AI HEADHUNTER – PRIVACY POLICY Effective Date: 30 May 2025
Last Updated: 30 May 2025

This Privacy Policy explains how AI Headhunter (the "Platform"), operated by **Stardom Innovations LLC**, a Florida limited-liability company doing business as "AI Headhunter" ("**Stardom**," "**we**," "**us**," or "**our**"), collects, uses, discloses, and safeguards your information. Stardom is a wholly-owned U.S. subsidiary of **Ehave Inc.** (OTCQB: **EHVVF**), an Ontario corporation. Unless noted otherwise, Stardom is the primary data controller for the processing activities set out below; Ehave acts as a joint controller for enterprise-level compliance, auditing, and cybersecurity functions.

1. Scope & Key Terms

- **Candidate** – an individual who submits a résumé/CV, answers screening questions, or records interview media on the Platform.
- **Recruiter / Client** – a business customer that posts positions, reviews applicants, or otherwise uses the Platform.
- **Personal Data** – any information that identifies or can reasonably be linked to an individual.
- This Policy applies to all websites, Chrome extensions, mobile experiences, APIs, and services branded "AI Headhunter" and operated by Stardom worldwide, unless a separate privacy statement is displayed.

2. Who Is Responsible for Your Data?

Role	Entity	Contact
Primary Data Controller	**Stardom Innovations LLC** (d/b/a AI Headhunter)	
Florida Dept. of State Document # TBD		
100 SE 2nd St., Suite 2000		
Miami, FL 33131 USA	**Email:** privacy@aiheadhunter.com	
Phone: +1 954-604-0324		
Joint Controller (parent)	**Ehave Inc.** (OTCQB: **EHVVF**)	

720 King St. W., Suite 905		
Toronto, ON M5V 2T3 Canada	privacy@ehave.com	
Data Protection Officer	**DPO, Stardom Innovations LLC**	dpo@aiheadhunter.com
EU GDPR Representative (Art. 27)	[Stardom EU Rep Ltd.]	
Brussels, Belgium	eu-rep@aiheadhunter.com	
UK GDPR Representative	[Stardom UK Rep Ltd.]	
London, UK	uk-rep@aiheadhunter.com	

3. Information We Collect

A. Information You Provide Directly

- **Contact details** – name, email, phone, mailing address, employer.
- **Account credentials** – username, password, MFA tokens.
- **Professional info** – uploaded résumé/CV, work history, skills, salary expectations.
- **Screening / interview content** – survey answers, free-text responses, audio- or video-recorded interviews, calendar preferences.
- **Company data** – recruiter billing details, user-seat lists, job descriptions, hiring-pipeline notes.

B. Information We Collect Automatically

- **Device & log data** – IP address, device identifiers, browser type, referrer URL, error logs, time stamps.
- **Usage analytics** – pages visited, feature clicks, search queries, interaction heat maps, email open/click events.
- **Cookies & similar tech** – first-party cookies for authentication and settings; optional third-party analytics cookies (e.g., Google Analytics, Mixpanel). See § 10.

C. Information from Third Parties

- **Linked Accounts** – limited profile data when you connect LinkedIn, Google, Microsoft 365, or similar services.
- **Background-check & assessment vendors** – only with your consent.
- **Enrichment partners (e.g., CompilerX.com)** – professional and contact data used to update candidate records for active recruiter accounts.

- **Public professional data** – information scraped from publicly available sources (e.g., company sites, public GitHub profiles) to enrich candidate and employer records.

4. Legal Bases for Processing

We process Personal Data only when at least one lawful basis applies:

1. **Contract Performance** – to deliver the services requested by Candidates and Clients.
2. **Legitimate Interests** – to improve products, prevent fraud, and maintain platform security. We balance our interests against your rights and expectations.
3. **Consent** – for optional features (e.g., marketing emails, analytics cookies, AI training on interview media). You may withdraw consent at any time.
4. **Legal Obligation** – to comply with U.S., Canadian, and international laws (e.g., payroll, tax, anti-money-laundering, equal-opportunity regulations).
5. **Vital Interests** – to protect the safety of individuals in extraordinary circumstances.

