Candidate Privacy Policy

This Candidate Privacy Policy ("**Policy**") describes how Aura Group, Inc, together with its subsidiaries and affiliates "**Aura**", "**we**", "**us**" and "**our**") collects, uses, and discloses "personal information" as defined under applicable data protection law from and about candidates for employment with Aura ("**personal information**"). We may update this Policy at any time. We may also provide you additional privacy notices regarding our collection, use, or disclosure of information.

This Policy does not form part of any employment contract or contract to provide services. If you provide services to Aura through or in connection with another company, we are not responsible for that company's privacy practices.

This Policy only applies to our handling of data gathered about you in your capacity as an applicant for employment with Aura. Our policies relating to your interaction with us as a user or customer of Aura services are available at https://www.aura.com/legal/privacy-policy.

1. Types of Personal Information We Handle

We collect, store, and use various types of personal information through the application and recruitment process. We collect such information either directly from you or (where applicable) from another person or entity, such as an employment agency or consultancy, background check provider, or other referral sources.

The type of information we have about you depends on the position you apply for and may include, where applicable:

- **Volunteered information** such as any information provided in a curriculum vitae/resume, cover letter, interview or correspondence.
- **Identification and contact information and related identifiers,** such as full name, date and place of birth, citizenship and permanent residence, home and business addresses, telephone numbers, and email addresses.
- **Professional or employment-related information**, including:
    - **Recruitment, employment, or engagement information** such as application forms and information included in a resume, cover letter, or otherwise provided through any application or engagement process; and copies of identification documents, such as driver's licenses, passports, and visas; and background screening results and references.
    - **Career information,** such as job titles; work history; work dates and work locations; employment, service or engagement agreements; appraisal and performance information; information about skills, qualifications, experience, publications, speaking engagements, and preferences (e.g., mobility); absence

and leave records; professional memberships; disciplinary and grievance information; and termination information.

- **Business travel and expense information,** such as travel itinerary information and receipts for travel expenses.

- **Education Information,** such as institutions attended, degrees, certifications, training courses, publications, and transcript information.

- **Internet, electronic network, and device activity and device information and related identifiers**, such as information about your use of our online Careers page and online application system, including user IDs, passwords, IP addresses, device IDs, web logs, and audit trails of system access.

- **Audio or visual information,** such as CCTV footage (if you visit an Aura facility in connection with your job candidacy), as well as other information relating to the security of our premises.

- **'Sensitive' personal information**, **which may have state-specific privacy rights,** such as race, sex/gender, religious beliefs, marital status, military service, nationality, ethnicity, where legally permitted, criminal history. We may also collect volunteered **health information**, such as disability status and requests for accommodation.

- **Third party, social or public record information**, including:

  - References from professional referees on request.

  - Information provided to us by recruitment agencies or other referring parties, and third-party talent prospecting services.

  - Information made publicly available by you via social media, such as LinkedIn.

2. How We Use Personal Information

We collect, use, share, and store personal information for Aura's and our service providers' business purposes, which include, where applicable:

- **HR management and administration,** including evaluation of applications, fraud prevention and investigation, preparing analyses and reports, and communicating with candidates about updates in the application or interview process or relevant information about perks and benefits.

- **Performance of business operations**, including providing and monitoring IT systems for any lawful purpose, maintaining accounts and internal directories, crisis management, protecting occupational health and safety, participating in due diligence activities related to the business, business succession planning, and conducting internal analyses and audits.

- **Recruitment,** including job advertising, interviewing, and selecting and hiring new staff.

- **Security operations,** including detecting security incidents, debugging and repairing errors, preventing unauthorized access to our computer and electronic communications systems and preventing malicious software distribution, and monitoring and controlling access to company premises and locations (including through use of CCTV).

- **Legal compliance** such as complying with anti-bribery, tax, social security, and immigration obligations, and responding to and cooperating with legal or regulatory requests and investigations.

3. With Whom We Share Personal Information

We will disclose workforce personal information to the following types of entities or in the following circumstances (where applicable):

- **Internally**: to people within Aura and its subsidiaries and affiliates to carry out the purposes described in this Policy, including to hiring managers, human resources, as well as personnel within Aura, such as legal and finance.

- **Service Providers**: such as external recruiters, tax and other professional advisors, technology service providers, travel management providers, travel providers, human resources suppliers, and background check companies.

- **Legal Compliance**: when required to do so by law, regulation, or court order or in response to a request for assistance by the police or other law enforcement agency.

- **Litigation Purposes**: to seek legal advice from our external lawyers or in connection with litigation with a third party.

- **Business Transaction Purposes**: in connection with the sale, purchase, or merger of a business.

4. Data security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality. We will notify you and any applicable regulator of occurred personal data breach where we are legally required to do so.

5. Data retention

After we have communicated to you our decision about whether to appoint you to work for us, we will retain your personal information as provided by law and as long as we need it for our business purposes. For example, we may retain your personal information so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. We will securely destroy your personal information in accordance with applicable laws and regulations. If you are hired, then we will retain this information as detailed in our Employee Privacy Policy.

6. State-Specific Consumer Disclosure

The California Consumer Privacy Act as well as laws enacted by certain other U.S. states grant applicants certain privacy rights. If you are a resident of a state with a specific privacy right for applicants, you may have the following rights:

- Right to know and access the personal information we have collected about you.
- Right to delete. If you request deletion during the application process, it may result in us not being able to evaluate your candidacy or employ you.
- Right to correct inaccurate information.
- Right to non-discrimination. You have the right to non-discrimination for exercising your privacy rights.
- Opt out of the "sale" or "share" of your personal information. With the exception of advertising cookies used on our website, Aura does not 'sell' or 'share' your personal information as defined by applicable data protection law.
- Limit the Use and Disclosure of Your Sensitive Personal Information. Aura only collects candidate sensitive personal information, which is necessary to evaluate candidacy and to prepare for employment. As such, limiting your use of your sensitive personal information would result in us not being able to evaluate your candidacy or employ you.

7. Exercise Your Privacy Rights or Contact Us About this Policy

If you would like to exercise your privacy rights listed above or have questions about this Policy, please email privacypolicy@aura.com

Last amended: May 31, 2024