security (RLS) on all database tables
- Secure authentication via Supabase Auth
- No direct database access — all data flows through authenticated APIs
- Regular review of security practices

While we take reasonable steps to protect your data, no method of transmission or storage is 100% secure.

5.1 Data Breach Notification (Florida Information Protection Act)

In the event of a security breach affecting your personal information, we will comply with the Florida Information Protection Act of 2014 (FL § 501.171), which requires:

- Individual Notification: We will notify affected Florida residents no later than thirty (30) days after determination of the breach or reason to believe a breach occurred.
- Notification Content: The notice will include the date (or estimated date) of the breach, a description of the personal information involved, and contact information for the Company.
- Regulatory Notification: If the breach affects 500 or more individuals, we will notify the Florida Department of Legal Affairs within 30 days of the breach determination.
- Large-Scale Breaches: If the breach affects 1,000 or more individuals, we will also notify all consumer reporting agencies.
- Notification Method: Notification will be provided by email (to your registered account email), by mail, or by substitute notice as permitted under FIPA if direct contact information is unavailable.

For details on our breach notification procedures and cooperation obligations, see our Data Processing Agreement (DPA), Section 9.

6. Your Rights

6.1 All Users

You have the right to:

- Access your personal data by viewing your profile and application history in the Service
- Update your personal data through your account settings
- Delete your account and associated data by contacting us or using the account deletion feature
- Export your data in a machine-readable format upon request
- Object to automated processing by contacting us at security@jobagent.sh

We may retain and use anonymized, aggregated data derived from your usage that cannot reasonably identify you, for service improvement and analytical purposes. Anonymized data is not subject to deletion requests and is not considered personal information.

6.2 California Residents (CCPA/CPRA)

If you are a California resident, you have additional rights under the California Consumer Privacy Act and California Privacy Rights Act:

- Right to Know: You may request details about the categories and specific pieces of personal information we have collected.
- Right to Delete: You may request deletion of your personal information, subject to certain exceptions.
- Right to Opt-Out of Sale or Sharing: We do not sell your personal information for monetary consideration. We use first-party conversion pixels (Reddit, Google Ads, X, Meta, TikTok) and Google Analytics 4 to measure the effectiveness of paid advertising; under Cal. Civ. Code § 1798.140(ah) this may be characterized as "sharing" for cross-context behavioral advertising. Zink Labs LLC currently operates below the CCPA/CPRA applicability thresholds (revenue, consumer count, and personal-information-revenue tests in Cal. Civ. Code § 1798.140(d)). To opt out of pixel-based measurement at any time, install a browser-based ad blocker or enable the Global Privacy Control signal in your browser; we will honor GPC for visitors who present it.
- Right to Limit Use of Sensitive Personal Information: We collect sensitive personal information (such as demographic/EEO data and email account credentials) solely to provide the Service. We do not use sensitive personal information for purposes beyond what is necessary to provide the Service.
- Non-Discrimination: We will not discriminate against you for exercising your CCPA/CPRA rights.

To exercise your CCPA/CPRA rights, contact us at security@jobagent.sh with "CCPA Request" in the subject line.

6.3 EU/EEA Residents (GDPR)

This Service is available to United States residents only (see Section 9). If you are located in the EU/EEA, you are not authorized to use the Service.

To the extent GDPR may nonetheless apply to any processing of personal data relating to EU/EEA residents, we note the following for transparency:

Data Category	Legal Basis (GDPR Art. 6)	Notes
Account data (name, email, password)	Art. 6(1)(b) — Performance of contract	Necessary to provide the Service
Profile data (resume, work history, skills, location)	Art. 6(1)(b) — Performance of contract	Core data used for job matching and application submission
Demographic / EEO data (gender, race, veteran, disability)	Art. 6(1)(a) — Consent	Voluntarily provided; used only to fill EEO fields at user direction
Gmail IMAP credentials	Art. 6(1)(b) — Performance of contract	Required to read verification codes and application status emails
Usage data and analytics	Art. 6(1)(f) — Legitimate interests	Service improvement and security monitoring
Payment data	Art. 6(1)(b) — Performance of contract	Required to process subscription billing
Legal consent records	Art. 6(1)(c) — Legal obligation	Retained as evidence of consent acceptance

Rights for EU/EEA residents (if GDPR applies): right of access, rectification, erasure, restriction of processing, data portability, and objection. Where processing is based on consent, you may withdraw consent at any time without affecting the lawfulness of processing prior to withdrawal.

Right to lodge a complaint: You have the right to lodge a complaint with your national supervisory authority (data protection authority / DPA) if you believe our processing of your personal data infringes applicable data protection law. A list of EU/EEA supervisory authorities is available at https://edpb.europa.eu/about-edpb/about-edpb/members_en.

EU Representative: Zink Labs LLC currently qualifies for the exemption under GDPR Article 27(2)(a) (fewer than 250 employees; processing is not large-scale, not systematic, and unlikely to result in high risk to data subjects' rights and freedoms).

Accordingly, we have not appointed a formal EU representative at this time. If our EU/EEA user base grows materially, this position will be reviewed and a representative appointed as required.

6.4 Florida Digital Bill of Rights

The Florida Digital Bill of Rights (FDBR, FL SB 262, effective July 1, 2024) grants certain privacy rights to Florida residents. However, the FDBR applies only to companies that have global annual revenues exceeding $1 billion and meet other threshold criteria. Zink Labs LLC does not currently meet these thresholds. Notwithstanding, we are committed to privacy best practices and voluntarily provide data access, correction, and deletion rights to all users regardless of jurisdiction (see Section 6.1 above).

7. Cookies

We use essential cookies for authentication and session management. For details, see our Cookie Policy.

8. Children's Privacy

The Service is not intended for individuals under the age of 18. We do not knowingly collect personal information from children. If we become aware that we have collected data from a child under 18, we will delete it promptly.

9. Geographic Restriction and Data Location

This Service is available to United States residents only. By using the Service, you represent and warrant that you are located in and a resident of the United States.

All personal data is processed and stored within the United States via the following infrastructure:

- Supabase (AWS us-east-1): Database, authentication, file storage
- AWS (us-east-1): Application pipeline compute (job matching, application submission, email scanning)
- Vercel (global edge network): Web application hosting
- Anthropic (United States): AI processing

We do not knowingly collect personal information from individuals located outside the United States. If you access the Service from outside the United States, you do so in violation of these terms and your use is unauthorized.

10. Changes to This Policy

We may update this Privacy Policy from time to time. We will notify you of material changes via email or through the Service. The "Last Updated" date at the top indicates the most recent revision.

11. Contact Us

If you have questions about this Privacy Policy or wish to exercise your data rights, please contact us:

Zink Labs LLC

Email: security@jobagent.sh

Web: https://jobagent.sh

Florida residents may also contact the Florida Attorney General's office with privacy complaints:

Office of the Attorney General, State of Florida
PL-01, The Capitol, Tallahassee, FL 32399-1050
Phone: 1-866-966-7226
Online: MyFloridaLegal.com