Personnel Privacy Policy and Notice at Collection

This Personnel Privacy Policy ("**Policy**") describes how People Data Labs, Inc. ("**People Data Labs**", "**Company**", "**we**", "**us**" and "**our**") collects, uses, and discloses information about our individual current and former employees, applicants for employment at People Data Labs, contractors, consultants, interns, and other workforce members (and their beneficiaries and emergency contacts) in the context of our working relationship with the relevant individuals ("**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. Please read this Policy and any other privacy notices carefully.

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

This Policy does not apply to our handling of data gathered about you in your role as a user of the Company's services. When you interact with us as in that role, the Privacy Policy associated with the relevant service applies.

This Policy will be posted on Rippling and as part of the Employee Handbook] . This policy will be provided to new workforce members as part of the onboarding process.

1. Types of Personal Information We Handle

We collect, store, and use various types of personal information through the application, recruitment, engagement, or employment, or contracting processes. We collect such information either directly from you or (where applicable) from another person or entity, such as an employment agency or consultancy, recruitment or professional networking website, background check provider, or others who provide references. We will collect additional personal information throughout the course of your employment or other provision of services to us.

The type of information we have or will have about you depends on your role with us and may include, where applicable:

- **Identifiers** such as full name, home and business addresses, telephone numbers, email addresses, and such information about your beneficiaries or emergency contacts.

- **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 licences, passports, and visas; 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.

- **Financial information** such as salary, payroll, pension or retirement contribution information; and bank account and tax information.

- **Business travel and expense information** such as travel itinerary information, corporate expenses, and Company credit card usage.

- **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 the Company network, information, and communication systems, including user IDs, passwords, IP addresses, device IDs, web logs, metadata, and audit trails of system access.

- **Geolocation information** for device recovery if you use a Company-issued device.

- **Audio or visual information** such as recorded presentations in which you participate, possibly including calls with customers; and audio or video recordings taken at Company functions.

- **Biometric information** that we use for authentication and security purposes, such as imagery of the iris, retina, fingerprint, face, hand, palm, or vein patterns; voice recordings; faceprints; and voiceprints.

- **Legally protected classification information** which may but does not necessarily include race, sex/gender, religious/ philosophical beliefs, gender identity/expression, sexual orientation, marital status, military service, nationality, ethnicity, request for family care leave, political opinions, and criminal history.

- **Medical information** about you, and, if applicable, your beneficiaries, such as medical conditions and other information provided in statements of health forms, disability status, health and safety incidents or accidents, sickness records, and health issues requiring adaptations to your working environment or working practices.

- **Government identification information** such as Social Security number and driver's licence number.

- **Other information that directly or indirectly identifies you**, such as date and place of birth, citizenship, and permanent residence (and such information about your dependents or emergency contacts); and information on any publicly available social media profile of yours that mentions your connection to us.

2. How We Use and Retain Personal Information

We have or will collect, use, share, and store personal information for the Company's and our service providers' and contractors' business purposes, which include, where applicable:

- **HR management and administration,** including training, compensation and benefits, invoices, leave, scheduling, career development, performance appraisals and

recognition, investigating and resolving inquiries and complaints, providing references, succession planning, organizational changes, fraud prevention and investigation, preparing analyses and reports, and communicating with our workforce about updates or relevant information about perks, benefits and discounts, and changes to Company products and services.

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

- **Recruiting and workforce planning,** including assignment planning and budgeting, job advertising, interviewing, and selecting and hiring new staff.

- **Security operations,** including detecting security incidents, debugging and repairing errors, and 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.

- **Exercising our legal rights,** including seeking legal advice from our external lawyers or in connection with litigation with a third party.

We may also use personal information for any other legally permitted purpose (subject to your consent, where legally required).