5. How We Use Your Information

- **AI-driven matching** – analyse résumés, screening answers, and interview media to rank fit and predict likely performance.
- **Recruiter dashboards** – populate talent pools, pipeline stages, interview scheduling, and feedback loops.
- **Transactional messaging** – send interview invites, offer letters, password resets, and account alerts.
- **Support & troubleshooting** – investigate tickets and resolve technical issues.
- **Model improvement** – develop and refine natural-language and video-analysis models (only on data you permit us to use or after anonymisation).
- **Security & fraud prevention** – monitor, detect, and block malicious or unauthorised activity.
- **Aggregated analytics** – create de-identified industry benchmarks and product insights.
- **Cross-platform screening** – pass candidate data to InterviewScreener.com for deeper AI-based interviews and contact-information extraction when requested by an authorised recruiter.
- **Partner marketing** – send optional productivity tips or offers from Stardom-approved partners (see § 7). You can opt-out any time.

6. Automated Decision-Making & Profiling

Our algorithms generate suitability scores and recommendations. Human recruiters can override algorithmic outputs at any stage. You may request human review of any decision that produces legal or similarly significant effects (GDPR Art. 22).

---

7. Data Sharing

We **never sell** your Personal Data. We disclose information only to:

- **Authorised recruiters/clients** when you actively apply or are sourced for their roles.
- **InterviewScreener.com** – our sister SaaS platform used for AI-driven interviews, résumé parsing, and contact-data extraction. Processing is covered by aligned privacy practices and a shared data-protection agreement.
- **Enrichment & contact-retrieval partners** such as **CompilerX.com**, engaged under written data-processing agreements to append or verify professional profiles for active recruiter accounts.
- **Marketing service providers & partner platforms** that distribute optional content or offers designed to increase user productivity. Marketing emails are sent only where lawful and may be declined at any time via the unsubscribe link or in-app settings.
- **Parent company Ehave Inc.** for consolidated auditing, compliance, financial reporting, and security monitoring.
- **Successors** in the event of a merger, acquisition, or asset sale, subject to equivalent safeguards.
- **Regulators or law-enforcement** when required by applicable law, court order, or to protect rights and safety.

8. International Transfers

- Primary storage is in AWS **us-east-1** (Northern Virginia) with backups in **ca-central-1** (Canada).
- For EU/UK residents, transfers to the United States or Canada rely on **Standard Contractual Clauses**, the **EU–U.S. Data Privacy Framework** (where certified), or other adequacy mechanisms.
- Canadian users are protected under **PIPEDA**; cross-border transfers occur under contractual safeguards.

9. Data Security

We employ technical and organisational controls such as:

- **TLS 1.3** encryption in transit, **AES-256** encryption at rest.
- Zero-trust network segmentation and firewalls.
- Annual **SOC 2 (Type II)** audits and third-party penetration tests.
- **Role-based access control**, single sign-on, and mandatory multi-factor authentication.
- 24 × 7 monitoring, incident-response plan, and breach-notification procedures in line with GDPR's 72-hour rule and applicable U.S. state laws (e.g., Florida Information Protection Act).

10. Cookies & Similar Technologies

Category	Purpose	Opt-out Options
Essential	Login sessions, load balancing	Browser settings may impair function
Functional	Remember preferences	Disable in Cookie Settings panel
Analytics	Measure usage & improve UX	Disabled by default where consent is required
Advertising	Retargeting & audience measurement	Off by default; enabled only with explicit consent

You may adjust preferences any time via our in-app **Cookie Settings** or through standard browser controls.

11. Data Retention

Data Type	Retention Standard
Candidate profiles & résumés	24 months after last activity or upon deletion request
Interview audio/video	18 months or until role is filled + 6 months
Recruiter account & billing records	Contract term + 7 years for tax compliance
Application & web logs	12 months (longer if needed for security investigations)
Marketing opt-in records	Duration of subscription + 3 years

---

12. Your Privacy Rights

Your rights depend on your location and include, where applicable:

- **Access** – obtain a copy of the Personal Data we hold.