Certain information we collect may be "**sensitive personal information**" under California law. We use such information as necessary to conduct our relationship with you, in the following ways:

- Social Security number or passport information for legal compliance, payroll, benefits, tax, and immigration purposes;

- Biometric information for physical security and access and/or timekeeping;

- Health information, which may include disability status, to provide reasonable workplace accommodations and manage absences, for workplace health and safety purposes, and for compliance with applicable law and contracts or to exercise rights thereunder.

- Racial/ethnic origin, sexual orientation, and/or disability status for equal opportunity and diversity and inclusion purposes and compliance with applicable law or to exercise rights thereunder.

California law places certain obligations on businesses that "sell" personal information to third parties or "share" personal information with third parties for cross-context behavioural advertising as those terms are defined under the California Consumer Privacy Act ("CCPA"). We do not "sell" or "share" the personal information covered by this Policy and have not done so in the twelve months prior to the effective date of this Policy.

The personal information we do or will collect, including sensitive personal information, will be retained for as long as necessary to satisfy the purposes for which it was collected and our legal obligations. As described above, these purposes include our business operations and complying with reporting, legal and accounting obligations. In determining how long to retain information, we consider the amount, nature and sensitivity of the information, the potential risk of harm from unauthorised use or disclosure of the personal information, the purposes for which we process the personal information and whether we can achieve those purposes in other ways, the applicable legal requirements, and our legitimate interests.

For example, we will keep certain information about former employees (e.g. name, job title, organizational hierarchy, and records of employment) for as long as necessary for our legitimate interests in keeping this information as part of our organizational history, to confirm the facts of their employment with us and to comply with law. The purposes for which we process information (as well as the other factors listed above) may dictate different retention periods for the same types of information.

3. How We Share Personal Information

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

- **Internally**: to people within certain parts of the company to carry out the purposes described in this Policy, including to your manager, human resources, as well as personnel within the Company, such as payroll, IT, legal and finance.

- **Service Providers and other Vendors**: such as compensation and benefits providers, tax, legal and other professional advisors, technology service providers, corporate card issuers, travel management providers, travel providers, human resources suppliers, background check companies, and employment businesses (in relation to contractors or agency workers). We also share personal information with service providers working on our behalf and vendors outside of People Data Labs as necessary to provide certain services. For example, all these types of vendors may receive your contact information from us, but vendors like compensation and benefits providers, corporate card issuers, travel management providers, and travel providers do not receive your internet, electronic network, and device activity. Our network security providers, on the other hand, may receive network activity but would not receive your government identification information.

- **Business operations:** to provide another entity (such as a potential or existing business counterparty or customer) with a means of contacting you in the normal course of business, for example, by providing your contact details, such as your phone number and email address.

- **Legal compliance and exercising legal rights**: when required to do so by law, regulation, or court order; and 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.

- **Consent**: with your consent and as permitted by law, we may share personal information with any other third parties in any other circumstances.

4. Additional Information for California Residents

California residents have certain rights regarding their personal information. Subject to certain exceptions, you may request:

- access to your personal information including the right to know the categories of personal information we have or will collect about you and the reason we will or have collected such information;
- correction of the personal information that we have or will hold about you that is inaccurate;
- deletion or removal of your personal information.

You also have the right not to be discriminated against (as provided for in California law) for exercising your rights.

Exceptions to Your Rights: There are certain exceptions to these above rights. For instance, we may retain your personal information if it is reasonably necessary for us or our service providers to provide a service that you have requested or to comply with law or to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity or prosecute those responsible for that activity.

Exercising Your Rights: To exercise one of the rights above, you may contact us in one of the following ways:

- By phone: 1 877-489-1058
- By email: privacy@peopledatalabs.com

We also will take reasonable steps to verify your identity before responding to a request. In doing so, we may ask you for verification information so that we can match at least two verification points with information we maintain in our files about you. If we are unable to verify you through this method, we shall have the right, but not the obligation, to request additional information from you.

5. How to Contact Us About This Policy

If you have questions about our collection, use, or disclosure of personal information, please contact privacy@peopledatalabs.com.